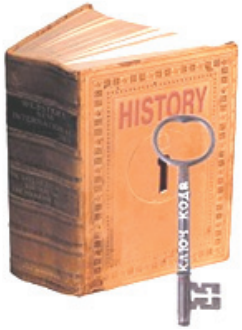
Гребенніков В.В.

ІСТОРІЯ КРИПТОЛОГІЇ & СЕКРЕТНОГО ЗВ'ЯЗКУ

Гребенніков В.В.

ІСТОРІЯ КРИПТОЛОГІЇ & СЕКРЕТНОГО ЗВ'ЯЗКУ

**Видання друге,
виправлене,
доповнене,
ілюстроване**



Ужгород

Гребенніков В.В.

Г 79 Історія криптології & секретного зв’язку

Книга написана ветераном Державної служби спеціального зв’язку та захисту інформації України полковником Держспецзв’язку Гребенніковим Вадимом Вікторовичем, Головою Ради ветеранів Закарпатської обласної організації ветеранів урядового зв'язку, відміченим державною нагородою «За бездоганну службу» та багатьма відомчими нагородами, зокрема: «Хрестом заслуги».

У виданні розповідається про історію народження й розвитку криптології та стеганографії, спеціальних видів засекреченого зв’язку у провідних країнах світу (СРСР, США, Великобританія, Німеччина), утворення їхніх криптологічних служб та апаратури засекречування, «шпіонську» діяльність спецслужб СРСР і США та їхню боротьбу у «полюванні» за шифрами супротивника, а також сучасний стан криптології у світі.

Книга побудована виключно на відкритих матеріалах, зібраних автором із надрукованих книг та мережі Інтернет.

Офіційна веб-сторінка книги: *www.cryptohistory.ru*

ББК 32.811.4

УДК 519.711

ЗМІСТ

Передмова 5

Частина 1. Історія європейської криптології 13
1.1. Поява шифрів 13
1.2. Становлення криптології як науки 23
1.3. Ера «чорних кабінетів» 47
1.4. Європейська криптологія у XIX ст. 62
1.5. Британські криптослужби 78
1.6. Німецькі криптослужби 93
1.7. Перші шифрувальні машини 120
1.7.1. Німеччина 125
1.7.2. Швеція 135
1.8. Розкриття «Енігми» 145
1.9. Операція «Ультра» 162
1.10. Комп'ютеризація криптології 178

Частина 2. Історія американської криптології 191
2.1. Американська криптологія до XX ст. 191
2.2. Винахід «лінійного» шифрування 208
2.3. «Чорний кабінет» Ярдлі 216
2.4. Армійська криптослужба 224
2.5. Перші шифрувальні машини 235
2.6. Криптослужба Фрідмена 247
2.7. Перша апаратура засекречування 255
2.8. Військова радіорозвідка 264
2.9. Агенція національної безпеки 277
2.10. Мережі спеціального зв'язку США 291
2.11. «Шпіонська» діяльність АНБ 305
2.12. Народження асиметричної криптології 330
2.13. Криптокартки «Fortezza» 342

Частина 3. Історія російської криптології 349
3.1. Давньоросійський тайнопис 349
3.2. Криптологія Петра Першого 356
3.3. «Чорний кабінет» XVIII ст. 365
3.4. Криптологія першої половини XIX ст. 380
3.5. Криптологія другої половини XIX ст. 388
3.6. Криптологія початку XX ст. 401

3.7. Революційна криптологія 421
3.8. Народження телеграфного зв'язку 438
3.9. Народження радіозв'язку 447
3.10. Військова криптологія 463

Частина 4. Історія радянської криптології 484
4.1. Народження радянських криптослужб 484
4.2. Становлення криптослужб СРСР 504
4.3. Створення радянської шифротехніки 516
4.4. Військова криптологія у 1940-50-і роки 524
4.5. Шифри радянської розвідки 534
4.6. Від ГУСС до ГУКДБ 555
4.7. «Полювання» за шифрами 573
4.8. «Втрати» російської криптології 587
4.9. Історія радіорозвідки 593
4.10. Спецзв'язок Росії 610

Частина 5. Історія секретної телефонії в СРСР 618
5.1. Народження телефонного зв'язку 618
5.2. Народження урядового зв'язку 628
5.3. Перша апаратура засекречування 650
5.4. «Рядянське вухо» і «Великий терор» 662
5.5. Урядовий зв'язок у Вітчизняній війні 673
5.6. Війська урядового зв'язку 684
5.7. Секрети Марфінської «шарашки» 703
5.8. Розробка стійких шифраторів 716
5.9. Утворення науково-промислової бази 732
5.10. Урядовий зв'язок другої половини XX ст. 741

Частина 6. Історія стеганографії 755
6.1 Невидимі чорнила 758
6.2 Маскування 767
6.3 Мікрокрапки 772
6.4 Цифрова стеганографія 779

Післямова 789

Використана література 793

Використані веб-сторінки 797

Рекомендовані фільми 798

«Хто володіє інформацією,
той володіє світом»
(Ротшильд)

Передмова

Майже чотири тисячі років тому в місті Менет-Хуфу на березі Нілу якийсь єгипетський переписувач намалював ієрогліфи, що розповіли історію життя його пана. Цей напис дійшов до наших днів та був вирізаний приблизно в 1900 році до н.е. на гробниці знатної людини на ім'я Хнумхотеп. Зробивши це, невідомий єгиптянин став родоначальником документально зафіксованої історії криптографії. Однак ці ієрогліфи все ж таки не були тайнописом у тому значенні, як його розуміють сьогодні. Для засекречування свого напису єгипетський переписувач не використав жодного повноцінного шифру, лише в окремих місцях намалював незвичайні ієрогліфічні символи замість більш звичних ієрогліфів.

Це свідчить про те, що вже з тих часів люди зрозуміли, що інформація становить визначену цінність та потребує захисту. В результаті її вирішили приховувати та почали робити це за допомогою доступних для свого часу способів. Спочатку писемність сама по собі була системою приховування інформації, тому що в давніх країнах нею володіли тільки обрані. Священні книги Давнього Єгипту та Давньої Індії тому приклади.

Поява писемності стала результатом потреби древньої людини виражати за допомогою символів божественні принципи. Форми цих символів (знаків) вона бачила в тріщинах каменів, на сніжному насті, у малюнках льоду… та вважала їх проявом божественної сили. Оскільки таким чином божество (або Природа) виражало свою волю, людина помічала ці символи та вважала їх священними.

Так, філософ Ф.Шеллінг писав: «Те, що ми називаємо природою, – лише поема, прихована в чудесному тайнописі». Такої ж думки і сучасний поет Ю.Мориць: «Тайнопис – почерк усієї світобудови, почерк поезії, кисті, клавіру! Тайнопис – це в тумані переказу вогненний шрифт сучасного світу».

Безперечно, найперші символи та знаки, написані чи видовбані в камені, або вирізані на дереві мали магічний характер. Найдавніші свідчення тому відносяться до 17-16 тисячоліття до н.е. На цих пам'ятниках писемності зображені фігури, що стали «прабатьками» відомих сьогодні магічних символів: хрестів, руней, колес, свастик. Згодом ці сакральні знаки накопичувалися, передавалися в одкровеннях, усно та до 3-1 тисячоліття до н.е. уже були системами, почали утворюватися перші магічні алфавіти.

Ці алфавіти осмислювалися в ті часи саме як набір священних символів із привласненими їм фонетичними значеннями, що дозволяло використовувати ці знаки для писемності. Так виникли родинні фінікійський, грецький, латинський, етруський і рунічний алфавіти, але досить значна частина древніх символів залишилася за межами цих алфавітів і продовжувала використовуватися винятково з магічною та художньою метою.

До нашого часу як магічний дійшов рунічний алфавіт. Руни (тобто знаки давньоскандинавського алфавіту) були розбиті на три групи по вісім штук у кожній. Основна система шифрування являла собою шифр заміни – кожній руні відповідали два знаки шифротекста (косі риски різної довжини). Число рисок зверху позначало номер групи, а знизу – номер руни в групі. Зустрічалися й ускладнення цієї системи, наприклад руни в групах перемішувалися.

До наших днів зберігся навіть пам'ятник давньої шведської криптографії – рекський камінь. Цей камінь висотою більше 4 метрів знаходиться на цвинтарі села Рьок. На ньому нанесено 770 зашифрованих руней.

Незважаючи на те, що пізніше в країнах Скандинавії стала застосовуватися латинська абетка, рунічне письмо використовувалося до XIX століття. Однак у XVI-XVIII століттях досить мало людей знало рунічні алфавіти, тому рунічний запис навіть без шифрування забезпечував збереження таємниці листування. Зокрема руни для захисту інформації використовував шведський генерал Якоб де ла Гарді під час тридцятирічної війни (1618–1646).

Готське слово «runa» означає «таємниця» і походить з древнього німецького кореня зі значенням «ховати». В сучасних мовах це слово також присутнє: німецьке «raunen» означає «нашіптувати», латиське «runat» – «говорити», фінське «*runo*» – «вірш, заклинання». Ще одним магічним алфавітом, який деякі автори відносять до «рунічних написів», є огамічний (*ogam, ogum, ogham*), розповсюджений в Ірландії, Шотландії, Уельсі та Корнуолі в III-X століттях н.е. У давньоірландських текстах було згадування про те, що «*ogam*» служив для

передачі таємних послань, а також для гадань.

Взагалі магічним алфавітом можна назвати будь-який алфавіт, тому що кожна буква кожного алфавіту має власне символічне значення. Особливо це стосується єврейського івриту та індійського санскриту, які поряд із грецьким і латинським алфавітами до цього часу використовуються окультистами. Однак, незважаючи на наявність сакральних значень у символів двох останніх, вони все-таки стали згодом, у першу чергу, ознаками вченості та культури тих, хто їх уживав.

Символізм, який був закладений у кожну букву, виконував дві функції: по-перше, він приховував таємниці від непосвячених, а по-друге, навпаки, відкривав їх тим, хто був цього гідний, хто розумів прихований зміст цих символів. Присвячені жреці вважали святотатством обговорення священних істин вищих світів або божественних одкровень вічної Природи на тій же мові, що використовувалася простим народом. Саме через це усіма сакральними традиціями світу розроблялися свої таємні алфавіти.

Іврит є одним із найпоширеніших алфавітів у Західній магічній традиції, а його букви вважаються умістищем божественної сили. Наприклад, буква єврейського алфавіту «алеф» означає владу, людину, мага; буква «бет» – науку, рот, двері храму; «гимель» – дію, протягнену для рукостискання руку тощо. В алхімії букви були також багатозначні: «*A*» виражало початок усіх речей; «*Y*» – відношення між чотирма основними елементами; «*L*» – розкладання; «*M*» – андрогінну природу води у її первісному стані тощо.

Грецький алфавіт, подібно івриту для євреїв, служив грекам одним із засобів пізнання світу. У греків букви «*A*», «*E*», «*H*», «*I*», «*O*», «*Y*» і «*Ω*» відповідали 7 планетам (небесам). Букви «*B*», «*Γ*», «*Δ*», «*Z*», «*K*», «*Λ*», «*M*», «*N*», «*Π*», «*P*», «*Σ*» і «*T*» приписувалися 12 знакам Зодіаку. Букви «*Θ*», «*Ξ*», «*Φ*» і «*X*» являли собою 4 світові елементи (стихії), а «*Ψ*» – «світовий дух». Алфавіт використовувався також для гадання та в різних містеріях. Так, наприклад, п'ята буква грецького алфавіту «*E*» (епсілон)

Α	α	альфа	Ν	ν	ню
Β	β	бета	Ξ	ξ	кси
Γ	γ	гамма	Ο	ο	омикрон
Δ	δ	дельта	Π	π	пи
Ε	ε	эпсилон	Ρ	ρ	ро
Ζ	ζ	дзета	Σ	σ	сигма
Η	η	эта	Τ	τ	тау
Θ	θ	тета	Υ	υ	ипсилон
Ι	ι	йота	Φ	φ	фи
Κ	κ	каппа	Χ	χ	хи
Λ	λ	лямбда	Ψ	ψ	пси
Μ	μ	мю	Ω	ω	омега

служила символом «Духовного Сонця» у великому храмі грецьких містерій у Дельфах, де протягом сімнадцяти століть проводилися елевсинські присвяти.

У латинському алфавіті голосні букви «*A*», «*E*», «*I*», «*O*», «*U*» і приголосні «*J*», «*V*» відповідали 7 планетам. Приголосні букви «*B*», «*C*», «*D*», «*F*», «*G*», «*L*», «*M*», «*N*», «*P*», «*S*» і «*T*» керували 12 астрологічними знаками. Букви «*K*», «*Q*», «*X*», «*Z*» відповідали 4 стихіям, а «H» являла собою «світовий дух». Латинський алфавіт використовувався в багатьох окультних значеннєвих фігурах.

У давніх цивілізаціях ми знаходимо два види письма: ієратичне, або священне письмо, що використовувалося священнослужителями для таємного спілкування один з одним, і демотичне письмо, що вживалося всіма іншими. Винахід першої системи скоропису, що споконвічно слугував як таємний лист, приписувався Туліусу Тиро, вільновідпущеному рабу Цицерона (106-43 роки до н.е.).

За свідченням Геродота в давньому Єгипті роль шифру відігравала спеціально створена жерцями мова. Там паралельно існували три алфавіти: письмовий, священний та загадковий. Перший з них відображав звичайну розмовну мову, другий міг використовуватися для викладу релігійних текстів, а третій застосовувався провісниками або для приховання змісту повідомлень. У давній Греції також існували десятки досить відмінних один від одного діалектів.

Діоген Лаертський так пояснював одну з причин вгасання філософії пифагорійців: «...записана вона була по-дорийські, а оскільки цей прислівник малозрозумілий, то здавалося, що й вчення, які на ньому викладають, не справжні й перекручені...». У книзі Е.Шюре «Великі присвячені» зустрічається фраза про те, що «з великою працею і великою ціною добув Платон один з манускриптів Піфагора, що ніколи не записував своє навчання інакше, як таємними знаками та під різними символами».

Фіванський алфавіт використовується й сьогодні завдяки старанням не тільки практиків середньовічних гримуарів, але й деяких містично налаштованих особистостей, що іменують себе «язичниками». Так само як і будь-який інший з категорії «магічних», фіванський алфавіт використовується для написання текстів заклинань та служить у таких випадках шифром (араб. *sifr* - ноль, ніщо, пустота).

Вчений Блез Паскаль писав: «Мови суть шифри, в яких не букви замінені буквами, а слова

словами, так що невідома мова є шифр, який легко розгадується». Так, мови американських індіанців неодноразово використовувалися як системи шифрування. Під час Першої світової війни індіанці племені «чокто (чахта)» були першими, хто допомагав Армії США шифрувати військові повідомлення, а на початку Другої світової війни для ВМС США це робили індіанці племені «навахо». У 1960 році ірландські збройні сили в Конго, направлені туди за рішенням ООН, здійснювали переговори на гельській мові.

З розвитком фонетичного письма писемність різко спростилася. У давньому семітському алфавіті у 2-му тисячолітті до н.е. було всього близько 30 знаків. Ними позначалися приголосні звуки, а також деякі голосні й склади. Спрощення письма стимулювало розвиток криптології та шифрувальної справи.

Правителям великих держав необхідно було здійснювати «приховане» керівництво намісниками в чисельних провінціях та одержувати від них інформацію про стан справ на місцях. Королі, королеви й полководці повинні були керувати своїми країнами та командувати своїми арміями, опираючись на надійний та ефективно діючий зв'язок. В результаті організація та забезпечення шифрованого зв'язку для них було життєво необхідною справою.

У той же час усі вони усвідомлювали наслідки того, що відбудеться, якщо їхні повідомлення потраплять не в ті руки, якщо ворожій державі стануть відомі важливі таємниці. І саме побоювання того, що вороги перехоплять повідомлення, послужило причиною активного розвитку кодів і шифрів – способів приховання змісту повідомлення таким чином, щоб прочитати його зміг тільки той, кому воно адресовано.

Прагнення забезпечити таємність означало, що в державах функціонували підрозділи, що створювали коди й шифри та відповідали за забезпечення таємності зв'язку шляхом розробки й використання самих надійних шифрів. А в цей же час дешифрувальники ворога намагалися розкрити ці шифри та видідати його таємниці.

Дешифрувальники являли собою алхіміків від лінгвістики, загін чаклунів, що намагалися за допомогою магії одержати осмислені слова з безглуздого набору символів. Історія кодів і шифрів – це багатовікова історія двобою між «творцями» та «зломщиками» шифрів, інтелектуальна гонка шифрувальної зброї, що вплинула на хід історії.

При написанні цієї книги я ставив перед собою чотири завдання. По-перше, викласти зібраний матеріал у хронологічній послідовності на українській мові, в чому і полягає новізна книги («фішка» - по молодіжній термінології). Історичні книги з питань криптології є тільки на російській та англійській мовах, тому я

вирішив виправити цей недолік. По-друге, доповнити історію криптології ще історією шифровально-документального та урядового телефонного зв'язку, оскільки для його функціонування також потрібні шифри. По-третє, показати еволюцію шифрів різних країн у хронологічній послідовності. Тут повною мірою підходить термін «еволюція», оскільки розвиток шифрів може розглядатися як еволюційна бо¬ротьба.

Шифр завжди є об'єктом атаки дешифрувальників. Як тільки дешифрувальники створюють новий засіб, що виявляє слабке місце шифру, подальше його використання стає безглуздим. Шифр або виходить із уживання, або на його основі розробляється новий, більш стійкий. У свою чергу, цей новий шифр використовується доти, поки дешифрувальники не знайдуть його слабке місце, і так далі.

Боротьба, що не припиняється між «творцями» та «зломщиками» шифрів, сприяла появі цілого ряду чудових наукових відкриттів. Шифрувальники постійно докладали зусиль для створення усе більш стійких шифрів щодо захисту систем і засобів зв'язку, у той час як дешифрувальники безупинно винаходили все більш потужні методи їхньої атаки.

У своїх зусиллях руйнування й збереження таємності обидві сторони залучали найрізноманітніші наукові дисципліни й методи: від математики до лінгвістики, від теорії інформації до квантової теорії. В результаті шифрувальники й дешифрувальники збагатили ці предмети, а їхня професійна діяльність прискорила науково-технічний прогрес, причому найбільш помітно це виявилося в розвитку сучасних комп'ютерів.

Роль шифрів в історії величезна. Шифри вирішували результати боїв і призводили до смерті королів і королев. Тому я звертався до історичних фактів політичних інтриг та розповідей про їхні життя й смерть, щоб проілюструвати ключові поворотні моменти в еволюційному розвитку шифрів. Історія шифрів настільки багата, що мені довелося опустити багато захоплюючих історій, що, у свою чергу, означає, що моя книга не занадто повна. Якщо ви захочете більше довідатися про розповіді, що вам сподобалися, або про дешифрувальника, що зробив на вас незабутнє враження, то я рекомендуювам звернутися до списку використаної літератури, що повинна допомогти тим читачам, які бажали б вивчити предмет більш детально.

Четверта мета книги полягає в тому, щоб показати, що шифри сьогодні мають набагато більше значення, ніж коли-небудь раніше. Оскільки інформація стає усе більше і більше цінним товаром, а революція у сфері комунікацій змінює суспільство, процес зашифровування повідомлень, або інакше, шиф-

рування, починає грати все більшу роль у повсякденному житті. Сьогодні наші телефонні розмови передаються по супутникових каналах, а наші електронні листи проходять через різні комп'ютери, і можна з легкістю здійснити перехоплення інформації, що ставить під загрозу наше приватне життя.

Шифрування – єдиний спосіб захистити наше приватне життя й гарантувати успішне функціонування електронного ринку. Мистецтво тайнопису, що перекладається грецькою як криптографія (гр. *kryptós* – таємний і *graphia* – пишу) дасть вам замки й ключі інформаційного століття. Щоб у подальшому вся викладена нижче інформація була зрозумілою, розглянемо основні поняття та терміни цієї науки.

Інформація, що може бути прочитана та зрозуміла без яких-небудь спеціальних заходів, називається відкритим текстом. Метод перекручування та приховування відкритого тексту таким чином, щоб сховати його суть, називається зашифруванням. Зашифрування відкритого тексту приводить до його перетворення у незрозумілу абракадабру, іменовану шифротекстом. Шифрування дозволяє сховати інформацію від тих, для кого вона не призначається, незважаючи на те, що вони можуть бачити сам шифротекст. Протилежний процес перетворення шифротексту в його вихідний вигляд називається розшифруванням.

Криптографія – це заходи щодо приховування та захисту інформації, а криптоаналіз (гр. *análysis* – розкладання) – це заходи щодо аналізу та розкриття зашифрованої інформації та криптографованих комунікацій. Разом криптографія та криптоаналіз створюють науку криптологію (гр. *lógos* – слово, знання).

Відкритий текст	Зашифрування	Шифртекст	Процес передачі	Шифртекст	Розшифрування	Відкритий текст

Криптологія – це наука про використання математики для зашифрування й розшифрування інформації. Криптологія дозволяє зберігати важливу інформацію при передачі її звичайними незахищеними каналами зв'язку (зокрема, Інтернет) у такому вигляді, що вона не може бути прочитаною або зрозумілою ніким, крім визначеного одержувача. Криптоаналіз являє собою суміш аналітики, математичних і статистичних розрахунків, а також спокою, рішучості та удачі. Криптоаналітиків також називають «зломщиками».

Криптографічна стійкість вимірюється тим, скільки знадобиться часу й ре-

сурсів, щоб із шифротексту відновити вихідний відкритий текст. Результатом стійкої криптографії є шифротекст , що надзвичайно складно «зламати» без володіння певними інструментами з дешифрування.

Криптографічний алгоритм, або шифр – це математична формула, що описує процеси зашифрування й розшифрування. Секретний елемент шифру, який повинен бути недоступним стороннім, називається ключем шифру.

Щоб зашифрувати відкритий текст або розмову, криптоалгоритм працює в поєднанні з ключем – словом, числом або фразою. Одне ж те саме повідомлення, зашифроване одним алгоритмом, але різними ключами, буде перетворювати його у різний шифротекст. Захищеність шифротексту цілком залежить від двох речей: стійкості криптоалгоритма та секретності ключа.

Найпростішим видом шифрування є кодування, де не використовується ключ. Хоча у сучасній криптології код не вважається шифром, однак він є таким – це шифр простої заміни. Кодування, як правило, містить у собі застосування великої таблиці або кодового словника, де перераховані числові відповідності (еквіваленти) не тільки для окремих букв, але й для цілих слів та найбільш використовуваних фраз і речень.

Отже, перейдемо до цікавої та захоплюючої історії криптології та спеціальних видів зв'язку...

Частина 1.

Історія європейської криптології

1.1. Поява шифрів

Взагалі всі шифри можуть бути розділені на два види: перестановка й заміна. При перестановці букви повідомлення просто переставляються, утворюючи анаграму. Для дуже короткого повідомлення, що складається, наприклад, з одного слова, такий спосіб досить ненадійний, оскільки існує вкрай обмежене число можливих способів перестановки жменьки букв. Так, 3 букви можуть бути розставлені всього лише 6 різними способами. Однак у міру збільшення чисельності букв кількість можливих перестановок стрімко зростає, і відновити вихідне повідомлення стає неможливо, якщо невідомий точний спосіб шифрування. Наприклад, якщо фраза складається з 35 букв, то кількість їхніх різних перестановок становить більше 50 000 000 000 000 000 000 000 000 000 000.

Якби одна людина змогла перевіряти одну перестановку в секунду, і якби всі люди на Землі працювали день і ніч, то, щоб перевірити всі можливі перестановки, треба було б часу в тисячі разів більше, ніж термін існування Всесвіту.

Створюється враження, що випадкова перестановка букв гарантує дуже високий ступінь безпеки, оскільки для супротивника дешифрувати навіть коротке речення виявиться нездійсненним. Однак при перестановці може утворитися неймовірно складна анаграма, і якщо букви випадково, ні з того ні із сього, переплутаються, то ні

одержувач, ні перехоплювач не зможуть її розшифрувати. Тому спосіб перестановки букв повинен бути заздалегідь обговорений відправником повідомлення і його одержувачем, але разом з тим зберігатися в таємниці від супротивника.

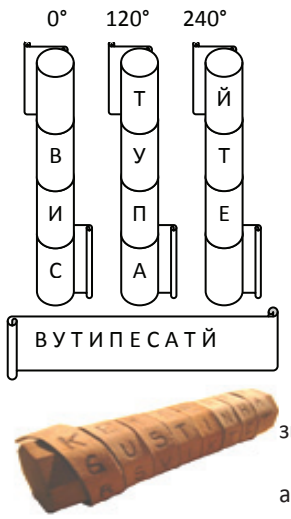
Першим шифрувальним пристроєм, який дійшов до нас та реалізовував шифр перестановки, була так звана «скитала» (scytale) або «сцитала» (близько VI-V ст. до н.е.), що використовувалась в античний період спартанцями.

Скитала являла собою дерев'яний циліндр, навколо якого намотувалася смужка шкіри або пергаменту. Відправник писав повідомлення по всій довжині скитали, а потім розмотував смужку, на якій після цього залишався безглуздий набір букв. Повідомлення виявлялося зашифрованим. Вісник брав шкіряну смужку й звичайно ховав повідомлення, використовуючи смужку як пояс, буквами усередину, тобто крім зашифровування застосовував також і стеганографію. Щоб одержати вихідне повідомлення, адресат просто намотував смужку шкіри навколо скитали того ж діаметра, що й скитала, якою користувався відправник.

У 404 році до н.е. до спартанського полководця Лісандра привели вісника, який був закривавлений та ледве тримався на ногах, одного з 5-ти вісників, що залишився живим після вкрай небезпечної подорожі з Персії. Вісник передав свій пояс Лісандру, що намотав його навколо своєї скитали й прочитав, що перський воєначальник Фарнабаз збирається напасти на нього. Завдяки скиталі Лісандр встиг підготуватися до нападу й відбив його.

Грецький історик Плутарх так описав цей спосіб шифрування:

«Відправляючи до місця служби начальника флоту або сухопутного війська, ефори вручають від'їжджаючому круглий ціпок. Інший, зовсім однакової довжини й товщини, залишають собі. Ці ціпки й називають скиталами. Коли ефорам потрібно повідомити яку-небудь важливу таємницю, вони вирізують довгу й вузьку, як ремінь, смугу папірусу, щільно, без проміжків намотують її на свою скиталу й пишуть на ній текст. Потім знімають смугу й без ціпка відправляють її воєначальнику. Оскільки букви на ній розміщують без усякого зв'язку, розкидані безладно, прочитати написане він може, тільки взявши свою скиталу й намотавши на неї вирізану смугу, щоб, водячи очами навколо ціпка й переходячи від попередньої до наступної, мати перед собою зв'язне повідомлення».



Це те ж саме, начебто букви писати не підряд, а через домовлене число по кільцю доти, поки весь

текст не закінчиться. Повідомлення «ВИСТУПАЙТЕ» при окружності палички в 3 букви дасть шифровку «ВУТИПЕСАТЙ».

Для прочитання шифровки потрібно було не тільки знати систему засекречування, але й мати ключ у вигляді палички визначеного діаметра. Знаючи тип шифру, але не маючи ключа, розшифрувати повідомлення було би складно. Шифр був досить популярний у Спарті й багато разів удосконалювався в пізніші часи. Про його важливе значення й велике поширення говорить свідчення Плутарха в «Порівняльних життєописах», коли історик повідомляє про життя грецького полководця Алкивіада: «Однак Лісандр звернув увагу на ці слова не раніше, ніж одержав з будинку скиталу з наказом відскіпатися від Алкивіада...»

Цей нехитрий спосіб часто використовувався через свою простоту та можливість оперативного розшифрування повідомлення. У той же час стійкість даного шифру була невелика, тому пізніше Архімед запропонував пристрій («антискитала»), за допомогою якого розшифровка подібного повідомлення без потрібного циліндра була досить простою та швидкою. Ремінь намотували на конічний «спис» і зрушували нагору й униз доти, поки не знаходили потрібний діаметр і текст повідомлення ставав зрозумілим.

Альтернативним шифру перестановки був шифр заміни, у якому кожна буква у вихідному тексті замінялася іншою буквою. Один з перших описів шифру заміни був приведений у «Камасутрі», тексті, написаному в 4-му столітті н.е. священиком-браміном Ватсьяяною, але заснованому на манускриптах, що відносяться до 4-го століття до н.е.

Згідно з «Камасутрою», жінки повинні опанувати 64 мистецтва, такі як готування їжі й напоїв, мистецтво одягання, масажу, готування ароматів. У цей список також входили менш очевидні мистецтва: чаклунство, гра в шахи, палітурна справа й теслярство. Під номером 45 у списку знаходилося мистецтво тайнопису *«mlecchita-vikalpa»*, призначене для того, щоб допомогти жінкам приховати подробиці своїх любовних зв'язків.

Один із рекомендованих способів полягав у тому, щоб розташувати попарно букви алфавіту випадковим чином, а потім заміняти кожну букву у вихідному повідомленні її парною (симетричною). Якщо застосуємо цей принцип до латинського алфавіту, то можемо скласти таку таблицю (лінійку) шифрування:

D	A	M	H	I	K	O	Z	R	S	U	W	Y
X	B	T	V	G	J	C	L	N	E	Q	F	P

Тоді замість слова «*UKRAINE*» відправник напише слово «*QJNBGRS*»**.**

На Близькому Сході один з перших шифрів заміни був розроблений древніми євреями та називався «темура» – «обмін». 22 букви єврейського алфавіту ділилися на дві частини, причому одна містилася над іншою; потім верхні букви замінялися

на нижні або навпаки. Можна було встановити всілякі комбінації залежно від місця поділу алфавіту й напрямку переміщуваних букв.

Найпростіший спосіб полягав у поділі алфавіту посередині так, щоб перші дві букви, «А» і «Б», збігалися із двома останніми, «Т» і «Ш». Ці букви й дали назву методу шифрування – «Атбаш» (англ. *Atbash*). Це був простий шифр одноалфавітної заміни для єврейського алфавіту. Таблиця (лінійка) шифрування цим методом для латинського алфавіту буде виглядати таким чином:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Бачимо, що у цьому шифрі заміна має симетричний вигляд. Так, наприклад, слово «*UZHGOROD*» перетворювалося у слово «*FASTLILW*».

Інший шифр «Альбам» полягав у розбивці алфавіту на дві частини та розташуванні однієї частини під іншою:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Слово «UZHGOROD» перетворювалося вже у слово «HMUTBEBQ».

Перше документально підтверджене використання шифру заміни у військових цілях з'явилося у «Записках про галльську війну» (лат. *Commentarii de Bello Gallico*) Гая Юлія Цезаря (I століття до н.е.). Цезар описував, як він послав повідомлення Цицерону, що перебував в облозі та був на грані капітуляції. У цьому листі латинські букви були замінені грецькими, тому ворог його не зміг би зрозуміти.

C. IVLII
CÆSARIS
COMMENTARII
DE BELLO GALLICO
ET CIVILI
TOMUS I.
VENETIIS MDCCLXXXIII

Цезар так часто користувався тайнописом, що Марко Валерій Проб написав цілий трактат про застосовувані ним шифри, який, на жаль, не дійшов до наших днів. Однак завдяки твору Гая Транквілла Светонія «Життя 12 Цезарів», написаному в 2-му столітті н.е., у нас є докладний опис одного з шифрів заміни, що застосовувалися Юлієм Цезарем. Він просто заміняв кожну букву в посланні буквою, що знаходилась в алфавіті на три позиції далі.

Ось як про це повідомляє Гай Светоній: «Існують і його листи Цицерону та листи до близьких про домашні справи: у них, якщо потрібно було повідомити що-небудь негласно, він користувався тайнописом, тобто міняв букви так, щоб з них не складалося жодного слова. Щоб розібрати й прочитати їх, потрібно читати щоразу четверту букву замість першої».

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Спочатку виписувався алфавіт у природному порядку, а потім під ним виписувався той же алфавіт, але зі зрушенням на 3 букви вліво. При зашифруванні буква «*A*» замінялася буквою «*D*», «*B*» замінялася на «*E*», «*C*» – на «*F*» й так далі. Так, наприклад, слово «*UZHGOROD*» перетворювалося у слово «*XCKJRURG*», а «*UKRAINE*» – у «*XNUDLQH*». Одержувач зашифрованого повідомлення шукав ці букви в нижньому рядку та по буквах над ними відновлював вихідне слово. Ключем у шифрі Цезаря була величина зрушення нижнього рядка алфавіту, тобто цифра 3. Спадкоємець Юлія Цезаря – Цезар Август – використовував той же шифр, але з ключем зрушення 4.

Вже у IV столітті до н.е. робилися спроби «механізації» криптологічної справи, пов'язані насамперед з ім'ям давньогрецького полководця Енея Тактики, захисника Трої, друга Гектора. Він створив так званий «диск Енея», що одержав у Давній Греції широке застосування. У диску діаметром 10-15 см і товщиною 1-2 см висвердлювалися отвори, що відповідали буквам алфавіту, через які просмикувалася нитка відповідно до букв шифрованого тексту. Для розшифрування нитку витягали, одержуючи зворотню послідовність букв. Цей примітивний на перший погляд спосіб шифрування був досить ефективний, тому що супротивнику, який перехопив повідомлення, було невідомо, яка буква відповідає кожному отвору. Крім того, якщо виникала небезпека перехоплення повідомлення, нитку можна було легко порвати, тим самим знищивши його.

Ідея Енея була використана при створенні й інших оригінальних шифрів заміни. Зокрема, в одному з варіантів замість диска використовувалася лінійка з кількістю отворів, рівних кількості букв алфавіту. Кожний отвір позначався своєю буквою, а букви по отворах розташовувалися в довільному порядку. До лінійки була прикріплена котушка з намотаною на неї ниткою. Поруч із котушкою був проріз. При шифруванні нитка простягалася через проріз, а потім через отвір, що відповідав першій букві шифрованого тексту, при цьому на нитці зав'язувався вузлик у місці проходження її через отвір. Потім нитка поверталася в проріз й

аналогічно зашифровувалася друга буква тексту й т.д. Після закінчення шифрування нитка витягалася й передавалася одержувачу повідомлення. Той, маючи ідентичну лінійку, простягав нитку через проріз до отворів, обумовлених вузлами, і відновлював вихідний текст по буквах отворів.

Цей пристрій одержав назву «лінійка Енея». Шифр, реалізований лінійкою Енея, був одним з прикладів шифру заміни: коли букви замінялися на відстані між вузликами з урахуванням проходження через проріз. Ключем шифру був порядок розташування букв по отворах у лінійці. Супротивник, що одержав нитку (навіть, маючи лінійку, але без нанесених на ній букв), не міг прочитати передане повідомлення. Аналогічне «лінійці Енея» «вузелкове письмо» отримало поширення в індіанців Центральної Америки. Свої повідомлення вони також передавали у вигляді нитки, на якій зав'язувалися різнобарвні вузлики, що визначали зміст повідомлення.

Ще один винахід стародавніх греків – так званий «квадрат Полібія». Грецький письменник Полібій (біля 200 – 120 до н.е.) використовував систему сигналізації, що була широко прийнята як метод шифрування. Він записував букви грецького алфавіту в квадратну таблицю та заміняв їх числовими координатами в таблиці номером рядка та номером стовпця. Пари чисел передавалися за допомогою смолоскипів. У варіанті з латинським алфавітом для передачі, наприклад, букви «U» потрібно було взяти 4 смолоскипи в праву руку та 5 – у ліву, або записати як цифру «45».

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Наприклад, слово «*UKRAINE*» можна записати як цифровий шифротекст «45254211243315» або «54522411423351».

Цікаво, що шифр Полібія дійшов до наших днів та одержав своєрідну назву «шифру в'язнів». Для його використання потрібно було тільки знати природний порядок розташування букв алфавіту (як у вищезазначеному прикладі для англійської мови). Число 3, наприклад, передавалося шляхом потрійного стукоту. При передачі букви спочатку відстукувалося число номера рядка, у якому знаходилася буква, а потім число номера відповідного стовпця. Наприклад, буква «F» передавалася подвійним стукотом (другий рядок) і потім одинарним (перший стовпець).

Із застосуванням цього шифру пов'язані деякі історичні казуси. Так, росій-

ські «*декабристы*», які були ув'язнені після невдалого повстання, не змогли встановити зв'язок з князем Одоєвським. Виявилося, що він (добре освічений за тих часів) не пам'ятав природний порядок розташування букв у російському та французькому алфавітах (іншими мовами він не володів). «Декабристи» для російського алфавіту використовували прямокутник розміру 5х6 (5 рядків та 6 стовпців) і скорочений до 30 букв алфавіт.

Пізніше букви стали розташовувати в квадраті хаотично, але це вимагало наявність такого квадрата у отримувача повідомлення, що також було небезпечно. Вихід був знайдений у застосуванні так званого ключового слова, що легко запам'ятовувалося. Обиралося недовге слово (наприклад, «UKRAINE»), з нього забиралися букви, що повторювалтся, а ті, що залишалися, записувалися в перші клітини квадрата по рядках. Порожні клітини заповнювалися буквами алфавіту, що залишилися, у природному порядку.

	1	**2**	**3**	**4**	**5**
1	U	K	R	A	I
2	N	E	B	C	D
3	F	G	H	L	M
4	O	P	Q	S	T
5	V	W	X	Y	Z

В результаті такого шифрування слово «*UZHGOROD*» перетворюється у цифровий шифротекст «11553332414125».

Полібійський квадрат став однією з найбільш широко розповсюджених криптосистем, що вживалися у той час. Цьому сприяла його досить висока стійкість (у всякому разі, до автоматизації дешифрувальних систем): квадрат 5х5 для латинського алфавіту містить 155112100433310000000000000 (розрахунок досить приблизний) можливих положень, що практично виключає його дешифрування без знання ключа.

Ледащі й тому винахідливі римляни в IV столітті до н.е., щоб спростити процедуру шифрування, почали застосовувати два шифрувальні диски. Кожний із дисків, розміщених на загальної вісі, містив на своєму ободі алфавіт у випадковій послідовності. Кожній букві першого диска відповідала буква другого, що й становило шифр. Знайшовши на одному диску букву тексту, з іншого диска зчитували відповідну їй букву шифру. Такі прилади, що породжували шифр простої заміни, використовувалися аж до епохи Відродження.

Ці криптосистеми активно застосовувалися в Давній Греції та Римі й надовго визначили характер криптології. В умовах потреби ручного розшифрування, по-

лібійський квадрат був практично невразливим шифром, а скитала та диск Енея були досить прості, проте дозволяли оперативно зашифровувати й розшифровувати інформацію, що робило їх вигідними, скажімо, в польових умовах для оперативної передачі наказів.

Із занепадом античної цивілізації та утворенням у Європі варварських держав, криптологія занепала. Велика шкода її розвитку була завдана в часи середньовічної інквізиції. Всі кращі досягнення цивілізації, а разом з ними й криптологія, були втрачені. За свідченням святого Джерома «увесь світ поринув у руїни». В умовах, коли грамотність була вкрай низька, зашифровувати повідомлення не було необхідності, тому й самих письмових повідомлень практично не було.

Так, король франків Карл Великий, заснувавший у 800 році Священну Римську імперію, навчився читати й писати тільки у 50 років. Проте Карл Великий знав і використовував у листуванні зі своїми генералами шифр заміни букв алфавіту групою символів.

Освіта й грамотність у ті часи зосередилися в церкві, тому тайнопис став її монополією. Церква ухвалила, що простим парафіянам не можна приховувати таємниці від «Господа», а тайнопис – це «єресь». За використання тайнопису передбачалися жорстокі заходи покарання, аж до страти.

Крім вищеперерахованих причин, криптологія перебувала в занепаді ще й тому, що в ній бачили елементи чаклунства. Набір незрозумілих букв або символів, сам по собі схожий на заклинання, сприймався як щось магічне, а люди, що розуміли у цьому наборі символів зміст, розцінювалися як чаклуни або ворожки, що не могло не накласти свій відбиток на ставлення до них у християнській Європі.

З перших днів свого існування криптологія мала на меті сховати зміст важливих розділів письмових документів, що мали відношення до таких сфер магії, як гадання й заклинання. В одному з рукописів про магію, що датується III століттям н.е., був використаний шифр, щоб сховати важливі частини чаклунських рецептів. Криптографія часто була на службі магії в часи середньовіччя, і навіть в епоху Відродження за допомогою шифрів алхіміки засекречували важливі частини формул одержання «філософського каменя».

До шифрування інформації «призивалися» містичні сили. Так, наприклад, рекомендувалося використовувати «магічні квадрати». У квадрат розміром 4 х 4 вписувалися числа від 1 до 16. Його магія полягала в тому, що сума чисел по

рядках, стовпцях і діагоналях дорівнювала одному й тому ж числу – 34. Уперше ці квадрати з'явилися в Китаї, де їм і була приписана деяка «магічна сила».

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Для зашифруваня слова «ЗАКАРПАТТЯ» букви вписувалися послідовно до квадрату згідно з записаними в них цифрами, а до пустих клітинок вписувалися будь-які букви.

16Ж	3К	2А	13Г
5Р	10Я	11Б	8Т
9Т	6П	7А	12В
4А	15Е	14Д	13

Після цього шифротекст записувався у рядок: ЖКАГРЯБТТПАВАЕДЗ. Даний шифр – це звичайний шифр перестановки, але вважалося, що особливу стійкість йому надають чари «магічного квадрата».

На перший погляд здається, начебто магічних квадратів дуже мало. Проте їхнє число дуже швидко зростає зі збільшенням розміру квадрата. Так, існує лише один магічний квадрат розміром 3х3, якщо не брати до уваги його повороти. Магічних квадратів 4х4 налічується вже 880, а число магічних квадратів розміром 5х5 близько 250000. Тому магічні квадрати більших розмірів могли бути гарною основою для надійної системи шифрування того часу, тому що ручний перебір всіх варіантів ключа для цього шифру був немислимий.

Подібність між магією та криптологією обумовлювалася й іншими факторами. Крім криптології, таємничі символи використовувалися в зрозумілих лише присвяченим сферах магічних знань – астрологія та алхімія, де подібно знакам відкритого тексту, кожна планета й кожна хімічна речовина мали спеціальний знак. Як і зашифровані слова, заклинання й магічні формули, начебто «абракадабри», нагадували нісенітницю, але в дійсності мали важливе значення.

Те, що писали або малювали астрологи та маги, було схоже на кодограму, де кожний символ або ієрогліф мав своє особисте як екзотеричне (матеріальне), так і езотеричне (духовне) значення. Наприклад, символ Сонця – це індивідуальність та духовність, Місяця – м'якість та душевність, Меркурія – мислення та інтелектуальність, Венери – жіночість та кохання, Марса – мужність та активність, Юпітера – законослухняність та релігійність, Сатурна – самотність та цілеспрямованість

тощо. Навіть місця символів, де вони були намальовані, теж визначали їх вплив на події життя та взаємовідносини з іншими чинниками долі. А те, що одним малюнком (гороскопом) можна відобразити долю та все життя людини або країни, здавалося справжньою магією чи чаклунством.

Солнце	☉	Юпитер	♃
Луна	☽	Сатурн	♄
Меркурий	☿	Уран	♅
Венера	♀	Нептун	♆
Марс	♂	Плутон	♇

Думка про те, що криптоаналіз є також за своєю суттю якоюсь магією, складалася у зв'язку з поверхневою подібністю криптоаналізу та гадання. Добування істинного змісту з шифротексту здавалося точно такою ж справою, що й одержання знань шляхом вивчення розташування зірок і планет, довжини ліній і місць їхнього перетинання на долоні, нутрощів овець, положення кавового осаду в чашці. Видимість брала гору над реальністю. Простодушні люди бачили магію навіть у звичайному процесі розшифрування. Інші бачили її в криптоаналізі, тому що розкриття чогось глибоко захованого здавалося їм незбагненним і надприродним.

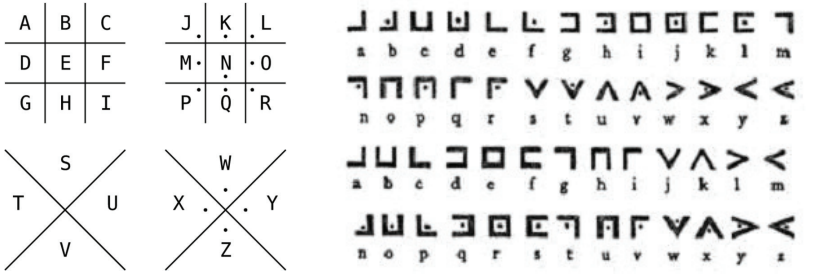
Не таким сильним був занепад криптології у Візантії, що зберегла багато античних традицій. Але й тут криптосистеми дуже спростилися та були легко вразливими. Найчастіше повідомлення просто писали у зворотньому порядку або заміняли кожну букву на наступну за алфавітом. Для засекречування повідомлень також використовували маловідомі іноземні мови, найчастіше вірменську або давньоєврейську. Але в цілому, у порівнянні з епохою античності, криптологія перебувала на вкрай низькому рівні.

В середньовічному Китаї у трактаті «Основи класичної військової науки», складеному в XI столітті нашої ери, були присутні лише кодувальні рекомендації. В них рекомендувалося співвіднести з різними простими повідомленнями перші 40 знаків якого-небудь вірша, відомого як відправнику, так і одержувачу. По першому знаку вірша, поставленому в домовленому місці цілком безневинного повідомлення, одержувач «зчитував» інформацію, наприклад, що потрібно послати більше провіанту. Такі коди практично не піддавалися розшифруванню, але вони могли використовуватися лише в дуже обмеженому масштабі.

Деякі окремі релігійні організації використовували особистий алфавіт як одноалфавітний шифр заміни. Так, шифри тамплієрів і розенкрейцерів були дуже схожими та знайшли своїх шанувальників в особі масонів (деякі дослідники, зокрема, О.П.Блаватська, так їх і називали – «масонський»). Масонський шифр використовувався їхніми «ложами» для таємного листування між присвяченими вищих ступенів.

У XVIII столітті франкмасонами використовувався для забезпечення таємності своїх документів так називаний шифр «Pigpen». У ньому кожна буква замінялася визначеним символом таким чином: щоб зашифрувати букву, визна-

чалося її місцезнаходження в одній з чотирьох сіток, а потім малювалася та частина сітки, що відповідала цій букві.

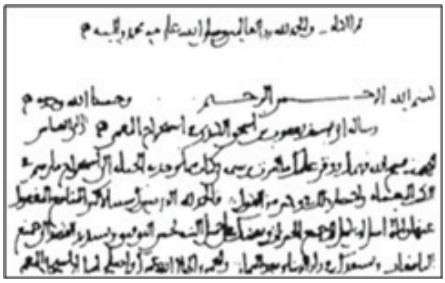


1.2. Становлення криптології як науки

В арабському світі криптологія не тільки не занепала, але продовжувала успішно розвиватися, досягши значних успіхів. Про тайнопис і його значення говорилося навіть у казках «Тисячі й однієї ночі». У 855 році арабський письменник, алхімік і єгиптолог Абу Бакр Ахмед ібн Вахш (Ахмад Бін Абубекр Бін Вахіші) описав відомі йому класичні шифралфавіти у своїй «Книзі про велике прагнення людини розгадати загадки давньої писемності» (араб. *Kitab Shawq al-Mustaham*). Видання арабського тексту з англійським перекладом з'явилося лише у 1806 році.

Це була одна з перших книг про криптографію з описами декількох шифрів, зокрема із застосуванням декількох алфавітів, де автор також обговорює деякі давні писемності та стверджує про дешифрування єгипетських ієрогліфів. Один із шифроалфавітів, що називався «дауді» (на ім'я ізраїльського царя Давида), використовувався для зашифрування трактатів з «чорної» магії. Він був складений з видозмінених букв давньоєврейського алфавіту.

Крім того, найбільш ранній із відомих описів методу використання частоти появи букв з метою «злому» шифрів належав перу арабського вченого Абу Юсуф Якуб ібн Ісхак ібн Сабах аль-Кінді (біля 800-879) та датований приблизно 850 роком. Відомий як «філософ арабського світу», аль-Кінді був автором 290 книг з медицини, астрономії, математики, лінгвістики й музики. Його найзнаменитіший трактат, що був виявлений заново лише у 1987 році в оттоманському архіві Сулайманія в Стамбулі, називався «Трактат про дешифрування криптографічних повідомлень аль-

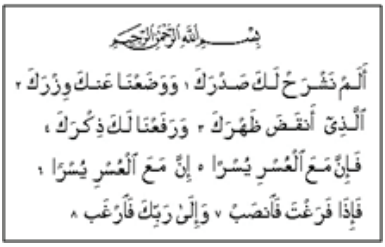


Кінді». Хоча в ньому був викладений докладний аналіз статистики, фонетики й синтаксису арабської мови, революційна система криптоаналізу аль-Кінді вміщається у два короткі абзаци:

«Один із способів прочитати зашифроване повідомлення, якщо ми знаємо мову, якою воно написано, – це взяти інший незашифрований текст на тій же мові, розміром приблизно на сторінку, і потім підрахувати появу в ньому кожної з букв. Назвемо букву, що найбільш часто зустрічається, «першою», букву, що за частотою появи знаходиться на другому місці, назвемо «другою», букву, що за частотою появи знаходиться на третьому місці, назвемо «третьою» і так далі, поки не будуть пораховані всі різні букви в незашифрованому тексті.

Потім подивимося на зашифрований текст, що ми хочемо прочитати, і таким же способом проведемо сортування його символів. Знайдемо символ, що найбільш часто зустрічається, і замінимо його «першою» буквою незашифрованого тексту, другий за частотою появи символ замінимо «другою» буквою, третій за частотою появи символ замінимо «третьою» буквою й так далі, поки не будуть замінені всі символи зашифрованого повідомлення, що ми хочемо дешифрувати».

Але по-справжньому характеризує пізнання арабів у сфері криптології енциклопедія з 14-ти томів «Шауба аль-Аша» (Світоч для незрячого в ремеслі писаря), що була написана вченим Шихабом ад-Дін Абу-л-Абас Ахмад ібн Алі ал-Калкашанді (1335-1418) у 1412 році. У розділі «Щодо приховання букв таємних повідомлень», автор виклав всі відомі йому на той час існуючі в арабському світі криптосистеми. Він містив дві частини: одна стосувалася символічних дій і натяків, а інша була присвячена симпатичному чорнилу та криптології.


بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ
أَلَمْ نَشْرَحْ لَكَ صَدْرَكَ ۝ وَوَضَعْنَا عَنكَ وِزْرَكَ ۝
ٱلَّذِىٓ أَنقَضَ ظَهْرَكَ ۝ وَرَفَعْنَا لَكَ ذِكْرَكَ ۝
فَإِنَّ مَعَ ٱلْعُسْرِ يُسْرًا ۝ إِنَّ مَعَ ٱلْعُسْرِ يُسْرًا ۝
فَإِذَا فَرَغْتَ فَٱنصَبْ ۝ وَإِلَىٰ رَبِّكَ فَٱرْغَب ۝

У роботі пропонувалося сім систем шифрування, що повторювали неопубліковані ідеї його попередника Ібн ад-Дурайхима (1312-1361), який був першим, хто використав частотний аналіз букв:

- замінювати одну букву іншою;
- писати слово у зворотному порядку;
- переставляти у зворотному порядку букви слів;
- замінювати букви на цифри згідно з прийнятою заміною арабських букв на числа;
- замінювати кожну букву відкритого тексту на дві арабські букви, які використовуються і як числа й сума яких дорівнює цифровій величині букви відкритого тексту, що шифрується;
- замінювати кожну букву на ім'я якої-небудь людини;

🗝 використовувати словник заміни, що описує положення Місяця, назви країн (у певному порядку), назв фруктів, дерев тощо.

Першого разу за всю історію шифрів в енциклопедії приводився список як систем перестановки, так і систем заміни. Більше того, у п'ятому пункті списку вперше згадувався шифр, для якого була характерна більш ніж одна заміна букв відкритого тексту. Однак яким би чудовим та важливим цей факт не був, він затьмарюється першим в історії описом криптоаналітичного дослідження шифротекста.

Його джерела, мабуть, варто шукати в інтенсивному й скрупульозному вивченні Корану численними школами арабських граматиків. Поряд з іншими дослідженнями вони займалися підрахунком частоти трапляння слів, намагаючись скласти хронологію глав Корана, вивчали фонетику слів, щоб установити, чи були вони справді арабськими або були запозичені з інших мов. Більшу роль у виявленні лінгвістичних закономірностей, що призвели до виникнення криптоаналізу в арабів, зіграв також розвиток лексикографії. Адже при складанні словників авторам фактично доводилося враховувати частоту трапляння букв, а також те, які букви можуть стояти поруч, а які ніколи не зустрічаються по сусідству.

Калкашанді писав у своїй книзі: «Якщо ви хочете прочитати повідомлення, що ви одержали в зашифрованому вигляді, то насамперед почніть підрахунок букв, а потім порахуйте, скільки разів повторюється кожен знак, і підбийте підсумок у кожному окремому випадку. Якщо винахідник шифру був дуже уважний та сховав у повідомленні всі границі між словами, то перша задача, що повинна бути вирішена, полягає в перебуванні знака, що розділяє слова. Це робиться так: ви берете букву та працюєте, виходячи з припущення, що наступна буква є знаком, що поділяє слова. І в такий спосіб ви вивчаєте все повідомлення з урахуванням різних комбінацій букв, з яких можуть бути складені слова... Якщо виходить, тоді усе в порядку; якщо ні, то ви берете наступну букву і т.д., поки ви не зможете установити знак розділу між словами. Потім потрібно знайти, які букви найчастіше трапляються у повідомленні, та порівняти їх зі зразком частоти трапляння букв, про яке згадувалося колись. Коли ви побачите, що одна буква трапляється частіше, ніж інші у даному повідомленні, ви припускаєте, що це буква «аліф». Потім ви припускаєте, що наступна за частотою трапляння буде буквою «лам». Точність вашого припущення повинна підтверджуватися тим фактом, що в більшості контекстів буква «лам» випливає за буквою «аліф»... Потім перші слова, що ви спробуєте розгадати у повідомленні, повинні складатися з двох букв. Це робиться шляхом оцінки найбільш ймовірних комбінацій букв доти, поки ви не переконаєтеся в тому, що ви знаходитеся на правильному шляху. Тоді ви дивитеся на їхні знаки і виписуєте їхні еквіваленти кожного разу, коли вони трапляються у повідомленні. Потрібно застосовувати точно такий же принцип стосовно трибуквених слів цього повідомлення, поки не переконаєтеся, що на щось натрапили. Ви виписуєте еквіваленти з усього повідомлення. Цей же принцип застосовується стосовно слів, що складають з чоти-

рьох і п'яти букв, причому метод роботи такий же. Коли виникає який-небудь сумнів, потрібно висловити два-три припущення або ще більше і виписати кожне з них, поки воно не підтвердиться на підставі іншого слова».

Давши це чітке пояснення, Калкашанді наводить приклад розкриття шифру. Дешифрована криптограма складається з двох віршованих рядків, зашифрованих за допомогою умовних символів. На закінчення Калкашанді відзначив, що вісім букв не було використано і що це саме ті букви, що знаходяться наприкінці переліку, складеного за частотою трапляння. Він підкреслив: «Однак це проста випадковість: буква може бути поставлена не на те місце, що вона повинна займати у вищезгаданому переліку». Таке зауваження свідчить про наявність великого досвіду в сфері криптоаналізу. Щоб розставити всі крапки над «і», Калкашанді приводить другий приклад криптоаналізу досить довгої криптограми. Цим прикладом він і закінчив розділ із криптології.

Араби першими звернули увагу на можливість використання стандартних слів і виразів для дешифрування. Так, перший широко відомий філолог серед арабів Халіль ібн Ахмад аль-Фарахіді (біля 718-791), дешифрувавши криптограму грецькою мовою, надіслану йому візантійським імператором, заявив: «Я сказав собі, що лист повинен починатися зі слів «В ім'я Бога» або як-небудь у цьому роді. Отже, я склав на основі цього перші букви, і все виявилося правильним». На основі відкритого ним методу дешифрування він написав книгу «Кітаб аль-маумма» (Книга таємної мови).

Історія замовчує те, як араби використали свої блискучі криптоаналітичні здібності, продемонстровані Калкашанді, для розкриття військових і дипломатичних криптограм, або який вплив це зробило на мусульманську історію. Однак зрозуміло, що незабаром ці знання перестали застосовуватися на практиці та були забуті. Один епізод, що відбувся майже 200 років по тому, яскраво демонструє ту деградацію у сфері криптоаналізу, що відбулася за той час.

У 1600 році мароканський султан Ахмед аль-Мансур направив до англійської королеви Єлизавети I посольство на чолі з довіреною людиною – міністром Абдель Вахід ібн Масуд ібн Мухамед Ануном. Посольство повинне було укласти з Англією союз, спрямований проти Іспанії. Анун відправив на батьківщину зашифровану простою заміною депешу, яка незабаром після цього якимось чином потрапила в руки одного араба. Араб той був, можливо, розумною людиною, але, на жаль, він нічого не знав про велику арабську спадщину у сфері криптоаналізу. Свідчення тому – пам'ятна записка, у якій він написав:

«Хвала Аллаху! Щодо листа міністра Абдель Вахід ібн Масуд ібн Мухамед Ануна. Я знайшов лист, написаний його рукою, у якому він за допомогою таємних знаків виклав деякі відомості, призначені для нашого заступника Ахмеда аль-мансура. Ці відомості стосуються султанші християн (хай покарає їх Аллах!), що жила в країні за назвою Лондон... З того моменту, як цей лист потрапив до

мене, я постійно час від часу вивчав знаки, що містилися в ньому. Пройшло приблизно 15 років, поки не настав той час, коли Аллах дозволив мені зрозуміти ці знаки, хоча ніхто не навчав мене цьому...».

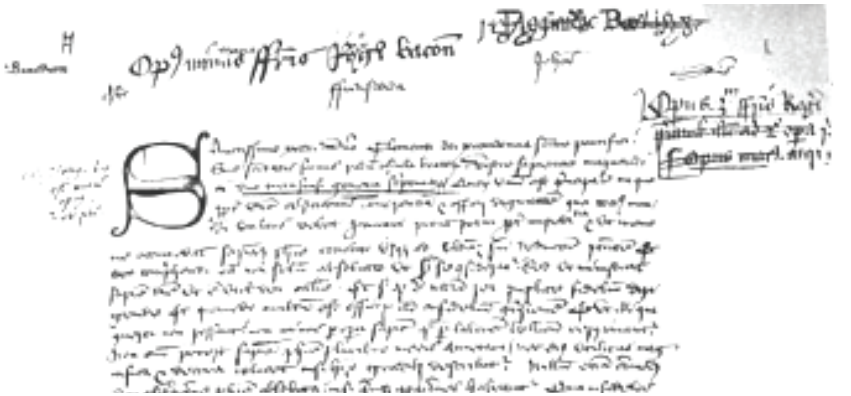
П'ятнадцять років! Подібне завдання Калкашанді вирішив би за кілька годин.

Невідомо, чи був тісний зв'язок між розвитком європейської та східної криптології. Безумовно подібного роду контакти могли відбуватися в Іспанії й під час Хрестових походів, але стверджувати, що європейська криптологія в той час використала арабський досвід, не можна. Праці Калкашанді не були перекладені з арабської мови, тому прямого зв'язку європейської криптології зі східною немає. Крім того, якщо на сході криптологія була скоріше частиною лінгвістики, то в Європі вона була ближче до математики й природничих наук, що також визначило її специфіку .

Європейська цивілізація почала користуватися криптологією з часів середньовічного феодалізму. Правда, спочатку тайнопис знаходився в зародковому стані, його застосовували рідко і мінливо. Навіть, церковні системи шифрування були простими, хоча в ту епоху церква користувалася найбільшим впливом у суспільстві. Цікаво, що в той час, коли прості люди шифрування вважали чаклунством, основні роботи в сфері криптології виконувалися в лоні католицької церкви.

У X столітті чернець Герберт Орильякський (Аврилакський), що правив католицькою церквою під ім'ям папи Сильвестра II (біля 946-1003) і вивчав «магічні» знання, вів записи за стенографічною системою, створеною Марком Туллієм Тіроном (103-4 до н.е.), вільновідпущеним і другом відомого Цицерона.

У 1267 році англійський монах-францисканець, професор в Оксфорді, універсальний вчений, математик, оптик, астроном Роджер Бекон (1214-1294) написав першу європейську книгу, яка була присвячена криптології та називалася «Послання ченця Роджера Бекона про таємні дії мистецтва і природи та нікчемність магії» (лат. *Epistola fratris Rogerii Baconis de secretis operibus artis et naturae, et de nullitate magiae*). У передмові він помітив: «Дурень той, хто пише про таєм-



ницю яким-небудь способом, але не так, щоб приховати її від простолюду».

У розділі «Сім способів захована таємниці» Бекон привів такі методи шифрування: повна заміна символів і знаків, використання загадкових і образних виразів, особливі способи запису, одночасне використання букв різних мов, застосування різних малюнків, скорочення голосних букв тощо. За свої наукові праці він був засуджений за «чорну магію» церковним судом і провів 14 років в ув'язненні.

У 1379 році антипапа Климент VII, який за рік до цього втік до французького Авіньону, звелів своїй канцелярії ввести в дію нові шифри. Секретар антипапи Габріель де Лавінда, що працював у його представництві в одному з північноіталійських міст-держав, виготовив індивідуальні ключі для всіх 24 кореспондентів антипапи. Ключі де Лавінда, що були найдавніші серед збережених на Заході, поєднували у собі елементи коду й шифру.

У своїй книзі «Трактат про шифри» Габріель де Лавінда описав новий тип шифру, що використовував «омофони», тобто припускав заміну букв декількома символами (знаками), кількість яких пропорційна трапляння букв у відкритому тексті. Імена, посади, географічні назви він рекомендував заміняти спеціальними знаками. Крім шифроалфавіту заміни з «пустишками» майже кожен такий ключ включав невеликий список з десятка широко розповсюджених слів або імен, яким приводилися у відповідність двобуквені кодові еквіваленти. Це самий ранній зразок «Номенклатора» – гібридної системи шифрування, який у наступні 450 років поширився по всій Європі.

Розвитку європейської криптології сприяло те, що середньовічні вчені, зробивши відкриття, аж ніяк не поспішали описати його в листах колегам, як це було тоді прийняте за відсутності періодичних наукових видань. Нерідко ту частину відкриття, що тепер називають «know how», вони шифрували анаграмою, переставляючи букви повідомлення за відомим тільки їм ключем. Наприклад, назви древньої та сучасної столиць Японії в російському написанні теж являють собою анаграму: КІОТО – ТОКІО.

Пояснюючи широке поширення тайнопису серед вчених середньовіччя, О.І.Герцен писав: «Гнані, блукачі із країни в країну, оточені небезпеками, вони не зарили з розсудливого страху істини, про яку були покликані свідчити; вони висловлювали її скрізь, де не могли висловлювати прямо – одягали її в маскарадне плаття, наділяючи алегоріями. Ховали під умовними знаками, прикривали тонким флером, що для когось проникливого нічого не приховував, але приховував від ворога: любов догадливіша й проникливіша ненависті. Іноді вони це робили, щоб не злякати боязкі душі сучасників; іноді – щоб не потрапити на багаття».

Найбільшого розквіту криптологія досягла в період Епохи Відродження. Творчі періоди життя таких великих людей, як Леонардо да Вінчі, кардинала Рішельє, Людовиків XII-XIV й інших дали поштовх до зародження наукового підходу до проблем

тайнопису. Саме в ці роки виникло поняття «кодування» повідомлень, тобто заміни букв і цифр відкритого тексту на букви, цифри, знаки, згідно із заздалегідь обумовленим правилом, законом.

Леонардо да Вінчі (1452-1519) також шифрував більшість своїх особистих записів. Найпростіший вид шифру, яким він користувався, це зворотнє (дзеркальне) написання тексту так, що прочитати його можна було лише у відбитті дзеркала, наприклад: слово «*UKRAINE*» перетворюється у шифротекст «*ENIARKU*». Однак Леонардо іноді використовував й більш серйозні шифри, тому далеко не всі його замітки та записи розшифровані й вивчені до цього часу. Невипадково вийшли в світ книга та фільм з назвою «Код да Вінчі».

Одним із провідних європейських криптологів був відомий англійський письменник, астроном-аматор, митний чиновник Джеффрі Чосер (1343-1400). В 1370-х роках він виконував секретні дипломатичні доручення свого короля в Італії й Франції. Все таємне листування Чосер здійснював, використовуючи шифр простої заміни. Його книга «Екватор Планет», що вийшла у 1390 році, містила окремі шифровані глави.

У 1401 році в Мантуанському герцогстві був знайдений шифр із використанням «омофонів» для голосних букв. Той факт, що «омофони» застосовувалися не для всіх букв, а тільки для голосних, свідчив про знання криптоаналітичних методів, заснованих на частоті трапляння знаків шифротекста.

Широкий розвиток торгівлі в середині століття спровокував появу специфічних шифрів, дуже простих і зручних, якими могли б користуватися купці для передачі, наприклад, дати приїзду або ціни товару. Це були прості шифри заміни цифр на букви, засновані на ключовому слові. Торговці заздалегідь домовлялися про використання загального ключового слова, букви якого відповідали б цифрам.

Наприклад, для ключа «ШИФРОВАНИЙ» цифра 0 означає букву «Ш», цифра 1 означає «И», 2 – «Ф», 3 – «Р» тощо. Тому одержавши від кореспондента повідомлення «ПРИБУВАЮ ИФШАЙР», вони його читали як «ПРИБУВАЮ 12/06/93». Простота та зручність цієї системи шифрування дозволили їй дожити до початку минулого століття без усяких змін. Крім цих шифрів, найчастіше використовувався шифр простої заміни, що полягав у заміні кожної букви повідомлення на відповідну їй букву шифру.

У ручних шифрах того часу часто використовувалися таблиці, які давали прості шифри перестановки. Ключем у них служив розмір таблиці та фраза, що задавала перестановку або спеціальну особливість таблиць. Проста перестановка без ключа – один із найпростіших методів шифрування, родинний шифру «скитала».

Наприклад, повідомлення «ЗУСТРІЧАЙ У ДЕСЯТЬ» записувалося в таблицю по стовпцях. Для таблиці розміром 4х4 це виглядало таким чином:

З	Р	Й	С
У	І	У	Я
С	Ч	Д	Т
Т	А	Е	Ь

Після того, як відкритий текст був записаний по стовпцях, для утворення шифровки він зчитувався по рядках. В результаті виходив шифротекст: «ЗРЙСУІУЯСЧДТТАЕЬ». Для використання цього шифру відправнику та одержувачу потрібно було домовитися про загальний ключ у вигляді розміру таблиці. Об'єднання букв у групи не входило у ключ шифру та використовувалося лише для зручності запису тексту.

Більш практичним був метод шифрування, який був названий одиночною перестановкою за ключем. Він відрізнявся від попереднього лише тим, що стовпці таблиці переставлялися за ключовим словом, фразою або набором чисел довжиною в рядок таблиці. Ключове слово (наприклад, «ШИФР») вписувалося у перший рядок таблиці, та здійснювалася перестановка стовпців відповідно до порядкових номерів букв ключа:

Ш	И	Ф	Р
4	1	3	2
З	Р	Й	С
У	І	У	Я
С	Ч	Д	Т
Т	А	Е	Ь

→

1	2	3	4
Р	С	Й	З
І	Я	У	У
Ч	Т	Д	С
А	Ь	Е	Т

В результаті зчитування по рядках повідомлення «ЗУСТРІЧАЙ У ДЕСЯТЬ» перетворялося у шифротекст «РСЙЗІЯУУЧТДСАЬЕТ».

Крім одиночних перестановок використовувалися ще подвійні перестановки стовпців і рядків таблиці з повідомленням згідно з попередньо визначеним порядком нумерування рядків і стовпців таблиці, що й було ключем шифру. При цьому перестановки визначалися окремо для стовпців та окремо для рядків. У таблицю вписувався текст по стовпцях, після чого здійснювалися перестановки стовпців та рядків:

	3	2	4	1
2	З	Р	Й	С
1	У	І	У	Я
4	С	Ч	Д	Т
3	Т	А	Е	Ь

→

	1	2	3	4
2	С	Р	З	Й
1	Я	І	У	У
4	Т	Ч	С	Д
3	Ь	А	Т	Е

→

	1	2	3	4
1	Я	І	У	У
2	С	Р	З	Й
3	Ь	А	Т	Е
4	Т	Ч	С	Д

В результаті кінцевого зчитування по рядках повідомлення «ЗУСТРІЧАЙ У

ДЕСЯТЬ» перетворялося у шифротекст «ЯІУУСРЗЙЬАТЕТЧСД». При розшифруванні порядок перестановок був зворотнім. Однак навіть шифри подвійної перестановкт були слабким видом шифру, тому що легко читалися при будь-якому розмірі таблиці шифрування.

Новий етап розвитку криптології розпочався у другій половині XV століття з введенням у практику криптології багатоалфавітних шифрів заміни. Батьком цього шифру виявився теоретик мистецтва Леон Батіста Альберті (1404-1472), який узагальнив досвід гуманістичної науки у вивченні античної спадщини, написав трактати «Про статую», «Про живопис», «Про зодчество», десять книг про зодчество, побудував палац Ручеллаї, церкву Іль Джезу та ряд інших чудових здобутків зодчества середньовічної Італії.

У 1466 році Альберті надав до папської канцелярії також і трактат про шифри, де здійснив аналіз частот букв, дослідив шифри заміни та перестановки, торкнувся питань стійкості шифрів. Підмічена Альберті різночастотність появи букв в осмислених текстах дала поштовх вивченню синтаксичних властивостей письмових повідомлень. При цьому основна увага приділялась буквам, що частіше зустрічались у тексті.

Альберті вперше висунув ідею «подвійного» шифрування – текст, отриманий в результаті першого шифрування, піддавався повторному зашифруванню. Він запропонував використовувати два або більше шифроалфавітів, переходячи від одного до іншого в процесі зашифровування й заплутуючи цим можливих криптоаналітиків.

Текст	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
Шифр 1	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C
Шифр 2	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T

Тут, наприклад, є два можливі шифроалфавіти, і ми можемо зашифрувати повідомлення, використовуючи по черзі то один, то інший. Таким чином, щоб зашифрувати слово «*UKRAINE*», зашифруємо першу букву за допомогою першого шифроалфавіту, так що «U» перетвориться в «*Z*», другу ж букву ми зашифруємо, використовуючи другий шифроалфавіт, при цьому «*K*» стане «*E*». Для зашифровування третьої букви ми повернемося знову до першого шифроалфавіту (*R* → *U*), а щоб зашифрувати четверту букву, ми знову звернемося до другого шифроалфавіту (*A* → *U*) і так далі: *I* → *M, N* → *H, E* → *H*. В результаті отримаємо такий шифротекст: «*ZEUUMHH*».

Основна перевага системи Альберті полягала в тому, що однакові букви у відкритому тексті не обов'язково залишалися однаковими у шифротексті. Точно так повторювані букви у шифротексті були різними буквами відкритого тексту.

В своїй книзі Альберті запропонував також свій власний шифр із нескромною назвою «шифр, гідний королів», який зробив шифровку дуже стійкою до «злому». Реалізація шифру забезпечувалась за допомогою механічного шифрувального диску, що було також одним з найважливіших винаходів Альберті.

Шифрувальний диск складався з великого зовнішнього диска та рухомого внутрішнього диска. Окружність зовнішнього диска була розділена на 24 рівні сектори, до яких були вписано 20 букв латинського алфавіту в їхньому природному порядку та 4 цифри. При цьому з алфавіту були вилучено 6 букв, без яких можна було обійтися – *H, J, K, U, Y, W*. Окружність внутрішнього диска була розділена також на 24 сектори, до яких були вписані букви змішаного латинського алфавіту.

Маючи два такі прилади, кореспонденти домовлялися про першу індексну букву на рухомому диску. При шифруванні повідомлення відправник ставив індексну букву проти будь-якої букви великого диска. Він інформував кореспондента про таке положення диска, записуючи цю букву зовнішнього диска як першу букву шифротекста. Чергова буква відкритого тексту відшукувалася на нерухомому диску, і буква меншого диска, що стояла проти неї, була результатом її шифрування. Після того, як були зашифровані декілька букв тексту, положення індексної букви змінювалося, про що також повідомлялося кореспонденту.

A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
L	G	A	Z	E	N	B	O	S	F	C	H	T	Y	Q	I	X	K	V	P	ET	M	R	D

Так, наприклад, для індексної букви «*L*» одним з багатьох варіантів шифрування слова «*PRESIDENT*» може бути «*ATQEIOZECX*», а іншим – «*BHYZQBAZFI*» тощо.

B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4	A
L	G	A	Z	E	N	B	O	S	F	C	H	T	Y	Q	I	X	K	V	P	ET	M	R	D

Такий шифр мав дві особливості, що робили винахід Альберті важливою подією в історії криптології. По-перше, на відміну від шифрів простої заміни шифродиск використовував не один, а декілька алфавітів для зашифрування. Такі шифри одержали назву багатоалфавітних. По-друге, шифродиск дозволяв використовувати так звані коди з перешифруванням, що одержали широке поширення лише наприкінці XIX століття, тобто через чотири століття після винаходу Альберті.

Для цієї мети на зовнішньому диску малися цифри. Альберті склав код, що складався з 336 кодових груп, занумерованих від 11 до 4444. Кожному кодовому

позначенню відповідала деяка закінчена фраза. Коли така фраза траплялася у відкритому повідомленні, вона замінялася відповідним кодовим позначенням, а за допомогою диска цифри зашифровувалися як звичайні знаки відкритого тексту, перетворюючись у букви.

У 1474 році був написаний перший у світі трактат, присвячений винятково криптоаналізу. Це зробив Чико Сімонетті, один із секретарів правителів Мілана – герцогів Сфорца. У ньому він виклав удосконалені шифри заміни, у тому числі шифр багатозначної заміни, у якому одній букві (голосній) відповідало декілька шифропозначень. Він розробив 13 правил розкриття шифрів простої заміни, у яких збережені роздільники слів. Рукопис, написаний на трьох шматках пергаменту, починався зі слів: «Перша необхідна умова полягає в з'ясуванні того, чи написаний документ латинською або місцевою мовою, а це можна установити в такий спосіб: з'ясуєте, чи мають слова в даному документі тільки п'ять різних закінчень, менше або більше. Якщо їх тільки п'ять або менше, ви праві, вважаючи, що документ написаний місцевою мовою...».

Сімонетті у своєму трактаті докладно описав шифри заміни, у яких для вирівнювання частоти трапляння букв у шифротексті голосним буквам ставився у відповідність не один знак, а декілька. Тут же вперше був наведений опис так званого «гаслового» шифру, що у різних модифікаціях буде застосовуватися й кілька століть пізніше. Правило заміни букв у ньому визначалося таким чином: під алфавітом писалася ключова фраза – гасло (наприклад, «Ukraine») без повторюваних букв, а потім букви, що у гаслі не зустрічалися, у природному порядку.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	K	R	A	I	N	E	B	C	D	F	G	H	J	L	M	O	P	Q	S	T	V	W	X	Y	Z

В результаті слово «*UZHGOROD*» перетворюється у шифротекст: «*TZBELPLA*».

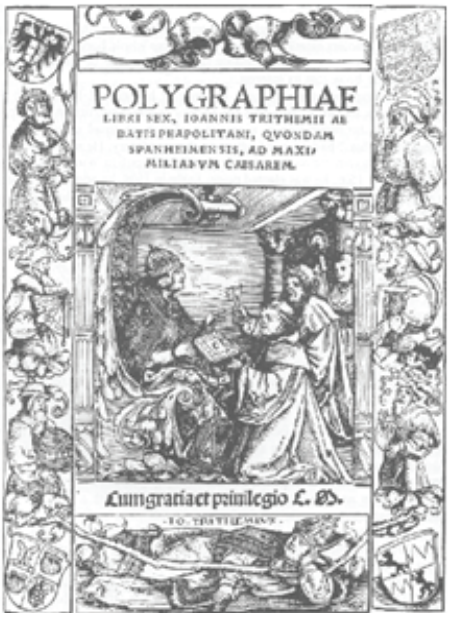
У 1518 році з'явилася перша друкована праця з криптології «Поліграфія» (лат. *Polygraphia*). Вона була написана Йоганом Гейденбергом (1462-1516), або Тритемієм (Трисемусом), абатом бенедиктинського монастиря Святого Мартіна (м. Вюрцбург, Німеччина), якого багато істориків вважають батьком європейської криптології. «Поліграфія» являла собою збірник з 6 книг і містила стовпці латинських термінів, слів, поставлених у відповідність буквам відкритого тексту, та першу квадратну таблицю, основу багатоалфавітної заміни.

Хоча у праці Тритемія було описано багато шифрів – як існуючих у той час, так і винайдених самим автором, вона була пронизана кабалістичними й окультними алюзіями.

В результаті книга викликала гнів багатьох монархових дворів Європи, які думали, що Тритемій видав у ній занадто багато таємниць. Крім того, Римська католицька церква вважала праці Тритемія єретичними та у 1609 році внесла

його книги до списку заборонених. Ця заборона тривала 250 років.

У 1541 році книга була перевидана французькою мовою, а незабаром був зроблений її переклад на німецьку мову. У цій книзі Тритемій зробив дві нові пропозиції в криптології: він запропонував шифр «Аве Марія» і шифр, побудований на основі ключа, що періодично зрушується.



Шифр «Аве Марія» ґрунтувався на принципі заміни заздалегідь обговорених слів на букви шифротексту. З таких слів складалося зовні «безневинне» повідомлення. Наприклад, замінимо букви «А», «К», «Т» на такі слова: «А» – чекаю, мій; «К» – вдома, ключ; «Т» – я, тут. У такому разі позитивна таємна відповідь на задане питання може мати декілька варіантів: «Я чекаю вдома» або «Тут мій ключ».

Другим більш серйозним шифром була «таблиця Тритемія» – квадратна таблиця розміром 24х24 з багатьма алфавітами, яка була названа «*tabula recta*». Алфавіти були записані в рядки таблиці один під іншим, причому кожний з них був зрушений на одну позицію вліво в порівнянні з попереднім.

Тритемій пропонував використовувати цю таблицю для багатоалфавітного шифрування найпростішим з можливих способів: перша буква тексту шифрувалася першим алфавітом, друга буква – другим тощо. У цій таблиці не було окремого алфавіту відкритого тексту, для цієї мети служив алфавіт першого рядка. Таким чином, слово «*UKRAINE*» перетворювалося у шифротекст «*ULTDNSL*».

Перевага цього методу шифрування в порівнянні з методом Альберті полягала в тому, що кожна чергова буква текста шифрувалася новим алфавітом. Альберті змінював алфавіти лише після трьох або чотирьох слів. Тому його шифротекст складався з відрізків, кожний з яких мав закономірності відкритого тексту, що допомагали розкрити криптограму. Побуквене шифрування не давало такої переваги.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B

D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C
E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D
F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E
G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F
H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G
I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H
K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K
M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L
N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M
O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N
P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

Крім того, Тритемій пропонував також використовувати одноалфавітне шифрування за допомогою квадрата Полібія та ключового слова - пароля. Обиралося яке-небудь слово, з нього прибиралися повторювані букви, а ті, що залишалися, записувалися в перші клітини квадрата. Порожні клітини заповнювалися буквами алфавіту, що залишилися, у природному порядку.

Розглянемо цю систему шифрування у варіанті для української мови, таблиця якої буде мати розмір не 5х5, а 5х6. Буква шифровки бралася з клітини, що знаходилася під клітиною букви повідомлення. Оскільки ключове слово легко було зберігати в пам'яті, то такий підхід спрощував процеси шифрування та дешифрування. Для ключа «ШИФРОВКА» таблиця буде мати такий вигляд:

Ш	И	Ф	Р	О	В
К	А	Б	Г	Д	Е
Є	Ж	З	І	Л	М
Н	П	С	Т	У	Х

Ц	Ч	Щ	Ю	Я	Ь

Для вищеописаного шифру за даною таблицею повідомлення «УХОДИМО» дає шифровку «ЯЬДЛАХД». Такі табличні шифри були названі монограмними, тому що шифрування велося по одній букві.

Тритемій також першим помітив, що можна шифрувати одночасно по дві букви, які стояли разом та були названі «біграмою». Такий шифр був названий «біграмним». Опишемо його на прикладі тієї ж таблиці. Відкритий текст розбивався на біграми, а текст шифровки виходив з нього згідно з двома такими правилами:

1. Якщо обидві букви біграми вихідного тексту належали до одного стовпця таблиці, то буквами шифру вважалися букви, які були під ними. Так, біграма «РІ» давала текст шифровки «ГТ». Якщо буква відкритого тексту перебувала в нижньому рядку, то для шифру бралася відповідна буква з верхнього рядка: біграма «ЛЯ» давала шифр «УО» (біграма з однієї букви або пари однакових букв теж підкорялася цьому правилу).

2. Якщо обидві букви біграми вихідного тексту належали одному рядку таблиці, то буквами шифру вважалися букви, які лежали праворуч від них. Так, біграма «АД» давала текст шифровки «БЕ». Якщо буква відкритого тексту була в правому стовпці, то для шифру бралася відповідна буква з лівого стовпця: біграма «ІМ» давала шифр «ЛЄ».

3. Якщо обидві букви біграми відкритого тексту лежали в різних рядках і стовпцях, то замість них бралися дві букви таким чином, щоб вся їх четвірка складала прямокутник. При цьому послідовність букв у шифрі була віддзеркаленням вихідної пари. Наприклад, «АУ» шифрувалося як «ДП», а «ТБ» – як «СГ».

При шифруванні фрази «ОГОЛОШЕНИЙ ЗБІР» по біграмах виходить шифрування «РДДУВИКХААСЗТГ»:

ОГ	ОЛ	ОШ	ЕН	ИИ	ЗБ	ІР
РД	ДУ	ВИ	КХ	АА	СЗ	ТГ

Шифрування біграмами різко підсилило стійкість шифрів до розкриття.

При всьому тому, що «Поліграфія» була досить доступною друкованою книгою, описані в ній ідеї одержали визнання лише трьома століттями пізніше. Скоріше за все це було викликано непопулярністю Тритемія серед професійних криптологів, який був не криптологом, а богословом, бібліофілом і засновником архівної справи.

Наступний крок у розвитку запропонованого Тритеміем способа шифрування був зроблений італійцем Джовані Батіста Белазо. У 1553 році він опублікував

брошуру «Шифр сеньйора Джовані Батіста Белазо» (італ. *La cifra del. Sig. Giovan Batista Belaso*), де запропонував використовувати для багатоалфавітного шифру буквений ключ, що був названий ним «паролем» та повинен був легко запам'ятовуватися. Пароль виписувався під або над рядком повідомлення. Буква пароля, що знаходилися над (під) буквою повідомлення, визначала номер рядка таблиці Тритемія, тобто алфавіт заміни, згідно з яким і здійснювалося шифрування. Буква повідомлення визначала номер стовпця таблиці, а буква шифротекста знаходилась на перетинанні рядка та стовпця таблиці.

ALL'ECCELLEN. ET
honoratiſs. Sig. il S. Giro-
lamo Ruſcelli,

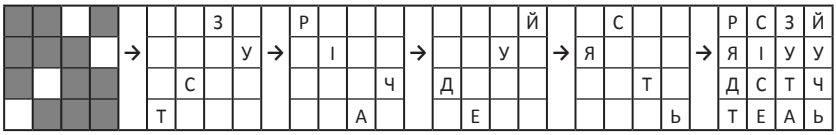
GIOVAN BATTISTA BELLASO.

Приблизно в той же час італійський математик і філософ Джироламо Кардано (1501-1576) запропонував використовувати як ключ сам текст повідомлення, тобто «самоключ» або «автоключ» (autokey). Наприклад, у фразі «ЗБІР СЬОГОДНІ» ключем було слово «ЗБІР»:

Текст	З	Б	І	Р	С	Ь	О	Г	О	Д	Н	І
Ключ	З	Б	І	Р	З	Б	І	Р	З	Б	І	Р

Шифрування здійснювалось за допомогою таблиці Тритемія.

Крім того, у 1556 році захоплення теорією магічних квадратів привело Кардано до відкриття нового класу шифру перестановок, названого ґратами або трафаретом. Вони являли собою квадратні таблиці, де чверть осередків прорізана так, що при чотирьох поворотах вони покривали весь квадрат. Вписування в прорізані осередки тексту й повороти ґрат тривали доти, поки весь квадрат не був заповнений. Наприклад, на малюнку нижче показаний процес шифрування ґратами 4х4. Трафарет мав 4 прорізані клітини, а повороти здійснювалися за годинною стрілкою на зазначений нижче кут:



У результаті зчитування по рядках повідомлення «ЗУСТРІЧАЙ У ДЕСЯТЬ» перетворюється у шифротекст «РСЗЙЯІУУДСТЧТЕАЬ».

Головна вимога до ґрат – при усіх поворотах «вікна» не повинні попадати на

одне й те місце у квадраті, у якому утвориться шифротекст. Якщо у квадраті після зняття грат утворювалися пусті місця, то в них вписувалися будь-які букви.

Кількість подібних ґрат швидко росте з їхнім розміром. Так, ґрати 2х2 єдині, ґрат 4х4 уже 256, а ґрат 6х6 понад сто тисяч. Незважаючи на певну складність, шифри типу ґрат досить просто розкривалися, тому не могли використовуватися як самостійний шифр. Однак вони були дуже зручними та ще довго використовувалися в практиці для посилення шифрів заміни.

Воскресити змішані алфавіти, що застосовував Альберті, та об'єднати ідеї Альберті з ідеями Тритемія і Белазо в сучасну концепцію багатоалфавітної заміни випало на долю італійця Джовані Батіста дела Порта (1535-1615). Йому було 28 років, коли він у 1563 році опублікував книгу «Про приховану значущість окремих букв» (лат. *De Furtivis Literarum Notis*). Її перші два розділи були присвячені криптографії, а в інших двох викладалися основи криптоаналізу та розглядалися лінгвістичні особливості, що допомагали розкриттю шифрів.

Книга Порти містила перший в Європі опис того, як варто розкривати шифр простої заміни, коли шифротекст не був розділений на слова або був розділений неправильно. Порта також описав те, що вважалося другим за значимістю прийомом у сучасному криптоаналізі:

«...Коли тема листування відома, дослідник може зробити проникливі припущення щодо слів, що звичайно вживаються в такому контексті. Ці слова можна без великої праці знайти, помічаючи в текстах кількість знаків, а також подібність і розходження букв... Для кожної теми характерні деякі загальні слова, що супроводжують її, будучи необхідними. Наприклад, у любові – це «пристрасть», «серце», «вогонь», «полум'я», «згоряти», «життя», «смерть», «жалість», «жорстокість»; на війні – «солдат», «командир», «генерал», «табір», «зброя», «боротися» і т.д. Таким чином, цей прийом розкриття, що не заснований на аналізі самих документів або на спробі розбити текст на голосні або приголосні, може полегшити задачу».

У своїй книзі Порта також дав одну мудру пораду, що й сьогодні корисна криптоаналітику такою ж мірою, якою вона була доречна в Італії епохи Відродження:

«Необхідні повна зосередженість і ретельність, щоб вільна від сторонніх думок голова, коли все інше відкладено убік, була цілком зайнята єдиною задачею доведення

початої справи до успішного завершення. І все-таки, коли така задача вимагає надмірного напруження і незвичайних витрат часу, напруження не повинно бути безперервним, не слід навантажувати мозок надмірно, тому що занадто великі зусилля і тривале розумове навантаження призводять до нервового виснаження, після якого голова вже менш придатна для подібних речей та з неї вже не вичавиш нічого...»

А далі Порта поділився з читачем своїм власним практичним досвідом роботи: «Крім того, дуже важливо, щоб повідомлення було написано рукою автора або митецького переписувача, тому що якщо перехоплене повідомлення буде скопійовано неправильно або якщо воно вийде з-під руки людини, незнайомого з мистецтвом шифру, то в результаті, оскільки правопис порушений, будь-яка інтерпретація повідомлення буде блокована».

Подібний досвід приходив тільки до криптоаналітика, що мав справу з повідомленнями, у яких букви часто були пропущені, переставлені або замінені на інші. Це траплялося лише при обробці дійсних криптограм. Завдання, що зустрічалися в книгах з криптоаналізу того часу, завжди були бездоганно складені з точки зору правопису й тому легко вирішувалися. Скоріше за все, Порта регулярно займався криптоаналізом, виконуючи доручення папської курії.

Повною мірою чудові здібності Порти проявилися при рішенні найбільш важкої проблеми криптоаналізу епохи Відродження – розкритті багатоалфавітних шифрів. Незважаючи на високу оцінку цих шифрів криптоаналітиками того часу, Порта відмовився визнати їхню невразливість і розробив для них методи розкриття. Хоча ці методи не були універсальними, їхня основна цінність складалася в застосованому Портою сміливому підході, що й привів його до успіху.

Для початку Порта спробував прочитати шифротекст, який його сучасниками був зашифрований за допомогою спеціального приладу. Цей прилад складався з двох дисків: внутрішнього нерухомого диска, на який за годинною стрілкою був нанесений алфавіт відкритого тексту, і зовнішнього рухливого диска з низкою вигадливих шифрознаків. Зовнішній диск після зашифрування чергової букви повертався за годинною стрілкою на один крок. Порта помітив, що якщо в якому-небудь слові відкритого тексту три букви підряд стояли в алфавітній послідовності, той самий шифрознак 3-разово повторювався у шифротексті. Це допомогло йому прочи-

тати криптограму.

Потім Порта модифікував розроблений ним метод, щоб дешифрувати іншу багатоалфавітну криптограму, яка була складена згідно з принципом Джовані Белазо. На думку Порти, у криптограмі 3-кратне повторення букви шифротекста сигналізувало про те, що ключем із трьох букв, розташованих в звичайному алфавітному порядку, був зашифрований відкритий текст, у якому було три букви в порядку, протилежному алфавітному. Міркуючи з цього приводу, Порта впритул підійшов до універсального методу розкриття багатоалфавітних шифрів, знайти який він так прагнув:

«Оскільки... між першими трьома «M» і цими ж трьома буквами, повтореними в 13-му слові, знаходиться 51 буква, я дійду висновку, що ключ повторений три рази, і правильно вважаю, що він містить 17 букв».

Однак Порта так і не скористувався своїм спостереженням. У результаті багатоалфавітний шифр продовжував вважатися надійним протягом трьох наступних століть.

У своїй книзі Порта ввів свою таблицю багатоалфавітного шифрування:

A	A	B	C	D	E	F	G	H	I	K	L	M
B	N	O	P	Q	R	S	T	U	W	X	Y	Z
C	A	B	C	D	E	F	G	H	I	K	L	M
D	O	P	Q	R	S	T	U	W	X	Y	Z	N
E	A	B	C	D	E	F	G	H	I	K	L	M
F	P	Q	R	S	T	U	W	X	Y	Z	N	O
G	A	B	C	D	E	F	G	H	I	K	L	M
H	Q	R	S	T	U	W	X	Y	Z	N	O	P
I	A	B	C	D	E	F	G	H	I	K	L	M
K	R	S	T	U	W	X	Y	Z	N	O	P	Q
L	A	B	C	D	E	F	G	H	I	K	L	M
M	S	T	U	W	X	Y	Z	N	O	P	Q	R
N	A	B	C	D	E	F	G	H	I	K	L	M
O	T	U	W	X	Y	Z	N	O	P	Q	R	S
P	A	B	C	D	E	F	G	H	I	K	L	M
Q	U	W	X	Y	Z	N	O	P	Q	R	S	T
R	A	B	C	D	E	F	G	H	I	K	L	M
S	W	X	Y	Z	N	O	P	Q	R	S	T	U
T	A	B	C	D	E	F	G	H	I	K	L	M
U	X	Y	Z	N	O	P	Q	R	S	T	U	W
W	A	B	C	D	E	F	G	H	I	K	L	M

X	Y	Z	N	O	P	Q	R	S	T	U	W	X
Y	A	B	C	D	E	F	G	H	I	K	L	M
Z	Z	N	O	P	Q	R	S	T	U	W	X	Y

Шифрування повідомлення здійснювалося за допомогою секретного гасла-пароля, що періодично виписувався над відкритим текстом. Буква гасла визначала алфавіт (заголовні букви першого стовпця), розташована під ключем буква відкритого тексту шукалася у верхньому або нижньому напівалфавіті та замінялася відповідною їй буквою другого напівалфавіту.

Наприклад, якщо як гасло використати слово «UKRAINE», то шифрування слова «UZHGOROD» буде виглядати таким чином:

Гасло	U	K	R	A	I	N	E	U
Відкритий текст	U	Z	H	G	O	R	O	D
Шифротекст	L	H	Q	T	K	L	M	N

За цей шифр Порту пізніше назвали батьком сучасної криптографії, але у той час цей шифр не знайшов широкого застосування. Причиною цього була необхідність постійно мати при собі вказану таблицю та складність процесу шифрування. Разом з тим, був даний імпульс для появи інших шифрувальних систем (наприклад, Віженера).

Також Порта запропонував шифр простої біграмної заміни з використанням квадратної таблиці зі змішаним алфавітом і паролем. У ньому пари букв (біграми) позначалися одним спеціальними графічними символами. Наприклад, біграма «EA» замінялася грецьким символом «Δ», біграма «LF» – символом «Ψ» тощо.

TRAICTE
DES CHIFFRES,
OV SECRETES
MANIERES
D'ESCRIRE
PAR
BLAISE DE VIGENERE,
BOVRBONNOIS.
A PARIS,

Вони заповнювали квадратну таблицю розміром 20x20, рядки й стовпці якої були занумеровані буквами латинського алфавіту. По суті справи це був той же шифр простої заміни, але на рівні двобуквених сполучень. Криптостійкість при такій заміні порівняно до побуквеного шифрування значно підвищувалась.

Французький посол у Римі Блез де Віженер (1523-1596), ознайомившись з криптологічними працями та ідеями Цезаря, Альберті, Тритемія, Белазо й Порта, захопився криптологією. У 1585 році він на-

писав книгу «Трактат про шифри» (фр. *Traité des chiffres*), де виклав основи криптології. В ній він висловив думку про те, що «усі речі у світі являють собою шифр. Уся природа є просто шифром і таємним листом». Пізніше цю думку повторили і Блез Паскаль, і батько кібернетики Норберт Вінер.

У своєму трактаті Віженер знову повторив ідею Кардано щодо використання «самоключа». Заздалегідь обмовлялася одна ключова буква алфавіта, та перша буква повідомлення шифрувалася за рядком таблиці Тритемія, що відповідав цій букві. Друга буква повідомлення шифрувалась за рядком, що відповідав першій букві шифротексту і так далі.

Другий варіант використання таблиці Тритемія, запропонований Віженером, полягав у застосуванні ключа-гасла. По суті Віженер, об'єднавши підходи Тритемія, Белазо, Порта до шифрування відкритих текстів, не вніс у них нічого оригінального.

Шифр Віженера містив у собі алфавітну квадратну таблицю Тритемія, що складалася з 24 покрокових ротацій у лівий бік прямого стандартного латинського алфавіту. У цій таблиці перший горизонтальний рядок називався «лінією мови», а перший вертикальний стовпчик ліворуч – «таємною лінією». Ключем могло бути будь-яке слово, букви якого виписувалися підряд над чи під буквами відкритого листа. Причому, коли воно закінчувалось, то записувалося знову, циклічно повторюючись, поки не закінчувався текст.

Цей ключ і був «таємницею», який Белазо називав «паролем», а Віженер назвав «гаслом». У наш час ключова послідовність букв або цифр одержала назву «гама» за аналогією з відомим музичним терміном. Таблиця Віженера легко відновлювалася перед самим процесом шифрування, після чого могла бути знищена.

Запропонована Віженером шифросистема стала першим великим відкриттям у криптології з часів Юлія Цезаря, яка протягом 350 років вважалася однією з найнадійніших систем. Головною її перевагою була простота.

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
D	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C
E	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D
F	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E
G	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F
H	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G
I	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I

L	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K
M	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L
N	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M
O	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N
P	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
X	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

Повідомлення шифрувалося буква за буквою, для чого в таблиці треба було знайти стовпець, позначений тією ж буквою, що й відповідна буква ключа, та рядок, позначений тією же буквою, що й буква відкритого тексту, що лежала під даною буквою ключа. Буква, що лежала у таблиці на перетинанні зазначених стовпця та рядка, й була потрібним шифросимволом.

Наприклад, якщо як ключ використати слово «*UKRAINE*», то шифрування слова «*UZHGOROD*» виглядатиме таким чином:

Відкритий текст	U	Z	H	G	O	R	O	D
Ключ	U	K	R	A	I	N	E	U
Шифротекст	P	H	W	G	Y	E	S	Z

Шифр Віженера мав також деякі з переваг більш раннього номенклаторного типу шифру. Кожна буква відкритого тексту могла передаватися в шифротексті таким числом різних шифросимволів, скільки різних букв утримувалося в ключі. Крім того, багатоалфавітна заміна дозволяла приховувати повторювані букви й інші внутрішньословні сполучення, характерні для даного відкритого тексту. При цьому в остаточному шифротексті використовувалися тільки 24 звичайні букви алфавіту, а які-небудь спеціальні символи або цифри були не потрібні.

Астрологічні захоплення Віженера привели його до шифру, у якому шифрознаками були положення небесних тіл у момент шифрування. Він спробував перевести свої послання на «мову неба».

У XIX сторіччі британський адмірал сер Френсіс Бофорт (1774-1857) запропонував свій різновид шифру Віженера – шифр (квадрат) Бофорта (Бьюфорта). Його рядками були рядки квадрата Віженера, але записані в зворотньому (зер-

кальному) порядку:

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A
B	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z
C	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y
D	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X
E	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W
F	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U
G	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T
H	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S
I	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R
K	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q
L	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P
M	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O
N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N
O	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M
P	K	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L
Q	I	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K
R	H	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I
S	G	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H
T	F	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G
U	E	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F
W	D	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E
X	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D
Y	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C
Z	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B

Ця таблиця мала одну перевагу – правила зашифрування та розшифрування були однакові: і в тому, і в іншому випадку букви, що шифрувалися та дешифрувалися, витягалися з верхнього алфавітного рядка.

Заради історичної справедливості необхідно зазначити, що таблиця Бофора була запропонована ще у XVIII сторіччі італійцем Дж.Сестрі. Однак його ім'я в історії виявилося забутим.

Людиною, що зуміла зробити криптологію окремою науковою дисципліною, став англійський філософ і державний діяч Френсіс Бекон (1561-1626), який був одним з розумніших людей свого часу та автором більше, ніж двох десятків робіт, опублікованих та визнаних сучасниками ще при його житті. Будучи лордом-канцлером при королі Якові I, він добре знав потреби держави

в надійних шифрах, тому його перша талановита робота, що відносилася до 1580 року, надалі одержала блискучий практичний розвиток.

Присвятивши криптології спеціальні роботи «Успіх пізнання» та «Про достоїнство і збільшення наук», він був не тільки теоретиком, але й мистецьки застосовував на практиці свої знання, завдяки чому зайняв почесне місце серед видатних європейських криптологів. Зокрема, саме він уперше запропонував свою систему тайнопису, назвавши її «двобуквеним» шифром. Практично це було «двійкове кодування» букв латинського алфавіту – те ж саме, яке використовується зараз у комп'ютерах.

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAABA	h	AABBB	o	ABBAB	u,v	BAABB
c	AAABB	i,j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

По суті, це була бінарна система стеганографії, оскільки за допомогою шрифтів двох видів (наприклад, «*A*» і «*B*») у букви довільного (нетаємного) тексту потай вносилася додаткова (таємна) інформація. Кожній букві таємного послання ставилося у відповідність п'ять букв звичайного відкритого тексту.

На початку XVII століття Матео Ардженті, криптолог папської канцелярії, склав посібник з криптології на 135 аркушах, що був виданий у плетінні з телячої шкіри. У цій книзі він повторив ідею Чико Сімонетті щодо використання деякого слова як ключа для отримання змішаного алфавіту. Наприклад, ключове слово «UKRAINE» дає такий змішаний латинський алфавіт:

U	K	R	A	I	N	E	B	C	D	F	G	H	J	L	M	O	P	Q	S	T	V	W	X	Y	Z

Такі змішані алфавіти часто використовувалися як алфавіти шифротексту в шифрах простої заміни. З метою ускладнення шифру простої заміни Ардженті рекомендував не розділяти слова, використовувати «омофонні» заміни, вставляти у шифротекст велику кількість «пустишок» (Ø), усувати пунктуацію, не вставляти у шифротекст відкриті слова («клер») тощо. Для букв, що часто траплялися у словах, він ввів декілька позначень, а для сполучень букв, що часто траплялися у текстах, – окремі позначення. Пізніше подібні ідеї одержали широке поширення.

Приведемо приклад шифру Ардженті:

A	B	C	D	E	F	G	H	I	L	M	N	O	P
1	86	02	20	62, 82	22	06	60	3	24	26	84	9	66

Q	R	S	T	U	Z	ET	CON	NON	CHE	Ø
68	28	42	80	04, 40	88	08	64	00	44	5, 7

Слово «*UZHGOROD*» може бути зашифровано багатьма способами, наприклад: 0488600659289720 або 754078856070692859205577.

Найбільшим досягненням Ардженті вважається розроблений ним буквений код (номенклатор), у якому 1200 букв, складів, слів та цілих фраз замінялися групами букв.

У XVII столітті найбільш цінною історичною працею в сфері криптології були твори Густава Селена (псевдонім Августа II герцога Брауншвейг-Люнебурга, князя Брауншвейг-Вольфенбюттеля) (1579-1666) «Криптописьмо і криптографія» (лат. *Cryptomenytices et cryptographie*): «Дев'ять книг Густава Селена, у яких викладається навчання про приховання змісту і тайнопису, написане Йоганом Тритемієм, настоятелем у Спенхеймі і Хербиполені, чоловіка чудесного розуму і схованих магічних здібностей. Тут же викладені важливі способи й інших авторів. 1624 р.». Ці книги, до речі, були навчальними посібниками російського криптолога XVIII століття Епінуса.

GUSTAVI SELENI
CRYPTOME-
NYTICES ET CRY-
PTOGRAPHIÆ
Libri IX.
In quibus & planissima
STEGANOGRAPHIÆ
JOHANNE TRITHEMIO,
ENODATIO
traditur.
Insperatis ubique Authoris ac

Криптологія вже була відома багатьом та застосовувалася в багатьох шарах суспільства. Так, англієць Самуель Пепіс (1633-1703) став всесвітньо відомим своїм зашифрованим щоденником, згідно з яким історики пишуть праці про перехід від Пуританства до Реставрації. Мистецтвознавці включили цей добуток у світову скарбницю літератури. Пепіс закінчив Кембридж завдяки кузену батька – адміралу Монтегю та мав багато друзів: ученого Ісаака Ньютона, архітектора Крістофера Рена, поета й драматурга Джона Драйдена. Пепіс був особисто свідком таких незабутніх для Англії подій, як повернення короля Чарльза II в Англію, велика чума 1664 року, пожежа Лондона 1666 року, революція 1688 року.

Свої мемуари Пепіс зашифрував за системою криптолога Томаса Шел-

тона та додатково своїм власним шифром, оскільки містили багато скандальних фактів про великих сучасників. Разом з його особистими книгами та паперами щоденник після смерті письменника потрапив у Кембридж, де відразу ж привернув увагу дослідників. Перший успіх у його розшифруванні був отриманий лише в 1822 році, а повністю він був розшифрований у 1899 році.

1.3. Ера «чорних кабінетів»

У 1506 році «секретарем з шифрів» Венеціанської республіки був призначений Джовані Соро. Він прославився тим, що з успіхом розкривав шифри численних європейських князівств. Слава Соро була настільки велика, що починаючи з 1510 року папська курія надсилала йому для розкриття шифри, з якими не могли справитися в Римі. У 1526 році папа Климент VII двічі направляв Соро перехоплені депеші для дешифрування, і обидва рази Соро домігся успіху. А коли одне з послань Климента потрапило в руки його супротивників, той викрикнув: «Соро може розкрити будь-який шифр!», – і направив Соро копію цього послання, щоб з'ясувати, чи надійно воно зашифровано. Климент заспокоївся тільки тоді, коли Соро повідомив, що не може його прочитати. Хоча хто знає, чи не намагався Соро навмисно ввести папу в оману помилковими заявами про надійність його шифру.

У 1542 році Соро отримав двох помічників. З цього часу Венеція мала вже трьох кваліфікованих криптоаналітиків. Їхнє приміщення знаходилося в палаці венеціанського правителя, де вони працювали за зачиненими дверима. Нікому не дозволялось їх турбувати, а їм самим не дозволялося залишати своє робоче приміщення, поки не буде знайдений відкритий текст чергової перехопленої криптограми. Криптоаналітики Венеції також писали трактати, у яких роз'яснювали методи своєї роботи. Праця Соро про дешифрування листування на латинській, італійській, іспанській та французькій мовах, написана ним на початку XVI століття, на жаль, була загублена. Але вціліли уривчасті записи його спадкоємця, а також дослідження в цій сфері інших венеціанських секретарів із шифрів.

Джовані Соро став першим, хто почав готувати професійні кадри для криптології, і хоча це була досить примітивна форма «учнівства», позбавлена достатньої теоретичної бази, вона була переважною протягом тривалого часу. Справа в тому, що люди, які працювали з шифрами того часу, були добре освічені, але успішно освоїти криптологічну справу, яка постійно еволюціонувала й ускладнювалася, можна було тільки за допомогою довгої практики, чим і займався Соро зі своїми учнями.

Спеціальних навчальних закладів, де навчали б криптологічної діяльності в той час не існувало. Криптологів рекрутували з найбільш освічених людей того часу, що знали математику й іноземні мови. Соро був першим, хто спробував спеціально навчати молодих криптологів цій науці, але знову ж на практиці. З іншої боку, сама проблема кадрів не стояла в той час так гостро, а посада секретаря з

шифрів була досить бажаною для багатьох обдарованих людей того часу, тому що давала славу, повагу й чималий матеріальний прибуток.

Багато видатних математиків, починаючи з тих часів, залучалися до криптологічних служб. Папи Римські завжди користувалися послугами криптологів, тому видатний італійський математик і філософ Джироламо Кардано в середині XVI століття перебував у них на службі, а також був і астрологом. Крім того, він винайшов шарнірний механізм та метод вирішення рівнянь третього ступеня, а у 1550 році опублікував книгу «De subtilitate libri xxi».

Римський Папа Павло III, що змінив Клімента VII, швидко зрозумів, що не в його інтересах посилати шифри для розкриття за кордон. У 1555 році в папській курії була заснована посада секретаря з шифрів. Перший успіх прийшов тільки через два роки, коли папські криптоаналітики розкрили шифр іспанського короля Пилипа II, що тоді воював з Папою Римським. А в 1567 році відзначився вікарій собору Святого Петра в Римі, який менше, ніж за шість годин зумів прочитати криптограму, написану турецькою мовою, на якому вікарій не знав і чотирьох слів.

У Флоренції Піро Музефілі, граф Сасетський, з 1546 по 1557 роки прочитав безліч шифрованих повідомлень, розкривши серед інших номенклатори, що використовувалися в листуванні між французьким королем Генріхом II і його послом у Данії. Криптоаналітична експертиза Музефілі була настільки кваліфікованою, що багато хто приїжджали до нього, як і до Соро, з проханням розкрити для них шифри. Серед клієнтів Музефілі був і король Англії, який надіслав йому криптограму, що була знайдена в підметках туфель, доставлених до його двору з Франції.

У XVI столітті не тільки італійські правителі славилися своїми криптоаналітиками. У Франції в дешифруванні перехоплених депеш найбільше процвітав Филібер Бабу (1484-1557), який був першим державним секретарем і казначеєм короля Франциска I. Один спостерігач описував, як Бабу, «не маючи алфавіту, часто дешифровував багато перехоплених депеш на іспанській, італійській та німецькій мовах, хоча він не знав жодної з цих мов або знав дуже погано, причому він завзято працював над повідомленням дні і ночі безперервно протягом трьох тижнів, перш ніж розгадував одне слово. Після того, як пролом був прорублений, інше відбувалося дуже швидко та нагадувало руйнування стін». Варто помітити, що в той час, як Бабу не покладаючи рук працював на короля, король приймав у себе коханку – чарівну дружину Бабу. Бабу одержав багато милостей від короля, але важко сказати, за що саме: за криптоаналітичні успіхи чи за дозвіл наставляти «роги».

У Голландії також працював блискучий криптоаналітик – фламандський дворянин Пилип ван Марнікс, барон де Сент-Альдегонд (1538-1598), автор мелодії сучасного національного гімну Голландії, права рука Вільгельма Оранського, що стояв на чолі об'єднаного повстання голландців і фламандців проти Іспанії. В

1577 році Голландією керував іспанський губернатор дон Хуан Австрійський, рідний брат іспанського короля Пилипа II. Його метою було скинення з трону королеви Англії Єлизавети, захоплення англійської корони та одруження з чарівною королевою Шотландії Марією Стюарт. Однак у червні того ж року у Франції були перехоплені шифровані листи дона Хуана.

Вони були переправлені Марніксу, який через місяць розкрив іспанський шифр. Після цього зміст листів через Вільгельма Оранського був доведений до відома міністра Єлизавети Френсіса Уолсінгема. Уолсінгем одразу ж здійснив заходи щодо отримання більш повної інформації та незалежності від іноземних криптоаналітиків. З цією метою він направив до Парижа талановитого юнака, який швидко розправлявся з шифрованими листами. Це був Томас Феліпес, перший видатний криптоаналітик з Англії.

За результатами проведених заходів все шифроване листування Марії Стюарт, в якому вона давала згоду на змову проти Єлизавети та рекомендаціїї щодо її здійснення, розшифровувалося Феліпесом та надходило до Уолсингема. Ці листи та шифр, яким вона користувалася разом з іншими зрадниками, послужили головним матеріалом для обвинувачення на засіданнях суду, який визнав Марію Стюарт винною у державній зраді. 8 лютого 1587 року о 8-ій годині ранку вона піднялась на ешафот, стала на коліна та мужньо прийняла від ката три удари сокирою. Таким чином, криптоаналіз прискорив смерть Марії, королеви Шотландії.

Шифр Марии, королевы Шотландии

У 1589 році королем Франції став Генріх IV, що відразу ж був змушений вступити в запеклу боротьбу зі Священною лігою. Священна ліга на чолі з герцогом Майенським контролювала столицю та всі інші великі міста Франції, одержуючи великі підкріплення у вигляді живої сили та грошей від іспанського короля Пилипа II. Генріх був з усіх боків оточений супротивником. Але

саме в цей важкий для нього час у його руки потрапила частина листування Пилипа з іспанським воєначальником Хуаном Моро.

Листи Пилипа були зашифровані, але в Генріха секретарем з шифрів у той час служив 49-літній математик Франсуа Вієт (1540-1603), засновник сучасної елементарної алгебри. Його теорему про коріння й коефіцієнти квадратних рівнянь дотепер вивчають у школі. Він також був членом таємної ради та займався адвокатською практикою. У 1588 році Вієт прочитав шифровану іспанську депешу, адресовану Олесандро Фарнезе, герцогу Парми, що командував іспанськими військами Священної ліги.

З тих пір Генріх передавав Вієту всі нові перехоплені депеші, щоб з'ясувати, чи зможе той повторити свій успіх. Вієт, працюючи разом з голландським криптоаналітиком Пилипом ван Марніксом, зумів приблизно за рік розкрити шифр короля Іспанії Пилипа II, що до цього часу вважали невразливим не тільки в Іспанії, але й у Ватикані – одному з найбільших криптологічних центрів того часу.

Розвиток криптоаналізу на Заході виявився в прямій залежності від розквіту дипломатії. З тих пір, як держави стали підтримувати постійні дипломатичні відносини, їхні посли, яких іноді іронічно називали «почесними шпигунами», регулярно відправляли до себе на батьківщину великі послання. Існуючі між державами суперництво й підозрілість змушували дипломатів зашифровувати свої депеші, оскільки їх нерідко перехоплювали та розкривали.

Поява постійних дипломатичних представництв та загострення політичної боротьби стимулювало послів зашифровувати свої повідомлення, побоюючись, що вони будуть перехоплені супротивником. До кінця XVI сторіччя криптоаналіз став грати настільки важливу роль, що в більшості європейських держав були введені посади секретарів з шифрів, які повний робочий день займалися шифруванням і розшифруванням своїх повідомлень, а також дешифруванням перехоплених депеш.

Взагалі ж, у XVI-XVII століттях криптослужби з'явилися практично в кожній європейській державі, причому до складу цих служб входила наукова еліта того часу: Франсуа Вієт і Антуан Россиньоль у Франції, Джироламо Кардано в Римі, Джон Валліс і Френсіс Бекон в Англії, Вільгельм Лейбніц у Німеччині. Європейські правителі нерідко залучали вже відомих криптологів-іноземців на службу, хоча це не завжди вдавалося. Мабуть, найнеуспішним із таких криптологів був Готфрід Вільгельм Лейбніц (1646-1716) – видатний німецький учений, математик, засновник Берлінської академії наук.

Англійський король Георг I хотів запросити Лейбніца, щоб той очолив британську криптослужбу, але натрапив на різку протидію в особі Джона Валліса (1616-1703), який побоювався конкуренції з боку свого німецького колеги та пригрозив королю перейти на бік Іспанії, видавши їй всі англійські секрети, яких Валліс за характером своєї діяльності знав чимало.

Активно виступав проти подібного призначення й Ісаак Ньютон (1642-1727) – голова Королівського наукового суспільства, який заперечував авторство Лейбніца у диференційному обчисленні. Не потпланило Лейбніцу й іншого разу, коли його запросив до Росії Петро I не тільки для організації Російської академії наук, але й для створення російської криптослужби за європейським зразком. Смерть Лейбніца не дозволила здійснитися планам Петра, змушеного скористатися послугами менш іменитих криптологів.

XVII століття ввійшло в історію криптоаналізу як ера «*cabinets noirs*», або «чорних кабінетів» (далі – ЧК). У цей час у різних країнах почали з'являтися перші служби перлюстрації (лат. *perlustro* - оглядаю) та дешифрування «розкритої» кореспонденції, які розташовувались у секретних кімнатах (тому й назва - ЧК).

В Англії лорд-протектор Олівер Кромвель створив «Інтелідженс сервіс», до складу якої входив підрозділ із дешифрування. Його очолював відомий математик Джон Валліс (Уолліс), який володів унікальними здібностями. Так, безсонними ночами він вираховував квадратний корінь із 50-значних чисел з точністю до 20-30-го знаків.

Англійський король Карл II цінував мистецтво Валліса та називав його «дорогоцінним каменем для короля…». Розквіт дешифрувального мистецтва Валліса припав на часи правління Вільгельма Оранського та його дружини Марії. Він продовжував служити криптоаналітиком і складав звіти для графа Нотінгемського, командувача морськими та сухопутними збройними силами Англії. Напруження, з яким він працював у ті роки, відбилося у одному з його листів: «… боюся, що взагалі збожеволію».

У 1689 році Валлісу вдалося «розкрити» шифр листування короля Франції Людовика XIV і французького посла у Польщі, тим самим здійснити значний вплив на зовнішню політику Англії. Зокрема, він розкрив наміри Людовика XIV втягнути Польщу у війну проти Пруссії. В результаті ефективне використання цієї інформації дипломатією Англії призвело до того, що французькі посланці були з ганьбою вигнані з Польщі.

Після смерті Валліса Англія зробила важливий політичний крок: офіційно оголосила про введення урядової посади криптографа-дешифрувальника. У 1703 році першим офіційно оголошеним дешифрувальником Англії став внук Валліса – Уільям Бленкоу. Він працював достатньо успішно, але не витримав робочого напруження. У нападі тимчасового божевілля Бленкоу вчинив самогубство.

Не відставала й Франція, де дешифрувальне відділення було створено при Людовику XIII за пропозицією кардинала Рішельє. Його очолив Антуан Россиньоль (1600-1682), який створив дипломатичний шифр, що представляв собою складово-словниковий код на 600 компонентів.

Антуан Россиньоль уперше придбав популярність у 1626 році. Йому передали зашифрований лист, захоплений у кур'єра, що пробирався з обложеного міста Реальмон, і до кінця дня він дешифрував його. З листа стало зрозуміло, що армія гугенотів, що утримувала місто, перебуваючи на грані загибелі. Французи, які до цього не підозрювали про розпачливе положення гугенотів, повернули лист разом з його розшифровкою. Тепер гугеноти знали, що їхній супротивник не відступить, і негайно здалися. Так перемога французів стала результатом дешифрування.

Могутність криптології сталася очевидною, тому Антуан Россиньоль і його син Бонавентур одержали високі посади при дворі. Видатна майстерність і накопичений досвід з розкриття шифрів дозволив Россиньолям зрозуміти, як створити більш стійкий шифр, і вони придумали так званий «Великий шифр». Він застосовувався для зашифровування найбільш таємних повідомлень короля, приховуючи деталі його планів, задумів і політичних інтриг. В одному з цих повідомлень згадувалася одна з найбільш загадкових особистостей у французькій історії, людина в залізній масці, але стійкість «Великого шифру» означала, що повідомлення залишиться нерозшифрованим і непрочитаним протягом двох сторіч.

«Великий шифр» виявився настільки надійним, що зумів протистояти зусиллям всіх криптоаналітиків тієї епохи, що намагалися вивідати французькі таємниці, і навіть наступних поколінь дешифрувальників. На жаль, після смерті батька й сина «Великий шифр» перестав застосовуватися, а його подробиці були швидко загублені, що означало, що зашифровані папери у французьких архівах більше не можна було прочитати.

Цей шифр французька армія буде використовувати більше 100 років. Відомо, що навіть Наполеон під час своїх походів використовував шифри, що були спрощеними варіантами шифру Россиньолів. Не менш відомим був і «шифр Рішельє» – при його використанні текст повідомлення розбивався на відрізки, букви яких переставлялися у визначеному порядку. Россиньолю належить також авторство відомої доктрини про те, що «стійкість військового шифру повинна забезпечити таємність повідомлення протягом терміну, необхідного для виконання наказу. Стійкість дипломатичного шифру повинна забезпечувати таємність протягом декількох десятків років».

Россиньолі надзвичайно плідно працювали в сфері криптоаналізу як при дворі Людовика XIII, так і у світі Людовика XIV. Наприклад, захоплення фортеці Еден королівською армією було прискорено завдяки тому, що Россиньолі прочитали зашифроване прохання її захисників про допомогу, а після цього тим же шифром склали відповідь, у якому жителі міста сповіщалися про даремність їхніх надій. Вони ніколи нікому не розповідали про те, скільки інших міст мусили скласти зброю і скільки зрад розкрили серед вищої знаті. Через цю їхню таємничість деякі придворні стверджували, що насправді Россиньолі не розкрили жодного шифру і кардинал поши-

рював чутки про їхні здібності з метою попередження потенційних змовників.

На смертному одрі Людовик XIII охарактеризував Антуана Россиньоля як людину, від якого залежало благополуччя його підданих. Не дивно, що через два роки, 18 лютого 1645 року, спадкоємець Рішельє кардинал Мазаріні призначив Россиньоля державним радником. Як і Рішельє, Мазаріні пересилав йому перехоплені шифроповідомлення. Наприклад, у 1656 році він направив зашифрований лист кардинала Реца з указівкою Россиньолю прочитати його. При Людовику XIV Россиньоль часто працював у кімнаті, що безпосередньо прилягала до кабінету короля у Версальському палаці. Звідси йшов весь потік дешифрованих ним повідомлень, що допомагали королю визначати політику Франції.

Одним із кращих друзів Россиньоля був поет Буаробер, ініціатор ідеї створення Французької академії. Коли Буаробер потрапив у немилість при дворі, він поскаржився на нещастя, що звалилося на нього, у вірші, адресованому своєму впливовому другу-криптоаналітику. Россиньоль показав цей вірш Мазаріні, який під час наступної аудієнції привселюдно похвалив Буаробера. Пізніше з почуття подяки Буаробер написав 66-рядковий вірш, у якому оспівував Россиньоля. Це перша віршована ода, присвячена криптоаналітику. Деякі її рядки звучать так:

Яке дивовижне твоє мистецтво і яскраве.
І яка важлива сила твоєї майстерності!
Тому що з її допомогою здобуваються провінції,
Розкриваються секрети всіх королів,
І з малими зусиллями вона
Змушує здаватися міста й форти.
...Дійсно, твоя майстерність
Вище мого розуміння,
І я ніколи не осягну
Твій секрет; але я зараз можу сказати,
Що вона служить тобі дуже добре,
Що ти заслуговуєш її. Не побоюся,
Твоя майстерність буде благоволіти тобі роками.
І доля буде тобі посміхатися,
Поки війни затьмарюють землю.

Праця Россиньолів зробила його видною фігурою при дворі Людовика XIV. Саме йому вдалося довести правителям Франції надзвичайну важливість дешифрування депеш для формування їхньої політики. Його робота демонструвала це настільки ефективно, що королівський військовий міністр Лувуа став енергійно заохочувати кожного, хто міг надати отриману таким чином інформацію. Зберігся лист Лувуа, у якому той висловлював подяку за добутий шифр ворога, завіряючи, що людині, спроможній прочитати декілька шифрованих листів,

«його величність подарує усе, що він попросить».

Россиньоль став першою людиною, що прославилася винятково завдяки своїм криптоаналітичним здібностям. Даниною загального захоплення вмінням «зламувати» шифри було те, що слово «россиньоль» стало французькою жаргонною назвою відмички. Шарль Перо, який більше відомий як автор казок, вніс біографію Россиньоля у свою книгу «Знамениті люди Франції в нинішнім столітті» поряд з життєписом Рішельє.

Після смерті Россиньоля у 1682 році «Великий шифр» вже не завжди застосовувався у королівському листуванні, і ця необачність дорого обійшлася Франції. Так, у 1774 році Людовику XV був доставлений пакет із Відня від секретаря французького посольства абата Жоржеля. Коли французький король розкрив його, то знайшов там копії відкритих текстів своєї шифрованої кореспонденції, що була «розкрита» у віденському ЧК.

У Німеччині був створений спеціальний орган – «криптографічна лабораторія» – під керуванням графа Гронсфельда, який удосконалив шифр Віженера, замінивши буквений ключ цифровим, цифри в якому позначали кількість кроків, на яке букву повідомлення зрушували вправо за алфавітом. Для цього під повідомленням писали ключ. Якщо ключ коротший повідомлення, то його повторювали циклічно. Шифровку одержували начебто за шифром Цезаря, але відраховували необов'язково тільки третю букву за алфавітом, а ту, яка була зрушена на відповідну цифру ключа. Завдяки простоті застосування цей шифр використовувався у той час надзвичайно широко.

Застосуємо як ключ групу з трьох початкових цифр числа «π» (314) та зашифруємо слово «ШИФРОВКА». Щоб зашифрувати першу букву повідомлення «Ш», використовуючи першу цифру ключа «3», відраховується третя одна за одною від «Ш» у алфавіті буква «Ш-Щ-Ю-Я» і виходить буква шифровки «Я». Далі використовуючи другу цифру ключа «1», відраховується перша від «И» у алфавіті буква ««И-І» і виходить буква шифровки «І» і так далі. В результаті отримуємо шифротекст:

Відкритий текст	Ш	И	Ф	Р	О	В	К	А
Ключ	3	1	4	3	1	4	3	1
Шифротекст	Я	І	Ш	У	П	Е	Н	Б

У той час також і Швеція приділяла увагу захисту власного дипломатичного та військового листування. Так, у 1676 році, за кілька днів до битви між шведською і датською арміями під містом Лунд, шведський король Карл XI відправив генералу Фабіану фон Ферсену шифрований лист зі своїми міркуваннями щодо стратегії й тактики військ у майбутній битві. Завдяки цій інформації шведи здобули перемогу в битві, яка стала однією з найкривавіших в історії Скандинавії.

У XVII столітті свій внесок у розвиток криптоаналізу зробив англієць Джон

Фальконер. У 1685 році він написав книгу «Розкриття таємних повідомлень, або Мистецтво здобувати таємні відомості без ключа» (англ. *Cryptomensis Patefacta: or the art of secret information disclosed without a key*), де виклав деякі розроблені ним методи дешифрування. Зокрема, він запропонував використовувати перебір можливих відкритих слів за їх довжиною (якщо у шифротексті слова розділялися).

Cryptomenysis Patefacta:
Or the
A R T
OF
SECRET INFORMATION
Difclofed without a KEY.
Containing,
Plain and Demonſtrative Rules,
for Decyphering all Manner of SECRET WRITING. With Exact Methods, for Refolving Secret Intimations by SIGNS or GESTURES, or in SPEECH. As alſo an Inquiry into the Secret ways of CONVEYING Written Meſſages: And the ſeveral MYSTERIOUS PROPOSALS for Secret Information, mentioned by Trithemius, &c.
By J. F.
Et varias uſus meditando extunderet Artes.
Virg. G. 1.
LONDON,
Printed for Daniel Brown, at the Black Swan and Bible, without Temple Bar, 1685.

До кінця XVII століття криптологія остаточно склалася як наукова дисципліна. Хоча в даний період панували «номенклатори», які не були шифрами в «чистому» вигляді, проте поява багатоалфавітної заміни, використання трафаретів, біграм і цифрових позначень стала величезним кроком уперед у порівнянні з найдавнішим періодом і персоніфікувала наступ нової ери в розвитку криптології, що впритул наблизилася до свого сучасного вигляду.

Однак XVIII століття стало для криптології періодом «застою», або навіть «занепаду». Великий «стрибок», який ця наука зробила в попередній період, дозволив упродовж майже 150 років не вводити ніяких нововведень у способи шифрування й дешифрування повідомлень. Розроблені раніше криптосистеми успішно застосовувалися на практиці, а трактати XVI-XVII століть служили навчальними посібниками для криптоаналітиків. Майже всюди до криптологічної діяльності залучалися видатні вчені, в основному, математики, однак жоден з них в XVIII столітті не залишив будь-якої значимої праці з криптології, не розробив нової шифросистеми або придумав більш ефективного способу дешифрування.

Існуючі шифри заміни були досить стійкі, але й кваліфікація криптоаналітиків була високою настільки, що більшість значимих повідомлень розшифровувалася. Цей час став періодом розквіту «номенклатора» (лат. *nomen* - ім'я і *calator* - раб, слуга) – шифру, що представляв собою сполучення шифру заміни та невеликого коду. Він зазвичай містив кодові еквіваленти букв алфавіту та найбільш уживаних складів, слів і словосполучень, а також ряд спеціальних символів. Найчастіше в ньому траплялися спеціально створені для цієї мети символи, але нерідко також використовувалася астрологічна й окультна символіка.

Номенклатор був розроблений як система шифрування, що була найкраще пристосована до методів криптоаналізу, які найчастіше використовувались у той час. Вони, як правило, містили підрахунок частоти появи в тексті кожного симво-

лу та пошук у шифротексті слів і виразів, що містили характерні для даної мови сполучення букв. Метод частотного аналізу букв був заснований на тому, що в будь-якій мові одні букви зустрічалися частіше, ніж інші. В англійській мові, наприклад, частіше, ніж інші траплялася буква «E». Іншими буквами, що найбільш часто зустрічалися, були *T, A, O, N, R* і *S*. А букви *J, K, X* і *Z* траплялися в англійській мові рідко. Оскільки в ході операції заміни частота букви не змінювалася, ключ до розгадки значення того або іншого шифросимволу полягала іноді в підрахунку частоти його появи в шифротексті. Так само операція простої заміни не вносила змін і в сполучення букв (буквені моделі).

Цей тип криптосистеми, що поступово ускладнювався протягом трьох попередніх століть, досяг в XVIII столітті піка свого розвитку. Стандартним був розмір «номенклатора» в 400-500 символів, але були й такі, які досягали 5-6 тисяч та заміняли особливими символами практично всі значимі поняття, імена, назви й цілі речення. У цей період «номенклатори» стали схожі більше не на шифр, а на форму ієрогліфічного листа, і незважаючи на це, їх все-таки «розкривали».

У XVIII столітті ЧК вже стали розповсюдженим явищем по всій Європі, а віденський ЧК (Geheime Kabinets-Kanzlei) користувався репутацією найкращого серед них. Він функціонував дуже ефективно. Мішки з поштою, що мали доставлятися посольствам у Відні щодня о 7-й годині ранку, з'являлися спочатку у приміщенні ЧК. Там листи розкривали, розтоплюючи печатки над свічею, відзначали порядок розташування сторінок у конверті та передавали їх помічнику директора. Той читав їх і давав указівки про зняття копій із найважливіших документів.

Довгі листи для економії часу копіювалися під диктування з використанням до чотирьох стенографістів одночасно. Якщо лист був на незнайомій помічнику директора мові, він передавав його тому службовцю ЧК, який володів цією мовою. Там були перекладачі з усіх європейських мов, а коли з'являлася потреба у фахівцях з невідомої іншим мови, один зі службовців у терміновому порядку брався за її вивчення. Після копіювання листи акуратно укладалися знову в конверти, що опечатувалися підробленими печатками та поверталися на пошту не пізніше 09.30 ранку.

Через півгодини до ЧК прибувала нова пошта. Вона оброблялася таким же чином, хоча і з меншою поспішністю, оскільки була транзитною. Як правило, ця кореспонденція поверталася на поштову станцію до двох годин дня, хоча іноді її затримували й до семи вечора. В 11.00 прибувала пошта, перехоплена поліцією. А в 16.00 кур'єри привозили листи, що відправляли закордонні посольства. Вони знову вливалися в потік поштової кореспонденції, що відправлялася з Відня в 18-30. Скопійований матеріал попадав на стіл до директора ЧК, що відбирав особливо важливу інформацію та направляв її зацікавленим особам – до двору, поліцейських чиновників, дипломатів і воєначальників. Таким чином, віденський ЧК зі штатом усього в 10 осіб обробляв у середньому сотню листів щодня.

Перехоплена зашифрована кореспонденція піддавалася криптоаналізу. У ньому віденці досягли чудових успіхів, якими були зобов'язані своїй прогресивній системі роботи з персоналом. За винятком надзвичайних випадків, австрійські криптоаналітики один тиждень працювали, а другий – відпочивали, щоб уникнути перевтоми від інтенсивного розумового навантаження. Хоча їхня заробітна плата була невисокою, за розкриття шифрів видавалися значні премії. Трохи менша премія покладалася за дешифрування з використанням украдених ключів. Наприклад, у 1833 році криптоаналітики одержали 3/5 усієї суми, призначеної для премій за читання шифровок французького посланника. Протягом однієї ночі ключ до його шифру був таємно вилучений, скопійований та знову повернутий у шафу в спальній кімнаті секретаря французької дипломатичної місії у Відні.

Віденський ЧК поставляв безцінну інформацію імператорам Австрії, але, крім цього, він також продавав зібрані ним відомості й в інші держави Європи. Так, у 1774 році в обмін на 1000 дукатів абат Жоржель, секретар французького посольства, одержав можливість двічі на тиждень переглядати отримані відомості, а потім відсилати листи з викладенням таємних планів монархів різних країн безпосередньо Людовику XV у Париж.

Австрійський канцлер Кауніц, що безпосередньо керував службою перехвату та дешифрування, створив цілу мережу відділень ЧК (Відень, Франкфурт, Нюрнберг, Майнце тощо). Ці відділення іноді працювали досить грубо. Так, англійський посол у Відні (Кейт) поскаржився Кауніцу, що він одержує копії замість оригінальної кореспонденції. На це канцлер віджартувався: «Такі неспритні ці люди!» Французький посол у Відні, знаючи про успіхи австрійської служби перехвату та дешифрування, повідомляв у Париж про те, що «секрет наших шифрів... не довговічний, враховуючи здібності австрійських дешифрувальників». Однак Париж не надавав таким відомостям належного значення.

Вражає та обставина, що «моторні» пальці співробітників віденського ЧК майже ніколи не вкладали листа до чужого конверту. Лише одного разу перехоплений лист для герцога Моденського був помилково опечатаний дуже схожою печаткою правителя Парми. Коли герцог помітив підробку, він відправив його до Парми з іронічною позначкою: «Не зовсім мені, але й не вам». Обидві держави заявили протест, але Відень відреагував на нього цілковитим здивуванням. Проте багато представників закордонних країн при австрійському дворі знали про існування у Відні ЧК.

Істотним стимулом у праці було й королівське визнання видатних заслуг австрійських криптоаналітиків. Карл VI вручав їм премії особисто, а ерцгерцогиня Марія-Терезія часто розмовляла зі співробітниками ЧК про надійність використовуваних шифрів і про досягнення інших країн у криптоаналізі.

Були розроблені «нормативні акти», що регулювали працю дешифруваль-

ників. Вони передбачали для них грошову компенсацію за вимушене «безробіття», яке могло бути викликане тим, що вдавалось агентурним шляхом отримати шифри. Також передбачалася виплата дешифрувальникам великих премій за серйозні успіхи у дешифруванні.

Підготовка криптоаналітиків також була націлена на одержання від них максимальної віддачі. Для роботи в ЧК набирали молодих людей у віці приблизно 20 років з високими моральними якостями. Вони повинні були швидко говорити французькою та італійською мовою, знати математику. Спочатку їм не розповідали про справжній характер майбутньої діяльності та навчали створенню надійних шифрів, а потім випробовували – чи зможуть вони розкрити розроблені ними ж шифри. Нездатним підшукували іншу державну службу, а інших присвячували в секрети криптоаналітичної майстерності та посилали в інші країни для лінгвістичної практики. Після розкриття першого шифру їхня платня подвоювалася. Крім того, для молодої людини відкривалася перспектива стати кваліфікованим фахівцем, який за досягнуті успіхи одержував аудієнцію у монарха з усіма відповідними привілеями.

Гарну можливість оцінити досягнення віденського ЧК дали листи барона Ігнаца Коха, що керував ним з 1749 по 1763 рік. Наприклад, 4 вересня 1751 року він послав австрійському послу у Франції якусь дешифровану кореспонденцію, що дозволяла, за його словами, «набагато краще зрозуміти основні політичні принципи, якими керується Урядовий кабінет у Франції». А ще через два тижні він написав: «Це вісімнадцятий шифр, який ми розкрили протягом року... На жаль, нас вважають надто здатними в цьому мистецтві, і думка про те, що ми можемо вторгнутися в їхню кореспонденцію, спонукує іноземні двори безупинно змінювати ключі, інакше кажучи, посилати щораз більш важкі щодо дешифрування повідомлення». До досягнень віденського ЧК відноситься читання шифрованого листування Наполеона, Талейрана, безлічі інших закордонних політичних діячів і дипломатів.

Англійський ЧК на відміну від віденського не мав власного приміщення. Тому його невеликий штат експертів працював, як правило, вдома, одержуючи матеріали через посильних. В англійського ЧК була відсутня чітка організаційна структура, старший дешифрувальник був у ньому просто першим серед рівних. Фінансування ЧК здійснювалося за рахунок коштів, що відпускалися Міністерству пошт Англії з додаткових доходів Парламенту. В усій країні тільки близько 30 осіб знало про те, що ЧК читав іноземне дипломатичне листування. З ним знайомилися тільки король і його головні міністри.

Однак, незважаючи на режим таємності, більшість ділових людей в Англії завбачливо шифрувала свою кореспонденцію або довіряла її приватним посильним. Причиною цього був англійський закон про пошту від 1711 року, що давав урядовим службовцем право розкривати будь-які поштові відправлення на підставі ордерів, які вони ж собі й видавали.

В ті часи в англійському ЧК працював талановитий криптолог і священнослужитель Едвард Уоллес, який завдяки своїм успіхам у дешифрувальній діяльності отримав сан єпископа. Серед його успіхів можна виділити такі:

- викриття спроби Швеції викликати повстання в Англії;
- дешифрування дипломатичного листування Франції.

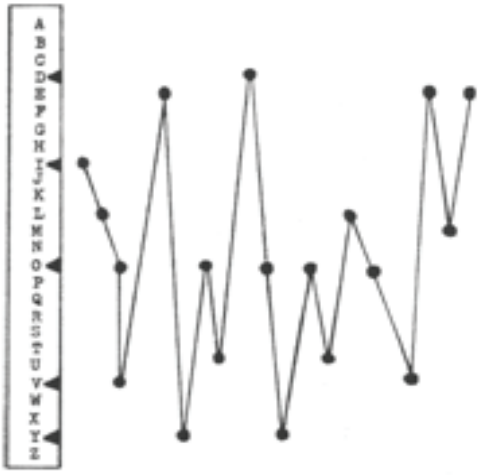
Англійський ЧК читав у середньому дві або три шифровані депеші за тиждень. Його криптоаналітики успішно розкривали шифри Австрії, Греції, Росії, Туреччини, Франції, а також Неаполя, Саксонії, Сардинії й інших італійських держав. Пізніше до цих країн приєдналися й Сполучені Штати Америки. Так, наприклад, архів французької кореспонденції, перехопленої в XVIII-XIX століттях, складався з п'яти томів, що нараховували, у цілому, більше 2000 сторінок. До них додатково додавалися ще три томи ключів до французьких шифрів. Іспанське досьє складалося з трьох томів на 872 сторінках. У ньому були зібрані повідомлення, перехоплені англійцями з 1719 по 1839 рік. Однак не всі іспанські шифровки були прочитані безпосередньо після того, як були перехоплені. Багато з них чекало своєї черги доти, коли їх накопичувалося у достатній кількості для успішного дешифрування або коли з'являлася необхідність у їхньому прочитанні.

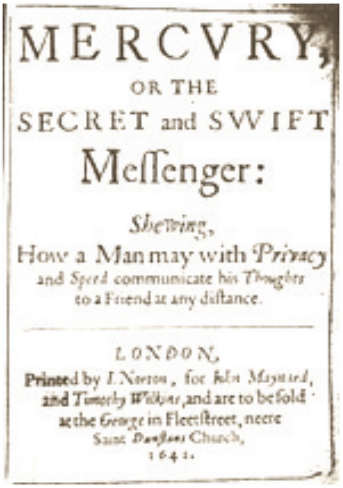
У 1723 році двоє криптоаналітиків англійського ЧК виступили свідками у Палаті лордів, де судили єпископа Френсіса Етенберга за обвинуваченням у змові. Оскільки головні викривні Етенберга докази були знайдені в дешифруваннях Едварда Уоллеса і Ентоні Корбіре, лорди «рахували доречним викликати в суд цих дешифрувальників, щоб переконатися у вірогідності їхнього дешифрування». Уіллес і Корбіре показали під присягою, що листування Етенберга було дешифровано ними незалежно один від одного, оскільки один з них знаходився у провінції, а іншій у столиці, але результати дешифрування збіглися.

Етенберг спробував поставити під сумнів вірогідність розшифрованих текстів, представлених Уоллесом і Корбіре. Підсудний підняв такий шум, що йому та його адвокату було наказано залишити приміщення суду, а лорди винесли на голосування пропозицію, відповідно до якої «будь-які питання дешифрувальнику, що здатні привести до розкриття способів або таємниць дешифрування, суперечать суспільній безпеці». Незважаючи на всі протести підсудного, дешифровані тексти були прийняті як доказ провини Етенберга. Його відсторонили від посади та «вигнали» з королівства.

Разом з Уоллесом в англійському ЧК працював Джон Уілкінс (1614-1672), єпископ Честера, засновник і перший секретар королівського наукового товариства. У 1641 році він написав книгу «Меркурій, або секретний та швидкий кур'єр» (англ. *Mercury, or the Secret and Swift Messenger*), де вперше в англійській мові з'явилися терміни «криптографія» і «криптологія». В ній Уілкінс запропо-

нував різновид так званого «геометричного» шифра. По суті це був шифр простої заміни, але із застосуванням стеганографії для передачі шифротекста, який мав вигляд безневинних геометричних фігур.




MERCVRY,
OR THE
SECRET and SWIFT
Messenger:
Shewing,
How a Man may with Privacy
and Speed communicate his Thoughts
to a Friend at any distance.
LONDON,
Printed by I. Norton, for Iohn Maynard,
and Timothy Wilkins, and are to be sold
at the George in Fleetstreet, neere
Saint Dunstans Church,
1641.

Уілкінс запропонував також оригінальний «музичний» шифр. У ньому секретні повідомлення мали вигляд музичних мелодій, тобто текст замінявся на нотні записи. До речі, ще Френсіс Бекон склав декілька музичних мелодій, що містили секретні повідомлення.

У 1786 році шведський фахівець Фредерік Грипенстерна підніс королю Густаву III свій винахід, який вже у XVIII столітті одержав у шведів назву «шифромашина». У Швеції вважається, що це був перший у світі шифратор. Не будемо заперечувати справедливість такої першості та перейдемо до опису пристрою.

Машина складалася з 57 колес, що у змінюваному порядку розташовувалися на загальній вісі. Ця конструкція містилася в циліндричному корпусі. На одному боці кожного колеса були нанесені букви шведського алфавіту в їхньому природному порядку. На іншому боці наносилися числа від 00 до 99, яких на кожному колесі малося 29 (за кількістю букв шведського алфавіту).

На різних колесах наявність чисел була незалежною, тобто те саме число могло з'явитися на різних колесах. На кожному боці корпуса уздовж вісі циліндра прорізалася щілина, через яку можна було бачити рядок з 57 символів. Один бік циліндра використовувався для набору відкритого тексту, інший – для зчитування шифротексту.

Перед початком роботи колеса (які могли обертатися на осі незалежно одне від одного) встановлювалися у вихідне положення таким чином, щоб букви алфа-

віту і числа шифропозначень знаходилися кожні на своєму боці. Кожний із боків машини обслуговував свій оператор. При шифруванні один з них шляхом обертання коліс набирав відкритий текст (57 букв). Після цього другий на своєму боці зчитував 57 відповідних чисел шифрованого тексту. При розшифруванні ролі мінялися: один оператор набирав рядок з чисел шифротекста, а інший – зчитував відкритий текст. Наступні 57 букв шифрувалися за тим же принципом і т.д.

Описана шифромашина за своєю конструкцією та принципом функціонування дуже нагадувала американський дисковий шифратор Джефферсона, також винайдений наприкінці XVIII століття. І це далеко не єдиний в історії криптології приклад того, що ніяк не пов'язані один з одним творці шифротехніки з різних країн незалежно один від одного приходили до схожих рішень.

Французький ЧК у 1811 році Наполеоном I був значно зміцнений та отримав філії по усій своїй величезній імперії: у Туреччині і Генуї, Флоренції і Римі, Амстердамі і Гамбурзі, де вони працювали досить ефективно. Перлюстрація дипломатичного листування прийняла величезні розміри та знаходилася під контролем міністра закордонних справ Талейрана.

Цікаво, що у 1808 році Талейран при особистій зустрічі з російським імператором Олександром I запропонував себе як платного інформатора. Після недовгих роздумів про те, чи не є пропозиція Талейрана провокацією, російський імператор прийняв позитивне рішення з цього питання та став досить щедро оплачувати його інформацію. Так Талейран став платним агентом російської розвідки. Надана ним інформація була досить важливою для російського двору. Подібні послуги Талейран запропонував й Австрії. Там його пропозиція також була прийнята, про що з агентурних джерел довідався й Олександр I. Це привело до поступового згортання контактів з Талейраном, що до того ж став вимагати за свої послуги величезні суми.

Ера «чорних кабінетів» у Європі була недовгою. Бурхливі політичні події середини XIX століття привели до обмеження абсолютної влади європейських монархів і їхніх поліцейських відомств. Проголошені принципи волі та рівності виявилися несумісними з цензурою листування. У червні 1844 року хвиля протестів

з боку громадськості з приводу перлюстрації листів змусила англійський уряд припинити перехоплення дипломатичного листування. В Австрії віденський ЧК був ліквідований у 1848 році. У Франції, де ЧК нормально не працював ще з часів Великої Французької революції, це відбулося також у 1848 році.

1.4. Європейська криптологія у XIX ст.

На початку XIX століття була надрукована Французька Енциклопедія. У ній були описані усі відомі на той час історичні шифри та способи їхнього дешифрування. Це сприяло широкому поширенню криптологічних знань у Європі. Енциклопедія зіграла роль підручника з криптології для широкого кола зацікавлених осіб у різних країнах (у тому числі, у Росії). Особливо це відносилося до революційних підпільних організацій, що не мали доступу до секретів державних криптослужб.

Під час своїх походів Наполеон і його генерали використовували дві системи шифрів. «Великий шифр» Наполеон використовував для зв'язку зі своїми командуючими. Дана система була подібна «великому шифру» Россиньоля, однак являла собою код на 200 величин замість 600, запропонованих Россиньолем. Це робилося для простоти роботи з шифром у польових умовах. Разом із тим, щоб ускладнити частотний аналіз букв, кожну букву тексту стали заміняти двома і більше шифросимволами. Така операція звичайно руйнувала і буквені моделі, від наявності яких значною мірою залежав успіх криптоаналізу.

Розглянемо як ілюстрацію «Малий шифр», що використовувався в наполеонівській армії для зв'язку між військами і генеральним штабом.

A-15; AR-25; AL-39	M-114; MA-107
B-37; BU-3; BO-35; BI-29	N-115; NE-94; NI-116
C-6; CA-32; CE-20	O-90; OT-153
D-23; DE-52	P-137; PO-152
E-53; ES-82; ET-50; EN-68	Q-173; QUE-136
F-55; FA-69; FE-58; FO-71	R-169; RA-146; RE-126; RI-148
G-81; GA-51	S-167; SA-171; SE-177; SI-134
H-85; HI-77	SO-168; SU-174
I-119; IS-122	T-176; TI-145; TO-157
J-87; JAI-123	U-138
K-?	V-164; VE-132; VI-161; VO-175
L-96; LU-103; LE-117	W, X, Y-?
LA-106	Z-166

«Малий шифр» був розкритий французьким криптологом Етьєном Базері (1846-1931). У наявних в його розпорядженні шифровках деякі букви (K, W, X і Y) не траплялися, тому він не зміг визначити їх шифроеквівалентів. «Малий шифр»

містив числові еквіваленти для всіх букв алфавіту, а також для біграм (двобуквених сполучень), що часто зустрічалися, і деяких триграм (трибуквених сполучень). За допомогою цього шифру, який фахівці назвали «силабарієм» (складовим алфавітом), слово «Наполеон», наприклад, може бути зашифроване по-різному:

N	A	P	O	L	E	O	N
115	15	137	90	96	53	90	115

або

N	A	PO	LE	O	N
115	15	152	117	90	115

Використання подібних прийомів сильно ускладнювало завдання криптоаналітиків. Хоча наполеонівський шифр був відносно невеликим, в епоху «номенклаторів» нерідко застосовувалися й криптосистеми, що містили сотні відповідностей.

Але й ці не дуже стійкі шифри використовувалися з серйозними помилками. Ключі не змінювалися тривалий час, у шифротекстах зберігалася розбивка на слова (відповідно до відкритого тексту), використовувалися стандартні звернення та підписи, значна частина повідомлення не шифрувалася (вона вважалася нетаємною) тощо. Усе це, безумовно, полегшувало дешифрування. Крім того, в екстрених випадках таємні повідомлення взагалі не шифрувалися та у відкритому вигляді попадали до супротивника.

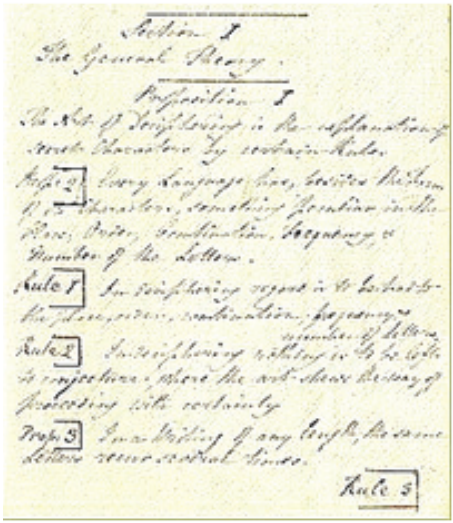
При Наполеоні також не були винайдені нові спеціальні шифри. Французька армія користувалася відомими на той час способами шифрування. Тому супротивники Наполеона досягли досить серйозних успіхів у дешифруванні його листування. До 1811 року французи для передачі повідомлень використовували прості шифри, що одержали популярність як «petits chiffres». Вони були рукописними та розшифровувалися в поспіху на полі бою. Як правило, це були короткі повідомлення, інструкції або накази, зашифровані кодом на основі 50 величин.

Одним з перших успіхів у розкритті французських шифрів домігся Джордж Сковелл (1774-1861). Він був шефом шифрувальників при командуючому англійською армією герцогу Веллінгтоні. Під час війни з французами в Іспанії (1808-1814) він розвив систему збору розвідінформації, за допомогою якої здійснювалося перехоплення пошти та фронтових повідомлень французів і робилося дешифрування. Англійські дешифрувальники під керівництвом Сковелла досить легко справлялися з цими кодами. Навесні 1811 року французи стали використовувати більш складний код, відомий як код португальської армії, що складався з комбінацій 150 чисел. Сковелл «зламав» цей код за два дні.

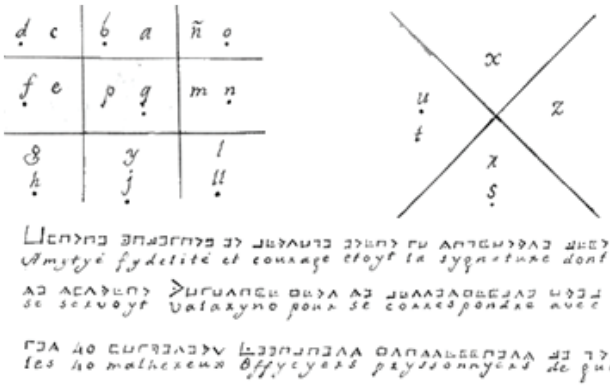
У 1811 році Сковелл одержав книгу «Криптографія або мистецтво розшифровки», написану Девідом Арнольдом Конрадусом. У книзі викладалися правила й принципи створення та «зламування» кодів і шифрів. Вона також описувала осо-

бливості англійських, німецьких, датських, латинських, французьких та італійських шифрів. Експерименти Сковелла з різними методами шифрування та кодування інформації ґрунтувалися на принципах, викладених у цій книзі.

Він придумав принцип, який гарантував нерозкриття загально-британського шифру. За цією системою позначення «56С2» направляло одержувача до 56-ої сторінки певної книги, 3-го стовпчика, 2-го слова знизу. Це був хоча і дуже простий, але досить надійний код. Питання було в тому, як довідатися, у якій саме книзі треба шукати потрібну сторінку. Фактично, це був один із варіантів книжкового шифру.

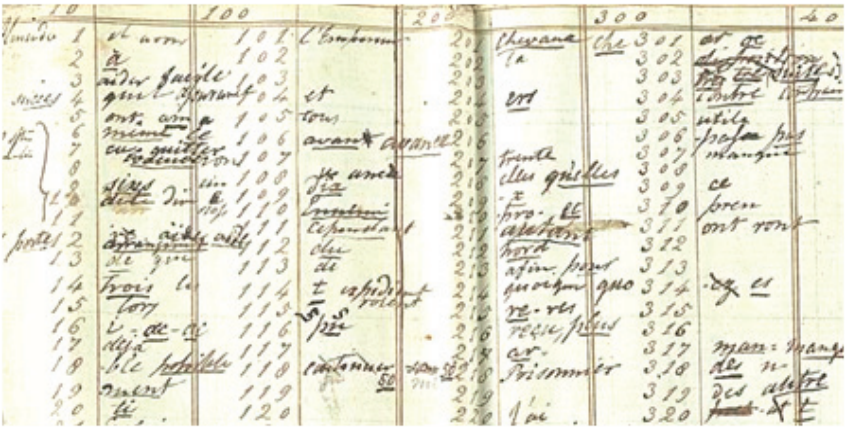

Section I
The General Theory.
Proposition I
Rule 1
Rule 2
Prop. 3
Rule 5

Наприкінці 1811 року нові таблиці кодів були розіслані з Парижа усім провідним французьким військовим. Вони були засновані на дипломатичному коді середини XVIII століття, і в них використовувалося 1400 кодовеличин. Такі таблиці відправлялися разом з інструкціями з їх використання, спрямованими на усунення деяких недоліків у використанні шифрів. Наприклад, наприкінці повідомлення рекомендувалося приписувати цифри – «пустишки», позбавлені всякого змісту. Це було зроблено для того, щоб утруднити роботу дешифрувальника, оскільки була висока ймовірність наявності наприкінці повідомлення стандартних фраз, якими зазвичай закінчувалася кореспонденція (наприклад, звання і прізвище особи, що відправила документ). Знання відкритого та шифрованого текстів, зрозуміло, полегшувало дешифрування.



Протягом наступного року Сковелл вивчав перехоплені документи французів. Він домігся успіху, працюючи з повідомленнями, що містили

незакодовані слова і фрази. Як уже згадувалося, для прискорення процесу французи часто шифрували не все повідомлення, а тільки найбільш таємні його частини. У таких повідомленнях значення зашифрованих уривків тексту ставало зрозумілим із контексту. Інформація про пересування військ, зібрана «армією провідників» Сковелла допомагала ідентифікувати конкретних людей і визначати населені пункти, що згадувалися в зашифрованих листах.



У 1812 році в руках Сковелла з'явився перехоплений лист Жозефа Бонапарта, адресований його брату – Наполеону. Сковеллу вдалося розшифрувати велику частину закодованої інформації, що стосувалася плану військової операції. Це дозволило Веллінгтону підготуватися до битви, від результату якої залежало, чи будуть французи контролювати Іспанію (битва під Вітторіа 21 червня 1813 року). Тієї ж ночі британські загони захопили екіпаж Жозефа та заволоділи копією «Великого» французького шифру. У результаті цей код був розкритий остаточно.

Яскравою фігурою в криптології XIX століття є англієць Чарльз Бебідж (1791-1871), який ще в юності захопився цією наукою. З роками він придбав славу кращого в Англії експерта з тайнопису. До нього зверталися з проханням про дешифрування найрізноманітніших документів, від записок першого британського придворного астронома Дж.Флемстіда та дружини Карла I Генрієти Марії до листів і написів, що фігурували в кримінальних справах. Основну увагу він приділив шифру Віженера, що славився у той час як «абсолютно» стійкий.

Незалежно від інших сучасників, він передбачив ідею Казиського щодо визначення довжини ключового слова-гасла (періоду гами) з наступним повним дешифруванням цього шифру. Він зробив це в середині XIX століття, але вчений світ про успіх Бебіджа довідався тільки в XX столітті, коли дослідники почали розбирати його

великі архіви. Ідеї Бебіджа були повторені Казиським, що описав його у 1863 році.

Бебідж уперше дав чітку математичну формалізацію основних понять криптології. Він запропонував алгоритм розкриття багатоалфавітних шифрів, які до цього часу вважалися такими, що не розкривалися. Йому ж належить одна з ідей розкриття систем з використанням «самоключа» (ключ залежав від відкритого тексту).

Бебідж одним із перших математиків почав застосовувати алгебру в сфері криптології. Алгебраїчне моделювання шифрів і їхній алгебраїчний аналіз допомогли йому проникнути у внутрішній зміст шифрів. Однак зміст його математичних задумів у сфері криптологічного застосування, на жаль, значною мірою втрачено.

У 1822 році Бебідж створив першу обчислювальну машину, здатну робити арифметичні операції з точністю до шостого знака після коми та обчислювати похідні другого порядку. Потім він намагався побудувати більш «просунуту» версію – аналітичну машину. За його задумом, вона повинна була уміти використовувати при обчисленнях результати попередніх операцій, наприклад, повторювати обчислення в циклі. Однак честолюбні плани Бебіджа не збулися, але його внесок у розвиток комп'ютерної техніки величезний.

Бебідж виявився також першим відомим ученим, чий проект натрапив на труднощі фінансування, оскільки у 1842 році англійський уряд припинив його грошову підтримку. А машину Бебіджа все ж таки побудували ентузіасти з Лондонського музею науки. Вона складалася з чотирьох тисяч залізних, бронзових і сталевих деталей та важила три тонни. Правда, користуватися нею дуже важко – при кожному обчисленні доводиться кілька сотень (а то й тисяч) разів крутити ручку автомата.

1854 рік, коли британський вчений Чарльз Уітстон (1802-1875) розробив біграмний шифр «Плейфер» (англ. *playfair* – честна гра), ознаменував новий етап у криптології. Вчений назвав його на честь свого друга барона Лайона Плейфера, який займався його популяризацією. Цей шифр був розроблений спеціально для шифрування телеграфних повідомлень і використовувався як польовий шифр британської армії підчас англо-бурської та Першої світової війни.

Для одержання такого шифру використовувалося полібійський квадрат і ключове слово, наприклад: Playfair. Ключове слово вписувалося в таблицю по рядках, а повторювані букви відкидалися. Таблиця дозаповнювалась буквами, що не увійшли до слова, згідно з латинським алфавітом, у природному порядку:

P	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Якщо букви біграми лежали в одному й тому же рядку або стовпці, то бралися дві букви, розташовані, відповідно, праворуч або внизу (у циклічній послідовності) від букв тексту. Якщо букви не лежали в одному й тому ж рядку або стовпців, то у квадраті уявно будувався прямокутник таким чином, щоб ці дві букви лежали в його протилежних вершинах, а інші дві вершини даного прямокутника давали букви шифротекста.

Якщо біграма складалася з двох однакових букв, то спочатку другу букву в ній заміняли на «X», «Z» або яку-небудь іншу рідкісну букву, після чого зашифровували отриману таким чином нову біграму. В результаті слово «UZHGOROD» перетворюється у шифротекст «VUKHGLTR»:

UZ	HG	OR	OD
VU	KH	GL	TR

Відкриття Уінстона було значимим не тільки саме по собі, але й тому, що привернуло увагу до більш простого шифру Тритемія, який взяли на озброєння англійські військові та використовували його до 20-х років XX століття. Сам же шифр Уітстона був настільки простим та надійним, що продовжував застосовуватися протягом першої половини XX століття у двох світових війнах дипломатичними службами всіх воюючих держав. Особливо ефективним цей шифр був для коротких повідомлень, тому що статистичні особливості мови в ньому чітко проявлялися лише при наявності 30 рядків тексту й більше.

Другий винахід Уітстона полягав у новаторському використанні шифрувальних дисків. Вперше Уітстон продемонстрував свій шифрувальний пристрій на Всесвітній виставці у Парижі у 1876 році. У ньому так само, як і у шифраторі американця Уодсворта, проглядався вплив ідей італійця Альберті. Навіть зовні пристрій нагадував диск Альберті. Зовнішній диск – диск алфавіту відкритого тексту – складався з 27 знаків (26 букв англійського алфавіту і спеціального знака «+», що означав пробіл). Внутрішній алфавіт визначав алфавіт шифрованого тексту та складався зі звичайних 26 букв, розташованих у довільному ключовому порядку. Новизна ідеї була в тому, що алфавіт відкритого тексту містив більшу кількість знаків, ніж алфавіт шифрованого. При дешифруванні в цих умовах з'являлася неоднозначність у визначенні букв переданого відкритого тексту.

Отже, на тій же вісі, що й диски (алфавіти) пристрою, які були з'єднані шес-

тірнями розміром 27х26 відповідно, були розташовані дві стрілки, як у сучасних годинниках. На початку шифрування велика (довга) стрілка вказувала на знак «+» (пробіл). Мала стрілка, пов'язана з великою різьбовою шестірнею, ставилася в те ж положення, тому «годинник» показував «12-00». Набір букв відкритого тексту робився поворотом великої стрілки за напрямком руху. Після такого повороту мала стрілка вказувала знак шифрованого тексту.

Таким чином, при повному повороті великого диска малий диск зміщався на одиницю стосовно вихідного взаємного стану двох дисків, що приводило до зміни алфавіту шифрованого тексту стосовно алфавіту відкритого тексту. По закінченні кожного слова велика стрілка ставала на знак «+», а буква, на яку при цьому вказувала коротка стрілка, записувалася як знак шифрованого тексту. Щоб уникнути неоднозначності розшифрування, подвоєння букв у відкритому тексті не допускалося. Повторну букву необхідно пропустити або ставити замість неї яку-небудь рідкісну букву, наприклад, «*Q*».

Ключем шифру був порядок розташування букв на внутрішньому диску. Приведемо формалізований приклад шифрування на пристрої Уітстона. Випишемо алфавіти в два рядки:

+	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	Q	D	A	S	R	B	U	O	P	V	T	F	X	E	G	Y	C	H	Z	J	K	W	I	M	L	

Слово «*UKRAINE*» шифрується в такий спосіб. Під першою буквою «*U*» стоїть відповідна буква шифротексту «*K*». Друга буква «*K*» міститься від «*U*» на 17 кроків; на цій відстані від букви шифротексту «*K*» знаходиться друга буква шифротексту «*F*». Третя буква «*R*» розташована від «*K*» на 7 кроків; на цій відстані від букви шифротексту «*F*» знаходиться третя буква шифротексту «*Z*» і так далі. Остаточно одержимо шифрований текст «*KFZATYS*». Розшифрування робиться у зворотньому порядку.

Помітимо, що якщо допустити подвоєння букв, наприклад, «*AA*», то шифротекст мав би вигляд «*QD*». Однак такий же шифротекст відповідає і біграмі «*AB*», отже, у цьому випадку розшифрований текст буде неоднозначний.

Однак шифр Уітстона один істотний недолік. Так, якщо в шифротексті і з'являлася подвоєна буква (наприклад, «*BB*»), яка означала, що у відкритому тексті стояли букви, що розташовувалися в алфавіті поруч, але в зворотньому поряд-

ку («*FE*»). Це вже було істотною слабкістю шифру та могло бути ефективно використане при дешифруванні. Винахід Уітстона не знайшов широкого застосування.

Широке використання багатоалфавітних шифрів зупинилося в 1863 році, коли майор пруської армії Фрідріх Вільгельм Казіскі (1805-1881) видав книгу на 95 сторінках «Мистецтво тайнопису та дефишрування» (нім. *Die Geheimschriften und die Dechiffrierkunst*), у якій виклав метод розкриття багатоалфавітного шифру з повторюваним ключовим словом (гаслом), що раніше вважався абсолютно криптостійким. Казіскі запропонував визначати довжину гасла статистично, довівши, що відстані між повтореннями в шифротексті будуть рівні або кратні довжині гасла. Після того, як кількість букв у гаслі була визначена, шифротекст розбивався на відрізки, що дорівнювали довжині гасла, і завдання зводилося до розкриття шифру простої заміни, що не складало особливих труднощів для криптоналітиків того часу.

Основний зміст книги полягав у викладенні методів розкриття шифрів типу шифру Віженера, що іноді називали короткоперіодичними шифрами гамування або лозунговими шифрами гамування. При використанні такого шифру періодично повторювані сполучення букв відкритого тексту, збігаючись з періодичними продовженнями гасла (вихідної гами), породжували збіг сполучення букв у шифрованому тексті. Ці повторення могли бути ефективно використані при дешифруванні.

Наприкінці XIX століття криптологія почала здобувати риси точної науки, а не тільки мистецтва, як це було раніше, її починають вивчати у військових академіях. Тут слід зазначити роль французької військової академії Сен-Сір, де до цього часу був розроблений свій власний військово-польовий шифр, який одержав назву «Лінійка Сен-Сіра». Лінійка являла собою довгий шматок картону з надрукованими на ньому буквами алфавіту. Ця послідовність букв називалася «нерухомою шкалою». Знизу, під нерухомою шкалою, у лінійці були зроблені вирізи, через які легко переміщався «движок» – вузька смужка з картону з нанесеним на нього (з подвійним повторенням) тим же самим алфавітом.

Шифрування здійснювалося таким чином: смужка («движок») переміщалася в положення, коли буква ключа-гасла виявлялася під буквою «А» нерухомої шкали. Утворювалася проста заміна першої букви відкритого тексту (букви «движка» утворювали нижній рядок підстановки-заміни). При шифруванні другої букви відкритого тексту друга буква ключа-гасла шляхом пересування «движка» ставилася під буквою «А» нерухомої шкали тощо. Гасло повторювалося періодично по буквах відкритого тексту.

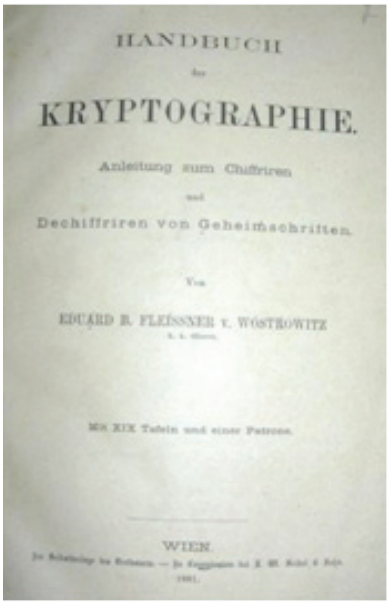
Таким чином, лінійка Сен-Сіра була простим механічним втіленням шифру Віженера. Вона дозволила істотно підвищити ефективність праці шифрувальника, по-

легшити алгоритм реалізації шифру Віженера. Саме в цій механізації процесів шифрування та дешифрування полягає внесок авторів лінійки в практичну криптологію.

Розвитком ідеї лінійки Сен-Сіра стало довільне розташування букв алфавіту на «движку». Секретне (ключове) розташування цих букв істотно підсилило криптостійкість шифру. Однак основна слабкість – короткоперіодичне продовження ключа-гасла збереглося, що й визначило наступні успіхи криптоаналітиків. У завершенні історичного епізоду з лінійкою Сен-Сіра відзначимо, що вона була найпростішою технологічною реалізацією диска Альберті. Реалізація шифру Віженера на рівні картонних смужок значно «дешевша», ніж створення оригінальних пристроїв типу дискового шифратора Альберті. Тому «лінійка» одержала досить широке поширення.

Наприкінці XIX століття прем'єр-міністр Франції Леон Мішель Гамбета (1838-1882) запропонував узагалі відмовитися від застосування приладів шифрування та замінити їх простими алгебраїчними операціями. Букви тексту й гасла замінювалися на числа (відповідно до порядку їхнього розташування в алфавіті), а потім складалися між собою, породжуючи шифрований текст (додавання ведеться за модулем, рівним потужності алфавіту). Іменем Гамбети був названий основний сучасний елемент шифрування – «гама» шифру.

У 1881 році у Відні була видана книга Флейснера (1825-1888) «Керівництво з криптографії» (нім. *Handbuch der Kryptographie*). Автор увійшов в історію криптології як винахідник ще одного шифру перестановки букв – знаменитих «ґрат» (або «просвердлених патронів»). Практично ж ним була розвинута ідея італійця Джироламо Кардано, який у 1556 році першим запропонував використовувати для таємного листування особливі трафарети, у віконця яких вписувалися букви шифру.


HANDBUCH

der

KRYPTOGRAPHIE.

Anleitung zum Chiffriren

und

Dechiffriren von Geheimschriften.

Von

EDUARD B. FLEISSNER v. WOSTROWITZ

Mit XIX Tafeln und einer Patrone.

WIEN.

У 1883 році криптологія одержала нові ідеї, викладені в праці за назвою «Військова криптографія» (фр. *La cryptographie militaire*) обсягом у 64 сторінки. Його автором був Жан Вільгельм Губерт Віктор Франсуа Олександр Огюст Керкхофс Ван Ньювенгоф (1835-1903). Цікаво, що він не був ні військовим, ні професійним шифрувальником, зате він викладав іноземні мови та математику. Спираючись на знання в галузі лінгвістики й математики, автор провів порівняльний

аналіз шифрів, на основі якого сформулював вимоги до шифрів і зробив висновок, що практичний інтерес представляли тільки ті шифри, що залишилися стійкими, навіть, при інтенсивному листуванні.

JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire puissant de la tactique militaire. »

(Général LEWAL, *Études de guerre*.)

I

LA CRYPTOGRAPHIE DANS L'ARMÉE

A. Notions historiques.

La *Cryptographie* ou l'*Art de chiffrer* est une science vieille comme le monde ; confondue à son origine avec la télégraphie militaire, elle a été cultivée, dès la plus haute antiquité, par les Chinois, les Perses, les Carthaginois ; elle a été enseignée dans les écoles tactiques de la Grèce, et tenue en haute estime par les plus illustres généraux romains [1].

Depuis la modeste scytale des Lacédémoniens et les trucs inventés ou rapportés par Æneas-le-Tacticien [2], jusqu'au fameux

[1] Quoi sous la rubrique : Stéganographie, chiffre ou écriture secrète, que certains dictionnaires encyclopédiques donnent les renseignements qui se rapportent à la cryptographie. Les anciens auteurs l'appellent plus ou moins correctement : *ars notarum*, *ars alphabetum*, *polygraphia*, *zootographia*, *cryptologia*, *steganologia*, *cryptomeneutica*, etc. ; les allemands disent aujourd'hui : *Geheimschrift* ou *Chiffreschrift* et les Anglais : *cryptography*.

Своє знайомство з криптологією Керкхофс почав з вивчення телеграфних військово-польових шифрів. Він особливо підкреслював, що на відміну від листування старого часу, телеграф значно збільшив обсяги обміну інформацією. Це породжувало нові вимоги до шифрів. У результаті Керкхофс сформулював загальні вимоги до шифрів, що актуальні й сьогодні:

- простота практичного використання;
- надійність;
- операції шифрування й дешифрування не повинні вимагати значних витрат часу тощо.

«Військова криптографія» уперше була опублікована двома частинами в журнальному варіанті в січні і лютому 1883 року, а пізніше, у тому ж році, була перевидана у вигляді окремої брошури. Керкхоф мав унікальну здатність виділяти головне в будь-якому предметі і всього на 64 сторінках своєї книги зумів знайти відповіді на багато питань, що постали перед криптологією в результаті виникнення нових умов. При цьому запропоновані рішення були розумними і добре обґрунтованими.

Керкхофс підтвердив той принцип, що тільки дешифрувальники могли зі знанням справи визначати надійність шифру. Зрозуміло, про це здогадувалися й до нього. У XVII столітті французький криптоаналітик Россиньоль створив досить стійкий «номенклатор», а в Англії їх складанням займалися винятково дешифрувальники. Але після закриття «чорних кабінетів» у багатьох країнах Європи про цей принцип якось забули.

У всякому разі даний критерій оцінки надійності номенклатора не застосовувався до більш складних шифрів, що пропонувалися в XIX столітті. Їхні винахідники замість того, щоб винести свої шифри на суд криптоаналітиків, які мали великий практичний досвід, прагнули оцінити їхню стійкість самостійно. Вони самовпевнено підраховували, скільки століть піде на випробування всіх ключів, або доводили, що практично неможливо пробитися через який-небудь елемент шифру. Керкхофс вивчив це негативне явище та виніс про нього таке судження:

«Я вражений тим, що наші вчені та професори викладають і рекомендують для

застосування у воєнний час системи, ключі до яких, безсумнівно, менш ніж за годину відкриє найнедосвідченіший криптоаналітик... Можна також думати, що відсутність серйозних робіт з мистецтва прочитання тайнопису сприяла поширенню найбільш помилкових ідей про стійкість наших шифросистем».

Різко виступаючи проти цього, Керкхофс довів, що єдиним засобом освіти в шифрувальній справі є криптоаналіз і що тільки деручись нагору крутою та «тернистою» стежкою криптоаналізу можна одержати щиру уяву про стійкість шифрів. Уся його книга «Військова криптографія» перейнята саме цією ідеєю і тому була фундаментальною роботою з криптоаналізу. У ній Керкхофс довів, що в нових умовах криптоаналіз – єдино вірний засіб щодо іспиту надійності шифрів. Такої думки продовжують дотримуватися і тепер.

Якби Керкхофс на цьому зупинився, то він і тоді б залишив глибокий слід у історії криптоаналізу. Але він зробив ще більше, розробивши криптоаналітичні методи, що грають важливу роль у сучасній теорії дешифрування. Один з них – накладенням або перекриттям – являв собою спосіб дешифрування багатоалфавітних систем заміни. Даний спосіб не ставив ніяких обмежень, потрібно було тільки мати кілька повідомлень, зашифрованих одним і тим ж ключем. Криптоаналітик виписував повідомлення одне під іншим так, щоб букви, зашифровані однією й тією ж буквою ключа, утворювали єдиний стовпчик. Кожен такий стовпчик можна було потім дешифрувати як звичайну одноалфавітну заміну.

Можна вважати, що саме Керкхофс написав основи сучасної криптології, один із головних принципів якої говорить, що стійкість криптосистеми залежить не від процесу шифрування, а від ключа, що використовується. Цей принцип не втратив своєї актуальності й сьогодні. Завдяки працям Керкхофса, у всіх провідних державах світу вже в 80-х роках XIX століття криптологію визнали наукою та в обов'язковому порядку почали викладати у військових академіях.

У 1888 році офіцер французької армії маркіз де Віарі став першим після Бебіджа, який запропонував використовувати алгебраїчні рівняння для опису процесів шифрування, зокрема, шифру Віженера. В одній зі своїх наукових статей, присвячених криптології, він позначив грецькою буквою «Х» будь-яку букву шифрованого тексту, грецькою буквою «Г» будь-яку букву «гами» та малою літерою «с» будь-яку букву відкритого тексту. Він, по суті, довів, що алгебраїчна формула ***X=(c+Г)mod26*** відтворює процес шифрування за системою Віженера при заміні букв алфавіту числами відповідно до наступної таблиці:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Тим самим була закладена алгебраїчна основа для дослідження шифрів заміни типу шифру Віженера. Використовуючи рівняння шифрування, можна було відмови-

тися від громіздкої таблиці Віженера. Пізніше «лозунгова гама» стала довільною послідовністю, а шифр із рівнянням шифрування став називатися шифром «гамування».

Крім того, Віарі сконструював шифрувальний пристрій разом з друкуючим механізмом, який досить простим способом реалізовував приведені вище правила шифрування. Додавання та вирахування здійснювалося простим обертанням дисків з нанесеними на них буквами алфавіту. Таким простим способом реалізовувалися операції в кільці відрахувань за модулем «n». Тим самим був покладений початок механічному, а пізніше й електричному впровадженню процесів шифрування.

Француз Етьєн Базері (1846-1931) на відміну від видатного теоретика криптоаналізу Керкхофса був великим практиком. Шифри буквально «плавилися» під впливом інтенсивної роботи його мозку. Складніші криптограми й урядові шифри, витончене таємне листування змовників – ніщо не витримувало неприборканого напору Базері.

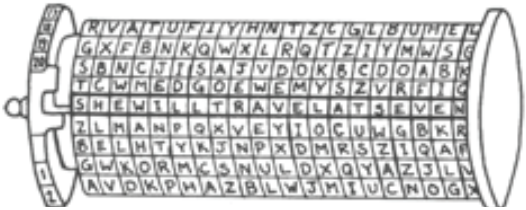
Інтерес до криптоаналізу виник у Базері, коли він намагався прочитати криптограми, що поміщалися в газетах у колонках для особистого листування. Пікантними подробицями цього листування він розважав своїх товаришів по службі. Одного разу, у 1890 році, коли його ескадрон стояв у Нанті, Базері заявив привселюдно своїм друзям офіцерам у штабі корпуса, що відомий йому французький військовий шифр можна читати без ключа. Всі розміялися, за винятком командира корпуса генерала Шарля Фея. Він прийняв кинутий Базері виклик і надіслав йому кілька телеграм, зашифрованих за допомогою цього шифру. Базері успішно їх дешифрував. Усі були здивовані, а Військове міністерство поспішило виготовити новий шифр.

Ознайомившись з криптограмами, «закритими» новим шифром, Базері розкрив його ще до того, як він був введений у дію. Слава Базері досягла Парижа, і в серпні 1891 року армійське командування направило його в розпорядження криптобюро французького МЗС. Саме в ці роки свого життя Базері найбільше часу присвячував криптоаналізу. Тільки нові шифри з'являлися – він відразу розкривав їх.

Цей факт поставив офіційних криптологів Франції в тупик. Почалися болісні пошуки методів шифрування, не пов'язаних з короткоперіодичним гамуванням за шифром Віженера. Основна проблема полягала у виготовленні та розподілі ключової інформації між абонентами мережі засекреченого зв'язку. Базері показав, що обмежений обсяг ключової інформації, що приводив до періодичного повторення гами шифру, дозволяв знайти досить прості методи криптоаналізу.

Здібності Базері в галузі дешифрування були ефективно використані французькими спецслужбами на початку Першої світової війни, коли Базері брав участь у дешифруванні німецьких військових шифрованих телеграм. Сучасники Базері вважали його «Наполеоном» криптоаналізу.

Одним із його винаходів у цьому плані було повторення дискового шифратора американця Джеферсона («циліндр Базері»). Вперше описаний у 1891 році, цей



пристрій складався з декількох дисків (у Базері їх було 20), закріплених на загальній осі. На кожний диск була нанесена своя (причому перемішана) алфавітна послідовність. При шифруванні текст розбивався на групи, довжина яких відповідала числу використовуваних дисків. Кожна група відкритого тексту встановлювалася на циліндрі в ряд (в один рядок), а в якості шифротексту вибирався кожний з інших 25 рядів. Дешифрувальник робив ту ж процедуру, але в зворотньому порядку: на циліндрі по черзі встановлювалася в ряд кожна група шифротексту, після чого проглядалися інші 25 рядів з метою визначити, який з них містить відкритий текст.

Цей тип шифру, який у той час вважався однією з кращих криптосистем, називається мультиплексною системою. Мультиплексна система широко застосовувалася військовими та дипломатичними службами США до, під час і після Другої світової війни. Диски часто заміняли на вузькі металеві пластинки, на кожну з яких була нанесена перемішана алфавітна послідовність, причому двічі циклічно повторена на тій же самій пластинці.

Маркіз де Віарі, супротивник ідей Базері, довів принципову можливість розкриття шифру Базері (при наявності в супротивника цього циліндра та незнання ним тільки разового ключа-порядку розташування дисків на вісі). Дешифрування полегшувалося невипадковим характером розташування букв на дисках, в основі якого лежали фрази типу: «Бог зберігає Францію», «Честь і Батьківщина» тощо. Військове міністерство відмовилося прийняти на озброєння винахід Базері, хоча аналогічний пристрій на початку 20-х років XX століття використовувала армія США.

Незважаючи на неуспіх свого винаходу Базері не зупинився. Він запропонував ще один військовий шифр, для реалізації якого потрібні були тільки папір і олівець. В основу шифру була покладена проста (одноалфавітна) заміна, змінювана з кожним новим повідомленням, і перестановка. Букви замінялися на числа (*A = 0, B = 1* тощо). Разовим ключем були дві букви, числові позначення яких записувалися прописом. Наприклад, ключ «*SG*» у числовому вигляді був «186» (*S=18, G=6*), і відповідний запис-ключ (гасло) був «*ONEHUNDREDEIGHTYSIX*». З цього гасла уже відомим способом породжувалася послідовність букв шифралфавіту: *ONEHUDRIGTYSXABCFJKLMPQVWZ*.

Після заміни за цим алфавітом (*A = O, B = N, C = E ... Z = Z*) отриманий текст поділявся на тризначні групи, та ці групи переставлялися між собою за ключем перестановки. У шифротекст вставлялися «пустишки» на заздалегідь обговорених «ключових» місцях. Однак і ця пропозиція Базері була відкинута під тим приводом, що даний шифр «не дає достатніх гарантій безпеки».

Коли начальник Генерального штабу особисто попросив Базері допомогти в прочитанні шифрованих повідомлень для вивчення військових кампаній Людовика XIV, він почав займатися шифрами минулих епох. Базері блискуче справився з поставленим завданням, але на цьому не зупинився: йому вдалося розкрити номенклатори Франциска I, Франциска II, Генріха IV, Мірабо і Наполеона. Виявивши, що шифри французького військового генія XIX століття були надзвичайно слабкими, у заголовку своєї монографії про них Базері презирливо поставив слово «шифри» у лапки. А в 1892 році, коли французька влада заарештувала та осудила групу анархістів, у числі незаперечних доказів фігурували й дешифровані Базері криптограми.

У 1899 році, навіть після того, як Базері офіційно вийшов у відставку, МЗС Франції продовжувало користуватися його послугами. У тому ж році воно рекомендувало його поліції як людину, що може прочитати шифровані повідомлення, захоплені у змовників-монархистів. Завдяки серії правильних здогадів у відношенні ймовірних слів Базері зрештою дешифрував ці повідомлення. Про них Базері пізніше дав показання на судовому процесі у справі змовників. Помер Базері в 1931 році у віці 85 років.

Наприкінці XIX століття француз Фелікс Марі Деластеле (1840–1902), який ніколи не працював криптологом, а лише захоплювався цією наукою, ускладнив шифр Уітстона «Playfair». Він написав книгу «Основи криптографії» (фр. *Traité Élémentaire de Cryptographie*) на 150 сторінках, у якій систематизував і надав роз'яснення основам важливіших криптометодів. Це дослідження дозволило йому створити у 1895 році одноалфавітний шифр «Біфід» (англ. *Bifid*) з використанням будь-якого пароля та процедури дроблення. При застосуванні цього шифру спочатку в таблицю вписувався по рядках пароль (наприклад, «Ukraine»), а потім вписувався алфавіт за правилами шифрувальної таблиці «*Playfair*». В результаті отримаємо нижченаведену шифротаблицю, де букві «*A*» відповідає координата 14, букві «*B*» – 23, букві «*C*» – 24 тощо.

	1	**2**	**3**	**4**	**5**
1	U	K	R	A	I
2	N	E	B	C	D
3	F	G	H	L	M
4	O	P	Q	S	T
5	V	W	X	Y	Z

Далі, у процесі шифрування під кожною буквою відкритого тексту у стовпчик записувалися її табличні координати – номер рядка і, нижче, номер стовпця, а потім виписувалася цифрова послідовність у один рядок. Цей цифровий рядок переводився за допомогою тієї ж таблиці назад у буквену форму, тобто 15 – буква «*I*», 33 – буква «*H*», 41 – буква «*O*» тощо. При такому шифруванні координати рядка й стовпця кожної букви виявлялися роз'єднаними, що було характерно саме для

шифру, який забезпечував процедуру дроблення.

Відкритий текст	UZHGOROD
Відповідний рядок	15334142
Відповідний стовпець	15321315
Цифрова послідовність	1533414215321315
Шифротекст	IHOPIGRI

Також Деластеле створив одноалфавітний шифр «Тріфід» (англ. *Trifid*), де букви позначалися вже трьома цифрами. При застосуванні цього шифру складалися три шифрувальні таблиці, куди вписувався один алфавіт у довільному порядку.

	1				2				3			
	1	2	3		1	2	3		1	2	3
1	F	J	O	1	V	Z	L	1	E	U	Q
2	R	X	C	2	G	D	P	2	N	H	A
3	Y	B	S	3	M	W	T	3	_	K	I

В результаті цифрові позначення букв алфавіту ставали такими:

A	B	C	D	E	F	G	H	I	J	K	L	M
332	123	132	222	311	111	212	322	333	121	323	231	213

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
312	131	232	331	112	133	233	321	211	223	122	113	221	313

Далі, у процесі шифрування під кожною буквою відкритого тексту у стовпчик записувалися її цифрові координати, а потім виписувалася цифрова послідовність у один рядок. Цей цифровий рядок переводився за допомогою тієї ж таблиці назад у буквену форму.

Відкритий текст	UZHGOROD
Перша цифра	32321112
Друга цифра	22213132
Третя цифра	11221212
Цифрова послідовність	323211122221313211221212
Шифротекст	KVXZ_VZG

Крім того, у 1901 році Деластеле створив 4-квадратний біграмний шифр з використанням 2-х ключових слів. Шифр складався з 4-х таблиць: у ліву верхню та праву нижню вписувався алфавіт у природному порядку, а у ліву нижню та праву верхню вписувалися спочатку ключові слова, а потім – алфавіт. У разі використання паролей

«*Ukraine*» і «*Playfair*» шифрувальні таблиці виглядають таким чином:

A	B	C	D	E		U	K	R	A	I
F	G	H	I,J	K		N	E	B	C	D
L	M	N	O	P		F	G	H	L	M
Q	R	S	T	U		O	P	Q	S	T
V	W	X	Y	Z		V	W	X	Y	Z
P	L	A	Y	F		A	B	C	D	E
I	R	B	C	D		F	G	H	I,J	K
E	G	H	K	M		L	M	N	O	P
N	O	Q	S	T		Q	R	S	T	U
U	V	W	X	Z		V	W	X	Y	Z

При шифруванні відкритий текст розбивався на біграми, букви яких шукалися у таблицях, де не було ключових слів. Перша буква біграми шукалася у лівій верхній таблиці, а друга – у правій нижній. В залежності від їх розташування у клітинах таблиць між усіма таблицями уявно будувався прямокутник таким чином, щоб ці дві букви лежали в його протилежних вершинах, а інші дві вершини даного прямокутника давали в таблицях з ключовими словами букви шифротекста. В результаті шифрування слово «*UZHGOROD*» перетворюється у шифротекст «*TZEBGSLY*»:

UZ	HG	OR	OD
TZ	EB	GS	LY

В цілому, у другій половині XIX століття застосування криптології стало посправжньому масовим. При цьому до нових шифросистем пред'являлися більші вимоги щодо стійкості та одночасно простоти й можливості масового використання. В Англії й США з'явилися, навіть, спеціальні періодичні видання з криптології, почали виходити спеціальні праці, присвячені різним аспектам цієї науки. У той час були закладені основні принципи криптології, що визначили її розвиток у період першої половини XX століття.

Не стояла осторонь і художня література. Так, у 1843 році з'явилася розповідь американського письменника Едгара По «Золотий жук», де найдокладнішим чином був викладений метод дешифрування простих шифрів заміни. Це був перший загальнодоступний «курс» з криптоаналізу, що мав небачену популярність в усьому світі.

Саме ця розповідь підштовхнула письменника-початківця Жюля Верна до написання його не менш знаменитих романів. У 1864 році в книзі «Подорож до центру Землі» фантаст пояснив найпростішу шифросистему перестановки букв. У 1880 році в романі «Жангада» він виклав «шифр Гронсфельда», а в 1885 році в іншій книзі «Матіас Шандор» описав «ґрати Флейснера». Зазначимо, що відо-

ма розповідь класика детективного жанру Конан Дойля «Танцюючі чоловічки» з'явилася набагато пізніше – тільки в 1905 році.

1.5. Британські криптослужби

5 серпня 1914 року, в один із початкових днів Першої світової війни, глава англійської військово-морської розвідки контр-адмірал Генрі Олівер попросив Альфреда Юінга (Евінга) (1855-1935), який займався в Адміралтействі питаннями військово-морської підготовки, зайнятися дешифруванням німецьких перехоплених повідомлень. У той час в Адміралтействі у великій кількості накопичилися шифровані німецькі радіограми, перехоплені військово-морськими та комерційними радіостанціями. Юінг виявив велику зацікавленість і попросив якомога швидше продемонструвати йому ворожі шифровки. Зрозумівши, що їхнє читання могло б мати величезне значення для перемоги над ворогом, Юінг попросив саме йому довірити вирішення цього складного завдання.

У 1914 році Юінгу виповнилося 59 років. Три роки тому він одержав дворянський титул за видатний внесок у науку та заслуги перед суспільством, серед яких особливо був відзначений його плідний посібник з військово-морської підготовки. І ось тепер, незважаючи на похилий вік, Юінг задумав заснувати криптоаналітичне бюро, якому було необхідно зробити безпосередній та дуже відчутний вплив на хід світової історії.

Юінг розпочав з ретельного вивчення криптологічних матеріалів, що знаходилися в книгосховищах бібліотеки Британського музею. Потім він перейшов до вивчення кодів на міському Центральному поштамті, де зберігалися примірники комерційних кодових книг. Одночасно Юінг залучив до своєї діяльності чотирьох викладачів військово-морських коледжів. Усі вони були його друзями, добре знали німецьку мову і, зібравшись разом за столом у кабінеті Юінга, вивчали незрозумілі рядки з букв і цифр, маючи лише загальну уяву про те, з чого треба починати роботу, пов'язану з розкриттям шифрів.

Серед перших перехоплених німецьких повідомлень було одне, яке, якби його вдалося розгадати, відразу могло направити плин війни зовсім в інше русло. Воно знаходилося в першій партії телеграм, показаних Олівером Юінгу 5 серпня. Це повідомлення було складено головним командуванням Військово-морських сил Німеччини 4 серпня вночі та негайно передано командуючому в Середземне море адміралу Вільгельму Сушону. У повідомленні говорилося: «3 серпня уклали угоду про союз із Туреччиною. Негайно випливайте в Константинополь». На важкому крейсері «Гебен» у супроводі легкого крейсера «Бреслау» Сушон вирушив із центральної частини Середземномор'я на схід.

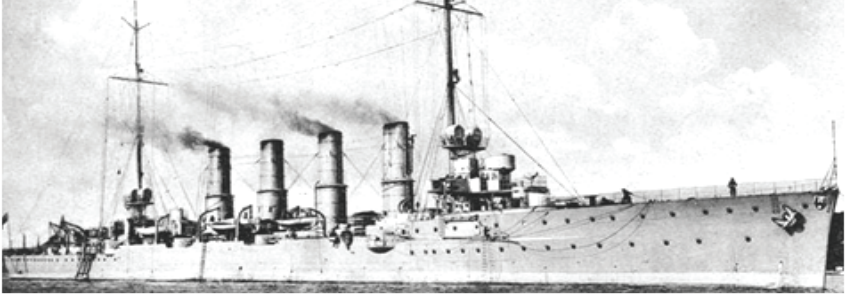
Англійська ж середземноморська ескадра, будучи абсолютно впевнена, що Сушон спробує прорватися через Гібралтарську протоку, ретельно борознила море на захід від Сицилії. Коли англійський крейсер нарешті знайшов Сушона,

який плив курсом на схід, англійці почали запеклу спробу наздогнати та знищити «Гебен» і «Бреслау». Однак ті все-таки зуміли вислизнути, загубившись серед грецьких островів, У неділю 10 серпня «Гебен» увійшов у Дарданелли та здійснив могутній артилерійський обстріл російських портів на Чорноморському узбережжі. Якби англійське Адміралтейство змогло прочитати передані з Берліна шифровані накази Сушону, Англія, скоріше за все, виграла б фатальну гру в схованки з «Гебеном» і «Бреслау».

Про цю втрачену можливість вплинути на хід війни в самому її початку Юінг так ніколи й не довідався. До цього часу ним були вивчені лише коди декількох німецьких комерційних фірм. Не набагато більш корисною стала шифрувальна «Книга торгового судноплавства» (нім. *Handelsverkehrsbuch*, *HVB*) з кодами, що використовувалися німецьким флотом, для спілкування з його торговими судами та була знайдена австралійцями 1 серпня 1914 року на німецько-австралійському пароплаві «Хобарт» біля Мельбурну. Цю книгу англійці отримали лише у жовтні, однак ніхто з невеликої групи перших англійських дешифрувальників не міг похвалитися ґрунтовними знаннями в сфері криптоаналізу, і тому в перші тижні війни їхні успіхи були мізерно малі.

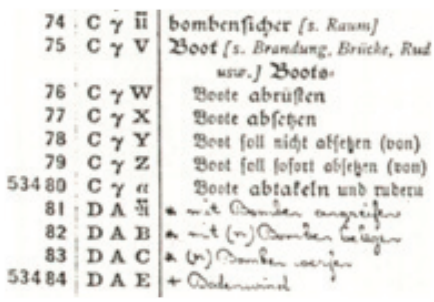
У вересні 1914 року Англії випав шанс, який дав такий могутній поштовх її зусиллям з організації криптоаналізу перехоплених криптограм супротивника, що протягом усього періоду війни вона набагато випереджала своїх супротивників у дешифруванні. Про те, що відбулося, найкраще розповів у своїх мемуарах Черчилль:

«На початку вересня 1914 р. на Балтійському морі був потоплений німецький легкий крейсер «Магдебург». Кілька годин потому росіяни виловили з води тіло затонулого німецького молодшого офіцера. Закостенілими руками мерця він притискав до грудей кодові книги ВМС Німеччини, а також розбиті на дрібні квадрати карти Північного моря та Гельголандської бухти. 6 вересня до мене з візитом прибув росій-



ський військово-морський аташе. З Петрограда він одержав повідомлення з викладом про те, що трапилося. Воно стверджувало, що за допомогою кодових книг російське Адміралтейство в змозі дешифрувати щонайменше окремі ділянки німецьких військово-морських шифротелеграм. Росіяни вважали, що Адміралтейству Англії, провідної морської держави, варто було б мати ці книги й карти. І якби ми надіслали корабель, то російські офіцери, у яких знаходилися книги, доставили б їх до Англії. Ми негайно відправили такий корабель, і жовтневим вечором принц Луї та я одержали з рук наших вірних союзників трохи зіпсовані морем безцінні документи».

Це відбулося 13 жовтня. Але навіть несподівана удача з отриманням «Книги сигналів імператорського флота» (нім. *Signalbuch der Kaiserlich Marine, SKM*) не дала групі Юінга можливості негайно приступити до читання німецьких військово-морських шифроповідомлень, тому що в них напряму не використовувалися кодові позначення з цих книг. Читання почалося тільки тоді, коли офіцер англійської інтендантської служби Чарльз Ротер, провідний експерт з Німеччини, знайшов, що кодові групи додатково перешифровувалися досить простим алгоритмом. Розкриття такого перешифрування не було занадто важкою проблемою, якщо в розпорядженні криптоаналітика була кодова книга. Як і у звичайному відкритому тексті, окремі кодові позначення повторювалися частіше, ніж інші. У таких сполученнях букви одного кодового позначення повторюються в інших кодових позначеннях, але в іншому розташуванні. Самим кодовим позначенням була притаманна визначена структурна система: у випадку з німецьким військово-морським кодом, отриманим англійцями від росіян, приголосні чергувалися з голосними. Коли характерні риси коду ставали відомими, умілий криптоаналітик міг ефективно використовувати їх для зняття перешифрування.


74 C γ ii bombenſicher [ſ. Raum]
75 C γ V Boot [ſ. Brandung, Brücke, Rud
wesr.] Boote
76 C γ W Boote abrüſten
77 C γ X Boote abſetzen
78 C γ Y Boot ſoll nicht abſetzen (von)
79 C γ Z Boot ſoll ſofort abſetzen (vom)
534 80 C γ α Boote abtakeln und rudern
81 D A ii
82 D A B
83 D A C
534 84 D A E

Але англійські криптоаналітики були ще настільки недосвідченими, що їм знадобилися майже три тижні, щоб почати читати окремі ділянки деяких німецьких військово-морських повідомлень. Ці повідомлення, за ствердженням Черчилля, «мали, головним чином, характер поточного службового листування: «У 8 годин вечора один із наших торпедних катерів виходить у квадрат 7» і т.д. Однак скрупульозне нагромадження цих уривчастих даних складало основу інформації, за якою з достатнім ступенем точності можна було визначати характер військових готувань супротивника у Гельголандській бухті, що прилягає до північно-західного узбережжя Німеччини».

У жовтні 1914 року кількість співробітників групи Юінга зросла настільки, що їм

стало тісно в службовому кабінеті свого начальника. Їх постійно дратувало, що доводилося відкладати роботу, коли Юінг приймав відвідувачів з питань військово-морської підготовки. Тому приблизно в середині листопада вся криптоаналітична група перебралася у велику кімнату за № 40, розташовану в старому будинку Адміралтейства. До кімнати прилягало маленьке приміщення, у якому знаходилося похідне ліжко для відпочинку. Розташовувалася кімната № 40 дуже вдало: вона знаходилася близько до оперативного відділу, який одержував від групи Юінга дешифровані радіограми супротивника, та осторонь від інших приміщень Адміралтейства. І хоча група стала офіційно іменуватися 25-м підрозділом Управління військово-морської розвідки «*NID-25*» (англ. *Naval Intelligence, Division 25*), назва «кімната сорок» (англ. *Room 40*) виявилася настільки зручною і нейтральною, що незабаром стала загальноприйнятою назвою цього підрозділу. Ця назва збереглася й тоді, коли відділення перевели в інше, більш просторе приміщення.

У листопаді 1914 року англійський траулер виловив важку шухляду, де були виявлені різні книги та документи німецькою мовою. Шухляда була викинута за борт з німецького есмінця «*S119*», що був потоплений в результаті морської битви біля острова Тексел. Серед іншого в шухляді знаходилася німецька шифрувальна «Книга судоходства» (нім. *Verkehrsbuch, VB*), якої бракувало в магдебурзькій знахідці. Криптоаналітики «кімнати 40» негайно використали її для читання повідомлень, які передавав німецький крейсер, що перешкоджав англійському судноплавству. Ідентичний код використовувався для засекречування телеграфного листування між Берліном і німецькими військово-морськими аташе за кордоном, однак про це в «кімнаті 40» довідалися тільки через декілька місяців.

У січні 1915 року дешифрувальники «кімнати 40» «розкрили» дуже важливе німецьке повідомлення, що було передане по радіо та зашифроване військово-морським кодом. Вони дізнались, що німецькі кораблі , які обстрілювали населені пункти на берегах Англії, планують 16 січня зібратися на Догер-банці, мілководій ділянці Північного моря на північ від узбережжя Англії. В результаті англійський флот у запеклій битві був потоплений німецький корабель «Блюхер», а кораблі «Дерфлінгер» і «Зейдліц» були пошкоджені.

У 1916 році Німеччина зробила ставку на ведення підводної війни, тому англійська радіорозвідка виявляла підвищений інтерес до радіоповідомлень німецьких підводних човнів. Спробуючи отримати будь-яку інформацію щодо апаратури зв'язку, встановленої на субмаринах супротивника, Адміралтейство обзавелося судном з водолазом, оснащеним спеціальним обладнанням для обстеження затонувлих підводних човнів. Робота була доручена молодому інструктору з водолазної справи Міллеру.

Незважаючи найнеприємніші боки своєї праці, Міллеру майже кожного разу

вдавалося відшукати стандартну залізну шухляду, знайому йому ще з найпершого занурення. На одному з німецьких підводних човнів, внутрішній пристрій яких Міллер знав як свої п'ять пальців, він знайшов зовсім новий військово-морський код, у якому криптоаналітики «кімнати 40» мали гостру потребу. Ця знахідка Міллера надала їм істотну допомогу в дешифруванні перехопленого шифролистування субмарин супротивника, яке постійно збільшувалося.

Зі зростанням обсягу шифролистування супротивника «кімната 40» перестала просто направляти відредаговані матеріали радіоперехоплення оперативному управлінню Адміралтейства, а стала посилати туди щоденні відомості, які включали криптоаналітичну, пеленгаційну та іншу радіорозвідувальну інформацію. Після війни було підраховано, що з жовтня 1914 по лютий 1919 років «кімнатою 40» було перехоплено та дешифровано більше 15 000 німецьких шифроповідомлень.

Робота велася цілодобово, навіть під час бомбардувань, коли з метою світломаскування вікна засмикували добре підігнаними непроникними шторами. Штат співробітників «кімнати 40» постійно збільшувався за рахунок поранених офіцерів і студентів німецьких університетів, які з початком світової війни повернулися до Англії. Останнім присвоювалося офіцерське звання в добровольчому резерві англійських ВМС для того, щоб вони могли носити форму для уникнення «косих» поглядів цивільного населення. На роботу в «кімнату 40» були також прийняті жінки, що звільнили криптоаналітиків від канцелярської роботи.

Найбільш важлива зміна в штаті співробітників «кімнати 40» відбулася у зв'язку з відставкою Юінга, якому в травні 1916 року запропонували посаду ректора Единбургського університету. Пропозиція була дуже привабливою, особливо, для Юінга, який протягом 25 років з успіхом займався лише науковою діяльністю, перш ніж у 1903 році перейшов до Адміралтейства. Крім того, до цього часу Юінг уже не брав активну участь безпосередньо в дешифрувальній роботі, оскільки в «кімнаті 40» з'явилися співробітники, чиї криптоаналітичні здібності набагато перевершували його власні. А Юінг перетворився у звичайного адміністратора.

Керівництво Адміралтейства заявило Юінгу, що не заперечує щодо його переходу, оскільки він настільки добре організував роботу довіреного йому колективу, що міг без усякого збитку справі передати свої повноваження іншій особі. Тому Юінг прийняв пропозицію з Единбурга, і з 1 жовтня 1916 року «кімнатою 40» почав керувати особисто директор військово-морської розвідки (англ. *Naval Intelligence Division, NID*) капітан Вільям Реджинальд Холл (1870-1943).

17 січня 1917 року сталася дуже важлива подія в історії криптоаналізу: «кімната 40» частково прочитала перехоплену німецьку шифротелеграму, яка містила унікальну інформацію, що при умілому використанні могла істотно вплинути на результат Першої світової війни. Шифротелеграма була дуже довгою та склада-

лася приблизно з тисячі цифрових кодових груп. Вона була надіслана з Берліна, датована 16 січня та адресована німецькому послу в США Іоганну Берншторфу.

Її відкритий текст був закодований за допомогою дипломатичного коду, відомого англійським криптоаналітикам як код «0075». Над ним у «кімнаті 40» працювали протягом останніх шести місяців. Допоміг їм у цьому чеський інженер О.Сцек, що під час Першої світової війни працював на радіостанції в Брюсселі та викрав звідти німецький дипломатичний код, яким була зашифрована телеграма німецькому послу в США.

Там знали, що код «0075» належав до серії неалфавітних кодів, які німецьке МЗС позначало чотиризначним числом, яке складалося з двох нулів і двох ненульових цифр, причому різниця між відмінними від нуля цифрами завжди дорівнювала двом. У список аналогічних кодів, що на той час уже були розкриті в «кімнаті 40», входили коди «0097» і «0086», які застосовувалися дипломатичними місіями Німеччини в Південній Америці, код «0064», який використовувався, наприклад, для зв'язку між Берліном і Мадридом, а також коди «0053 » і «0042».

МЗС Німеччини вперше направило код «0075» своїм місіям у Берні, Бухаресті, Відні, Гаазі, Константинополі, Копенгагені, Осло, Софії та Стокгольмі в липні 1916 року. У листопаді «кімната 40» почала здійснювати перехоплення зашифрованих тим же кодом телеграм, спрямованих посольству Німеччини в Сполучених Штатах. У результаті англійці нагромадили достатню кількість копій німецьких телеграм, засекречених за допомогою коду «0075», що дало «кімнаті 40» можливість просунутися в роботі над його розкриттям. Пізніше, наявність двох копій однієї і тієї ж шифротелеграми Циммермана допомогла уникнути перекручувань у криптоаналітичній роботі, у результаті якої вона була розкрита.

WESTERN UNION

TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310

18147 18222 21560 10247 11518 23677 13605 3494 14936

98092 5905 11311 10392 10371 0302 21290 5161 39695

23571 17504 11269 18276 18101 0317 0228 17694 4473

13284 22200 19452 21589 67893 5569 13918 8958 12137

1333 4725 4458 5905 17166 13851 4458 17149 14471 6706

Шифротелеграма від 16 січня 1917 року складалася з двох частин і була підписана міністром закордонних справ Німеччини Артуром Циммерманом:

«Абсолютно секретно. Для особистої інформації вашого превосходительства і для передачі надійним шляхом імперському посланцеві в Мехіко... З 1 лютого ми маємо намір почати необмежену підводну війну. Незважаючи на це, ми повинні прикласти зусилля для того, щоб Сполучені Штати Америки залишалися нейтральними. У випадку, якщо домогтися цього виявиться неможливим, ми зробимо пропозицію Мексиці про укладення союзу на наступних умовах: спільне ведення війни, спільне укладення миру, щедра фінансова підтримка і розуміння з нашого боку того, що Мексика повинна одержати назад утрачені території в Техасі, Нью-Мексико й Аризоні. Докладна розробка даної угоди доручається вам.

Ви секретно інформуєте президента про вищевикладене, як тільки буде визначений початок війни зі Сполученими Штатами Америки, і доповните цю інформацію пропозицією про те, щоб він за власною ініціативою запросив Японію невідкладно приєднатися до угоди й у той же самий час виступив як посередник між Японією і нами.

Зверніть увагу президента на те, що рішуче використання наших підводних човнів протягом декількох місяців змусить Англію укласти мир. Циммерман».

Ця шифротелеграма була направлена німецькому посланцеві в Мексиці Генріху Екардту через Вашингтон для надійності по двох каналах зв'язку. Однак обидва вони контролювалися англійцями.

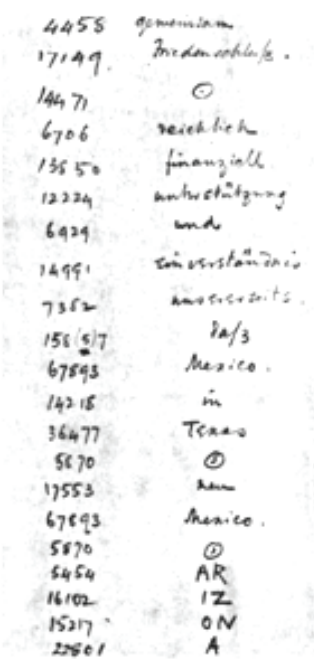
Один маршрут англійці називали «шведським обхідним шляхом». Швеція, що формально була нейтральною, але фактично орієнтувалася на німців, із самого початку війни допомагала МЗС Німеччини в подоланні англійської блокади, направляючи німецькі телеграми під виглядом своїх власних. Однак англійці розкрили цей обман. Тому, коли влітку 1915 року Швеція офіційно висловила своє невдоволення тим, що Англія необґрунтовано затримує її телеграми, англійці натякнули шведам, що їм відомо про вищезазначену діяльність Швеції, не сумісною з її статусом нейтральної країни. У відповідь шведський уряд пообіцяв, що надалі не буде направляти ні однієї німецької телеграми до Вашингтона, після чого став відправляти їх до Буенос-Айреса. Там шведи передавали отримані телеграми в руки німців, і тільки потім вони попадали до німецького посольства у Вашингтоні. Це й був «шведський манівець».

Кабель зі Стокгольма до Південної Америки проходив через Лондон. Німці справедливо побоювалися, що англійська цензура може впізнати німецькі кодові групи у шведських телеграмах. Тому МЗС Німеччини ховав ці кодові групи шляхом їхнього перешифрування. Перешифрування накладалося на німецькі телеграми, що відправлялися через Стокгольм у Південну Америку, після їхнього зашифрування кодом «13 040». На жаль, для німців, перешифрування не ховало всіх слідів коду «13 040», що викликало підозру в криптоаналітиків «кімнати 40».

Вони зняли перешифрування та побачили код «13 040», після чого уважно придивилися й до інших офіційних шведських телеграм. Багато з них після перевірки також виявилися німецькими. Наприклад, під одним перешифруванням англійці знайшли код «0075». Але цього разу Англія не заявила протест Швеції. «Кімната 40» була переконана, що вигідніше було знати зміст листування німецьких дипломатів, ніж перешкодити їм це робити.

Ідея другого маршруту, який Циммерман використав для передачі своєї шифротелеграми до Вашингтона, зародилася в Едварда Хауза, близького друга президента США Томаса Вудро Вільсона. У 1915 році під час одного зі своїх відвідувань Європи Хауз улаштував так, що всі кодовані повідомлення з американських посольств стали надходити безпосередньо на його адресу, минаючи Держдепартамент США. Коли 27 грудня 1916 року німецький посол у Вашингтоні Берншторф обговорював з Хаузом нову мирну ініціативу Вільсона, він підкреслив, що її шанси на успіх значно зростуть, якщо уряд Німеччини зможе зв'язуватися через Хауза безпосередньо зі своїм послом у Сполучених Штатах. Хауз доповів про це президенту. Наступного дня Вільсон дозволив німецькому уряду, використовуючи власний код, передавати телеграми між Берліном і Вашингтоном під американським дипломатичним прикриттям.

Шифротелеграма Циммермана була доставлена до посольства США в Берліні 16 січня о третій годині дня. Однак її не можна було направити безпосередньо до Вашингтона. Тому спочатку її відіслали до Копенгагена, а потім до Лондона. І лише звідти вона могла бути направлена до Вашингтона. В результаті Англія перехопила й другий примірник шифротелеграми Цимермана. У «кімнаті 40» украй здивувалися, побачивши німецький код у американській телеграмі, що прийшла з Копенгагена. Впродовж місяця англійці розкрили код та прочитали шифротелеграму



22 лютого 1917 року МЗС Англії довело відкритий текст шифротелеграми Цимермана до американського посла в Лондоні. 24 лютого вона була передана в Держдепартамент США, а 1 березня опублікована на перших шпальтах ранкових газет під величезними заголовками. Цікаво, що проблема вірогідності опублікованого тексту шифротелеграми, що так турбувала англо-американських офіційних осіб, була усунута самим Циммерманом. Зовсім зненацька він зізнався: «Я не можу заперечувати цього. Це правда». Від поінформованості в існуванні змови

завзято відмовлялись і мексиканці, і японці. Тому донині незрозуміло, чому Циммерман зізнався. Однак незалежно від мотивів, якими він керувався, його визнання поховало останні сумніви в тому, що повідомлення про німецьку змову проти США могло бути обманом.

2 квітня 1917 року Президент США Вільсон заявив, що «справедливість дорожче миру», і звернувся до Конгресу з закликом будь-якими засобами домогтися торжества справедливості. У своєму виступі перед Конгресом він послався на шифротелеграму Циммермана:

«Про те, що німецький уряд має намір нацькувати на нас ворогів біля самого нашого порога, красномовно свідчить перехоплена телеграма, адресована німецькому посланцю в Мехіко. Ми приймаємо цей ворожий виклик... Я рекомендую Конгресу оголосити, що курс імперського уряду Німеччини, який проводився ним останнім часом, в дійсності є не чим іншим, як справжньою війною проти уряду й народу Сполучених Штатів, і офіційно проголосити статус воюючої сторони, що був нам нав'язаний у такий спосіб».

Конгрес задовольнив прохання свого президента. Так прочитання дипломатичної шифротелеграми Німеччини допомогло підштовхнути Сполучені Штати до вступу в Першу світову війну, що дало Англії й Франції змогу здобути перемогу над ворогом і зайняти командні висоти в післявоєнному світі. Ніяка інша криптоаналітична розробка не мала таких величезних наслідків. Ніколи, ні до цього, ні після, не було ще випадку, щоб наслідком дешифрування одного лише таємного повідомлення стало так багато важливих подій, що вплинули на весь подальший хід світової історії.

Крім того, у зв'язку з розвитком у той час дротового телеграфного та телефонного зв'язку виникло завдання ефективного «зняття» інформації з ліній зв'язку. Справа полягала в тому, що безпосереднє «гальванічне» підключення до лінії не завжди можна було реалізувати таємно. Тому у 1915 році англійський капітан Р.Стенлі (у минулому професор Белфастського університету) створив апарат, що дозволяв індуктивним способом перехоплювати інформацію з дротів із відстані до 100 метрів від них. Незабаром удалося створити приймач, який «знімав» цю інформацію з відста-

е аналогічні апарати були сконструйовані й у Німеччині.

ож працювали над розробленням ручних шифраторів. Так, на початку Першої світової війни Дж. Сент-Вінсент Плетс з британської секції перехоплення та дешифрування Директорату військової розвідки «*MI-1*» (англ. *Military Intelligence, Section 1*) придумав дисковий криптопристрій, пізніше названий шифратором Плетса. Освіта і досвід Плетса, який до вступу на службу до військової розвідки був інженером, дозволили йому ство-

рити поліпшений варіант шифратора Уітстона. Британська влада сподівалася використати адаптований шифратор Плеттса в якості польового шифру на останніх етапах війни.

Шифратор Плетса складався з двох латунних дисків. Зовнішній диск - статор - був нерухомим, а внутрішній - ротор - рухомим. Вони з'єднувалися ексцентриком, що обертався на стержні. Білі кола на обох дисках ділилися на сектори (26 на роторі і 27 на статорі), в які можна було записати алфавіти; додатковий сектор на статорі призначався для пропуску. Поверх статора і ротора розташовувалося ручка, в отворі якої можна було поєднати дві букви.

Кожен поворот ручки та ексцентрика призводив до пересування ротора на одну букву відносно статора, забезпечуючи тим самим можливість виконання багатоалфавітної заміни. На статорі шукалася буква відкритого тексту. Потім обертанням ручки ця буква виставлялася в її отворі, а з ротора зчитувалася буква шифротексту. Щоб здійснити шифрування, користувач повинен був скористатися ключовим словом і заздалегідь обумовити початкове положення шифратора і напрям обертання ручки (наприклад, за годинниковою стрілкою). Адресат, який мав аналогічний шифратор, розпочинав із заданої відправної точки і, рухаючись в зворотному порядку, відновлював початковий відкритий текст.

Британська влада передала винахід Плетса для перевірки американським криптоаналітикам. Уільям Фридман, якому допомагала його дружина Елізабет, зумів розгадати ключові слова і зламати шифр. В результаті пристрій визнали непридатним до використання як бойовий шифр.

1 листопада 1919 року «*NID-25*» ВМФ була об'єднана з бюро криптоаналізу «*MI-1b*» Директорату військової розвідки, в результаті чого при Адміралтействі була утворена «Урядова школа коду й шифру» (англ. *Government Code and Cypher School, GC&CS*). Основним завданням школи було забезпечення шифрованим зв'язком усіх підрозділів Уряду, але була також ще таємна директива, щоб «вивчати методи шифрозв'язку іноземних держав». Директором «*GC&CS*» став Еліс-тер Денністон (1881-1961), а керівником секції, що працювала проти Росії, став колишній російський криптолог Ернест Фетерлейн.

Першу кодограму школа декодувала 19 жовтня 1922 року. Оскільки основна робота школи була пов'язана з дипломатичним листуванням, за ініціативою Лорда Керзона, вона була передана від Адміралтейства до МЗС. З 1923 року як керівником секретної служби розвідки, так і директором школи був Хуг Сінклер. У 1925 році обидві організації були розташовані на різних поверхах будинку на Бродвеї, напроти парку Св.Джеймса. Повідомлення, декодовані криптоаналітиками, вкладалися в сині конверти, і тому називалися «*BJs*» (англ. *blue jacketed files*). У 1920-х роках англій-

ські криптоаналітики успішно розкривали дипломатичні коди Радянського Союзу.

У зв'язку з необхідністю концентрації зусиль на розкритті шифру німецької машини «Енігми» у 1939 році «*GC&CS*» переїхала до містечка «Блетчлі Парк» (англ. *Bletchly Park*) неподалік від Лондона. Офіційно вона стала називатися «Школа коду й шифру в Блетчлі Парку» (англ. *Code and Cipher School at Bletchly Park*) та отримала кодове ім'я «Станція Ікс» (англ. *Station X*). У той же час там почав працювати талановитий інженер Алан Тюрінг, який створив обчислювальну машину для розкриття шифрів. У зв'язку з важливістю подій того часу для історії криптології про них буде розказано в окремій главі.

Крім дешифрування листування супротивника школа також займалася розробкою різних систем кодування для потреб армії та флоту. Так, у 1930-х роках була розроблена ручна картково-трафаретна система кодування «*SIGPOSI*», яка використовувалася під час Другої світової війни. Крім того, з 1943 року в британській армії була введена в дію ручна система кодування «*SlideX*» (англ. *slide* - ковзання), яка використовувалася в невеликих бойових підрозділах (взвод, загін, секція) тільки для короткострокових тактичних повідомлень. Як основна система захисту повідомлень застосовувалась союзними військами у червні 1944 року під час операції «Оверлорд» - десантування на узбережжі Нормандії (Франція).

«*Slidex*» використовувала серії паперових словникових карт, які містили грати розміром 12x17 осередків. Кожен з 204 осередків мав як слово або фразу, так і букву або номер. Карти містилися у футлярі, який закривався та мав декілька курсорів, щоб полегшити розташування осередків. Повідомлення кодувалися та декодувалися з використанням кодових смуг, які могли бути розміщені в утримувачі уздовж верхнього та лівого боків словникової карти. Не дивлячись на те,

REVISED INSTRUCTIONS FOR THE USE OF

SLIDEX R/T CODE, 1944

Slidex training in England during WW II

що вона дуже швидко була «розкрита» німецькими криптоаналітиками, система знаходилася в експлуатації до 1980-х років.

У 1946 році на базі школи в Блетчлі Парку була створена «Штаб-квартира Урядового Зв'язку» (далі – ШКУЗ) (англ. *Government Communications Headquarters*, *GCHQ*). Крім ШКУЗ, криптологічною діяльністю у Великобританії у післявоєнний час займався ще так званий «Комітет з цільової розвідки» (англ. *Target Intelligence Committee, TICOM*), про який можна дізнатися з книги Джеймса Бемфорда «*Body of Secrets*». В останні місяці війни за завданням «*TICOM*» дві сотні провідних криптологів Німеччини були таємно перевезені до Великобританії для роботи проти СРСР. Згодом протягом декількох років цей підрозділ забезпечував для США й Англії дешифрування й читання таємного радянського листування.

У березні 1945 року шість спеціально підготовлених розвідувальних груп «розсипалися» по Німеччині, націлившись на німецькі криптологічні центри, місце розташування яких було встановлено, головним чином, завдяки розкриттю шифратора «Енігма» в Блечлі Парку. Завдання груп «*TICOM*» полягала в тому, щоб захопити стільки німецького криптообладнання, скільки буде можливо. Одна з груп була послана для захоплення замка в Саксонії, де знаходився архів радіорозвідки МЗС Німеччини. За результатом успішної операції весь цей об'єкт, включаючи й штатних співробітників, був переправлений до Британії.

Крім того, навесні 1945 року з містечка Розенхайм біля Мюнхена до Британії була вивезена семитонна обчислювальна машина, за допомогою якої німці розкривали шифри вищого ешелону радянського військового командування. Коли цю техніку змонтували, машина дійсно стала дешифрувати військове таємне шифролистування СРСР. Про це розповідає польський художній фільм «Таємниця секретного бастіона» (пол. *Taemnica twierdzy szyfrow*), знятий у 2007 році.

Зібрана «*TICOM*» інформація дозволила згодом читати не тільки російські шифри, але й таємне листування ще принаймні 35 країн, включаючи Францію, Італію, Японію, Іспанію, Швейцарію й Ірландію. Правда, читання радянських телеграм продовжувалося не дуже довго. Відповідно до недавно опублікованих документів АНБ, приблизно через три-чотири роки кожний із шифрів, що розкривався, поступово замінювався на новий та в результаті дешифрування втрачався.

Крім того, Майкл Сміт у своїй книзі «Шпигунська гра» пише, що на початку холодної війни британці домовилися про спільну роботу з американцями над радянськими кодами і шифрами. До вересня 1946 року британські криптологи посилали американцям матеріал, створений радянською шифрувальною телепринтерною системою, що отримала кодову назву «Ікра». Але головним успіхом став «злом» головних радянських машинних шифрів, відомих під назвою «Поети». Перша така система була «зламана» на початку 1946 року. Вона називалася «Кольрідж» і використовувалася радянськими сухопутними військами, ВПС і ВМФ в го-

ловних комунікаційних мережах СРСР. «Кольрідж» давала Заходу уявлення про радянську військову силу, її можливості і місця дислокації. За своєю значущістю для британської розвідки вона поступалася лише радянським ядерним секретам. Але 29 жовтня 1948 року, в день, згодом названий «чорною п'ятницею», коди, шифри і комунікаційні процедури Варшавського договору були змінені. Секрет зломщиків видав СРСР радянський агент в армії США Вільям Вейсбенд.

У даний час ШКУЗ, яка у 1953 році була переведена до Челтенхему (129 кілометрів від Лондона), з метою прикриття включена до структури британського МЗС. Її керівник є заступником міністра, але фактично це незалежний орган, що підкоряється безпосередньо Прем'єр-міністру. В її структурі є група безпеки електронних комунікацій (англ. *Communications-Electronics Security Group, CESG*), яка забезпечує захист урядового зв'язку та інформаційних систем. Периферійні підрозділи ШКУЗ, ті, що розташовуються на території англійських військових баз, підпорядковані структурі Міністерства оборони.

ШКУЗ відповідає за безпеку урядових ліній зв'язку, розробку кодів і процедур з метою захисту повідомлень (забезпечення таємності зв'язку) Уряду Великобританії. Також забезпечує планування, контроль, координацію дій і обробку даних перехоплення всіх органів міністерства оборони (ВПС, ВМФ і сухопутних військ) як у країні, так і за кордоном.

Завдання радіорозвідки вирішується станціями спостереження і перехоплення, розташованими як на території Великобританії, так і за кордоном. ШКУЗ має мережу станцій радіоперехоплення по усьому світі (близько 25), найбільша з яких знаходиться в місті Менвіт-Хілл (графство Йоркшир). Закордонні пункти перехоплення знаходяться в Німеччині, Гібралтарі, Туреччині, Омані, на Кіпрі та на острові Вознесіння.

Ця робота координується Організацією з комплексного перехоплення сигналів (англ. *Complex Signal Organization, CSO*). Більшість станцій, що працюють в інтересах

«*CSO*» і військових баз, що знаходяться на території Великобританії, входять до складу Міністерства оборони, і тільки станція в м. Морвенстоун підпорядкована ШКУЗ.

ШКУЗ складається з 6 управлінь, найважливішим з яких є управління збору даних, що формулює потреби в розвідувальній інформації та забезпечує обробку зібраних відомостей. Це управління складається з відділів, основними з яких є:

- відділ «J» (спеціальна технічна розвідка) – відповідає за ведення технічної розвідки у країнах Східної Європи, у тому числі СНД. Штатна чисельність відділу складає близько 1 000 службовців;
- відділ «K» (загальна технічна розвідка) – відповідає за ведення технічної розвідки у інших регіонах земної кулі;
- відділ «H» (криптоаналіз) – відповідає за дешифрування даних;
- відділ «X» (інформатика) – інформаційний центр керування, оснащений сучасними ЕОМ великої потужності типу «*CRAY-3*»;
- відділ «Z» (взаємодія) – відповідає за зв'язок і взаємодію зі службами союзних держав, з якими існують відповідні угоди.

Управління організації та особового складу виконує, в основному, адміністративні завдання, займається питаннями навчання й розподілу особового складу у Великобританії та закордоном, а також призначає особовий склад технічної розвідки у посольства.

Управління забезпечення скритності зв'язку відповідає за забезпечення захищеності повідомлень британського уряду, розробляє технічні директиви щодо захисту інформації та технічних засобів і керує криптологічною діяльністю в державі.

Управління планування відповідає за розробку довгострокової стратегії системи технічної розвідки (розміщення станцій радіоперехоплення, їх забезпечення та інше).

Управління телемовлення являє собою організацію прикриття для мережі станцій радіоперехоплення ШКУЗ, розташованих по усьому світі.

Об'єднана технічна служба перекладів, в основному, відповідає за переклад на англійську мову перехоплених повідомлень будь-якого характеру (переговори льотчиків, повідомлення посольств та інше).

Друге завдання ШКУЗ покладене на Групу безпеки електронних комунікацій (англ. *Communication Electronics Security Group, CESG*). Група працює в інтересах Уряду і Збройних Сил Великобританії, надаючи допомогу в захисті ліній зв'язку й інформаційних систем, що використовуються ними. «*CESG*» є офіційним органом, що регулює питання використання криптології у Великобританії, а також відповідальною за безпеку інформації в цілому. Крім Уряду і спецслужб під юрисдикцію «*CESG*» підпадають усі юридичні особи, що працюють на Уряд Великобританії. Крім того, ця група тісно співпрацює з промисловістю з метою забезпечення державних органів відповідними технологіями та системами.

Крім того, ШКУЗ має саме безпосереднє відношення до становлення спецслужб США, зокрема, АНБ, що було створено при особистій участі фахівців ШКУЗ. Не дивно, що вони тісно співпрацюють, утворивши єдину систему радіотехнічної і радіоелектронної розвідки (так називаний «Ешелон»).

Незважаючи на загальне скорочення збройних сил, чисельність і фінансування служб розвідки й безпеки Великобританії щорічно збільшуються приблизно на 2-5%. За оцінками західної преси, штатний склад британських спецслужб у даний час досягає 20 тисяч осіб, а річний сумарний бюджет перевищує 1 мільярд фунтів стерлінгів.

1.6. Німецькі криптослужби

У 1734 році начальник першого дешифрувального відділення Німеччини граф де Гронсфельд запропонував ідею застосування ключа без використання таблиць, що була спрощеним варіантом шифра Віженера. Замість буквеного гасла-ключа він узяв числовий, що складався з небагатьох цифр, які легко запам'ятовувалися. Замість великої громіздкої квадратної таблиці використовувався тільки один алфавіт із правильним розташуванням літер. Буква відкритого тексту замінялася буквою алфавіту, що стояла від неї вправо або вліво на кількість знаків, що дорівнювала відповідній цифрі ключа.

Для використання шифру спочатку випишемо латинський алфавіт:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Числовий ключ оберемо найпростіший, наприклад, «1234567», який записувався під текстом. Зашифруємо цим способом слово «*UKRAINE*». При шифруванні перша буква «*U*» заміняється на букву, що знаходиться за нею в зазначеному алфавіті на відстані 1 (тобто, на букву «*V*»). Друга буква «*K*» замінялася на букву на відстані 2 – «*M*», третя буква «R» замінялася на букву на відстані 3 – «*U*» тощо:

Відкритий текст	U	K	R	A	I	N	E
Цифровий ключ	1	2	3	4	5	6	7
Шифротекст	V	M	U	E	N	T	L

В результаті слово «*UKRAINE*» перетвориться у шифротекст: «*VMUENTL*».

Разом із тим, у Першу світову війну німці вступили не маючи військової криптослужби. Лише у 1916 році вони утворили «службу перехоплення» (нім. *Abhörchdienst*), що розпочала займатися перехопленням повідомлень супротивників і випробувати практично усі відомі криптосистеми в різних варіаціях. У той час німецький талановитий криптоаналітик Людвіг Дойбнер розпочав «розкривати» та читати російські військові шифротелеграми, що й призвело до поразки

деяких російських армій на Західному фронті під час Першої світової війни.

Офіцери німецького Генерального штабу мали «Довідкову книжку», де був приведений зразок шифру, що не вирізнявся хитромудрістю, але був надзвичайно простим у користуванні. Вхідною фразою до нього повинна була служити умовна фраза, наприклад, «GERMANY». Під цією, написаною в один рядок, фразою робилася сітка з 7 вертикальних стовпців за кількістю букв цього слова, у які і вписувався у декількох горизонтальних рядках по 7 букв відкритий текст повідомлення. Після цього починали брати букви, дотримуючись алфавіту, тобто 5-й ряд, що відповідав першій букві алфавіту, а далі 2-й, що відповідав букві «E», потім 1-й, що відповідає букві «G», і так далі.

G	E	R	M	A	N	Y		A	E	G	M	N	R	Y
1	2	3	4	5	6	7		5	2	1	4	6	3	7
А	Т	А	К	У	В	А	→	У	Т	А	К	В	А	А
Т	И	З	А	Р	А	З		Р	И	Т	А	А	З	З

Отримані букви розбивалися у групи по п'ять букв і відокремлювались тире. В результаті фраза «АТАКУВАТИ ЗАРАЗ» перетворюється у шифротекст: «УТАКВ-ААРИТ-ААЗЗ».

Найбільш відомим німецьким шифром того періоду була система «ADFGX», побудована на сполученні базових операцій заміни, дроблення та перестановки. Цей шифр розробив офіцер зв'язку Фріц Небель, що служив у штабі німецької армії, та був введений у дію у 1918 році. Свою назву ця система одержала через те, що її шифрограми містили тільки букви «A», «D», «F», «G» і «X».

Причина вибору саме цих букв була в тому, що якщо їх перевести у вигляд крапок і тире коду Морзе, то вони будуть істотно відрізнятися одна від іншої, тим самим мінімізуючи небезпеку появи помилок під час телеграфної передачі.

Фактично це був полібійський квадрат, в який вписувався латинський алфавіт визначеним порядком. Розташування букв у таблиці служило частиною ключа, тому одержувачу, щоб розшифрувати повідомлення, необхідно було знати, як вони в ній розташовувалися.

	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	l,j	c	u	x
X	m	r	e	w	y

Зашифруємо цим шифром, наприклад, фразу «Атакуйте одразу» (англ. *Attack at once*). Використовуючи цей квадрат, повідомлення записувалося таким чином:

A	T	T	A	C	K	A	T	O	N	C	E
AF	AD	AD	AF	GF	DX	AF	AD	DF	FX	GF	XF

Потім, повідомлення записувалося по рядках у квадратну таблицю під ключевим словом «DARTS», а потім стовпці переставлялися за алфавітним порядком:

D	A	R	T	S		A	D	R	S	T
A	F	A	D	A		F	A	A	A	D
D	A	F	G	F		A	D	F	F	G
D	X	A	F	A	→	X	D	A	A	F
D	D	F	F	X		D	D	F	X	F
G	F	X	F	X		F	G	X	X	F

Шифротекст отримували виписуванням букв по стовпцях:

FAXDF ADDDG AFAFX AFAXX DGFFF.

У червні 1918 року з метою ускладненя шифру до нього була додана ще буква «V», і шифр став називатися шифром «ADFGVX». Він став містити 36 символів, до яких крім всіх букв алфавіту були додані ще цифри від 0 до 9. Це допомгло значно скоротити шифрограми, які містили багато цифр.

Повідомлення, зашифровані цим шифром, першими перехопили французи у березні 1918 року. Робота з «розкриття» цього шифру була доручена криптоаналітику капітану Жоржу Пенвену. 2 червня 1918 року в результаті копіткої роботи він розшифрував шифрограму, де були визначені цілі майбутнього наступу німецьких військ.

Усвідомлюючи слабкість вищезазначеного шифру, німці ускладнили шифр Плейфера та використовували не один, а два квадрати, тому цей шифр назвали «подвійним квадратом». Його застосовували для секретного листування на рівні батальйону до 1944 року.

На відміну від полібійського, «подвійний квадрат» використовував дві таблиці, розташовані по горизонталі, а шифрування відбувалося як у шифрі Тритемія. Ці, здавалося б, не настільки значні зміни привели до появи нової криптосистеми

ручного шифрування.

Алгоритм шифрування складався у випадковому заповненні двох таблиць символами алфавіту, а самі таблиці були таємним ключем. Щоб загальна кількість букв алфавіту у разі розміру квадрата 5x5 не перевищувало 25, буква «J» опускалася (оскільки ця буква, з одного боку, мало вживалася, а з іншого боку – цілком могла бути замінена буквою «I» без будь-якої втрати для змісту).

Як варіант таблиці «подвійного квадрату» могли виглядати таким чином:

H	N	B	P	I,J		E	L	E	Q	P
W	K	M	D	Y		I,J	D	R	A	H
G	O	V	E	F		W	X	V	K	C
L	Q	X	A	T		U	N	B	F	Y
U	R	C	Z	S		M	T	Z	H	G

При шифруванні відкритий текст розбивався на біграми. Перша буква біграми шукалася у лівій алфавітній таблиці, а друга – у правій. Шифрування відбувалося в залежності від їх розташування у клітинах квадратів. Якщо букви біграми лежали в одному рядку, то букви вихідний біграми вибиралися в тому же рядку, але з протилежними номерами.

Якщо букви не лежали в одному рядку, то між двома таблицями уявно будувався прямокутник таким чином, щоб ці дві букви лежали в його протилежних вершинах, а інші дві вершини даного прямокутника давали букви шифротекста. В результаті шифрування «подвійним квадратом» слово «UZHGOROD» перетворюється у шифротекст «MCPUVKXK»:

UZ	HG	OR	OD
MC	PU	VK	XK

Система Уітстона повторювала пропозиції Тритемія та Порти щодо біграмного шифрування, однак уже на новому рівні. Зручність цього алгоритму шифрування полягала в тому, що розмір алфавіту був нічим не обмежений, тому можна було будувати таблиці будь-яких потрібних для конкретного алфавіту розмірів.

На початку 1919 року в німецькому МЗС була утворена власна криптоаналітична спецслужба – відділення «Z» (Per Z). Його очолив 32-річний капітан армійської служби радіоперехоплення Курт Зелхов. Спочатку відділення «Z» було укомплектовано, в основному, фахівцями, з якими Зелхов познайомився ще під час Першої світової війни. Однак після приходу Гітлера до влади в 1933 році воно почало неухильно розширюватися. До 1939 року криптоаналітиків у відділенні «Z» було вже стільки, що вони були поділені на дві групи, кожна з яких мала свою спеціалізацію. Перша займалася шифрами, причому склад і професійний підбір співробітників цієї групи визначив її математичний ухил. Друга група займалася лінгвістикою, тому взя-

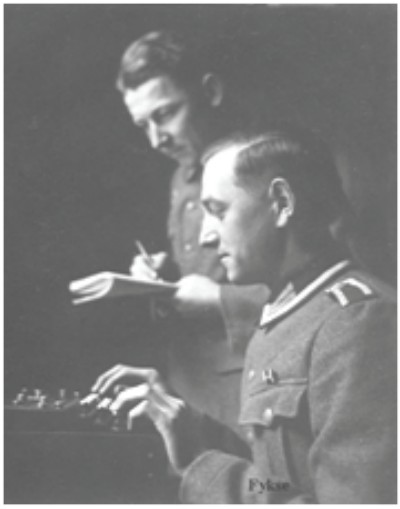
ла під свою опіку розкриття кодів.

Ці групи очолили три старші криптоаналітики відділення «Z». Шауфлер, який до Першої світової війни викладав у школі, і Пашке, уродженець Санкт-Петербурга, спільно керували так званою лінгвістичною групою, тому що вона була більшою за чисельністю, а Кунце, що прослужив усю війну кавалеристом, керував математиками. Усі троє були професіоналами високого класу.

Шауфлер був фахівцем зі східних мов з гарною математичною підготовкою, націленим на теоретичні дослідження. Пашке – природжений лінгвіст, який цілком присвятив себе криптоаналізу. Кунце був доктором математики Гейдельберзького університету. Усі троє почали професійно займатися криптоаналізом ще до створення відділення «Z», але послужний список Кунце був найбільш вражаючим. У його доробку було розкриття декількох англійських шифрів і французького дипломатичного коду в 20-х роках XX сторіччя, а також двох японських машинних шифрів, відомих американським криптоаналітикам під умовними назвами «Пурпурний» (англ. *Purple*) і «Червоний» (англ. *Red*).

Крім того, Німеччина приділяла велику увагу радіорозвідці як важливому елементу досягнення перемог у військових баталіях. Недаремно фельдмаршал Пауль фон Гінденбург був нагороджений Зіркою Великого Хреста за битву під Танненбергом і розгром російських військ у Пруссії. Один з головних «архітекторів» перемоги під Таннербергом, німецький полковник Макс Хоффман, який керував радіоперехопленням, писав: «Ми знали все про плани росіян з їх радіопереговорів, що прослуховували».

Після Першої світової війни відповідно до Версальського Договору збройні сили Веймарської республіки виконували виключно оборонні функції. Секретна служба займалася тільки захистом власних державних і військових секретів, а утворена 1 січня 1921 року військова контррозвідка, Абвер (нім. Abwehr – оборона, віддзеркалення), безпосередньо підпорядковувалася військовому міністру.



Цікаво відзначити, що на початку 1922 року засновниками майбутньої найпотужнішої німецької криптослужби були вихідці з Росії: професор Пулковської обсерваторії Петро Новопашенний і Вільгельм Феннер. Вони продемонстрували свої дивовижні здібності в галузі криптології представникам німецької армії (далі – рейхсвер). За

декілька тижнів вони зламали російський шифр, який використовував Центральний комітет (далі – ЦК) Всеросійської комуністичної партії більшовиків (далі – ВКП(б)) для зв'язку зі своїм агентом у Комуністичному Інтернаціоналі (далі – Комінтерн) Я.Рейхом, завідувачем Західноєвропейського Бюро Комінтерна у Берліні.

З розшифрованих повідомлень контррозвідка Німеччини дізналася, що Росія планує революцію у Німеччині та виділяє на це 50 мільйонів золотих марок. Цей намір Росії щодо підриву політичного устрою Німеччини повністю суперечив Рапалльському договору між РРФСР і Веймарською республікою, укладеному 16 квітня 1922 на Генуезькій конференції у місті Рапалло (Італія).

Надалі ВКП(б) направляв безліч шифрованих вказівок у Відділ міжнародного зв'язку Виконкому Комінтерну для підготовки соціалістичної революції. Для координації дій з німецькими комуністами 21 серпня 1923 року була створена Комісія, до якої увійшли Зіновьєв, Каменєв, Троцький, Сталін, Радек, Чичерін, Дзержинський, П'ятаков і Сокольніков. К.Б.Радека послали до Німеччини керувати революцією та забезпечили персональним шифром для зв'язку з ЦК ВКП(б).

Новопашенний і Феннер легко розкрили і цей шифр. Таким чином, контррозвідка і поліція Німеччини була обізнана про підготовку німецьких комуністів до повстання у жовтні 1923 року. Тому німецькі війська, що мали тоді назву «рейхсвер» (нім. reichswehr від reich – держава, імперія та wehr – оборона) були завчасно введені до Саксонії та «придушили» повстання комуністів у Гамбурзі, що почалося 23 жовтня. Слід віддати належне тому, що такому успіху дешифрування повідомлень сприяло невміле поводження з шифрами співробітників ЦК ВКП(б), які їх готували.

Такий низький ступінь підготовки партійних шифрувальників пояснювався тим, що керівники ВКП(б) побоювалися розповсюдження відомостей про свої махінації з валютними засобами країни, оскільки частина надісланих до Німеччини грошей «безслідно» зникла. Як потім з'ясувалося, це було пов'язано з примітивним «відмиванням» грошей. Розслідування справи доручили Г.Бокію, начальнику Спецвідділу при Всеросійській надзвичайній комісії. На підставі його аналізу шифрів, якими були зашифровані надіслані до Німеччини повідомлення, він визначив їх низьку стійкість і доповів про це у ЦК ВКП(б). Тоді Сталін 7 грудня 1923 року направив цикуляр у всі підрозділи ЦК ВКП(б) про те, які шифри потрібно застосовувати, порядок їх відправлення та зберігання.

Робота з дешифрування телеграм Комінтерна Новопашенного та Феннера так вразила керівництво рейхсвера, що вони створили спеціальне Криптобюро при рейхсвері на чолі з ними. Спочатку у їх підпорядкуванні було дві людини. Потім, коли Криптобюро перемістилося на вулицю Бендлершрассе у Берліні, у їх підпорядкуванні було вже 11 осіб. Їх робота з дешифрування була вражаючою. За короткий період часу вони розшифрували 6 російських кодів, 2 британські коди, проаналізували французьку та італійську військову систему шифрування.

До 1932 року Криптобюро під управлінням Вільгельма Феннера розшифрувало більше 40 різних шифрів різних країн. Команда Феннера могла читати польські дипломатичні і військові шифровані повідомлення, 2 дипломатичні шифри Італії і 1 код італійської армії, декілька французьких дипломатичних шифрів і шифри військово-повітряних сил Франції, британські дипломатичні коди і системи кодів, які захищали зв'язок Британської імперії з її колоніями, 2 американські коди «Сірий» (англ. *Grey*) і «Зелений» (англ. *Green*), 2 шифри чеської армії, коди Бельгії, Румунії і Югославії, а також деякі шифри СРСР.

Розширенню діяльності Абверу сприяла істотна реорганізація, проведена в 1925 році. Тоді ж був організований підрозділ «Абт-II», який відповідав за радіорозвідку, розробку шифрів і дешифрування. З 1932 по 1939 рік чисельність військовослужбовців у німецькій радіорозвідці, включаючи сухопутні війська, що мали назву «вермахт» (нім. *wehr* – оборона, *macht* – сила), військово-морський флот (далі – ВМФ), що мав назву «кригсмарине» (нім. *krieg* - війна, *marine* - морський) і військово-повітряні сили (далі – ВПС), що мали назву «люфтваффе» (нім. *luft waffe* – повітряна зброя), збільшилася в 18 разів.

До 1926 року стаціонарні пости радіоперехоплення існували вже в Кенігсберзі, Франкфурті-на-Одері, Бреслау, Мюнхені, Штутгарді і Мюнстері, а через два роки німці організували станції перехоплення в демілітаризованій Рейнській області під виглядом цивільних радіостанцій. Надалі чисельність таких постів і служб перехоплення збільшувалася. Наприклад, 2-й відділ головного штабу ВПС у 1935 році складався з 20 осіб, і до 1940 року – більше 1000 осіб.

Крім того, існувала служба перехоплення Германа Герінга – Наукове Дослідне Управління (далі – НДУ) Міністерства Авіації, що складалося з 12 «дослідних бюро» і величезної мережі постів перехоплення інформації не тільки усередині рейху, але й за кордоном. Його регіональні станції знаходилися у Берліні, Штутгарді, Гамбурзі, Мюнхені і Кельні. НДУ підслухував телефонні розмови, перлюстрував листи та дешифровував криптограми. Надалі Герінг монополізував у Німеччині службу перехоплення і дешифрування, і підпорядкував НДУ Абверу.

На початку Другої світової війни в службах радіоперехоплення,

шифрування і дешифрування Німеччини працювало більше 100 тисяч осіб. Найважливішою причиною видатних успіхів німецьких криптослужб були дослідження та унікальні розробки німецьких учених і інженерів у сфері математичного аналізу, прийому, передачі й обробки сигналів різної форми, частоти та потужності.

Німецький уряд фінансував їх в таких же обсягах, як і звичайні системи озброєння Німеччини. Герман Герінг безпосередньо відповідав за розвиток озброєнь Німеччини і, природно, не забував про своє улюблене дітище – НДУ, яке забезпечувало йому величезну владу не тільки у Німеччині, але і у всьому світі. Приведемо деякі приклади науково-технічних досягнень німецьких інженерів у сфері радіоперехоплення і криптології.

Для перехоплення та аналізу телеграм, що передавалися кодом Морзе, німецькі інженери винайшли «ондулятор». Це самописний пристрій, що протягував рулонний папір, на якому виписувалися зигзагоподібні прямокутні зображення крапок і тире коду Морзе. Спеціальна група аналітиків за довжиною нанесених інтервалів могла досить точно ідентифікувати підкреслення радиста, а потім визначити його приналежність до конкретного надводного або підводного човна супротивника. На підставі цього аналізу створювалися автоматичні імітатори роботи ворожих радистів, що дозволяло німецькій розвідці ефективно вести радіоігри.

Криптоаналітики Німеччини використовували навіть обчислювальні машини, а також різні табулятори для сортування текстів і підрахунку частоти символів і інтервалів. За допомогою криптоаналізу вони швидко і ефективно відшукували ті, що повторювалися або були віддаленими один від одного на однакову величину групи, визначали довжину ключа, шукали гами та стійкі з'єднання.

Німецькі інженери розробили унікальні системи прослуховування та реєстрації телефонних розмов на мережах стандартних АТС. Ці пристрої, встановлені в будівлях, де знаходилися АТС, дозволяли контролювати одночасно до 1000 абонентів і записувати їх розмови на спеціальні пристрої (магнітофони).

До 1938 року Німеччина стала світовим лідером з виробництва спеціальної техніки для розвідки. Різноманітні магнітофони, у тому числі і малогабаритні, мініатюрні мікрофони, системи підслуховування вважалися кращими в світі, адже вони були розроблені у відповідності з останніми досягненнями німецької науки у сфері радіотехніки та хімії.

У 1939 році всі партійні та урядові поліцейські організації Німеччини, за винятком НДУ Герінга, були об'єднані в одну – Головне Управління імперської безпеки (далі – ГУІБ). Його VI управління за мету надавати таємну інформацію про інші країни. Спочатку воно сконцентрувало увагу на найбільш традиційних методах її збору. Але після анексії Австрії Німеччиною в 1938 році один співробітник VI управління знайшов в архівах австрійської таємної служби найцікавіші документи з криптоаналізу.

Ця знахідка нагадала Вільгельму Хетлю, іншому співробітнику цього управління, про славні справи австро-угорських криптоаналітиків у Першу світову війну. Довідавшись, що генерал Фігль, який був главою австрійської дешифрувальної служби, у 1938 році був арештований та знаходився у в'язниці, Хетль домігся від начальника VI управління звільнення Фігля та призначення його викладачем з криптоаналізу у Берліні. Таким чином Фігль передавав свій досвід новому поколінню німецьких криптоаналітиків.

Однак підготовка криптоаналітичних кадрів вимагала часу, а поки інформація, отримана шляхом дешифрування, надходила до VI управління з інших джерел. Одного разу його співробітникам якимось чином удалося дістати іспанський код, який потім успішно використовувався для читання шифроперехоплення. Дещо саме «пливло» в руки.

Так, під час хірургічної операції в одному з берлінських госпіталів пацієнт під наркозом раптом заговорив про необхідність змінити шифр і кілька разів викрикнув: «Чому Москва не відповідає?». Лікар-хірург поспішив у компетентні органи повідомити про цю подію. Виявлена в результаті радянська розвідгрупа нараховувала, в цілому, 16 осіб, включаючи й прооперованого радиста. Незабаром після цього прийшла ще одна удача: глава японської шпигунської мережі в Європі запропонував продати гуртом діючі коди югославського Генерального штабу, а також дипломатичних служб Бразилії, Ватикану, Португалії й Туреччини. Пропозиція була негайно прийнята.

На початку Другої світової війни німецькі криптологи могли розшифрувати велику частину шифрованих повідомлень, що передавалися по кабельних та радіолініях зв'язку Європи. Цьому сприяло те, що безліч міжнародних телефонних і телеграфних кабелів проходило через територію Німеччини. Криптологи Німеччини досягли значних успіхів у дешифруванні шифраторів «С-36» і «С-37» виробництва компанії Хагеліна, якими були оснащені найважливіші урядові і військові організації Франції, Бельгії, Данії, Нідерландів і Норвегії.

Аналізуючи політичні кроки Гітлера напередодні і на початку Другої Світової війни, ми можемо припустити, що всі його дії були обумовлені отриманням величезного фактичного матеріалу, заснованого на прослуховуванні та перехопленні державного і військового листування країн, які він планував анексувати або захопити.

З початком Другої світової війни підбір у криптослужбу МЗС - відділення «Z» здійснювався в «пожежному» порядку. Там виявилася негайна потреба в розумних фахівцях-криптоаналітиках, і тому німецькій владі доводилося робити винятки навіть для людей «неарійського» походження. Так, Людвіг Дойбнер при нацистах за свої успіхи в дешифруванні був відзначений званням «почесного арійця». Його сина Отфрида, наполовину єврея, у пам'ять про заслуги батька взяли на роботу у відділення «Z» для розкриття італійського шифролистування.

Значну допомогу німецьким криптоаналітикам з відділення «Z» робила інформаційна група, яку очолював пастор Цигенрюкер. Ця група збирала дані з радіопередач, меморандумів міністерств закордонних справ, закордонних газет і матеріалів відділення «Z».

Велику стимулюючу роль у відділенні «Z» грали грошові винагороди за знання іноземних мов. Їхня величина напряму залежала від труднощів тієї чи іншої мови. Нічого не платили там тільки за англійську та французьку мови, оскільки вважалося, що кваліфікований криптоаналітик у будь-якому випадку без їхнього знання обійтися не міг. Дешифрувальникам доводилося кожні чотири роки складати іспити з мови, щоб підтвердити своє володіння нею. Перед кожним іспитом вони поповнювали свої знання в Берлінській школі іноземних мов. У відділенні «Z» були фахівці з мови кожної великої країни, яка мала за кордоном свій дипломатичний корпус.

Німецькі криптоаналітики відділення «Z» працювали досить плідно, тому що розкривали шифри 34 країн світу, включаючи Англію, США і Францію. Дешифровані у відділенні «Z» і видрукувані на машинці матеріали надходили прямо до Зелхова, який потім відправляв їх міністру закордонних справ третього рейха Ріббентропу. А той вже відбирав інформацію для ознайомлення з нею Гітлера. Однак останній не завжди оцінював її по достоїнству. Наприклад, так відбулося з текстом одного великого повідомлення, що містило важливу інформацію про положення в сільському господарстві СРСР, стан справ у якому не міг не позначитися на військовому потенціалі Радянської держави. Гітлер написав на ньому резолюцію: «Цього не може бути».

Відділення «Z» відзначилося й тим, що зробило свій внесок у розв'язання Німеччиною Другої світової війни. У 1939 році в останній день мирного життя шведський бізнесмен Далерус зустрівся з Ріббентропом у Берліні. Коли вони спілкувались, у кабінет Ріббентропа ввійшов його ад'ютант і вручив йому червоний конверт державної важливості, що застосовувався в особливо термінових випадках. Ознайомившись з його змістом, Ріббентроп заявив, що має у своєму розпорядженні докази саботажу з боку поляків будь-якого кроку Німеччини в напрямку мирного врегулювання.

У руках у нього був відкритий текст шифротелеграми польського уряду своєму послу в Берліні. Криптоаналітики з відділення «Z», що розкрили польський дипломатичний код, прочитали шифротелеграму і зробили переклад прочитаного з польської на німецьку мову. Уся процедура від перехоплення шифротелеграми до вручення перекладу її відкритого тексту Ріббентропу зайняла менше години.

Наприкінці шифротелеграми стояло спеціальне розпорядження польському послу: «Ні при яких обставинах не починайте дійсні переговори». Ріббентроп власноручно зняв копію з перекладу та вручив Далерусу для передачі англійському послу. Він додав, що Англія повинна довідатися від Німеччини, наскільки віроломні поляки, хоча б і ціною ризику позбавитися корисного джерела інформації. Таким чином, дешифрована польська телеграма просто продемонструвала всю точність і ефективність одного з головних знарядь шпигунства Німеччини в момент розв'язання нею Другої світової війни.

Відділення «Z» було не єдиною криптослужбою у гітлерівській Німеччині. У збройних силах функціонувало військове шифрувальне бюро «Шифрабтайлунг», що скорочено на армійському сленгу називалося «Ши». Його функції полягали в забезпеченні безпеки власних комунікацій зв'язку, здійсненні перехоплення іноземного листування та контролі над відповідними службами армії (вермахт), ВПС (люфтваффе) і ВМФ (кригсмарине). Бюро очолював полковник Зиґфрід Кемпф, а його група, відповідальна за перехоплення агентурних повідомлень, зазвичай іменувалася «функабвером».

Відразу треба відзначити, що «Ши» після невдалої спроби в 1922 році домогтися від Австрії криптоаналітичної допомоги почало співробітничати з угорськими колегами. У той період віденські колеги не захотіли допомогти Берліну в забороненій Версальським мирним договором діяльності, але порекомендували звернутися до Будапешта, недавніх сусідів по Австро-Угорській імперії. Угорщина стала першою державою, з якою Німеччина забезпечила взаємодію в сфері радіорозвідки та дешифрування.

Керівник криптослужби угорського генерального штабу полковник Вільгельм Кабіна від імені своєї країни підписав так звану «Берлінську угоду» про таємне співробітництво. Крім іншого, документ передбачав взаємне інформування про аналогічні договори, що кожна зі сторін може укласти з третіми державами. Основна ідея «Берлінської угоди» полягала в спільній роботі над італійськими дипломатичними шифросистемами, але незабаром вона поширилася також на польські, румунські й турецькі системи. Партнери обмінювалися як добутими ключами до шифрів, так і інформацією про структуру й уразливі місця шифрів і кодів супротивників. Зокрема, добуті угорцями матеріали з дипломатичного багажу американського військового спостерігача в Єгипті дозволили німцям розкрити «Чорний код» військових аташе США.

Угорщина виявилася для німців вигідним партнером, з 1920 по 1944 рік її криптоаналітики розкрили деякі дипломатичні шифри США і 12 держав Європи, серед яких були Франція, Італія, Швеція, Ватикан і Туреччина. Однак найбільше «Ши» цікавило одержання текстів радіограм. У передвоєнний період угорські пости перехоплення покривали всю територію Південно-Східної Європи, тому німці могли зосередити власні зусилля на інших напрямках і створити на них більш високу щільність пеленгаторів і приймачів. З листопада 1940 року, після приєднання Будапешта до «Потрійного пакту», угорці почали перехоплювати і передавати до Берліна переговори радянських ВПС.

До початку війни нормативні документи передбачали, що начальник Управління зв'язку вермахту за узгодженням з Абвером «займається... питаннями ведення розвідки за допомогою засобів зв'язку, так само як і розвідувально-технічними питаннями, що стосуються контролю за роботою органів зв'язку». Служба військової радіорозвідки мала у своєму розпорядженні головні пости перехоплення у Лауфі і Троенбрайтцені та пости у Мадриді, Севільї, Лоррасі, Тененлосі.

Шифробюро вермахту та його підрозділи з самого початку війни контролювали досить значний обсяг повідомлень супротивника. Наприклад, у січні 1940 року ними були перехоплені 796 британських радіограм, 460 французьких, 209 турецьких, 163 американські, а в березні того ж року – 1649 радянських, 838 британських, 676 французьких, 49 іспанських, 43 польські, 40 ватиканських, 39 португальських. Усього ж у цьому місяці армійські радіорозвідники перехопили радіограми 27 дер-

жав. Крім того, до 1944 року близько 12% текстів радіограм «Ши» одержувало з угорських джерел, зокрема, від прикомандированих до підрозділів вермахту радіорозвідувальних рот.

У червні 1941 року німецька розвідка захопила шифри і ключі до систем секретного зв'язку військових підрозділів радянської армії Західного Військового Округу. В результаті радянська армія, в основному, залишилася без шифрованого зв'язку та могла зв'язуватися тільки по відкритих каналах Наркомату зв'язку СРСР, які прослуховувалися німецькою розвідкою. В результаті німецьким арміям вдалося в короткі терміни розгромити її найбільші військові з'єднання, що призвело до величезних людських і матеріальних втрат СРСР.

Вальтер Шеленберг, який на початку 40-х років був призначений начальником VI управління ГУІБ, ще в 1938 році зіштовхнувся з необхідністю застосовувати у своїй діяльності криптоаналітичні методи, коли йому довелося виконувати завдання з арешту начальника розвідувального відділу австрійського Генерального штабу полковника Ронге. При перегляді документів, захоплених під час його арешту, за свідченням самого Шеленберга, «для одержання цікавих результатів довелося вдатися до допомоги дешифрувальників».

У липні 1940 року в Мадриді Шеленберг мав можливість ознайомитися з роботою військового сектора посольства Німеччини, що складався з сотні службовців і був одним із найбільших німецьких шпигунських підрозділів за кордоном. Співробітники військового сектора розміщувалися безпосередньо в посольському будинку та активно займалися дешифруванням перехоплених повідомлень, користуючись винятково сприятливим географічним положенням Іспанії для здійснення перехоплення з її території.

У результаті Шеленберг прийшов до однозначного висновку про те, що для підвищення ефективності операцій VI управління потрібне, по-перше, встановлення контролю над усією системою поштово-телеграфного зв'язку Німеччини за кордоном, а по-друге, перетворення криптоаналізу в одне з головних знарядь шпигунства й контршпигунства.

На той час VI управління стосовно інформації, що одержувалась за допомогою криптоаналізу, продо-

вжувало залежати від Абверу і НДУ Герінга. Наприклад, восени 1941 року Шеленберг був змушений звернутися з проханням до Гейдриха, який очолював тоді Головне управління імперської безпеки, націлити засоби перехоплення Абверу і НДУ на листування Франції з Белградом для одержання необхідної Шеленбергу інформації.

Гімлеру не подобалася така залежність. У березні 1942 року він послав Шеленберга до заміського будинку Герінга, щоб переконати останнього ввести «Дослідний відділ» до складу VI управління. Герінг зустрів Шеленберга в римській тозі, сандалях і з маршальським жезлом у руці. Вислухавши посланця Гімлера, він сказав: «Добре, я поговорю з Гімлером».

Однак після цієї розмови нічого не змінилося. Тільки в 1944 році Герінг, нарешті, погодився передати свій НДУ у підпорядкування Гімлеру, перевівши його в систему Головного управління імперської безпеки. Відповідні проекти розпоряджень і указів про переведення уже були ними обговорені в спільних бесідах. Наближався момент, коли Гімлер і Герінг повинні були поставити свої підписи під цими документами. Але оскільки мова в них йшла про реорганізацію складного та великого апарата, що нараховував кілька тисяч осіб, Шеленберг не став наполягати на швидкому ухваленні остаточного рішення. Оскільки «тисячолітній рейх» вже «агонізував», то у його керівників були інші невідкладні справи. В результаті НДУ до складу VI управління так і не увійшов.

Ставши начальником VI управління, Шеленберг відразу створив відділ для проведення досліджень у сфері засобів секретного зв'язку, який добре фінансувався. Однак новий відділ не виправдав надій, покладених на нього. Кількість інформації, що добувалася ним за допомогою криптоаналізу, була невеликою, тому Шеленберг, як і раніше, продовжував одержувати її переважно ззовні.

Починаючи з 1942 року, через кожні три тижні начальник VI управління регулярно організовував у своєму будинку звані обіди. На них керівники дешифрувальних спецслужб Міністерства оборони, Міністерства пошти, що вело дешифрування трансатлантичних телефонних розмов, і НДУ обговорювали останні досягнення в сфері криптоаналізу та допомагали один одному порадами у вирішенні проблем, що стояли перед ними. Представник відділення «Z» на цих нарадах у Шеленберга не був присутній, що свідчило про особисту ворожнечу та боротьбу за владу між Гімлером з Герінгом, з одного боку, та Ріббентропом, з іншого.

Шеленбергу належать слова подяки криптоаналітикам від імені «лицаря плаща і кинджала»: «Саме співробітництво та інтерес, що виявлявся з боку цих людей до мене особисто, зробили можливим досягнення більшої частини моїх успіхів в операціях таємної служби».

Шеленберг скористався цією щедрою допомогою при проведенні однієї з найбільших шпигунських операцій Другої світової війни, що одержала назву «Цицерон». Камердинеру англійського посла в Анкарі вдалося зняти воскові відбитки з ключів від

сейфа, де посол зберігав важливі таємні документи, які часто переглядав до пізньої ночі. Документи являли собою головним чином відкриті тексти шифротелеграм із помітками про місце й час зашифрування.

Замість відділення «Z», що за логікою речей повинне було одержати їх у першу чергу, Шеленберг передав ці тексти своїм друзям з військових дешифрувальних підрозділів із проханням негайно зайнятися розкриттям англійського шифру на підставі документів, придбаних у «Цицерона». Кращі військові німецькі криптоаналітики кілька тижнів підряд безуспішно «билися» над цим шифром, поки їм не вдалося розгадати його частину, що дозволило довідатися тільки про малозначущі технічні подробиці передачі шифротелеграм із Лондона до англійського посольства в Анкарі.

Лише після того, як військові фахівці з криптоаналізу зазнали невдачі, з англійськими телеграмами ознайомили Кунце та Пашке, але задача розкриття дипломатичного шифру Англії на лінії зв'язку Анкара-Лондон не викликала великого ентузіазму й у них. Справа в тому, що англійці перешифровували свої найбільш важливі телеграми за допомогою одноразових блокнотів, а це робило їхнє розкриття малоймовірною подією. Таким чином, операція «Цицерон», яка була повним успіхом у сфері агентурного шпигунства Німеччини, стала не менш повним провалом німецьких криптоаналітиків.

Зі зростанням військової активності збільшувалися не тільки німецькі збройні сили, але й їх дешифрувальні органи. Але це не означало підвищення ефективності праці, оскільки була недостатня кількість кваліфікованих фахівців у цій сфері. Декого з військових дешифрувальників перевели для зміцнення НДУ, інших – у так звану «озерну» службу Міністерства пропаганди, що займалася перехопленням закордонних передач новин і постачала матеріал для боротьби з пропагандою супротивника.

У жовтні 1943 року Шифробюро очолив полковник Хуго Кеттлер і в наступному році здійснив його реорганізацію. Тепер воно складалося з 8 груп:

🗝 Ц - центральна група: кадри, фінанси, адміністративні питання, розміщення, націонал-соціалістське виховання;

🗝 I - організація і контроль:

- Ia - керівництво міжнародною службою перехоплення:
- Ib - вивчення іноземних систем зв'язку;
- Ic- забезпечення телетайпним зв'язком, у тому числі VIII управління ГУІБ;

🗝 II - розвиток німецьких методів шифрування та контроль за їхнім використанням:

- IIa - маскування телеграфного і радіообміну, техніка перехоплення, у тому числі проводового зв'язку, криптографічна політика та нагляд за використанням шифрів;
- IIb - розвиток німецьких систем шифрування (методи маскування, таємне листування, секретна телефонія);
- IIc - криптографічні системи для агентурного радіозв'язку;

🗝 III - постачання шифрами: контроль за продукцією, друкуванням і поширенням шифрів і ключів;

🗝 IV - аналітичний криптоаналіз:

- IVa - іспити німецьких військових шифросистем і телефонних скремблерів на стійкість, оцінка винаходів;

- IVb - розвиток і створення дешифрувальної апаратури для криптоаналітичних підрозділів вермахту;

- IVc - розвиток криптоаналітичних методів;

- IVd - інструктажі;

🗝 V - практичне дешифрування листування іноземних урядів, військових аташе й іноземних агентів:

- Va - кодові слова для вермахту;

🗝 VI - V22 – регіональні підрозділи;

- VI - перехоплення радіомовлення та повідомлень преси:

- VIa - техніка радіоприйому;

- VIb - перехоплення радіоповідомлень преси та телетайпних передач і міжнародного радіообміну;

- VIc - нагляд за вихідними з рейха радіопередачами;

- VId - оцінка радіомовлення та повідомлень преси, звіти про результати перехоплень відкритих повідомлень, спеціальні звіти;

🗝 VII - назви не мала:

- VIIa - оцінка та розсилання продукції;

- VIIb - ведення журналу підрозділу.

Групи «Ц», «I», «VI» і «VII» підпорядковувалися безпосередньо полковнику Кеттлеру, «II» і «III» входили до головної групи «А» (криптографія), а «IV» і «V» – до головної групи «В» (криптоаналіз). 150 фахівцями груп «*А*» і «*В*» з 1922 року керував міністерський радник Вільгельм Феннер, а його помічником був Петро Новопашенний. Полковник Кеттлер керував також 6 радіорозвідувальними ротами та очолював робочий комітет з безпеки німецьких криптосистем.

У 1945 році «Ши» було знову реорганізоване і розділене на 7 груп:

🗝 Ц - адміністративна;

🗝 I - організація і контроль;

🗝 II - дослідження в криптографії;

🗝 III - перехоплення повідомлень радіомовлення та преси;

🗝 IV - криптоаналіз;

🗝 V - забезпечення телетайпним зв'язком;

🗝 X - оцінка інформації і її розсилання;

«Ши» тісно співпрацювало з абвером, де не було власної криптослужби. Функці-

ональні обов'язки будь-якого органу військового зв'язку передбачали, що він «знаходиться в розпорядженні управління розвідки і контррозвідки незалежно від його службового підпорядкування управлінню зв'язку збройних сил і виконує його вказівки в частині, що стосується:

- одержання розвідувальних даних, добутих за допомогою технічних засобів зв'язку;
- створення і забезпечення роботи каналів далекого зв'язку для зв'язку з закордоном і для вирішення задач усієї розвідувальної служби.

На Східному фронті німці розгорнули мережу підпорядкованих штабам армій радіорозвідувальних рот. На кожній ділянці фронту довжиною від 100 до 150 кілометрів діяли до двох таких рот, що складали основу німецької системи перехоплення радянських повідомлень. У військах цю функцію виконували також радіорозвідувальні взводи батальйонних рот зв'язку. Радисти вермахту займалися не тільки перехопленням і його аналізом, але й вели активну радіоелектронну боротьбу з супротивником шляхом перестановки цифрогруп у перехоплених радянських радіограмах і повторній їх передачі у «перекрученому» вигляді на тих же частотах.

Тим часом дешифрувальний орган німецького ВМФ, який зробив найбільший істотний вплив на хід війни, виявився нечисленним і найменш відомим серед аналогічних йому спецслужб. Він підпорядковувався головному командуванню ВМФ Німеччини. Командувач ВМФ адмірал Деніц називав його «службою спостереження» (нім. *Beobachtungdienst, B-Dienst*). «Служба спостереження» підтримувала слабкий контакт з іншими дешифрувальними спецслужбами, проте її успіхи найчастіше виявлялися більш значимими.

Створена на початку 20-х років XX сторіччя, «служба спостереження» через два десятиліття зуміла розкрити деякі з найбільш секретних шифрів англійського Адміралтейства. Ця служба достатньо легко розкрила британські військово-морські коди з перешифруванням. Один з них іменувався «Військово-морським шифром». Британські флотські зв'язківці ще більш полегшили роботу німецької дешифрувальної служби, оскільки не забезпечували шифрування умовної групи, яка вказувала, з якого місця книги додавань необхідно починати

читання повідомлень. В результаті до 1940 року німецька криптослужба могла швидко читати три чверті британської кореспонденції, а остання розкривалася з невеликою затримкою.

Були розкриті «Військово-морський код № 2» і «Конвойний шифр», тому німці знали час відправлення і прибуття британських судів, маршрути їх проходження і розосередження по портах. Це давало можливість німецьким підводним човнам ухилятися від небезпечних зіткнень із флотом Англії, а важким німецьким кораблям – уникати випадкових зустрічей з більш сильним супротивником. Тільки за три місяці 1940 року завдяки використанню інформації від «служби спостереження» були потоплені відразу шість англійських підводних човнів.

Підібрати ключі до англійських кодів німцям допоміг випадок. У листопаді 1940 року німецький рейдер «Атлантіс» атакував і захопив британський пароплав «Отомедон», що перевозив у тому числі й цілком таємний документ – книгу кодів. З цього моменту німці були в курсі практично всіх англійських військово-політичних рішень. Зокрема, їм удалося розшифрувати документи, що стосувалися планів Англії у відношенні Японії. Гітлер негайно передав цю інформацію японському імператору Хирохіто, який у свою чергу, відзначив капітана «Атлантіса», нагородивши його самурайським мечем.

Дані, отримані «службою спостереження», зробили неоціненну та вирішальну допомогу в здійсненні плану окупації Норвегії. Самі істотні труднощі в його реалізації складалися в забезпеченні безпечного пересування слабко озброєних військових транспортів з Німеччини до Норвегії без перешкод з боку могутнього англійського флоту. Довідавшись від «служби спостереження» про військову операцію англійців з блокування постачань залізної руди в Німеччину, нацистський флот завдав відволікаючого удару по англійських кораблях, що брали участь в операції. Для їхнього захисту Англія вислала туди іншу частину своїх військових кораблів, що дозволило німецьким транспортам спокійно досягти берегів Норвегії, не побоюючись великих морських атак супротивника.

«Служба спостереження» продовжувала читати шифроване листування англійського Адміралтейства також у критичне літо 1940 року, коли Гітлер готувався до операції «Морський лев» – вторгненню в Англію. Розвідувальні дані, отримані в результаті криптоаналізу, з самого початку Другої світової війни використовувалися німцями для оперативного планування, і головне командування ВМФ Німеччини стало значною мірою залежати від них. Але 20 серпня, коли Англія вже напружувала в боротьбі з нацистами всі сили, її Адміралтейство, здогадавшись, нарешті, про дешифрування німцями своїх шифротелеграм, змінило шифри.

Головне командування ВМФ Німеччини відразу «оглухнуло», тому що одна лише розвідка з повітря не могла дати німцям достатньої інформації. Німецькі судна більше не могли за своїм розсудом завдавати ударів по переважаючих силах англійського флоту чи уникати зустрічі з ними. В результаті Головне команду-

вання ВМФ Німеччини, що й раніше ніколи не виявляло особливо теплих почуттів до операції «Морський лев», охолонуло до неї ще більше.

Навесні 1941 року німецькі криптоаналітики розкрили англійський «Військово-морський код № 3». Інформація з дешифрованих англійських повідомлень часто дозволяла німецьким кораблям і підводним човнам ухилятися від зіткнень з переважаючими силами англійського флоту. Надходила й інша важлива інформація. Так, у 1941 році криптоаналітики надавали капітанам своїх підводних човнів вказівки командувача англійським флотом капітанам конвоїв, що випливали в Англію, як їм минати небезпечні зони на підході до рідних берегів. Зрозуміло, така інформація була вкрай корисна німецьким підводникам, тому що дозволяла «вовчим зграям» німецьких підводних човнів влаштовувати ефективні засідки.

На жаль, для англійців зміни в організації шифрованого зв'язку, що були зроблені ними у вересні 1941 року та мали своєю метою ще більше ускладнити працю німецької дешифрувальної служби, навпаки, її полегшили. До початку 1942 року фахівці «служби спостереження» знову поставляли керівництву ВМФ важливу інформацію. На підставі німецьких архівів, захоплених після війни, англійцям стало відомо, що в той період керівництво ВМФ одержувало від дешифрувальників аналітичну інформацію на підставі змісту більше 2000 радіограм на місяць.

У 1942 році німцям випадково вдалося отримати цікаву інформацію. Німецький рейдер «Тор» захопив в Індійському океані австралійський лайнер «Нанкін». Капітан встиг викинути за борт усі коди та таємні документи корабля, але 120 мішків з дипломатичною поштою, де виявилися й оперативні документи британського командування, дісталися німцям. Серед них виявилися повідомлення про розкриття союзниками японських шифрів. У вересні на мілководді в Атлантиці німцями був потоплений англійський есмінець «Сікх», з якого їм удалося підняти кодові книги.

Die Kriegsmarine
Deutsche Marine-Zeitung
Deutsche U-Boote vor New York!

Німці одержували досить докладні відомості про час прибуття атлантичних конвоїв у прибережні води Великобританії, дані про розподіл суден, що прибували, по портах призначення,

районах підходу конвоїв або поодиноких суден, їхній кількості, про метеорологічні умови. Вони одержували інформацію про успіхи ескортних сил, про атаки німецьких підводних човнів і заподіяні їм ушкодження.

До лютого 1942 року «служба спостереження» досягла значних результатів у розкритті «конвойного шифру» та читала велику частину зашифрованих за його допомогою радіограм, що відносилися не тільки до північноатлантичних конвоїв, але й до операцій у середземномор'ї та інших районах світу.

До жовтня 1942 року дешифрувальники читали радіообмін з конвоями союзників настільки швидко, що Деніц іноді одержував інформацію про майбутній рух суден за десять-двадцять годин до фактичного здійснення того або іншого маневру. Ця інформація доповнювалася тією, яку німці без труднощів отримували з повсякденного радіообміну між командуванням британського ВМФ на західних підходах до Британських островів і Галіфаксом (містом у Канаді, де був розташований штаб конвойних операцій). Згідно з цими повідомленнями німці, зокрема, знайомилися зі вказівками командирам конвоїв про обхід небезпечних зон біля берегів Англії.

«Служба спостереження» розкрила основні англійські морські шифри до осені 1942 року, а нові радистам британського ВМФ доставили лише у червні 1943 року. 10 червня був нарешті замінений код № 3, новий же виявився набагато більш стійким. Тим часом, у торговельному флоті англійців старі шифри використовувалися ще близько 6 місяців.

Вдалося німцям також вторгнутися в радіотелефонну мережу урядового зв'язку Вашингтон-Лондон. Усі переговори (а їх було до 2 тисяч на місяць) вони успішно розшифровували, одержуючи цінну інформацію. Завдяки цьому німецький ВМФ, зокрема підводний, топив численні британські конвої в Атлантиці. Англійські манірність і безтурботність призвели до втрати сотень кораблів і загибелі близько 300 тисяч моряків.

У січні й лютому 1943 року «служба спостереження» опанувала навичками розкриття англійських військово-морських шифросистем настільки добре, що читала навіть англійську «Доповідь про місцезнаходження німецьких підводних човнів», яка регулярно передавалася в зашифрованому вигляді по радіо командирам караванів, що знаходилися в морі. Деніц писав у своєму щоденнику про те, що ці «доповіді про місцезнаходження» мали величезне значення для успішного визначення можливостей та заходів супротивника щодо виявлення німецьких підводних човнів.

Як ВМФ використовував інформацію, що отримувалася з радіоперехоплення та дешифрування, і наскільки цінною вона була для командирів підводних човнів, добре видно на специфічному прикладі проведення конвоїв «HX.229» і «SC.122», яким довелося вести тривалу боротьбу з великою групою німецьких підводних човнів у період з 16 по 19 березня 1943 року. До першої атаки човнами цих конвоїв штаб німецького ВМФ прочитав шістнадцять радіограм, де була завчасна інфор-

мація про рух обох конвоїв.

Особливо важливими серед них були радіограми, відправлені 4 та 13 березня. У першій повідомлялися подробиці океанського маршруту для конвою «HX.229» і для відсталих від нього одиночних суден, а в другій обом конвоям давався наказ ухилитися від маршруту на підставі даних про диспозиції німецьких підводних човнів, повідомлених оперативно-інформаційним центром Адміралтейства. Добре інформований штаб німецького ВМФ зосередив для атаки цих конвоїв сорок підводних човнів, і це закінчилося для союзників утратою двадцяти одного судна сумарною водотоннажністю 140 000 тонн, у той час як німці втратили всього один підводний човен. Офіційний англійський військово-морський історик назвав це «серйозним нещастям для справи союзників».

У тому, що період жахливих втрат і криз швидко змінився періодом тріумфального контрнаступу, у результаті якого до червня 1943 року німецькі підводні човни були змушені піти з Північної Атлантики, не останню роль зіграла та обставина, що з того часу й надалі «служба спостереження» перестала забезпечувати підводні сили інформацією, до якої вони так звикли. Саме в червні 1943 року була введена в дію нова система шифру, що вирішила багато проблем для англійських ВМС.

У «служби спостереження» почалися серйозні труднощі, оскільки читання шифролистування союзників майже припинилося. Деніц визнав поразку своїх підводних сил 24 травня, коли «наказав підводним човнам перейти в район до південно-заходу від Азорських островів, дотримуючись при цьому надзвичайних заходів безпеки». Щомісячні втрати німецьких підводних сил у процентному відношенні до кількості човнів, що діяли в морі, стали різко збільшуватися: з 3,9% у першій половині 1942 року до 9,2% у першому кварталі 1943 року.

Англійські фахівці, що відповідали в британських ВМС за безпеку зв'язку, робили все можливе, щоб ускладнити роботу німецьких дешифрувальників. Так, наприклад, німці дуже рідко могли завчасно отримувати інформацію про пересування англійських військових кораблів. Зокрема, вони не прочитали ні однієї радіограми під час операції британського ВМФ по затопленню «Шарнхорста» біля норвезьких берегів у грудні 1943 року, хоча перехопили їх близько 30.

У ході операції «Торч» (висадження союзників у Марокко і Тунісі) у листопаді 1942 року був використаний спеціально створений для цього шифр, що залишився нерозкритим. Спеціальні шифри застосовували і під час інших великих операцій: при висадженні на Сицилії в 1943 році й в Анціо (Італія) у січні 1944 року. Під час останньої «службі спостереження» німецького ВМФ удалося перехопити 158 радіограм, але жодної прочитати вона не змогла.

Однак на останніх стадіях війни криптоаналітики кригсмарине знову змогли прочитати деякі тактичні коди й шифри супротивника. Сприятливим фактором тут було те, що бойові дії надводних кораблів і авіації союзників у битві за Атлантику на той час

активізувалися. До ефіру стали відправляти більшу кількість повідомлень, і це полегшувало німцям процес дешифрування. Вони у той період читали до 1500 радіограм на місяць. Однак улітку 1944 року союзники ввели новий, більш надійний шифр для зв'язку з суднами конвоїв. Усі спроби німців розкрити його успіху не мали.

Хоча основні зусилля служб радіоперехоплення та дешифрування кригсмарине були зосереджені проти західних союзників, не обійшли вони своєю увагою і східний фронт. У 1941–1944 роках німецькі підводні човни активно діяли в радянському Заполяр'ї. Їхньою метою були конвої й окремі судна, що здійснювали перевезення Північним морським шляхом. Німецькі підводники активно діяли у Баренцевому, Білому та Карському морях, нерідко їхні човни заходили і далі на Схід. До нападу на СРСР, для спостереження за районом Баренцева моря німці використовували радіопеленгаторну станцію у норвезькому місті Кіркенес. Більш східні райони були взагалі не доступні. Зрозуміло, така ситуація німців не влаштовувала.

У 1942 році на радянській території – острові «Земля Олександра» архіпелагу «Земля Франца-Йосипа» таємно була розгорнута 24-а база метеорологічної та пеленгаторної служби кригсмарине. Тут знаходився пункт відпочинку та поповнення запасів німецьких підводників, а також аеродром. Посади радіоперехоплення були розгорнуті й на інших таємних базах німецьких підводників у радянській Арктиці. Радянська служба радіорозвідки неодноразово фіксувала сеанси зв'язку німецьких підводних човнів з радіостанціями, що знаходяться на території СРСР.

На жаль, радянські моряки в початковий період війни не завжди належним чином захищали інформацію. Якщо на військовому флоті завжди розуміли необхідність забезпечення таємничості та безпеки зв'язку, то співробітники Головного Управління Північного морського шляху (далі – ГУПМШ) таких заходів не здійснювали. Капітани торгівельних суден і криголамів, льотчики полярної авіації, зимівники полярних станцій практично не користувалися шифрозв'язком. Переговори про місцезнаходження суден, маршрути конвоїв тощо велися відкритим текстом. Незважаючи на багаторазові попередження військових фахівців про неприпустимість подібних дій, стан справ у полярників стосовно безпеки зв'язку не покращився.

Мало того, на деяких судах шифри взагалі були відсутні. Тільки втрати від дій німецьких підводних човнів змусили співробітників ГУПМШ усвідомити необхідність використання шифрованого радіозв'язку. Влітку 1943 року передачі відкритим текстом важливої інформації припинилися.

У цьому «театрі» військових дій німці іноді одержували доступ до криптографічної інформації в ході бойових операцій. Так, у вересні 1944 року німецький десант, що висадився з підводного човна, захопив на добу радянську полярну станцію на мисі Стерлігова, де серед інших трофеїв німцям дісталися радянські радіошифри.

Крім того, німцям допомагали фінські криптоаналітики. Так, на початку липня

1942 року фінський центр радіоперехоплення в Сортавалі перехопив шифротелеграму з радянської авіабази, розташованої неподалік від Мурманська. Телеграма була зашифрована двозначним цифровим кодом, яким звичайно шифрувалися другорядні повідомлення. Код був давно «розкритий» фінськими аналітиками, які визначили, що листування нецікаве, тому читали його лише час від часу про всяк випадок. Оскільки телеграма виявилася досить довгою, а інших телеграм у цей день не було, то її вирішили дешифрувати. Через погану чутність, або через недостатню кваліфікацію радиста, одержувач багаторазово запитував її повторення, тому в результаті фіни одержали ідеально розшифрований текст.

Можете уявити собі подив фінських дешифрувальників, коли замість очікуваної незначної інформації про доставку пайків і онуч вони одержали повний опис великого конвою з військовим вантажем, що направлявся до СРСР з Ісландії. Мова йшла про караван «PQ-17». Було зазначено усе: його склад, назви кораблів супроводу, точний маршрут із указанням часу відправлення й прибуття в порт призначення. Фіни негайно передали цю телеграму німцям, які одержали можливість ґрунтовно підготуватися до нападу на нього.

Далі події розгорталися приблизно так, як описано у романі Валентина Пікуля та показано у художньому фільмі. Спочатку німці спробували використати для перехоплення конвою великі військові кораблі, зокрема, важкий крейсер «Тирпиц» і есмінці супроводу, але при виході з бази вони були виявлені англійськими підводними човнами. Через це німці вирішили повернути надводні кораблі до бази, а удар по конвою завдати бомбардувальниками та підводними човнами. У той же день німці довідалися, що кораблі супроводу залишили конвой без прикриття, і тому німецькі бомбардувальники та підводні човни могли діяти безкарно.

Варто сказати, що отриманий страшний урок не був врахований (Черчилль не поділився зі Сталіним інформацією та зволів жертвувати англійськими кораблями й матросами). Трохи пізніше фіни знову перехопили телеграми, зашифровані двозначним кодом, а також добре відомим фінам чотиризначним кодом, яким користувався Балтійський флот. У них містилися аналогічні відомості про конвої «PQ-18», що випливав до Архангельська, і «QP-14», що повертався без вантажу до Англії. Дешифровані криптограми знову були передані німцям, по конвоях знову

завдано підготовленого удару, і третина суден була потоплена.

Протягом більшої частини війни дешифрувальна служба кригсмарине складалася не більш ніж з п'ятдесятьох криптоаналітиків. В результаті недостатньої кількості дешифрувальників значна частина матеріалів радіоперехоплення залишалася неопрацьованою. В останні дні існування Третього рейха Деніц наказав фахівцям «служби спостереження» виїхати з Берліна до Фленсбурга (місто на півночі Німеччини недалеко від датської границі) і вступити в співробітництво з англійцями й американцями шляхом надання їм будь-якої інформації з криптологічних питань.

Улітку 1945 року англійці активно допитували полонених німецьких фахівців. У Лондон були перевезені німецькі військово-морські архіви. Англійці хотіли знати, які зміни й удосконалення, здійснені ними в шифрах і кодах, спрацювали, як і коли німецькі дешифрувальники розкрили високонадійні коди й шифри, які поразки в операціях флоту можна віднести цілком на рахунок німецької радіорозвідки і дешифрувальної служби, які сили і засоби мали у своєму розпорядженні ці служби.

Факт за фактом, документ за документом переконливо доводили, що успіхи німецької дешифрувальної служби в розкритті англійських кодів і шифрів виявилися набагато більшими, ніж припускали англійці. Через декілька місяців для вищого керівництва Адміралтейства була підготовлена доповідь, що узагальнила отримані англійцями відомості про діяльність «служби спостереження» кригсмарине.

У даний час також стало відомо, що всупереч поширеній думці німецькі криптоаналітики працювали дуже успішно та для свого часу були одними з кращих у світі. Зокрема, розкривався й американський шифратор «М-209» (більш відомий під назвами «Хаг» або «Хагелін»). Ця інформація, до речі, дуже цікава, оскільки для США в роки війни «М-209» був приблизно тим же, що «Енігма» для Німеччини, оскільки американські збройні сили закупили тоді близько 140 тисяч шифраторів.

Підтвердження цим словам знайшов німецький журналіст Клаус Шмех, який розшукав учасника тих подій. Їм виявився 84-літній житель Франкфурта Райнольд Вебер, який у роки війни зовсім молодим потрапив у дешифрувальний підрозділ Вермахту «*FNAST-5*» у Парижі. Всі інші співробітники цієї служби – колишні економісти, математики, викладачі – були щонайменше років на 10 – 15 старше Вебера, якому поталанило лише завдяки досконалому знанню англійської мови (перед війною він підлітком шість років прожив у США з батьками-емігрантами). З докладних спогадів Вебера стало відомо, що німці не тільки розкривали шифратор «М-209» вручну кропіткими розрахунками з олівцем і папером, але й сконструювали машину для автоматизації найбільш трудомістких етапів розкриття.

Причому відбувалося це в 1943-44 роках – тоді ж, коли англійці створювали свій знаменитий суперкомп'ютер «Колос» для автоматизації дешифрування німецького шифролистування. Але «фортуна» в той час уже відвернулася від Німеччини, і

компанія «*Dehomag*», якій у 1944 році намагалися зробити замовлення на масове виготовлення апаратів-дешифраторів для «М-209», визначила термін створення серійного зразка в два роки. Однак настільки довгі терміни в той час нікого влаштувати не могли, тому далі працездатного макету справа так і не пішла.

Цікаво, що американець Джеймс Бемфорд знайшов свідчення того, що німці все-таки застосовували електронні обчислювальні машини для дешифрування шифролистування супротивників, але не на західному, а на східному фронті. Він з'ясував, що англо-американський «Комітет з цільової розвідки» (*TICOM*) навесні 1945 року до Британії з містечка Розенхайм біля Мюнхена вивіз семитонну обчислювальну машину, за допомогою якої німці розкривали шифри вищого ешелону радянського військового командування. Про це розповідає польський художній фільм «Таємниця секретного бастіона», знятий у 2007 році.

Однак запеклі бої Другої світової війни між німцями та англійцями розверталися не тільки в Атлантиці чи в Європі, але й на далекому Африканському континенті. Американський військовий аташе в Каїрі мав набагато більше можливостей спостерігати за воєнними діями, ніж його колеги в Москві.

Полковник Боннер Феллерс, кадровий військовий, був призначений на цю посаду в жовтні 1940 року. Він без утоми роз'їжджав по місцях ведення бойових дій, вивчав тактику і специфіку війни в пустелі. Англійці довіряли йому деякі зі своїх не занадто важливих секретів, сподіваючись, що це приведе до якісного поліпшення американського спорядження, що поставлялося їм за «ленд-лізом». Феллерс аналізував цю інформацію та відправляв її до Вашингтона у вигляді об'ємних повідомлень.

Він писав про англійські війська, їхні завдання, можливості та ефективність дій, а також про очікуване підкріплення та транспортні кораблі з уже доставленим вантажем. Аналізував різні тактичні схеми, що обговорювали з ним англійці, і навіть, повідомляв про конкретні плани воєнних операцій. І коли його повідомлення передавалися на батьківщину по радіо, у них завжди був ще один слухач – Німеччина. Перехоплені німцями шифротелеграми Феллерса після дешифрування попадали безпосередньо на стіл генералу Роммелю, командуючому німецьким корпусом у Північній Африці. Той міг оцінити їх по достоїнству.

Отримана через Феллерса інформація

давала Роммелю більш широку та чітку картину про наміри супротивника, ніж та, якою володів будь-який інший німецький воєначальник протягом усієї війни. Телеграми Феллерса являли собою найбільш помітні фрагменти тієї багатої подробицями інформаційної мозаїки, що була в розпорядженні Роммеля та допомогла йому заслужити прізвисько Лис пустелі.

Попереджені Феллерсом про заплановану операцію англійських диверсійних частин із нападу на 9 німецьких аеродромів, німці улаштували загонам англійських «командос» криваву різанину. Ретельно підготовлена операція провалилася. А наступного дня німецькі літаки, що щасливо уникли знищення, провели могутні атаки проти англійського конвою, який рухався з Олександрії на Мальту, потопивши 3 есмінці та 2 торгові судна. Конвой повернув назад. Як наслідок, підходи зі сходу до Мальти, що служила базою для англійських кораблів, підводних човнів і літаків, які завдавали ударів по конвоях Німеччини, що забезпечували армію Роммеля всім необхідним, виявилися закритими. З того часу жоден англоамериканський конвой більше не намагався пройти цим шляхом, а лінії постачання Роммеля продовжували безперешкодно діяти.

Стратегічну інформацію з телеграм Феллерса доповнювали тактичні розвідані, що добувала для Роммеля спеціальна рота під командуванням капітана Зеєбома. Вона записувала всі переговори, за допомогою пеленгації визначала концентрацію військ і танків супротивника на тій чи іншій ділянці, добувала дані про дислокацію й найменування частин супротивника, вивчала англійські шифротелеграми з метою дешифрування. Однак 10 червня 1942 року рота Зеєбома виявилася на шляху танкового удару англійців: сам Зеєбом був убитий, велика частина його роти знищена чи узята в полон, а її архіви потрапили до англійців. Таким чином, Роммель утратив «мікроскоп», який давав йому можливість ретельно вивчати позиції супротивника.

Приблизно в цей же час Роммель позбавився і свого «телескопа», оскільки, крім німців, шифролистування Феллерса почали читати й англійці. Після тижня вивчення великих і повних песимізму послань американського аташе вони повідомили американців про можливе попадання інформації Феллерса до супротивника та про його позицію, несумісною з посадою аташе. Самому Феллерсу нічого сказано не було, але його незабаром відкликали до Вашингтона. Цікаво, що у тому ж 1942 році Феллерс був нагороджений медаллю «За видатні заслуги» за свою роботу аташе.

Новий американський військовий аташе в Каїрі змінив шифр, який витримав усі спроби німців його розкрити. Роммель виявився відрізаним від стратегічної інформації, якою так довго користувався. В результаті восени 1942 року його корпус був розгромлений.

Однак щоб ні в кого не виникло ілюзій, начебто сильна криптослужба з більшими витратами на неї здатна вирішити всі проблеми радіорозвідки, варто при-

вести один з прикладів її поразки. По-перше, читання всього радіообміну фашистської армії Роммеля не врятувало союзників від нищівних поразок в Африці. А по-друге, саме розкриття кодів найбільше сприяло невдачам.

Так, одного разу з пустелі Роммель доповів Берліну про своє невтішне становище. Коли ж натхнена цією звісткою британська армія спробувала оточити його, то була розбита. Виявилося, що стан німецьких військ був нормальним. Схоже, Роммель намагався привернути увагу генштабу до своїх проблем, перебільшуючи їх до гротеску. При Кассерині він ще раз розбив англійців, тому що вони з шифровки знали наказ німецького генштабу виступати йому в одному напрямку, а він пішов у іншому, бо краще бачив ситуацію, що склалася.

Американці ж за день втратили половину бронетанкової дивізії через те, що Роммель розпочав наступ на два місяці раніше зазначеного йому генштабом у шифровці терміну. Читати шифровки ворога – не означає читати його думки! Проникливий та незалежний німець Роммель добре довів цю тезу своїми справами.

Як відомо, після війни Німеччина була розділена на дві окремі держави: Федеративна Республіка Німмечини – ФРН (під контролем США) та Німецька Демократична Республіка – НДР (під контролем СРСР), які створили власні шифрувальні служби у складі своїх органів державної безпеки.

Так, у НДР у квітні 1950 року була сворено Міністерство державної безпеки (нім. *Ministerium für Staatssicherheit*), скорочено – «Штазі» (нім. *Stasi*). До середини 1952 року «Штазі» фактично керувалася винятково радянськими генералами й офіцерами. Її структура та діяльність із самого початку були побудовані так, як і у КДБ СРСР. Зокрема були такі відділи: XI - шифрувальний, «*О*» - прослуховування телефонів, «*F*» - радіоконтррозвідка.

У ФРН 27 вересня 1950 року була створена контррозвідувальна спецслужба – Федеральне управління із захисту Конституції (нім. *Bundesamt for Verfassungsschutz, BfV*), де питання щодо забезпечення функціонування систем секретного зв'язку та інформації, а також підслуховування телефонних розмов було покладено на перший відділ.

У 1955 році у ФРН була створена Федеральна розвідувальна служба (нім. *Bundesnachrichtendienstes, BND*), де питання щодо одержання інформації з каналів зв'язку за допомогою технічних засобів, а також «розкриття» шифрів було покладено на друге відділення (технічна розвідка), що у даний час складається з 1450 співробітників. Технічна розвідка за своїми завданнями та методами схожа на Директорат науки і технології ЦРУ, що нараховує близько 5000 співробітників і займається операціями радіорозвідки.

У 1991 році на базі Центральної шифрувальної служби «*BND*» у Бонні-Мелє-

мі була створена Федеральна служба безпеки в інформаційній техніці (нім. *Bundesamt für Sicherheit in der Informationstechnik, BSI*), на яку було покладено вирішення питань з безпеки в області інформаційної техніки. До цього відносилися перевірка ризиків для безпеки в інформаційно-технічній сфері федеральних органів влади, створення, перевірка та застосування криптографічного матеріалу для інформаційного обміну (наприклад, шифрування таємних документів) на федеральному рівні, а крім того – перевірка та сертифікація інформаційно-технічних систем, підтримка та консультації федеральних відомств, правоохоронних органів, відомств з охорони конституції в інформаційно-технічній сфері, а також підприємств і організацій для протидії економічному шпигунству.

1.7. Перші шифрувальні машини

Історія науки та наукових винаходів багата збігами. Так, наприклад, англійський астроном Д.Адамі та його французький колега У.Левер'є майже одночасно зробили висновок про існування планети Нептун. Винахід «радіо» був майже одночасно зроблений німцем Г.Герцем, росіянином О.Поповим і американцем Г.Марконі. Один з основних методів перетворення аналогових сигналів у цифрову форму – дельта-модуляція – був винайдений незалежно декількома вченими у Франції (Е.Делорейн, С. ван Мієро і Б.Дерьявич), СРСР (Л.Коробок) і США (К.Катлер, Ф. де Яджер).

Не дивно, що подібні збіги мали місце й у криптології. У період між двома світовими війнами одне і те ж відкриття було зроблене відразу кількома людьми у різних країнах. Як і Вернам, спонукувані широким використанням секретного зв'язку у воєнний час і наступом епохи механізації, вони незалежно один від одного винайшли машину, принцип дії якої протягом дуже тривалого часу знаходив найбільш широке застосування в криптології.

Такими талановитими винахідниками були:

- Едвард Хеберн у США;
- Хуго Кох і Артур Шербіус у Німеччині;
- Арвід Дамм і Борис Хагелін у Швеції.

Винайдений ними принцип ґрунтувався на використанні шифродиска – колеса з перепайками. Шифродиск являв собою товсту круглу пластину, виготовлену з ізоляційного матеріалу (наприклад, із твердої гуми). По обидва боки шифродиска по окружності на рівній відстані один від одного закріплено по 26 електричних контактів (найчастіше вони робилися з латуні). Кожен контакт з'єднувався перепайкою з яким-небудь іншим контактом на протилежній поверхні шифродиска. Таким чином, утворювалося електричне коло, що починалося на одному боці

шифродиска та закінчувалося на іншому.

У найпростішому варіанті контакти на одній поверхні диска являли собою букви відкритого тексту (вхід), а контакти на іншій поверхні – букви шифротексту (вихід), а дротові перепайки між входом і виходом забезпечували перетворення відкритого тексту в криптограму. Для зашифрування букви відкритого тексту потрібно було тільки подати імпульс струму на вхідний контакт, що відповідав цій букві. Струм проходив з'єднувальним провідником та з'являвся на вихідному контакті, який являв собою букву шифротексту. Якщо записати всі перепайки диска, зафіксувавши з'єднання між входом і виходом, то виходив шифр одноалфавітної заміни. Таким чином, шифродиск здійснював процес шифрування у формі, зручній для електромеханічних маніпуляцій.

Для виконання цих маніпуляцій шифродиск установлювався між двома нерухомими (фіксованими) круглими пластинами, кожна з яких також виготовлена з ізоляційного матеріалу та забезпечена 26 контактами, що закріплені по колу та відповідають контактам, які були на шифродиску. Контакти вхідної пластини були з'єднані з клавішами друкарської машинки, на якій набивається відкритий текст. А кожен контакт вихідної пластини був пов'язаний з яким-небудь пристроєм, призначеним для виводу шифротексту (наприклад, із сигнальною лампочкою). У результаті, наприклад, коли шифрувальник натискав на клавішу «A» на друкарській машинці, він посилав струмовий імпульс від джерела струму на контакт нерухомої вхідної пластини, закріплений за буквою «A». Потім цей імпульс попадав на вхідний контакт шифродиска, що відповідав «A», далі через перепайку проходив на вихідний контакт, а з нього – на лампочку, що засвічувалася над буквою шифротексту (наприклад, буква «R»), що відповідала букві «A».

Якби все, однак, на цьому й закінчувалося, то шифродиск не був би таким чудовим пристроєм. Тоді щоразу при натисканні на клавішу «A» струм протікав би по одному й тому ж електричному колу та в результаті вказував би на ту ж саму букву шифротексту «R». Але вся справа була в тому, що шифродиск не залишався нерухомим, оскільки він обертався.

Припустимо, що він повернувся на одну позицію. Струм, що раніше з контакту «A» вхідної пластини попадав на контакт «R» вихідної пластини, тепер попаде на зовсім іншу букву. Подібним же чином всім іншим буквам відкритого тексту ставилися у відповідність інші букви шифротексту. Виходив новий шифроалфавіт, причому щоразу, коли шифродиск повертався, використовувався інший шифроалфавіт.

Можна виписати всі ці шифроалфавіти у вигляді таблиці з 26 рядків і такої ж кількості стовпців. Якщо шифромашина була сконструйована таким чином, що шифродиск повертався рівно на одну позицію щоразу, коли зашифровувалася яка-небудь буква відкритого тексту, то підсумковий результат був таким же, як і при циклічному використанні цієї таблиці – рядок за рядком зверху вниз. Виходи-

ло не що інше, як шифр багатоалфавітної заміни з періодом 26.

Така машина, як і раніше, не виправдовувала покладених на неї надій, оскільки реалізований за її допомогою процес шифрування був нестійким. Однак, якщо замість нерухомої вихідної пластини установити поруч з першим диском другий та змусити його переміщатися на одну позицію кожного разу, коли перший диск робить повний оборот, то це дозволить істотно вдосконалити процес шифрування. За рахунок повороту другого шифродиска створюється новий шифроалфавіт – 27-ий. І кожний новий варіант розташування цих двох шифродисків між нерухомими пластинами буде приводити до створення нового шифроалфавіту. Отже, дводискова шифромашина реалізовувала багатоалфавітну заміну зі значно більшим періодом, ніж однодискова. Тепер він дорівнював 676.

Додавання третього диска приводить до того, що це число помножується на 26, тому що всі три диски повертаються у своє вихідне положення тільки через 17576 послідовних тактів зашифрування. При чотирьох і п'ятьох дисках періоди рівні 456976 і 11881376 відповідно.

Виходило, що кожна буква відкритого тексту зашифровувалася за допомогою різних шифроалфавітів. У цьому й полягала перевага дискової системи: застосування додаткових дисків швидко доводить число шифроалфавітів до таких астрономічних величин, що кількісні розходження переростали у якісні. Тепер можна було створити свій шифроалфавіт для кожної букви відкритого тексту, довжина якого набагато перевершувала повне зібрання творів декількох письменників.

Подібна довжина зводила нанівець усяку практичну можливість безпосереднього розкриття шифросистеми на основі частоти повторюваності букв. Для такого розкриття потрібно було приблизно 50 букв на кожний шифроалфавіт, а це означало, що всі п'ять дисків повинні були по 50 разів зробити свій повний оборот. Ніякий криптоаналітик не міг всерйоз розраховувати на те, щоб стати власником такого трофея, навіть, якщо він зробив би це метою усього свого життя.

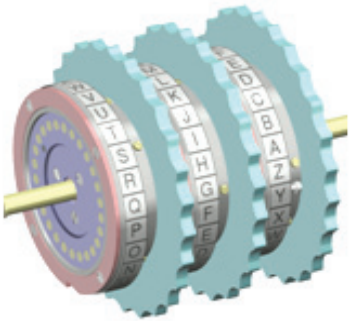
Тому при розкритті дискових шифраторів криптоаналітик повинний був використовувати особливі способи, наприклад, для одержання відкритого тексту в повному обсязі. Отримати його криптоаналітик міг декількома шляхами. Бувало так, що для шифрування двох і більше повідомлень застосовувалася та ж сама початкова установка шифродисків, або що ці установки дуже близькі одна до іншої та послідовність шифроалфавітів перекривалася декількома повідомленнями. Іноді двом криптограмам відповідав той же відкритий текст (так бувало при розсиланні ідентичних наказів до декількох підрозділів). Час від часу відкритий текст ставав відомим у результаті помилок шифрувальника чи опублікування дипломатичних нот. На практиці подібні ситуації траплялися досить часто, що дозволяло криптоаналітику використовувати їх з найбільшою вигодою для себе.

При розкритті дискових шифраторів криптоаналітики зазвичай застосовували

методи вищої математики, що дуже добре підходили для роботи з багатьма невідомими, пов'язаними з шифродисками. В основному, цими невідомими були перепайки в кожному шифродиску. Криптоаналітик математично розмежовував їх, вимірюючи зрушення між вхідними та вихідними контактами. Наприклад, перепайка з вхідного контакту 3 на вихідний контакт 10 означала зрушення, що дорівнювало 7. Подібним же чином усім буквам привласнювалися числові значення, найчастіше: A=0, B=1,..., Z=25. Використовуючи числові значення відомого чи передбачуваного відкритого тексту, криптоаналітик складав рівняння, в яких зрушення в декількох дисках було невідомими величинами, та потім вирішував ці рівняння.

Такими були основні принципи розкриття дискових шифраторів. Але їхнє застосування на практиці прирікало криптоаналітика на найжорстокіші іспити інтелекту, що тільки могли випасти на долю людини. Кількість рівнянь і невідомих, як правило, перевищувала кількість піщин у пустелі, а самі рівняння були складними та заплутаними подібно «гордієву» вузлу. Частково ця складність виникала з необхідності вказати всі зрушення стосовно нерухомої вхідної та вихідної пластини. З іншого боку, це пов'язано з тим, що одне зрушення обчислюється через декілька інших. Зрушення на 3-му шифродиску могло бути відоме тільки як сума зрушень на 1-му і 4-му шифродисках, а зрушення на 4-му шифродиску могло, у свою чергу, дорівнювати сумі зрушень на 2-му і 5-му шифродисках. Таким чином, одне невідоме могло бути виражене через чотири чи п'ять величин. Математична теорія груп дуже підходила для вирішення рівнянь такого типу, але вона також була піддана помилкам.

Характер зрушень, відновлених криптоаналітиком, міг виявитися тільки відносно правильним, та було потрібно додатково знайти перестановку, за допомогою якої можна було одержати абсолютно точні значення цих зрушень. Крім того, шифрувальники супротивника рідко робили послугу, встановлюючи шифродиски в однакові первісні положення при шифруванні усіх своїх повідомлень. Розкриття також дуже ускладнювалося використанням пристроїв, що забезпечували нерівномірний рух шифродисків. Сам шифрувальник міг внести додаткові виправлення, просто переставивши шифродиски. Коротше кажучи, дискова шифросистема створювала винятково складний та стійкий шифр, що містив досить прості елементи.



На початковій стадії появи серійно виготовлених електромеханічних шифрувальних машин вони були віднесені до техніки особливої таємності, і навіть, інструкції з їх експлуатації прирівнювалися до шифрів. Такий порядок був виправданий, оскільки не тільки наявність самої шифрувальної машини, але і будь-яка інформація про неї дозволяла дешифрувальникам

розкривати перехоплені криптограми, виявляти ключі та тривалий час читати таємні повідомлення супротивника. Зрозуміло, багато в чому цьому сприяла слабкість (за сучасною оцінкою) самих ключів, що до того ж мінялися рідко, а часом, навіть, використовувалися повторно, наприклад, у віддалених одна від від одної мережах шифрованого зв'язку.

Крім того, первісні конструкції шифрувальних машин були порівняно прості, що дозволяло математично визначати алгоритми шифрувального перетворення знаків, відштовхуючись від якої-небудь крапки відліку, припустимо, узятої навмання, а потім послідовно визначати алгоритми перетворення всіх інших знаків криптограми. Зазвичай, для дешифрування конкретної криптограми необхідно було знати ключі, що визначали початкові установки шифратора, і все-таки знання алгоритму шифрування, в цілому, зменшувало час і обсяг криптоаналізу, що було також небажано для супротивника.

Утім, пізніше, коли криптологи стали розробляти та впроваджувати в експлуатацію конструкції, що реалізували більш складні машинні шифри, ввели в регламент заміни ключів жорсткі обмеження часу їхнього використання, а також категоричну заборону повторного використання ключа в будь-якій іншій системі шифрованого зв'язку, інформація про шифрувальні машини все одно продовжувала залишатися засекреченою. Причому таке положення справ зберігалося незважаючи на те, що при конструюванні кожної шифрувальної машини розробники завжди враховували та враховують імовірність її захоплення супротивником у процесі бойових дій.

Наявність шифромашини супротивника дозволяла дешифрувальнику, створивши математичні або натурні моделі «антишифратора», використовуючи весь накопичений арсенал засобів і методів криптоаналізу, а також новітні прийоми дешифрування, намагатися виявити ключі та прочитати перехоплені криптограми. Це був хоча і дуже важливий, але лише перший крок на довгому шляху, що проходив дешифрувальник, щоб домогтися позитивного результату, який досягався далеко не завжди. Тому для такої специфічної і «делікатної» науки, як криптологія, характерним і цілком природним є бажання протиборчих сторін виключити витік будь-якої інформації, що може послужити «зачіпкою» для дешифрувальників.

Саме цей підхід і був покладений в основу загальної стратегії забезпечення інформаційної безпеки при використанні електромеханічних шифрувальних машин, аж до самого факту наявності й експлуатації таких. Тому впродовж усього періоду їхнього використання на діючих шифрованих зв'язках, крім самої техніки та документації з її експлуатації та користування, засекречувались відомості про конструкторські бюро та заводи, що розробляли спеціальну техніку, про їхню дислокацію, виробничі потужності, обсяги випуску та інші дані.

Наприклад, при виготовленні німецької «Енігми» у кожному територіально автономному цеху випускалася тільки одна деталь, специфічна для шифрувальної

машини. Особливо охоронявся збірний цех, а контингент робітників ретельно підбирався службою безпеки. Ще далі пішли американці. При виготовленні шифрувальної машини «М-209» на завод, де здійснювалася її зборка, деталі надходили взагалі з інших підприємств.

Слід зазначити, що багато урядів капіталістичних країн скептично відносилися до купівлі дорогої шифрувальної техніки. Після закінчення Першої світової війни і Великої депресії в керівників держав не було бажання витрачати гроші на шифрувальні машини. Бюджети збройних сил були скорочені до мінімуму. Війна, у якій шифрувальна техніка буде затребувана максимально, здавалася досить далекою, тому справа з механізації шифрування у військах рухалася повільно, за винятком країн, що активно готувалися до нової війни, наприклад таких, як СРСР, Німеччина і Японія.

1.7.1. Німеччина

7 жовтня 1919 року голандський винахідник Хуго Олександр Кох (1870-1928), коли йому було 49 років, одержав у Нідерландах патент № 10700 на найвідоміший дисковий шифратор в історії криптології – «таємну друкарську машинку». Він дуже захоплювався конструюванням різних дивовижних пристосувань і справедливо думав, що його новий винахід у сфері криптології буде мати комерційний успіх. Кох вказав у своєму патенті, що проникаючі промені світла та повітря, а також вода чи олія, що протікають по трубках, можуть переносити шифруючий імпульс так же добре, як і електрика, передана по дротах. Він віддавав перевагу дисковому механізму, але не встиг створити жодної шифрувальної машини, що були запропоновані ним у патенті. У 1922 році Кох важко захворів і, передчуваючи швидку смерть, передав усі права на свої патенти іншому німецькому винахіднику.

Крім того, у 1924 році Олександром Кригою (1891-1955), німцем українського походження, прізвище якого переводиться на російську мову як «*лёд*», була створена ланка шифромашин «Крига» (нім. *Kryha*). При чому він розробив три моделі: механічну «*Kryha Standard*», кишенькову «*Kryha Liliput*» і електричну «*Kryha Electric*».

April 14, 1925. 1,533,252

H. A. KOCH

CODING AND DECODING MACHINE

Filed Sept. 10, 1920 3 Sheets-Sheet 3

Fig. 9.

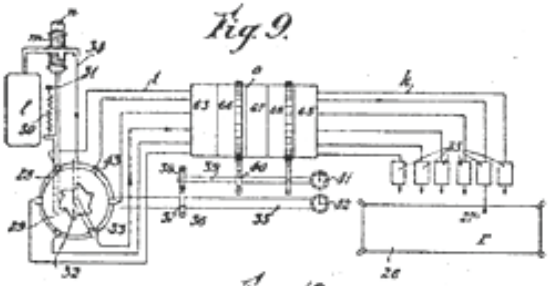
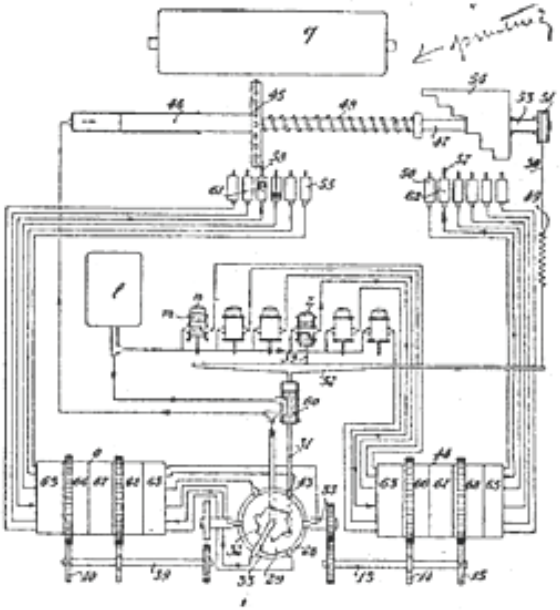


Fig. 10.



Inventor
H. A. Koch
By A. R. Kerslake.
Attorney.

Jan. 21, 1930. A. VON KRYHA 1,744,347

CODING MACHINE

Filed Feb. 20, 1925 2 Sheets-Sheet 2

FIG. 7.

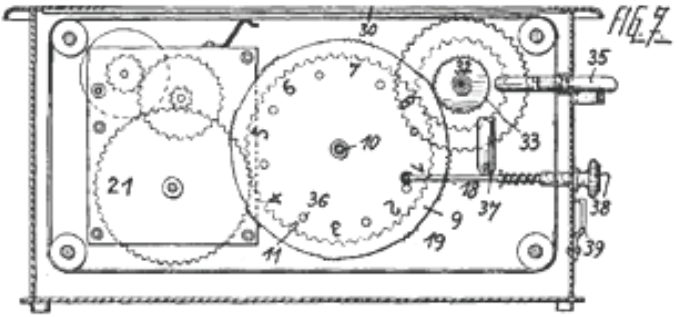


FIG. 8.

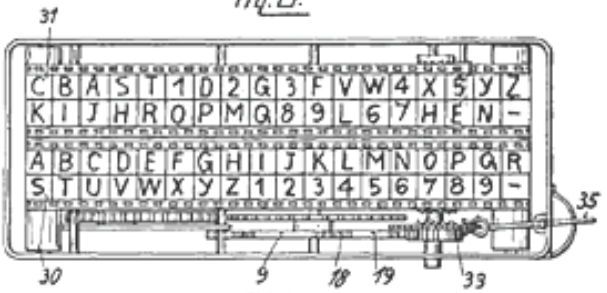
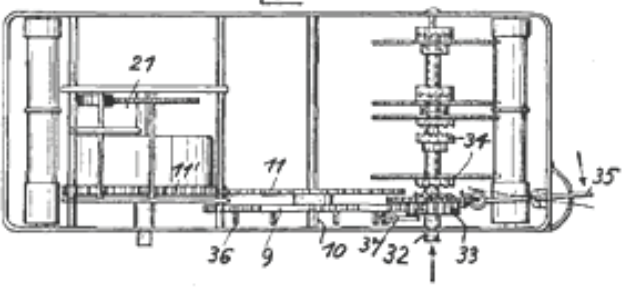


FIG. 9.

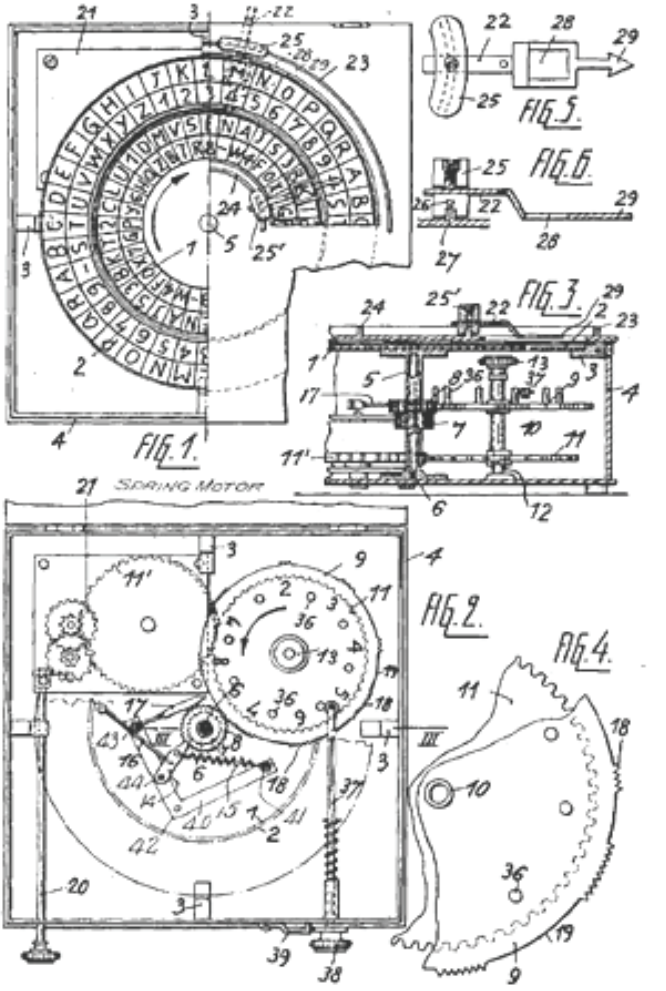


Inventor
A. von Kryha
By Marks & Clerk
Attys.

Jan. 21, 1930. A. VON KRYHA 1,744,347

CODING MACHINE

Filed Feb. 20, 1925 2 Sheets-Sheet 1



Inventor
A. von Kryha
By Marks & Clerk
Attorneys

Механічна шифромашина, яка важила 5 кілограм і в якій шифродиск приводився у дію за допомогою пружинного двигуна, активно використовувалася німецькими дипломатами в роки Другої світової війни, під час якої Крига служив офіцером у вермахті. Електрична шифромашина могла підключатися до телеграфного обладнання компанії «Сіменс і Гальське» і працювати зі швидкістю 360 знаків за хвилину.

Німецьким же винахідником, що успадкував патентні права Коха, став німецький інженер Артур Шербіус (1878-1929), який мав ступінь доктора наук і ряд патентів, у тому числі й у такий далекій від криптології галузі, як кераміка. Перший придуманий ним криптографічний пристрій перетворював цифрові кодові позначення у вимовні слова, по черзі заміняючи цифри на відповідні їм голосні і приголосні букви за допомогою спеціального пристрою. Цей пристрій складався з декількох комутаторів, що з'єднували кожен вхідний провідник з одним з вихідних провідників і які були влаштовані так, що можна було легко змінювати характер цих з'єднань.

Саме він став прообразом дискового (роторного) шифратора, пізніше винайденого Шербіусом і докладно описаного в його черговій патентній заявці. І хоча диски в цьому шифраторі застосовувалися тільки для перетворення цифрових послідовностей, у подібних йому пристроях Шербіус збільшив кількість контактів з 10 до 26, тому ці пристрої цілком могли використовуватися для шифрування букв.

Ще 18 лютого 1918 року Шербіус надав запит на отримання патенту на роторну шифрувальну машину та спільно з Ріхардом Ріттером заснував компанію «Шербіус і Ріттер». Вони намагалися налагодити відносини з німецьким ВМФ і МЗС, але на той момент ті не були зацікавлені в шифрувальних машинах. Надалі вони зареєстрували патенти на підприємство «*Gewerkschaft Securitas*», яке 9 липня 1923 року заснувало корпорацію виробників шифрувальних машин «*Chiffriermaschinen AG*». Шербіус і Ріттер входили до її Ради директорів.

Шербіус назвав свою машину «Енігма» (нім. *Enigma* - загадка). «Енігма» мала істотну відмінність від інших дискових шифраторів: рух шифродисків керувався спеціальними зубчастими колісьми, щоб зробити його нерівномірним. Первісна кількість зубців була занадто малою, щоб істотно ускладнити розкриття шифратора, однак у більш пізніх моделях «Енігми» цей недолік усунули.

Машина мала рухомі на одній вісі диски (ротори), які забезпечували більше мільйона варіантів шифру простої заміни, обумовленого поточним положенням дисків. На кожному боці диска по окружності розташовувалося 25 електричних контактів, стільки ж, скільки було букв в алфавіті. Контакти по обидва боки диска з'єднувалися попарно випадково 25 дротами, які формували заміну символів. Диски складалися разом так, що їхні контакти, торкаючись один одного, забезпечували проходження електричних імпульсів крізь весь пакет дисків. Перед початком роботи диски повер-

Jan. 24, 1928. 1,657,411

A. SCHERBIUS

CIPHERING MACHINE

Filed Feb. 6, 1923

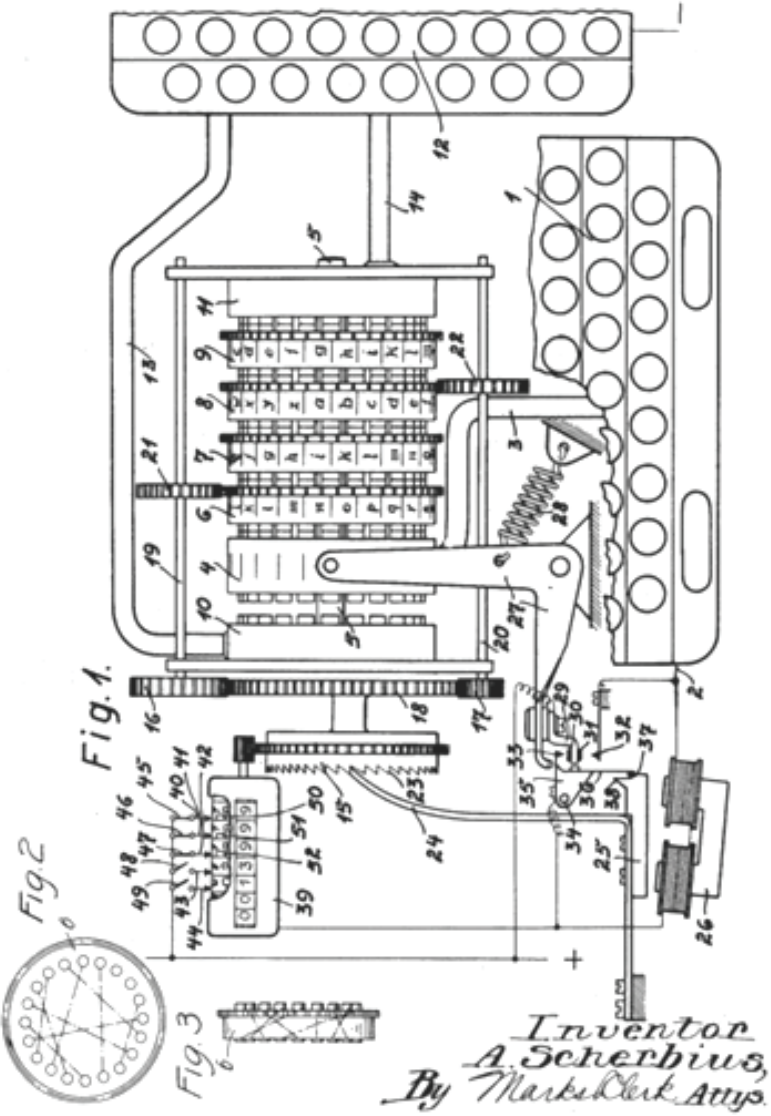


Fig. 1.

Fig. 2

Fig. 3

Inventor
A. Scherbius,
By Marks & Clerk Attys.

талися так, щоб установлювалося визначене ключове слово, а при натисканні клавіші та кодуванні чергового символу правий диск повертався на один крок. Після того, як він робив оберт, на один крок повертався наступний диск. Таким чином, створювався ключ набагато більш довгий, ніж текст повідомлення.

Наприклад, у першому правому диску дріт від контакту, що відповідав букві *U*, був приєднаний до контакту букви *F* на іншому його боці. Якщо ж барабан повертався на один крок, то це вже відповідало заміні наступної за *U* букви *V* на наступну за *F* букву *G*. Оскільки барабани стикалися контактами, то електричний імпульс від натиснутої клавіші з буквою вихідного тексту перш ніж досягав виходу робив декілька замін: по одній в кожному диску. Для ускладнення розшифрування диски з кожним днем переставлялися місцями або мінялися. Подальше вдосконалення цієї машини зробило рух дисків хаотичним, а їх кількість постійно збільшувалася (від 3 до 8). Весь пристрій міг поміститися в портфелі та був такий простий, що обслуговувався звичайними зв'язківцями.

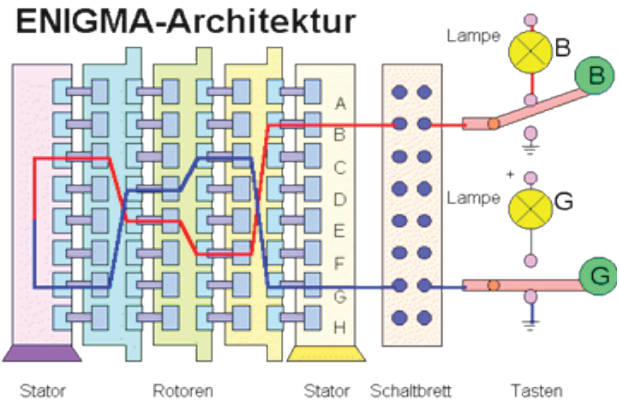
Отже, ключами до «Енігми» були:

– первісне розташування роторів;

– установка обертових роторів у визначену позицію;

– з'єднання пар розеток за допомогою шнурів (за наявності комутаційної панелі).

Тобто загальна кількість можливих ключів виражалася числом з 92 знаків. Крім того, періодично відбувалася зміна ключів, а будь-яке повідомлення повинне було містити не менше десяти груп з п'яти букв у кожній, що ускладнювало дешифрування мате-



матичними методами.

Корпорація «*Chiffriermaschinen AG*» почала рекламувати роторну машину моделі «*Enigma A*», яка була виставлена на огляд на конгресі Міжнародного поштового союзу у 1923 і 1924 роках. Машина була важкою і дуже великою та нагадувала друкарську машину. Її розміри були 65x45x35 см, і важила вона близько 50 кг. Пізніше, була представлена модель «*B*». Моделі «*A*» і «*B*» були зовсім не схожі на пізніші версії (були різних розмірів і форми). Відрізнялися вони і з шифрувальної точки зору - в них не було рефлектора, який був запропонований колегою Шербіуса - Віллі Корном і був встановлений на моделі «*C*» у 1926 році.

Модель «*C*» була менша за розміром і більш портативною, ніж попередники. Вона мала рефлектор - відбивач: усі його контакти розташовувалися винятково на одному боці і були з'єднані тільки між собою. Імпульс, що приходив на цей шифродиск, розвертався на 180 градусів і знову відправлявся через шифродиски, через які він тільки що пройшов, але іншим шляхом. У цій моделі вже не було друкарської машинки, щоб замінити додаткового оператора, який стежить за лампочками, звідси і альтернативна назва «*Glowlamp Enigma*». У 1927 році на заміну моделі «*C*» прийшла модель «*D*».

На перших порах «Енігма» не мала особливого попиту - у 1926-28 роках Рейхсвер (військове відомство Веймарської республіки, яка існувала на території Німеччини у 1919-35 роках, - до приходу до влади Гітлера) придбав всього декілька її примірників для свого ВМФ. У 1934 році Шербіус відійшов від цього проекту, але їм зайнялися доктор Рудольф Хеймсоет і Елсбет Рінке. З цієї миті почався справжній бум у продажу цих машин – їх торгова фірма «*Heimsoeth & Rinke*» з 1935 року і до другої половини Другої світової війни поставляла різні моделі і модифікації «Енігми» як німецьким, так і іноземним відомствам - Іспанії, Італії і Японії. Всього було продано понад 1000 примірників.

Німецький ВМФ першим почав ви-

користовувати машини «Енігма». Модель, яка була названа «Радіоключ С» (нім. *Funkschlüssel C*), почала розроблятися з 1925 року та випускатися з 1929 року. Клавіатура і панель з лампочками складалися з 29 букв від *A* до *Z*, а також *A*, *O* і *U*, розташованих в алфавітному порядку, на відміну від системи «*QWERTZU*». Ротори мали по 28 контактів, буква *X* передавалася безпосередньо, тобто не шифрувалася. Три ротори з п'яти і рефлектор могли бути встановлені в чотири різні позиції, позначені буквами *α*, *β*, *γ* і *δ*. Незначні виправлення в машину були внесені у липні 1933 року.

15 липня 1928 року вермахт впровадив свою власну модель - «*Enigma G*», що була модифікована у червні 1930 року у модель «Енігма I». Вона була також відома як «Військова Енігма», яка широко використовувалася німецькою військовою владою та іншими державними організаціями (наприклад, залізницею) під час Другої світової війни. Значною різницею між «Енігмою I» і комерційною моделлю була комутаційна панель для заміни пар букв, що складалася з 26 пар розеток і штепселів та дозволяла робити ще одну перестановку до надходження сигналу на систему роторів, чим значно підвищувала рівень захисту шифрограм. Також були інші відмінності: використання нерухомого рефлектора та переміщення прорізів з тіла ротора на рухомі буквені кільця. Машина мала розміри 28x34x15 см і важила близько 12 кг.

У 1934 році ВМФ прийняв свій варіант «Військової Енігми», який був названий «*Funkschlüssel M*» або «*M3*». У той час, як вермахт використовував три ротора, для більшої безпеки у морській модифікацій можна було вибрати три з п'яти роторів. У грудні 1938 року у вермахті також були додані два додаткові ротора. Пізніше у 1938 році у військово-морський варіант були додані два додаткових ротори, а у 1939 році - ще один, тому з'явилася можливість вибирати три з восьми роторів.

У серпні 1935 року ВПС також почали використовувати «Військову Енігму» для власного секретного зв'язку. З 1 лютого 1942 року німецькі підводні човни стали використовувати 4-роторну «Енігму», яка була названа «*M4*». Додатковий ротор не занімав більше простору за рахунок розділення рефлектора на комбінацію більш тонкого рефлектора та більш тонкого четвертого ротора.

Також існувала «Енігма II» - велика 8-роторна друкуюча модель, яка використовувалася для зв'язку вищих армійських структур, але незабаром Німеччина припинила її використання - машина була дуже ненадійна і часто заклинювала.

Німецька військова розвідка (абвер) використовувала модель «*Enigma G*». Ця була 4-роторна модель «Енігми» без контактної панелі, але з більшою кількістю виїмок на роторах. Ця модель була оснащена лічильником натиснень клавіш, тому вона також відома як «рахункова машина».

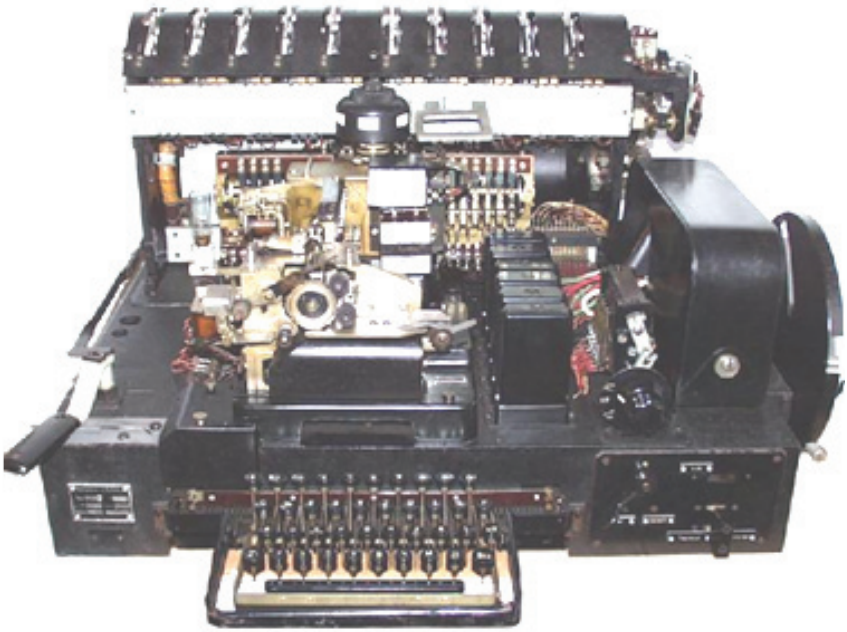
Інші країни також використовували «Енігму». Італійський ВМФ використовував комерційний варіант «Енігми» під назвою «Морський шифр Д» (англ. *Navy Cipher D*), іспанці також використовували комерційну «Енігму» під час громадянської війни.

Швейцарці використовували для військових і дипломатичних цілей модель «*Enigma K*», яка була схожа на комерційну модель «*Enigma D*». Модель «*Enigma T*» (кодова назва «Тірпіц») була випущена для Японії. За приблизними підрахунками всього було випущено близько 100 000 примірників шифрувальних машин «Енігма».

Німецькі військові зв'язківці вважали її дуже надійною та думали, що вона забезпечує необхідну безпеку зв'язку. Її єдиний видимий недолік полягав у тому, що вона не могла друкувати текст, і для швидкої роботи з нею було потрібно, принаймні, троє людей: один читав текст, що вводився, і натискав клавіші, другий вимовляв букви вголос, у міру того як вони засвічувалися, а третій записував текст на папір.

В основних центрах зв'язку Німеччини під час Другої світової війни також використовувалась громіздка шифромашина Т-52 «Таємний писар» (нім. *Geheimschreiber, G-Schreiber* або *Schlüsselfernschreibmaschine, SFM*) компанії «Сіменс і Гальське». Цей електромеханічний пристрій, назва якого в перекладі з німецької означала «хтось, що пише щось таємне», мав 10 або, навіть, 12 шифрувальних дисків-роторів. Із зрозумілих причин розкрити шифр цієї машини було винятково важко.

Таким же складним шифратором була й машина «Ключовий додаток» (нім. *Schlüsselzusatz, SZ*) компанії «Лоренц», яка накладала на відкритий текст одноразову псевдовипадкову шифропослідовність. Вона забезпечувала шифроване листування між ставкою Гітлера і штабами основних армійських угруповань Ні-



меччини.

Крім шифротехніки в Німеччині на початку 30-х років також почали створювати техніку секретної телефонії. Перші випущені апарати датувалися 1932-1933 роками. До роботи були залучені великі німецькі компанії «AET», «Телефункен» і «Сіменс». До кінця Другої світової війни цими фірмами було розроблено до 15 типів апаратури та виготовлено 2180 апаратів. Серійність для складних апаратів була вкрай невеликою – декілька зразків, а основну масу складали «інвертори» різних типів, яких було виготовлено більше 2100.

Паралельно з розробкою техніки у військовому відомстві під керівництвом доктора Лотце велися дослідження можливості дешифрування розробленої апаратури. Доктор Лотце став «грозою» для розроблювачів техніки засекречування телефонних переговорів, давши негативний висновок про гарантії стійкості всіх розроблених фірмами апаратів. Отже, до кінця війни Німеччина не мала апаратів засекречування, що були б стійкі проти дешифрування.

1.7.2. Швеція

Зазначимо, що найскладніший із дискових шифраторів, винайдених на початку XX століття, був запатентований лише через три дні після найпростішого. Хуго Кох одержав свій патент 7 жовтня 1919 року, а 10 жовтня шведу Арвіду Дамму був виданий у Стокгольмі патент № 52279.

Дамм розробив шифромашину та розповів про свій винахід своєму знайомому, який працював у шведському посольстві у Берліні, що і організував зустріч винахідника з капітаном 3-го рангу Олафом Гюльденом, начальником Королівського морського училища в Стокгольмі. У 1915 році Гюльден і Дамм заснували акціонерну компанію (шв. *Aktiebolaget, AB*) «Криптограф» (шв. *Cryptograph*). Компаньйони збиралися продавати шифромашини, спроектовані Даммом після Першої світової війни.

За перші п'ять років існування компанії було створено декілька прототипів роторних шифрувальних машин, зокрема: «*Electrocryptograph B-1*». Проте машини виявлялися ненадійними, їх було неможливо продати, і розробка зупинялася на стадії прототипу. До 1921 року у компанії виникли фінансові труднощі. В цей час

Дамму вдалося знайти нового інвестора Еммануїла Нобеля, який втратив власність в Росії із-за революції. Нобель і його колега Карл Хагелін вирішили, що криптологія може зіграти вирішальну роль в діловій кореспонденції.

В цей час Дамм займався розробкою шифрувальних машин для радіотелеграфії і намагався зацікавити крупні телеграфні компанії. Після приходу в компанію Бориса Хагеліна, Дамму вдалося привернути увагу чотирьох найбільших телеграфних компаній, для роботи з якими Дамм переїхав до Парижа. Тоді ж Дамм розробив шифрувальну машину «*Electrocrypto B-18*» зі спрощеними роторами. Однак у 1927 році Дамм помер, до того, як його роботи отримали визнання.

Безумовно, найбільший внесок у світову криптологію серед шведських фахівців зробив Борис Цезар Вільгельм Хагелін (1892-1983). Він народився на Кавказі, де якийсь час працював його батько, який був керівником російського відділення нафтовидобувної компанії Альфреда Нобеля, винахідника динаміту та засновника знаменитої Нобелівської премії. Протягом декількох років Борис навчався у Санкт-Петербурзі, а потім поїхав у Швецію, де у 1914 році закінчив Королівський технологічний інститут у Стокгольмі, одержавши диплом інженера-механіка. Потім 6 років працював у шведській філії американської компанії «*General Electric*», а згодом близько року провів у США на службі в компанії «*Standard Oil*».

Борис виявляв тягу до винахідництва, захоплювався технікою. У коло інтересів молодого Хагеліна входила й криптологія. Останній він приділяв підвищену увагу. У 1920 році Хагелін зумів утворити перший у світі електромеханічний шифратор. У ньому були клавіатура й індикаторні лампи для набору й отримання відкритих і шифрованих текстів.

У 1921 році батько Бориса Цезар Хагелін і племінник Альфреда Нобеля Еммануїл влаштували його у фірму «*AB Cryptograph*», засновником якої був А.Дамм, а Ц.Хагелін і Е.Нобель були основними акціонерами. Борис фактично представляв інтереси головних акціонерів підприємства. Увійшовши до фірми Дамма, Б.Хагелін активно включився в роботу щодо створення нових шифромашин із прийнятними для потенційних споживачів розмірами, ціною та криптостійкістю.

Першим великим успіхом Б.Хагеліна стала модифікація одного з дискових шифраторів, розроблених Даммом. У 1925 році він довідався, що Генеральний штаб Швеції вирішив ознайомитися з німецьким шифратором «Енігма». До

цих шифромашин увагу шведських збройних сил звернула одна німецька компанія, що збиралася зайнятися їх постачанням у Швецію за умови схвалення пристрою шведською стороною. Хагелін повідомив штабу, що фірма, у якій він працює, готова розробити та запропонувати більш досконалу шифромашину шведського виробництва. Для виконання цієї роботи військовими було виділено 6 місяців.

Виготовлення дослідного зразка шифратора, що одержав назву «*B-21*», обійшлося фірмі «*AB Cryptograph*» у 500 шведських крон (приблизно 110 доларів у той час). Дамм досить критично поставився до роботи свого колеги, а от шведські військові залишилася задоволені «*B-21*» і у 1926 році зробили велике замовлення на її постачання. Хагелін виграв змагання з «Енігмою», і для останньої шлях у Швецію був закритий. Після смерті на початку 1927 року Дамма Б.Хагелін очолив акціонерну компанію, що одержала назву «Криптотехніка» (шв. *AB Cryptoteknik*).

Він зосередив свої зусилля на створенні шифраторів із можливістю друкування шифротекста. У «*B-21*», як і у шифраторі «Енігма», використовувалися електричні лампочки, що загоралися, відзначаючи поточну зашифровану букву при наборі букви відкритого тексту на клавіатурі. Для стаціонарного використання була створена модифікація «*B-22*», що передбачала можливість підключення до стандартних електромеханічних друкарських машинок, так що шифрований і розшифрований тексти автоматично роздруковувалися.

Однак шифрувальний пристрій, що вийшов у результаті, виявився занадто громіздким. Тому незабаром Хагелін вирішив об'єднати в одній машині і друкуючий, і шифруючий механізми.

Пізніше, у 1932 році Франція оголосила конкурс на розробку шифратора для своєї армії. Ця система повинна була стати настільки компактною, щоб міститися в кишені армійської шинелі та застосовуватися безпосередньо на поле бою. Крім того, шифратор необхідно було забезпечити незалежним друкувальним пристроєм. Вже наявні шифратори не відповідали цим вимогам, тому Хагелін створив новий компактний пристрій «*B-211*».

Розглянемо криптологічні принципи роботи шифратора.

Попередньо букви алфавіту відкритого тексту записувалися в таблицю розміром 5x5 (одна буква з найменшою частотою повторюваності викидалася, для шведської мови – буква *W*). Порядок запису алфавіту в таблицю міг бути різним і додатковим ключовим параметром. Кожна буква відкритого тексту пред-

ставлялася парою чисел, що задавали положення букви у відповідній таблиці по горизонталі й вертикалі.

Процес шифрування букви полягав у шифруванні кожної координати окремо, що здійснювалося двома роторами, які реалізовували перетворення комутації. Кутові положення роторів відзначалися відповідною буквою латинського алфавіту від *A* до *K* (без *J*) - всього 10 позицій.

Ротори «*B-211*» відрізнялися від роторів «Енігми». Замість 26 входів і 26 виходів (як у «Енігми») у «*B-211*» кожен ротор містив 5 вхідних контактів і 10 вихідних.

Таким чином, формувалася одна з двох можливих комутацій для кожного ротора при поточному кутовому положенні в залежності від парності такту шифрування. Обертанням роторів керували 4 штифтові колеса, що мали різну кількість кутових положень: 23, 21, 19 і 17.

Кутовим положенням коліс відповідали такі букви латинського алфавіту:

- для 1-го - від *A* до *X*;
- для 2-го - від *A* до *V*;
- для 3-го - від *A* до *T*;
- для 4-го - від *A* до *R*.

На кожному колесі були штифти (стрижні), що відповідали кожному кутовому положенню колеса, яке могло знаходитися або в робочому, або в неробочому положенні. У поточному такті шифрування штифти всіх коліс, що впливали на рух роторів, формували поточну штифтову комбінацію.

Колеса 1 і 2 (з періодом обертання 23 і 21) керували рухом першого ротора за таким принципом: якщо один із двох або обидва штифти в поточній штифтовій комбінації цих коліс знаходилися в робочому положенні, то перший ротор після зашифрування букви відкритого тексту зрушувався на один крок, інакше простоював.

Аналогічним чином рухом другого ротора керували третє й четверте колеса. У результаті рух роторів став нерегулярним, на відміну від регулярного, послідовного руху відповідних роторів «Енігми». Після шифрування кожної букви колеса зрушувалися на одну позицію. Повний період коліс дорівнював:

23 x 21 x 19 x 17 = 156 009.

Початкове положення роторів і коліс було сеансовим ключем і визначалося набором із 6 букв латинського тексту: дві перші букви – для визначення початкових кутових положень роторів, інші – для положень коліс. Процес розшифрування був зворотним щодо процесу зашифрування. При цьому спеціальна ручка на шифраторі переводилася в положення «розшифрування».

Цей шифратор важив близько 17 кг, працював зі швидкістю 200 знаків у хвилину та містився у дерев'яному футлярі розміром з великий портфель.

Звичайно, до «кишенькових розмірів» було ще далеко, але у першій половині 1930-х років це був найбільш компактний друкуючий шифратор, що відповідав

потребам французької армії того часу, тому був взятий нею на озброєння.

У 1934 році французький генеральний штаб попросив Хагеліна створити «кишенькову» шифромашину. Винахіднику вдалося виконати доручення – розробити компактний механічний друкуючий шифратор, придатний для використання в польових умовах, причому для роботи з ним було достатньо однієї людини. У результаті з'явився шифратор, названий «*C-35*».

Його механічну схему можна умовно розділити на три блоки: набірно-друкуючий, блок обертових коліс і барабан з лінійками.

Набірно-друкуючий блок дозволяв виставляти букву відкритого тексту та зчитувати її шифрований еквівалент із можливістю друкування його на паперову стрічку.

Блок обертових коліс являв собою 5 коліс із різним періодом обертання, що відповідав кількості їхніх кутових положень, позначених буквами латинського алфавіту (без букви W):

- 25 для першого: *A B C D E F G H I J K L M N O P Q R S T U V X Y Z*;
- 23 для другого: *A B C D E F G H I J K L M N O P Q R S T U V X*;
- 21 для третього: *A B C D E F G H I J K L M N O P Q R S T U*;
- 19 для четвертого: *A B C D E F G H I J K L M N O P Q R S*;
- 17 для п'ятого: *A B C D E F G H I J K L M N O P Q*.

Після кожного такту шифрування всі колеса зрушувалися на одну позицію. У зв'язку з тим, що періоди обертання коліс були попарно взаємно простими числами, повний період обертання всіх коліс дорівнював:

17 x 19 x 21 x 23 x 25 = 3 900 225.

Тобто, якщо на початку процесу шифрування кутовим положенням коліс відповідало «AAAAA», то дана комбінація вперше з'явиться знову через 3 900 225 тактів роботи шифратора.

На кожному колесі були спеціальні штифти, кількість яких відповідала числу кутових положень колеса. Кожен штифт міг бути висунутий або вправо й бути «неробочим» (при цьому значення даного штифта дорівнювало «0»), або вліво й стати «робочим» (значення штифта відповідало «1»). Розташування штифтів на колесах утворювало

Aug. 10, 1937. B. C. W. HAGELIN 2,089,603

CIPHERING MACHINE

Filed Aug. 23, 1935 2 Sheets-Sheet 1

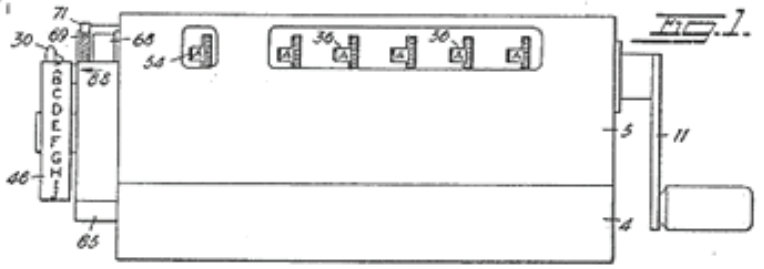


FIG. 1.

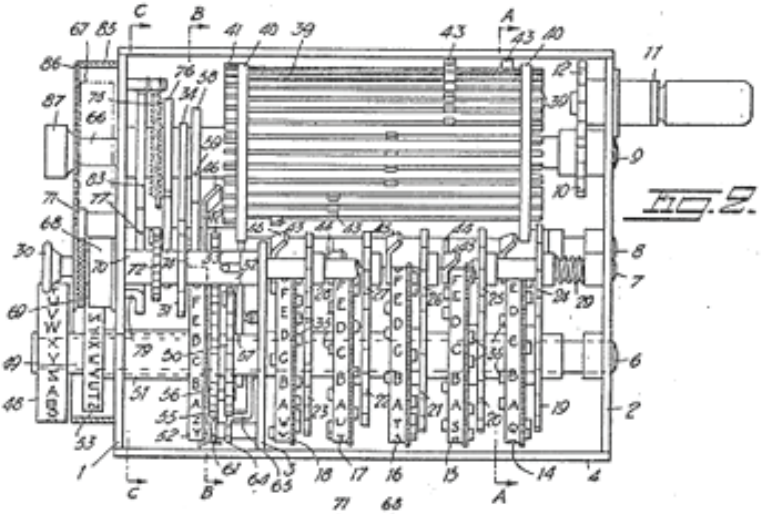


FIG. 2.

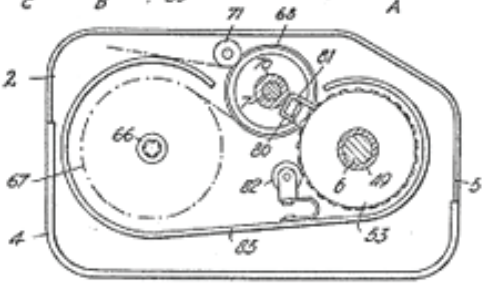


FIG. 3.

Inventor
Boris C. W. Hagelin
By Sommers & Young
Attys

довгостроковий ключ шифратора.

Над кожним штифтовим колесом з лівого боку розташовувалися спеціальні важільці. Якщо на даному колесі в поточній штифтовій комбінації штифт знаходився в робочому положенні (значення штифта дорівнювало «1»), то відповідний важілець висувався нагору. Штифти коліс, що знаходилися у верхній позиції, утворювали так звану поточну штифтову комбінацію, що була двійковим вектором, наприклад «10101».

Барабан із лінійками складався з двох дисків, з'єднаних 25 сталевими лозинами – лінійками. На кожній лінійці навпроти коліс знаходилися нерухомі затиски – рейтори. Розташування рейторів на лінійках у шифраторі «*С-35*» було фіксованим:

- на першій лінійці - навпроти 1-го колеса (всього 1 рейтор);
- на другій і третій лінійках - навпроти 2-го колеса (всього 2 рейтора);
- на четвертій - сьомій лінійках - навпроти 3-го колеса (4 рейтора);
- на восьмій - п'ятнадцятій лінійках - навпроти 4-го колеса (8 рейторів);
- на шістнадцятій - двадцять п'ятій лінійках - навпроти 5-го колеса (10 рейторів).

Натискання на рукоятку шифратора з правого боку приводило до обертання барабана з лінійками.

При цьому рейтори, що мали спеціальні скоси, стикалися з висунутими важільцями та переміщали лінійку, на якій вони розташовувалися, вліво. Висунуті в такий спосіб лінійки утворювали шестірню із змінною кількістю зубів, що, у свою чергу, через шестірньо-передатний механізм приводило до обертання колеса набірно-друкуючого блоку на визначену, довільну кількість кутових положень.

Таким чином, розглянутий шифратор являв собою механічний приклад шифру гамування. Оскільки кількість рейторів була фіксованою, зрушення колеса могло змінюватися від 0 (якщо поточна штифтова комбінація була нульовим вектором) до 25 (при одиничному штифтовому векторі). Після такту шифрування всі колеса блоку штифтових коліс зрушувалися на одну кутову позицію, і нова штифтова комбінація, що з'явилася, висувала відповідні важільці.

Ініціалізація шифратора полягала у встановленні «робочих» і «неробочих» штифтів на колесах (довгострокового ключа) і виставлянні їх початкових кутових положень, яким відповідала п'ятиграма букв латинського алфавіту, розташованих на колесах (разовий ключ, як правило, був свій при шифруванні кожної телеграми).

У жовтні 1937 року французи схвалили шифромашину. Шість примірників модифікованого шифратора, названого «*С-36*», були передані шведським військово-морським силам для іспитів. Фактично новинка являла собою шифратор «*С-35*», але з двома досить істотними доповненнями: наявністю додаткової кришки, що закривала шифратор на ключ, і рухомих рейторів, розташування яких тепер було не фіксованим, а служило ще одним ключовим

параметром (довгостроковим ключем).

Цей апарат реалізовував шифр гамування та відрізнявся невеликими габаритними розмірами (83х140х178 мм) і масою. Хагелін навіть домігся, щоб «*С-36*» роздруковував шифротекст із розбивкою на п'ятизначні групи, а відкритий текст – у вигляді звичайних слів. Швидкість роботи нового шифратора складала в середньому 25 букв у хвилину.

«*С-36*» одержав високі оцінки французьких фахівців, і в результаті Франція замовила відразу 5 тисяч шифраторів, що принесло «*AB Cryptoteknik*» істотний прибуток. В передвоєнні роки машини типу «*С-36*», крім Франції, закупили для використання на лініях зв'язку Великобританія, Італія, Німеччина (за деякими даними німці навіть організували у себе «піратське виробництво» шифромашин і випустили близько 1000 примірників, що використовувалися Абвером і МЗС) і деякі інші європейські країни.

У 1936 році син одного з засновників фірми Верб Гюльден проаналізував стійкість «*С-36*» і порекомендував внести в нього деякі зміни, що були схвалені самими Хагеліном. У результаті було додане ще одне, шосте колесо, а кількість лінійок збільшилася до 29. Новий шифратор одержав назву «*С-38*» і був взятий на озброєння шведської армії.

Приблизно в цей же час Хагелін створив мініатюрні шифратори для французької поліції. Це була дійсно кишенькова апаратура. Вона приводилася в рух великим пальцем лівої руки, а правою рукою можна було записувати шифротекст. Певна кількість цих апаратів також була закуплена Францією. Після війни ідея портативного кишенькового шифратора знайшла свій розвиток у моделях «*CD-55*» і «*CD-57*».

У 1939 році Хагелін створив шифратор «*BC-543*» – електромеханічну реалізацію «*С-36*».

Однак головний успіх чекав Б.Хагеліна в США. Ще в 1936 році він почав листування з американцями щодо можливих закупівель «*С-36*», а в 1937 і 1939 роках зробив тривалі ділові поїздки за океан. Сполучені Штати виявили велику зацікавленість і вирішили закупити модернізований шифратор («*С-38*»). Однак незаба-

ром стало зрозуміло, що організація масового виробництва шифраторів у Європі і відправлення їх в Америку будуть украй скрутні через Другу світову війну, що почалася. Хагелін вирішив виїхати в США й організувати виробництво «*С-38*» безпосередньо в Америці, але виїхати з воюючої Європи було непросто.

Пізніше він згадував: «Звичайну візу одержати було неможливо, тому я переконав шведське міністерство закордонних справ послати мене в Америку як дипломатичного кур'єра. Ми з дружиною відправили наш багаж заздалегідь і сіли в потяг, що вирушав у Стокгольм. Там ми довідалися, що стокгольмські бюро подорожей скасували всі поїздки до США.

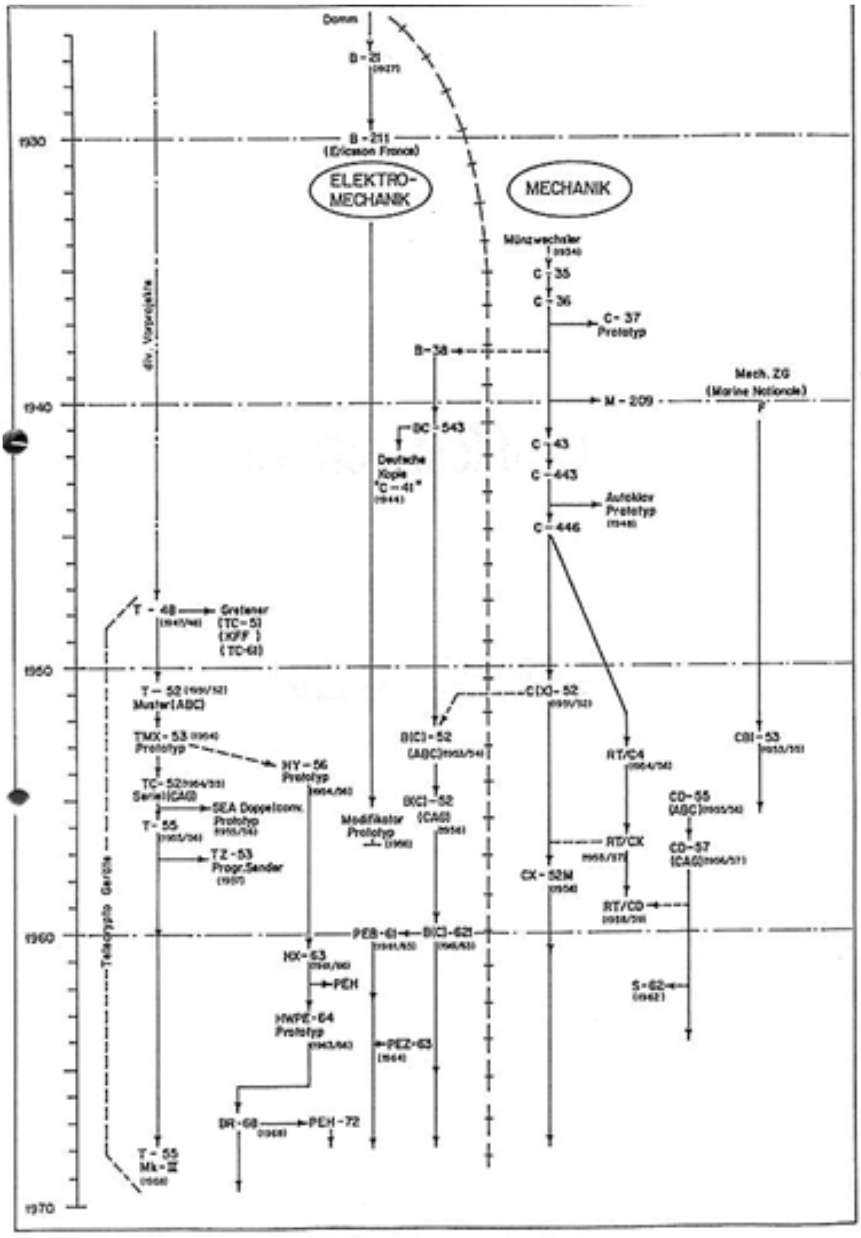
Тоді ми вирішили спробувати відплисти з Італії. З кресленнями в портфелі і двома розібраними шифраторами в сумці ми сіли в експрес «Стокгольм – Берлін». Нам супроводжувала удача. Ми з гуркотом промчалися через саме серце Німеччини і через три дні прибули в Геную. У ту ніч скло у вікнах готелю, у якому ми зупинилися, було побите – ми зовсім випадково вирішили розташуватися в готелі «Лондон», а Італія вже знаходилася в стані війни з Англією. Але ми все-таки зуміли відправитися в Нью-Йорк з останнім рейсом пароплава, що відпливав з Генуї».

Незважаючи на труднощі, Хагелін добрався до США. «*С-38*» американцям дуже сподобався, і вони розгорнули його масове виробництво. В результаті відрахування Хагеліну, як власнику патенту на винахід, склали мільйони доларів. Він став першою людиною, яка нажила багатомільйонний статок завдяки криптології.

У 1944 році Хагелін, уже будучи мультимільйонером, повернувся у Швецію. Після початку «холодної війни» і розвалу старих колоніальних імперій сформувався новий, ще більш ємний ринок шифраторів. «*AB Cryptoteknik*» стала одержувати численні замовлення, як від «старих знайомих», так і від щойно утворених на мапі світу держав. Незабаром до них приєдналися і недержавні організації (у першу чергу банки і великі корпорації, що закуповували шифробладнання для захисту своїх комерційних таємниць).

У перші післявоєнні роки Хагелін зосередив усі свої науково-дослідні підрозділи і виробничі потужності в Стокгольмі. Однак шведське законодавство дозволяло уряду реквізувати винаходи, які були потрібні для забезпечення національної безпеки.

Це змусило Хагелі-


Damm
B-21
1930
B-211
(Ericsson France)
ELEKTRO-
MECHANIK
MECHANIK
Münzwechsler
C-35
C-36
C-37
Prototyp
B-38
Mech. ZG
(Marine Nationale)
1940
M-209
BC-543
Deutsche
Kopie
"C-41"
C-43
C-443
Autoklav
Prototyp
C-446
T-48
Gretener
(TC-5)
(XFF)
(TC-61)
1950
T-52
Muster (ABC)
C(X)-52
TMX-53
Prototyp
HY-56
Prototyp
B(C)-52
(ABC)
RT/C4
CBI-53
TC-52
Serie (CAG)
SEA Doppelconv.
Prototyp
B(C)-52
(CAG)
CD-55
(ABC)
T-55
Modifikator
Prototyp
RT/CX
CD-57
(CAG)
TZ-53
Progr.Sender
CX-52M
RT/CD
1960
PEB-61
B(C)-621
HX-63
PEH
S-62
HWPE-64
Prototyp
PEZ-63
BR-68
PEH-72
T-55
Mk-II
1970
div. Vorprojekte
Telecrypto Geräte

на у 1948 році перенести свою науково-дослідну роботу та самому переїхати у швейцарське місто Цуг, яке виявилося настільки привабливим для підприємницької діяльності (перш за все через податкові пільги), що у 1952 році він заснував там фірму «*Crypto AG*», а у 1959 році перевів туди й інші частини своєї шведської фірми «*AB Cryptoteknik*».

Борис Хагелін працював у фірмі «*Crypto AG*» до 1970 року, а помер у 1983 році, але й донині заснована ним фірма є одним із найбільших світових виробників криптотехніки.

1.8. Розкриття «Енігми»

Існують декілька версій «розкриття» таємниці німецької шифромашини «Енігма»: польська, французька, англійська та шведська.

Найбільш ймовірно, що першими успіхів у дешифруванні «Енігми» досягли польські криптологи. Шифрорган польської армії був утворена 8 травня 1919 року Джозефом Станслицьким відразу ж після проголошення незалежності країни та вже через декілька місяців була перейменована у «Бюро шифрів». Під час громадянської війни в Росії та радянсько-польської війни (1919-1921) поляки перехоплювали та дешифрували радянські військові й дипломатичні повідомлення. Тільки за серпень 1920 року польські криптоаналітики дешифрували 410 таємних телеграм, підписаних Троцьким, Тухачевським, Гаєм і Якіром.

Структура «Бюро шифрів» у ті часи складалася з 4 відділів:

- відділ польських шифрів (захист власних ліній зв'язку);
- відділ радіорозвідки;
- відділ російських шифрів;
- відділ німецьких шифрів.

З 1926 року польські радіорозвідники стали перехоплювати німецькі повідомлення, зашифровані новим невідомим їм шифратором – «Енігмою». У січні 1929 року на варшавську митницю з посольства Німеччини в Польщі прийшло повідомлення, відповідно до якого необхідно було якомога швидше передати працівникам посольства коробку, що потрапила через непорозуміння на варшавську митницю. Коли заінтриговані поляки розкрили коробку, у ній вони знайшли комерційний варіант «Енігми». За іншою версією перше знайомство поляків з ним відбулося ще раніше – у 1927 році.

За дорученням начальника польського шифробюро майора Гвідо Лангера на митницю негайно прибули інженери радіотехнічної фірми «*AVA*», що працювали в тісному контакті із шифробюро. Керував ними Антоній Паллътх – не тільки інженер і співвласник фірми, але й криптоаналітик. Ці люди ретельно вивчили машину, що потрапила до рук польських митників, після чого вона була передана до посольства Німеччини. Ніяких протестів звідти не надійшло: вочевидь, ніхто з працівників посольства не запідозрив, що поляки ознайомилися із вмістом коробки.

Однак спроби співробітників польського шифробюро прочитати німецькі повідомлення, зашифровані за допомогою «Енігми», не дали результату. Справа була в тому, що у Міністерстві оборони Німеччини був прийнятий на озброєння шифратор, що відрізнявся від комерційного варіанта «Енігми».

У 1928-1929 роках у Познані були організовані курси з вивчення криптології для студентів-математиків зі знанням німецької мови. Акцент зробили на поглиблення математичних знань. Таким чином, поляки почали активну підготовку спеціалістів-криптологів. У Познаньському університеті прочитав курс лекцій з криптології начальник «німецького» відділу шифробюро Міністерства оборони Польщі лейтенант Максиміліан Ченжський. У числі приблизно 20 студентів курсу були Маріан Реєвський (1905-1980), Генріх Зигальський (1908-1978) та Єжи Рожицький (1909-1942).

Ці фахівці згодом поступили на службу до шифробюро та першими одержали результати з дешифрування «Енігми». В результаті у Польщі розробили перший математичний апарат для дешифрування «Енігми» та дешифрували деякі перехоплені криптограми. Слід зазначити, що на початку 1930-х років польські криптологи вважалися досить авторитетними фахівцями.

Так, наприклад, японці запросили читати лекції з криптології фахівця з кодів, капітана польської армії Яна Ковалевського. Пізніше до нього в Польщу була направлена група японських студентів, серед яких був Різобар Іто (майбутній великий японський

криптолог), що займався розробкою шифрів і шифромашин, а також криптоаналізом. Зокрема, саме він розкрив шифросистему типу «Playfair», що застосовувалася в 1930-і роки на англійських лініях зв'язку.

У 1931 році польські криптоаналітики одержали досить істотну допомогу з Франції. Влітку того року співробітник німецького військового шифроргану (нім. *Chiffrierstelle*) Ганс Тіло Шмідт через французьке посольство в Берліні запропонував продати уряду Франції деякі таємні документи. Серед них він особливо виділив посібники з експлуатації «Енігми», тому восени того ж року Шмідт декілька разів зустрівся з представниками 2-го бюро розвідувальної спецслужби Франції.

У контакт зі Шмідтом вступили агент 2-го бюро німець за національністю Рудольф Лемуан (справжнє прізвище Шталлман) і начальник шифрувального відділу 2-го бюро Гюстав Бертран. 8 листопада 1931 року Шмідт передав їм довідковий посібник із використання «Енігми» та обіцяв добути діючі ключові установки для шифратора. Лемуан і Бертран зрозуміли, що французька розвідка одержала джерело найціннішої інформації, що може надати велику допомогу в забезпеченні безпеки Франції.

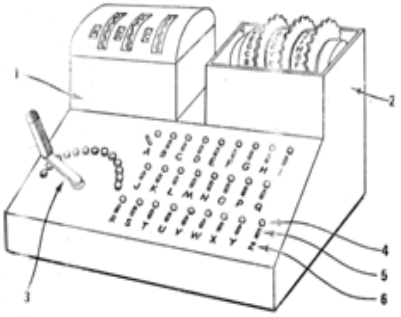
Незабаром за інформацією, отриманою від Шмідта, були ознайомлені французькі криптологи. З цих матеріалів вони з'ясували лише, як шифрувати повідомлення за допомогою «Енігми», однак не зрозуміли, як читати німецькі шифроповідомлення. Тому Бертран був дуже розчарований та вирішив проконсультуватися з англійськими фахівцями: їхня думка збіглася з французькою. Оскільки було відомо, що поляки також ведуть роботи з дешифрування «Енігми», Бертран із дозволу керівництва передав інформацію Шмідта польським колегам.

Інформація французів про німецький шифратор виявилася для поляків украй корисною. Бертран передав фотокопію посібника з використання «Енігми» керівнику польського шифробюро майору Гвідо Лангеру. Після її вивчення поляками був зроблений висновок про те, що німецькі військові адаптували для власних нестатків комерційний варіант шифромашини. Однак співробітники шифробюро підтвердили вердикт, винесений французькими колегами: отримані матеріали не дозволяють читати німецьке військове листування.

У зв'язку з цим Лангер попросив Бертрана спробувати роздобути через свого агента ключові установки «Енігми». Незабаром, коли Шмідт передав їх французам, вони були негайно надіслані до Польщі. У травні і вересні 1932 року від Шмідта були отримані нові ключові установки «Енігми», що знову були доведені до Лангера. При цьому слід зазначити, що поляки не квапилися поділятися інформацією про те, наскільки їм удалося просунутися у «розкритті» «Енігми», з французами.

У 1932 році однокурсникам Реєвському, Зигальському та Рожицькому, які стали на той час офіційними співробітниками шифробюро, вдалося «розкрити» таємницю

«Енігми». У 1934 році Реєвський зробив перший криптоаналітичний «циклометр» (англ. *cyclometer* - лічильник циклів), а у 1938 році сконструював криптоаналітичний пристрій, названий «Бомбою» (пол. *Bomba*), що був здатний швидко перебирати кожну з 17 576 установок, поки не буде отриманий збіг.



Під керівництвом Реєвського на радіозаводі «*AVA*» біля Варшави була розроблена електромеханічна машина «Бомба» - 6 з'єднаних між собою «Енігм», у кожній з яких було встановлено одне з можливих розташувань шифраторів. Разом вони утворювали пристрій висотою близько 1 метра, що був здатний знайти ключ поточного дня менше, ніж за 2 години. Вже з 1939 року у Польщі було налагоджено серійне виробництво таких машин.

Для прискорення процесу «розкриття» ключових установок використовувалася рівнобіжна робота декількох «Бомб». Уперше для керування «Бомбою» стали використовуватися нові носії інформації – перфокарти, винайдені Зигальським. Продовжувала в Польщу надходити і нова інформація від Шмідта, що була досить корисною. Однак поляки як і раніше не квапилися ділитися своїми досягненнями із союзниками – французами та англійцями.

У грудні 1938 року німецькі криптологи підвищили стійкість «Енігми». Всім операторам «Енігми» були передані два нові шифратори, отже, в машині могли застосовуватися будь-які 3 з 5 наявних шифраторів. Коли було тільки 3 шифратори, їх можна було розташувати лише шістьма різними способами, але тепер, коли з'явилися 2 додаткові шифратори, кількість способів їхнього розташування зросла до 60.

Першим завданням Реєвського стало визначення внутрішньої проводки 2-х нових шифраторів. Йому також довелося в 10 разів збільшити кількість «Бомб», щоб врахувати всі можливі розташування шифраторів. Однак вартість утворення такої кількості «Бомб» у 15 разів перевищувала весь річний бюджет Бюро на устаткування. На початку 1939 року ситуація стала ще гірше, коли число кабелів для штепсельної комутаційної панелі зросло з 6 до 10. Тепер, замість 12 букв, для яких виконувалася перестановка перед проходженням шифраторів, їх стало 20. А кількість можливих ключів збільшилася до 159 000 000 000 000 000 000.

У 1938 році кількість перехоплень і дешифрування повідомлень у Польщі досягла максимуму, але до початку 1939 року застосування нових шифраторів і додаткових кабелів штепсельної комутаційної панелі призупинило потік інформації. Польські криптоаналітики відчули, що не маючи ресурсів, необхідних для перевірки всіх можливих установок шифраторів, неможливо знайти ключ поточ-

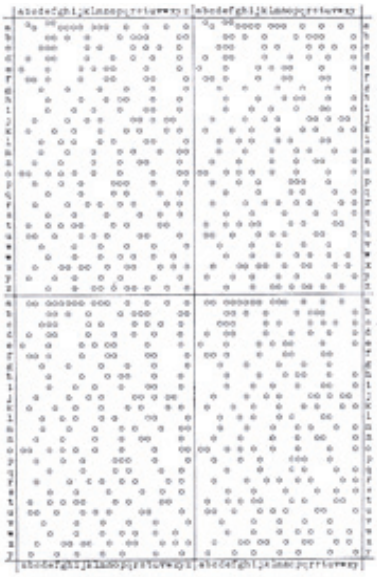
ного дня та здійснити дешифрування.

До червня 1939 року вони зрозуміли, що досягли межі своїх можливостей та нарешті вирішили поділитися своїми досягненнями із союзниками. 30 червня Лангер телеграфував своїм французьким і британським колегам, запрошуючи їх у Варшаву, щоб обговорити деякі невідкладні питання, що стосувалися «Енігми». 24 липня провідні криптоаналітики Франції й Англії прибули до штаб-квартири польського шифробюро.

Була проведена нарада, у якій брали участь англійський криптолог Діллі Нокс, директор англійської урядової криптологічної школи Алістер Денністон, начальник шифрувального відділу французького 2-го бюро Гюстав Бертран і французький криптолог Генрі Бракені. Вони довідалися, нарешті, від своїх польських колег про дешифрування ними «Енігми» та побачили 2 точні її копії й креслення «Бомби».

Присутні на нараді англійці і французи одержали від польських фахівців по одній копії шифратора разом з інструкціями щодо виготовлення та використання перфокарт (плахт Зигальського) для розкриття ключових установок. 16 серпня одна з «Енігм» була переправлена у Лондон.

Після німецької окупації Польщі більшість співробітників польського шифробюро перебралася до містечка Гре-Анвервайс під Парижем. У французькому спеціальному центрі «Бруно» польські криптологи почали працювати під керівництвом французів і спільно досягли певних успіхів. У період з жовтня 1939 по квітень 1940 року ними було дешифровано близько 15 000 німецьких документів (наказів, директив і інших військових повідомлень).



Після того, як Франція була повністю окупована Німеччиною у листопаді 1942 року, Реєвський і Зигальський перебралися через Іспанію, Португалію і Гибралтар у Великобританію. Там вони працювали в підрозділі Польської Армії, розкриваючи німецькі шифри низького рівня.

Після закінчення війни Єжи Рожицький залишився в еміграції у Великобританії, де викладав математику в провінційній школі. Маріан Реєвський у 1946 році повернувся до своєї сім'ї у Польщі і працював бухгалтером, зберігаючи мовчання про свою дешифрувальну роботу до 1967 року. В честь

польських криптоаналітиків у 2002 році у Блетчлі-Парку була відкрита меморіальна дошка, а у 2007 році - в Познані (Польща) перед Імператорським замком був споруджений меморіальний обеліск.

Шведська версія стверджує, що їм також вдалося «розколоти» шифромашину «Енігма» завдяки спільним зусиллям шведської служби радіоперехоплення, агентурної розвідки, що добувала примірники шифровок та їхніх розшифровок у німецькому посольстві, а також професора математики Арне Беурлінга, що розгадав принцип роботи цієї машини. Ну, а керівник служби безпеки Швеції майор Тернберг ділився інформацією з британським військово-морським аташе Денхемом, який відсилав свої повідомлення до об'єднаного розвідувального центру ВМС. Правда, інформація надходила туди з запізненням на 1-2 доби.

Беурлінг не тільки розгадав дуже складний пристрій цієї машини, що дозволяла видавати до 300 трильйонів коливань, але й допоміг сконструювати дешифрувальний пристрій, що перетворював набір цифр у нормальний текст. З того моменту шведи змогли стежити за усім, що відбувалося в німців по сусідству з їхніми границями. Однак у червні 1942 року німці зрозуміли, що шведам вдалося розшифрувати їхній код, і шифр був замінений.

Коли в 1940 році гітлерівські війська окупували Данію і Норвегію, а також знаходилися у Фінляндії, шведські спецслужби виявили максимум зусиль щодо розкриття німецьких шифрів, за допомогою яких відбувався напружений радіо- та телеграфний обмін повідомленнями між Берліном і німецьким посольством в Осло.

Ця історія розкриття шведами німецького шифру знаменна ще й тим, що в цій справі брала участь радянська розвідка. Вона робила це так. Зі служби електронної розвідки Швеції розшифровані німецькі телеграми доставлялися по різних адресах кур'єром Нюбладом, що діяв під виглядом листоноші. Він і був

завербований радянською розвідкою, що навчила його розкривати замок портфеля, у якому лежали телеграми, та швидко їх фотографувати. Плівки відразу передавалися радянському розвіднику та без особливої затримки з'являлися у Москві. Наявність фотокопій розшифрованих телеграм напевно допомогла радянським фахівцям самостійно розкрити німецький шифр, маючи перехоплення з їхніх ліній зв'язку.

Крім того, агент шведських спецслужб Еріка Швартце у 1942-1944 роках працювала секретарем шефа гестапо в німецькому посольстві у Швеції. З її допомогою шведам вдалося розкрити код, яким користувалося німецьке посольство в Стокгольмі. Процес цей проходив унікально. Щодня, ідучи на обід, Еріка відривала невеликий шматочок від копії гестапівської телеграми і, кладучи його під язик, виносила з посольства. Операція продовжувалася кілька тижнів, а шведські криптологи склеювали отримані папірці та проводили дешифрування, накладаючи отриманий відкритий текст на радіоперехоплення зашифрованої телеграми.

А у 1937 році агент британської розвідки Бетті Торп, дружина британського дипломата Артура Паку, спокусивши помічника польського міністра закордонних справ, здобула шифрувальні ключі до шифромашини «Енігма». Після цього Бетті розлучилася з Паком та виїхала на свою батьківщину у США. Свою розвідувальну діяльність у Вашингтоні Торп почала зі здобуття італійського шифру. Вона встановила зв'язок з італійським військово-морським аташе, який під її впливом передав їй італійський шифр. Так британські ВМС отримали дешифровані повідомлення італійського флоту, після чого 28 березня 1941 року цей флот був розбитий британським поблизу грецьких берегів. А здобуті за допомогою Торп французькі шифри мали життєво важливе значення для союзників при висадженні їхніх військ в Алжирі та Марокко.

Англійська ж версія стверджує, що їхні криптоаналітики були добре знайомі з конструкцією «Енігми» ще з середини 20-х років. У червні 1924 року німецька компанія «*Chiffriermaschinen AG*», яка виготовляла цю шифромашину, запропонувала британському уряду закупити партію машин за ціною 190 доларів за штуку. Уряд же ухилився, запропонувавши німцям для початку зареєструвати апарат у Британському патентному бюро, оскільки лише за такою умовою розгляд угоди вважався можливим. Німецька компанія погодилася та надала до Бюро повну документацію з описом роботи шифратора. У результаті криптослужба Британії, не докладаючи скільки-небудь серйозних зусиль, одержала доступ до криптосхеми комерційної версії «Енігми». Але, як свідчать розсекречені недавно документи, військову версію шифратора наступних 15 років англійцям розкрити ніяк не вдавалося.

Як з'ясувалося, британські криптоаналітики зробили невірне припущення щодо логіки супротивника. «Енігма» за своїм виглядом була схожа на звичайну

друкарську машинку, але при натисканні клавіші електричний імпульс надходив у схему криптоперетворення, реалізовану за допомогою набору обертових дисків, що заміняли вихідну букву на зашифровану. Оскільки з кожним натисканням клавіші диски проверталися, то кожного такту знак шифрувався ніби вже новим шифром. Англійці розробили цілком гарні методи для розкриття комерційної версії шифратора, але з відновленням схеми військового варіанту у них нічого не виходило.

За свідченнями Пітера Твіна, одного з учасників тієї криптоаналітичної роботи, вони були впевнені, що «німці не ідіоти, і напевно ввели [у військовому варіанті] додаткові ускладнення там, де їх вочевидь можна внести». Зокрема, усі були абсолютно впевнені, що клавіші машинки приєднані до шифруючих дисків через яку-небудь комутацію, що перемішувала дроти. Але лише після допомоги поляків відкрилася приголомшлива істина: дроти були приєднані за абеткою – буква «А» до першого контакту, «В» до другого і так далі. Власне, саме цей варіант був реалізований і в патентній документації, але спробувати саме його на військовому шифролистуванні – така «дика» думка нікому й у голову не надходила...

Після з'ясування цих подробиць британці 17 січня 1940 року прочитали декілька німецьких шифровок, які були датовані 25 і 28 жовтня 1939 року. До квітня 1940 року час розшифрування радіограм, зашифрованих машиною «Енігма», скоротився до 5 годин. Але перед наступом на Заході у травні 1940 року німці кардинально змінили метод шифрування, і союзникам не вдалося у перші десять вирішальних днів наступу розшифрувати ні однієї радіограми. Десять днів потрібно було криптоаналітикам, щоб навчитися розшифровувати по-новому закодовані радіограми, але за цей час союзне командування уже встигло втратити зв'язок з військами. Однак вже наприкінці травня 1940 року англійські криптоаналітики остаточно розкрили щойно сконструйований код ВПС Німеччини.

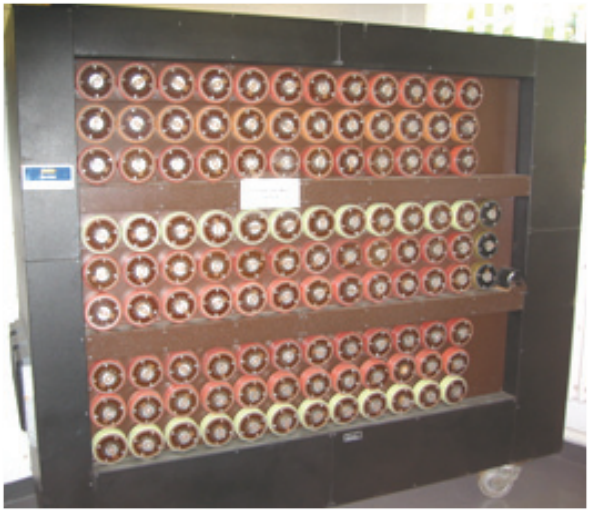
Коли було доведено, що в принципі існувала можливість знаходити ключ і читати шифротелеграми аналітично, шляхом перебору величезної кількості варіантів ключа, народилася ідея механізації процесу криптоаналізу. Британський уряд зміг знайти 100 тисяч фунтів стерлінгів, щоб перетворити цю ідею у працюючі пристрої, що охрестили «бомбами», оскільки за принципом дії вони нагадували «Бомби» Реєвського.

Молодий та дуже талановитий математик Алан Тюрінг (1912-1954) на базі польської «Бомби» розробив свою «бомбу», яка складалася зі 108 електромагнітних барабанів та інших допоміжних блоків. У цілком зібраному стані пристрій Тюрінга складав 2 метри у висоту, 3 метри в довжину, 1 метр у ширину та важив 2,5 тонни. Він завершив розробку своєї конструкції на початку 1940 року, а замовлення на виготовлення машини було передане на завод лічильно-аналітичних машин у Летчворті.

Перший дослідний зразок «бомби», що був названий «Перемога» (англ. *Victory*), прибув у Блетчлі Парк 18 березня 1940 року. Машину відразу ж запустили, але перші результати виявилися незадовільними. Вона працювала набагато повільніше, ніж очікувалося; щоб відшукати ключ, машині потрібно було до тижня часу. Об'єднаними зусиллями ефективність «бомб» підвищили, а 8 серпня розпочала роботу модифікована конструкція, що була названа «Агнець божий» (фр. *Agnus Dei*), або для стислості – «Агнес» (англ. *Agnes*).

Протягом 18 місяців було виготовлено та запущено в роботу ще 15 «бомб», які перевіряли установки шифраторів і відшукували ключі, при цьому кожна стукала немов мільйон в'язальних спиць. Для кожного можливого значення ключа, заданого положеннями роторів (кількість ключів дорівнювала приблизно 10^{19} для сухопутної «Енігми» і 10^{22} для шифрувальних машин, що використовувалася в підводних човнах), «Бомба» виконувала звірку з відомим відкритим текстом, що виконувалася електрично. Якщо все йшло нормально, «бомби» могли знайти ключ «Енігми» протягом 1 години. Після того, як були визначені розташування кабелів на штепсельній комутаційній панелі та установки шифраторів (разовий ключ) для окремого повідомлення, то встановити ключ поточного дня вже було не складно. Слідом за цим могли бути дешифровані й всі інші повідомлення, відправлені того ж дня. «Бомба» серійно випускалася до вересня 1944 року, коли хід війни зробив непотрібним збільшення їх кількості. Всього було побудовано 210 машин.

Доля самого Тюринга після війни склалася трагічно. Він був визнаний неблагонадійним і засуджений у 1952 році за нетрадиційну сексуальну орієнтацію. Вчений покінчив із собою через два роки, не одержавши ніякого визнання й винагороди за внесок у перемогу над фашизмом. Помилка була виправлена лише через багато років, коли на його будинку була встановлена меморіальна дошка, а у 2006 році було ухвалене рішення про створення йому пам'ятника.



У 2007 році британці, оцінивши значний внесок Алана Тюрінга у перемогу Великобританії над

фашизмом, встановили йому пам'ятник роботи скульптора Стівена Кеттла у маєтку «Блетчлі-Парк». Статуя вченого в натуральну величину вагою близько півтора тонни була виготовлена приблизно з півмільйона шматочків чорного уельського сланцю віком 500 мільйонів років. Кількість «деталей» пам'ятника – своєрідний символ неймовірного числа комбінацій, які доводилося аналізувати при розшифруванні секретних кодів.

Успіху британських криптоаналітиків сприяли також помилки німецьких шифрувальників. Так, на початку 1940 року спецгрупа англійської поліції, що займалася прослуховуванням радіоефіру для виявлення можливих нацистських шпигунів на території острова, випадково «відловила» незвичайну шифровану німецьку радіопередачу.

Новий матеріал радіоперехоплення був переданий аналітикам англійської криптослужби, що в ту пору вже займалися в умовах найсуворішої таємності розкриттям і читанням німецького листування, що здійснювалось за допомогою шифромашин «Енігма». Невідомий шифр зовсім не нагадував «Енігму», але надзвичайно зацікавив британських криптологів, оскільки мав ознаки потокового шифрування (хоча в ту пору це називалося інакше), а значить, можна було пошукати в ефірі одноключові комплекти та спробувати їх прочитати.

Цілеспрямовані пошуки незабаром привели до успіху, комплекти дійсно вдавалося зрідка знаходити й частково розкривати, однак і цього вистачило, щоб зрозуміти, що шифролистування відносилося до високого рівня військового командування вермахту. Але, на жаль, не знаючи конкретного пристрою криптосистеми, далі англійським криптоаналітикам просунутися ніяк не вдавалося.

І отут надійшов подарунок «фортуни». 30 серпня 1941 року один з німецьких шифрувальників зробив дивовижну помилку – двічі на одному ключі передав довгу (близько 4 тисяч 5-бітових знаків коду Бодо) телеграму, причому в другий раз, трохи скорочуючи текст, оскільки при запитах прийомної сторони на повторну передачу послання доводилося знову набивати вручну. Робити подібні речі, тобто застосовувати той самий ключ для неідентичних текстів, було категорично заборонено шифрувальникам усіх країн. Однак це було зроблено, а супротивник завжди був напоготові.

Служба англійського радіоперехоплення зафіксувала обидві передачі, а

аналітики, зрозумівши, який коштовний улов потрапив цього разу, старанно «розкрили» шифроповідомлення. В результаті була не тільки цілком прочитана телеграма, але – що найголовніше – з високою точністю відновлена величезна, довжиною майже в 20 тисяч битів шифруюча послідовність. Англійські аналітики не мали ні найменшого поняття, який це був шифратор, але вони вже точно знали, який шифруючий потік він виробляв. Цей шифротрафік у подальшому вони назвали «Риба» (англ. *Fish*).

Те, що відбулося далі, було прикладом рідкісного поєднання небувалої удачі, геніальних прозрінь математиків і майстерності конструкторів-інженерів. На основі розкритої послідовності математикам вдалося цілком відновити досить нетривіальну схему невідомого шифратора (12 шифродисків з різною довжиною періоду і складним законом обертання). Дійсна німецька назва шифратора «*Lorenz Schlüsselzusatz*», який британці умовно назвали «Тунець» (англ. *Tunny*), і його зовнішній вигляд стали відомими набагато пізніше, у самому кінці війни. Таким же складним німецьким шифратором була машина Т-52 «*Geheimschreiber*» компанії «Сіменс і Гальське», яку британці умовно назвали «Осетр» (англ. *Sturgeon*).

Двом британським дешифрувальникам Джону Тільтману (1894-1982) і Біллу Тьюту (1917-2002) вдалося відшукати вади у способі використання шифру Лоренца – ті слабкі місця, якими зуміли скористатися у Блетчлі-Парку та завдяки цьому прочитати листування Гітлера. Для дешифрування повідомлень, зашифрованих шифром Лоренца, було потрібно здійснювати перебір варіантів, порівнювати їх, проводити статистичний аналіз і на підставі отриманих результатів давати оцінку, – нічого подібного «бомби» Тюринга робити не могли. Вони могли з величезною швидкістю вирішувати визначену задачу, але не мали достатню гнучкість, щоб упоратися зі складним шифром Лоренца. Спосіб механізації криптоаналізу шифру Лоренца запропонував Макс Ньюмен (1897-1984), математик із Блетчлі-Парку.

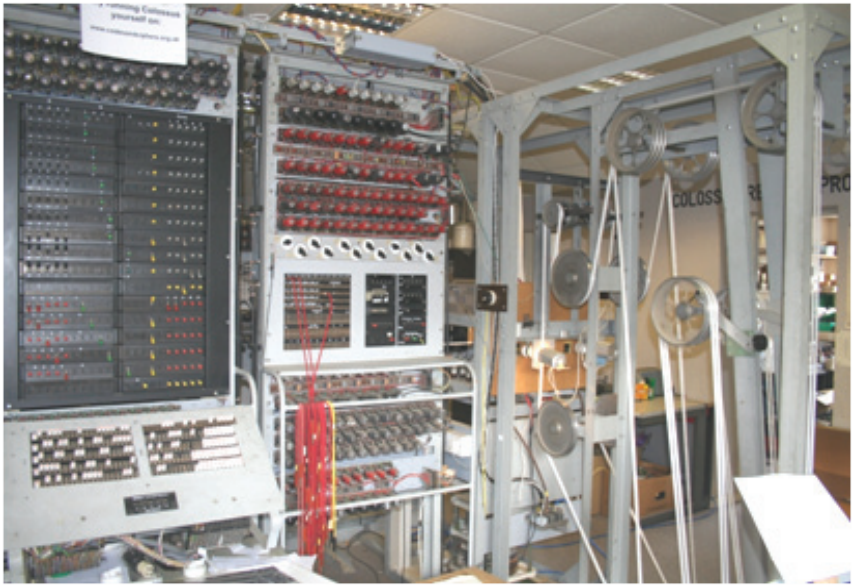
У дослідницькому центрі Управління пошт і телеграфу в Долліс-Хілл (Північний Лондон) інженер Томмі Флауерс (1905-1998) за кресленнями Ньюмена витратив п'ять місяців, щоб створити машину «Хіт Робін-

сон» (англ. *Heath Robinson*), яку у червні 1943 року передав у Блетчлі-Парк. Назва машини була пов'язана з ім'ям американського мультиплікатора, який малював гумористичні абсурдноскладні механічні пристрої.

Однак машина була малошвидкістною та ненадійною, тому спільна робота Флауерса та Ньюмена над вирішенням проблеми дешифрування «Тунця» не припинялася. Постійно вдосконалюючи свій пристрій, вони вже у грудні 1943 року створили електронно-цифрову машину, яка отримала назву «Колос» (англ. *Colossus*). Машина складалася з 1500 електронних ламп, що діяли значно швидше повільних електромеханічних релейних перемикачів «Бомби» і «Хіт Робінсон». Але набагато важливіше швидкості «Колоса» було те, що цю машину можна було програмувати.

У січні 1944 року вона була змонтована у Блетчлі-Парку та 5 лютого розпочала свою роботу. З того часу британський уряд був в курсі практично всіх серйозних операцій німецьких збройних сил. 1 червня того ж року розпочала свою роботу вдосконалена модель «Колос II», яка складалася вже з 2000 ламп і була розроблена інженером дослідницького центру Управління пошт і телеграфу Аленом Камбзом (1911-1995). Всього до кінця війни їх було змонтовано дев'ять.

Після війни «Колос», як і все інше в Блетчлі-Парку, був демонтований, а усім, хто так чи інакше був пов'язаний з роботою над «Колосом», було заборонено навіть згадувати про нього. Інформація про існування цієї машини трималася в секреті до 1970-х років. Уїнстон Черчилль особисто підписав наказ про руй-



нування машини на частини, не перевищують розміром людської руки. Коли Томмі Флауерсу наказали знищити креслення «Колоса», він слухняно відніс їх у котельню та спалив. Так були назавжди втрачені креслення першого у світі комп'ютера. Через свою таємність «Колос» не був згаданий в багатьох працях з історії комп'ютерів, тому визнання за винахід комп'ютера одержали інші вчені.

Тепер повернемося до захоплюючої історії боротьби британців за здобуття шифромашини «Енігма». Відзначимо, що німецькі криптоаналітики сподівалися на те, що навіть у випадку отримання супротивником шифромашини з усіма документами, він недовго зможе читати німецькі радіограми: усього лише до закінчення терміну дії регламентуючих шифрозв'язок документів, що вводилися на суворо обмежений період часу. Тим паче, що всі інструкції друкувалися на розчинному у воді папері, що гарантувало їхнє знищення при спробах захоплення.

Але британці, проте, вважали, що саме володіння шифромашиною забезпечить їм можливість упевнено читати радіопереговори супротивника. Британським командуванням було поставлено завдання – за будь-яких умов добути шифромашини «Енігма». В результаті за німецькими таємницями розгорнулося дійсне «полювання».

Спочатку зі збитого в Норвегії бомбардувальника був знятий авіаційний варіант шифромашини з повним набором ключів. Під час Французької кампанії, коли німці стрімко наступали, одна рота зв'язку набрала таку швидкість, що навіть, обігнала своїх танкістів і заїхала до розташування союзників. У командира цієї роти був вилучений армійський варіант «Енігми». В результаті англійцям залишалося одержати ще морський варіант «Енігми». До її таємниці вони змогли доторкнутися у 1940 році: у лютому на підводному човні «*U33*» були захоплені два ротори, у квітні на судні «Поларіс» - документація, а в червні на підводному човні «*U13*» – сама шифромашина та примірник інструкцій.

Під час рейду на Лофотенські острови 4 березня 1941 року британською абордажною командою з есмінця «Сомалі» під командуванням лейтенанта Уормінгтона на борту німецького сторожового корабля «Краб» були захоплені ротори «Енігми» та різноманітні документи, у тому числі таблиці її ключів, що дозволили читати німецькі переговори протягом декількох тижнів. Знання, отримані при розшифруванні лютневих повідомлень, дозволили дешифрувати усі військово-морські повідомлення за квітень і травень 1941 року, хоча продуктивність і оперативність роботи залишали бажати кращого.

У районі острова Ян-Майен у результаті спецопераций, проведених за даними радіопеленгування, британськими есмінцями «Сомалі» і «Тартар» відповідно були перехоплені німецькі траулери «Мюнхен» (7 травня) і «Лауенбург» (28 червня), що використовувалися як судна метеорологічної розвідки. Оскільки ці траулери впродовж трьох місяців курсували в океані і регулярно передавали відомості щодо по-

години, запеленгувати їх не складало великої праці.

На борту «Мюнхена» були захоплені: шифромашина, шифрувальна книга ближнього зв'язку, кодова метеорологічна книга та військово-морська координатна сітка! Це був «улов», що приніс величезну користь англійцям – середній час між перехопленням повідомлення та його дешифруванням скоротився з 11 днів (на 21 травня) до 4 годин (на 1 червня). Однак захоплення «Мюнхена» було лише тимчасовим рішенням, тому що як тільки термін дії захоплених ключів минув, було необхідно одержати нові. На траулері «Лауенбург» були захоплені ключові установки вже на липень, які у паніці були залишені екіпажем. У результаті цього захоплення було забезпечене дешифрування німецьких повідомлень з серпня 1941 року практично аж до кінця війни.

Але головний «подарунок» британці одержали 9 травня 1941 року при захопленні німецького підводного човна «*U110*». Цього разу до них потрапила не тільки справна шифромашина, але й весь комплект документів таємного зв'язку, що діяв до кінця червня 1941 року, зокрема, резервний ручний шифр «*RHV*» (нім. *Reservehandverfahren*).

27 серпня того ж року був захоплений підводний човен «*U570*», де були знайдені деякі зашифровані та відкриті тексти радіограм за останні 3 дні, а також фрагменти переліку ключових установок «Енігми». Наприкінці грудня 1941 року на захоплених у берегів Норвегії німецьких патрульних кораблях і траулерах були отримані 2 машини «Енігма», ключові установки, таблиці біграм та 5 дисків до неї. Все це 1 січня 1942 року було доставлено у Блетчлі-Парк.

В результаті британці отримали можливість читати німецькі радіограми, передані з використанням шифру «Гідра». Навіть після закінчення терміну дії цих документів у британців виникали тільки короткочасні труднощі при «розкритті» нових шифрів. Будь-який місячний ключ німецьких підводних сил розкривався за дві доби.

1 лютого 1942 року німці додали ще один диск і рефлектор у «Енігму», яка використовувалась підводним флотом у Атлантиці. Нову шифрувальну мережу вони

назвали «Тритон», а британські криптоаналітики - «Акула» (англ. *Shark*), натякаючи на згубні наслідки, які обіцяло це нововведення. Крім того, за 10 днів до цього німці змінили свої «погодні» коди.

В результаті британцям тільки і залишалося сподіватися на захоплення нової шифромашини або документації, що і було зроблено 30 жовтня 1942 року на підводному човні «*U559*», а 17 лютого 1943 року - «*U205*». Криптоаналітики отримали новий «погодний» код та іншу документацію. До цього, протягом майже цілого року, навіть їхні ЕОМ не могли їм допомогти. Після цього шифр «Тритон» став читатися у Блетчлі-Парку, що дозволяло британським ВМС оперативно наносити удари по німецьких підводних човнах, а втрати союзного флоту скоротилися вдвічі.

Як наслідок, 24 травня 1943 року через понесені німцями колосальні втрати підводних човнів адмірал Деніц наказав усім своїм субмаринам залишити Північну Атлантику. У перемозі, здобутій Великобританією на морі, велика заслуга належала британським криптоаналітикам.

Першим з них, хто знайшов спосіб «розкриття» шифру «Тритон» з додатковим диском і рефлектором, був Річард Пендеред (1921-2010). У червні 1943 року він зумів «розкрити» ключові установки «Тритону» за 27 травня, а наприкінці серпня спільними зусиллями у Блетчлі-Парку були прочитані всі німецькі радіограми, отримані з 1 по 18 серпня.

Наприкінці війни британці вже втратили інтерес до «колекціювання» німецьких шифромашин. Вони вважали, що німці вже не зможуть придумати нічого принципово нового, та й дешифрувальна техніка на той час працювала бездоганно. Хоча їм вдалося захопити 4 червня 1944 року ще одну «Енігму» з пошкодженого німецького підводного човна «*U505*», а американцям – 12 квітня 1945 року – «*U1024*».

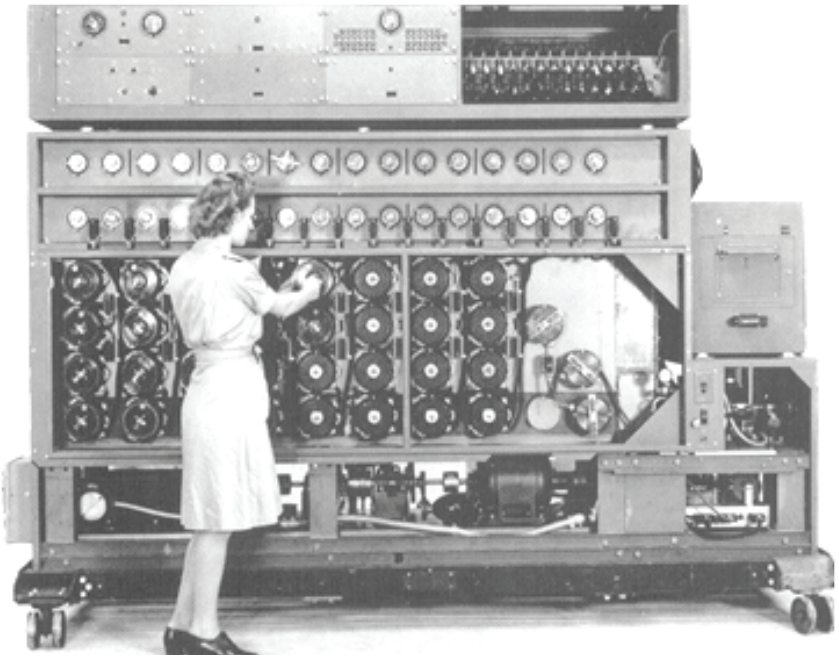
Таким чином, британські криптоаналітики могли менше ніж за день «розколоти» будь-яку шифровку «Енігми», методично перебираючи всі можливі ключі. У той час їм вже допомагали і американські криптоаналітики, які 3 травня 1943 року ввели в дію свою першу «Бомбу» для обчислення ключових установок 4-дискової «Енігми». Американських «Бомб», які працювали швидше та надійніше, було зроблено 121. Виробництво було припинено у вересні 1944 року.

Однак повернемся до німецьких шифросистем. Треба визнати, що в німецьких шифрувальників були підстави покладатися на досконалість своєї «Енігми». Їхні експерти-аналітики вважали, що застосування машинного шифру з перемінними кодами та практично нескінченною кількістю варіантів завалить дешифрувальників ручною роботою на роки. Вони й не передбачали, що їхні шифри будуть «розкривати» обчислювальні машини.

Так, німецькі ВМС для різних цілей використовували різні коди та шифри, яким з травня 1941 року стали привласнювати спеціальні кодові найменування. Найбільш

важливими шифрами німецького ВМФ були такі:

- «Гідра» - застосовувався всіма надводними кораблями на Балтиці й у Північному морі, а також кораблями, що діяли на морських театрах окупованих територій;
- «Тритон» - застосовувався в Атлантиці підвідними човнами, що діяли під безпосереднім керівництвом штабу підводного флоту;
- «Тетіс» - для підводних човнів, що проходили бойову підготовку на Балтиці;
- «Медуза» - для підводних човнів у Середземному морі;
- «Егір» - застосовувався всіма надводними кораблями при дії поза Балтійським і Північним морями;
- «Нептун» - для важких кораблів при виконанні спеціальних завдань;
- «Зюйд» - для надводних кораблів у Середземному і Чорному морях;
- «Слейпнер» - для кораблів при навчальних торпедних стрільбах у Балтійському морі;
- «100» - для рейдерів, допоміжних крейсерів і суден постачання;
- «Тибет» - для суден постачання у далеких водах;
- «Фрейя» - шифр ОКМ і військово-морських командувань на суші. Звичайно, варто відзначити, що для передачі по наземних лініях зв'язку існувала інша



система шифрів;

🗝 «Берток» - шифр для зв'язку між ОКМ і військово-морським аташе в Токіо.

Кожен місяць майже всі шифри (крім «Егіра» і «100») піддавалися серйозним змінам, а дрібні зміни вносилися кожної доби. Також мала місце практика використання коротких умовних позначок.

У ході робіт із розкриття шифрів британські криптоаналітики провели величезну аналітичну роботу. Ґрунтуючись на здогадах і припущеннях, будуючи всілякі гіпотези, багато експериментуючи, вони намагалися за структурою буквених сполучень у зашифрованих повідомленнях розпізнати початкову установку німецьких шифромашин. Так, наприклад, математик Гордон Уелчман розробив своєрідний мережний аналіз, що допомагав відслідковувати, з яких саме організацій супротивника надходили зашифровані повідомлення. Це дозволяло ідентифікувати модель «Енігми», що використовувалася для зашифрування, і заощаджувати багато часу при розкритті її шифру.

Треба відзначити, що домігшись успіхів у розкритті шифрів «Енігми», британці настільки занедбали питання вдосконалення своїх методів шифрування, що німці не мали проблем з їхнім «зламом». За заявою полоненого німецького криптоаналітика, вони не читали все британське листування лише тому, що не вистачало перекладачів із серйозною мовною практикою. Тепер підраховано, що союзники через це втратили 50 тисяч життів моряків, тому що шифри для караванів суден були особливо слабкими.

Британцям також не вдалося прочитати всі шифротелеграми «Енігми» під час війни. Як повідомило 1 березня 2006 року «*CNET News*», тільки через більш ніж 60 років після закінчення Другої світової війни учасникам проекту розподілених обчислень «*M4*» вдалося прочитати одне з трьох повідомлень, зашифрованих за допомогою чотиридискової машини «Енігма» і перехоплених у 1942 році. У Німеччині в той час вважали, що такий захист неможливо зламати при всьому бажанні, оскільки теоретично вона припускала 2x10145 варіантів кодування.

У процесі дешифрування були застосовані як перебір усіх можливих варіантів, так і спеціальні алгоритми добору найбільш ймовірних комбінацій. У результаті одне з повідомлень не встояло перед обчислювальними потужностями сучасних комп'ютерів і було розшифроване. У ньому говорилося: «Під час атаки змушений піти під воду. Глибинні бомби. Остання позиція супротивника 0830h AJ 9863, [курс] 220 градусів, [швидкість] 8 вузлів. Іду [за супротивником]. [Барометр] упав до 14 мілібар, [вітер] північно-східний, [сила] 4, видимість 10 [морських миль]».

Що стосується власної шифротехніки, то британські фахівці, вивчивши ні-

мецьку «Енігму», у 1937 році розробили свою роторну машину «*TypeX*» (*Typex*), яка мала 5 рухомих роторів і нерухомий напівдиск-рефлектор. Всього до закінчення Другої світової війни «*Typex*» було виготовлено близько 12 тисяч штук, а в деяких підрозділах британських збройних сил її використовували до 1970 року.

У 1941 році британці розпочали виробництво спецтехніки лінійного шифрування «*Telekrypton*», яка одночасно шифрувала текст та передавала його в телеграфну лінію. Під час Другої світової війни за її допомогою були створені мережі спеціального зв'язку між посольствами, консульствами та представництвами спецслужб Великобританії у багатьох країнах.

У 1944 році для заміни «*Typex*» була виготовлена шифромашина «*Rockex*», яка мала середню швидкість роботи 75 слів у секунду, працювала у комплексі з телетайпом, постійно вдосконалювалась і мала варіанти від «*Mk1*» до «*Mk6*». Вона використовувалась у більшості британських консульств і місіях у всіх країнах, а також у підрозділах британської армії у період з 1943 по 1973 роки. Деякі британські закордонні пости радіоперехоплення використовували її до 1980 року. Для британських ВПС на базі «*Typex*» була розроблена шифромашина «Меркурій» (англ. *Mercury*), яка мала вже 10 роторів і використовувалась у період з 1950 по 1963 роки.

1.9. Операція «Ультра»

Роботи з дешифрування шифромашини «Енігма» велися в містечку Блетчлі-Парк, куди відразу після початку війни начальник британського департаменту

координації систем зв'язку командор Алістер Деннистон перевів дешифрувальну службу. Там був створений центр, у якому зібрали лінгвістів, криптологів, математиків. Операція по здобуттю та накопиченню інформації, що отримувалась британськими криптоаналітиками та протягом усієї війни поставлялася політичному й військовому керівництву Великобританії, була суворо засекречена під кодовою назвою «Ультра» (англ. *ultra* – понад, украй).

За однією з версій назва операції з'явилося таким чином. У Великобританії, як і в багатьох інших країнах, для позначення ступеня таємності інформації існували грифи «Секретно» і «Абсолютно секретно». Коли постало питання щодо грифа таємності інформації, що одержувалась в результаті дешифрування «Енігми», то був запропонований гриф «Ультрасекретно», який потім скоротився до «Ультра».

Наприкінці 1939 року керівник відділу військової розвідки «*MI-6*» полковник Мензіс призначив капітана ВПС Уінтерботема відповідальним за операцію «Ультра», яка полягала в постачанні командування даними з дешифрованих радіограм. Джерело інформації при цьому ретельно приховувалося. Ступінь таємності операції була така, що кодові слова «Енігма» і «Ультра» були оприлюднені лише через кілька десятків років після війни.

З кінця квітня 1940 року радіограми, що йшли зі ставки Гітлера, вищих штабів вермахту командувачам і від них до ставки, перехоплювалися, розшифровувалися та доповідалися британському та американському керівництву - Черчилю, Рузвельту, командувачам військ на театрах військових дій та іншим особам за суворо обмеженим списком. Оскільки німці передали «Енігму» Японії, американське командування користувалось системою «Ультра» на Далекому Сході та у районах Тихого океану.

Таким чином, на протязі всієї війни як німецьке, так і японське військове командування було практично позбавлено можливості використовувати такий важливий фактор як раптовість. Точні відомості про супротивника, які мало ан-

гло-американське керівництво, полегшували йому планування та ведення військових операцій, давали величезни перевагу. Система «Ультра» забезпечила союзникам можливість успішного проведення бойових дій у Франції та евакуації британських військ із району Дюнкерка, під час «битви за Британію», в операціях у Північній Африці та Італії, при підготовці та здійсненні операції «Оверлорд», в битвах у Нормандії та Західній Європі, під час війни на морі.

Схема роботи була побудована таким чином. Оператори пеленгаторних станцій, які вже у 1940 році контролювали усі потрібні частоти, записували радіограми. Тексти радіограм відразу телеграфом передавалися до Блетчлі-Парку, де сортувалися за ключовими групами та надсилалися для розшифрування до відповідних відділів, що розміщалися у різних будівлях:

1) командування вермахту та люфтваффе - Казарма № 6 (англ. *Hut 6*);

2) командування кригсмарине - Казарма № 8 (англ. *Hut 8*).

Розшифровані радіограми передавалися до Казарми № 3 (англ. *Hut 3*), де вони кваліфікувалися за терміновістю. Після сортування вони розсилалися адресатам через спеціальні підрозділи зв'язку (далі - СПЗ), які були організовані у всіх штабах діючих військ. Для цього СПЗ забезпечувалися постійними лініями радіозв'язку з Блетчлі-Парком, на яких використовувалися машини «*Typex*» та одноразові шифрувальні блокноти. Разом з тим, кожний СПЗ мав термітну бомбу для знищення апаратури та документів у разі надзвичайної ситуації.

Прем'єр-міністр Великобританії Уінстон Черчиль особисто курирував операцію «Ультра», забезпечуючи її гігантський розмах. Хоча британці і могли розшифровувати радіограми, плани верховного німецького командування залишалися для них таємницею, оскільки накази Гітлера передавалися по телефону й телетайпу, доступу до яких у британців не було. Однак їм допомагав французь-

кий шифрувальний відділ, який був розташований під Парижем та забезпечував зв'язок з Блетчлі-Парком.

Черчиль, якому доповідалися відомості згідно з дешифрованими повідомленнями, далеко не завжди знайомив із ними навіть членів свого Кабінету міністрів. Матеріали дешифрування надходили тільки начальникам розвідувальних служб Великобританії. В інші інстанції направлялися тільки розпорядження, засновані на даних, отриманих у ході операції «Ультра». Але і вони складалися так, щоб у Німеччині не змогли здогадатися про джерело інформації.

Не можна не привести трагічний епізод, пов'язаний зі збереженням таємниці «Ультра». 15 листопада 1940 року німці провели проти Англії операцію, що назвали «актом залякування». У результаті масованого нальоту авіації вони майже цілком зруйнували англійське місто Ковентрі. У нальоті брало участь 437 літаків, що скинули на місто 56 тонн запалювальних бомб, 394 тонни фугасних і 127 парашутних мін. Результат був сумним: значні людські жертви, руйнування систем водо- і газопостачання, місцевих авіазаводів, через що випуск літаків у Великобританії знизився на 20%.

При цьому німці утратили всього один літак. Захоплений успіхом операції Гітлер пообіцяв «ковентрізувати» й інші британські міста. Однак трагедії цілком можна було уникнути.

Блетчлі-Парк завчасно одержав інформацію про наліт, що готувався німцями. Можна було розпочати дії для захисту міста та його населення: підсилити протиповітряну оборону, евакуювати жителів тощо. Однак ці заходи могли насторожити німців, що, безсумнівно, спробували б виявити канал витоку інформації про наліт (про планування операції по знищенню Ковентрі в Німеччині знало дуже вузьке коло осіб).

Британські аналітики дійшли висновку, що у випадку прийняття яких-небудь заходів для протидії нальоту німці розгадають таємницю «Ультра», і операція на цьому закінчиться. Трагічне рішення про неприйняття захисних заходів прийняв

особисто Прем'єр-міністр. Довідавшись про це, Президент США Рузвельт написав Черчиллю: «Війна змушує нас усе частіше діяти як Бог. Не знаю, як би я зробив...».

Приведемо ще один трагічний приклад. Британський актор Л.Ховард, що мав світову популярність і одночасно був співробітником однієї зі спецслужб Великобританії, одержав завдання передати важливі таємні документи одному з адресатів розвідки. З цією метою він повинен був полетіти на цивільному літаку. Німецька розвідка агентурним шляхом довідалася про цю операцію.

Німці прийняли рішення знищити літак. У свою чергу, британці, завдяки інформації «Ультра», довідалися про намір супротивника, однак не скасували свою операцію. Літак був збитий, і Ховард загинув. Так Великобританія захищала джерела своїх важливих розвідувальних даних.

Таємницю «Ультра» зберігали і французи, коли дозволили німцям розбомбити свою столицю. Так, наприклад, влітку 1940 року М.Режевський з дешифрованих повідомлень люфтваффе довідався про планований наліт німецької авіації на Париж. Польський криптолог довів до відома французів кількість літаків, маршрут і висоту польоту, а найголовніше – точну дату і час нальоту. Для вжиття заходів залишався цілий тиждень, але зроблено нічого не було, і 3 червня 1940 року літаки люфтваффе провели перше бомбардування Парижа, не зустрівши ніякого опору з боку французьких ВПС і ППО.

Поки обсяг інформації, що отримувалася в результаті дешифрування «Енігми», був відносно невеликий, забезпечення збереження таємниці організувати було нескладно. Зі збільшенням інформаційного потоку та числа його потенційних споживачів ситуація ускладнилася. Повідомляти великій кількості осіб інформацію «Ультра» було ризиковано. У когось з них могло з'явитися бажання поділитися інформацією зі своїми підлеглими, які у свою чергу могли поділитися ще з кимось тощо. У результаті інтенсивність радіообміну через передачу даної інформації зросла б, і німці могли запідозрити, що в англійців з'явилося якесь нове важливе джерело інформації. А отут уже недалеко до підозр про ненадійність своїх шифрів, у тому числі й «Енігми».

У зв'язку з цим, жодному одержувачу інформації «Ультра» не дозволялося передавати будь-кому або копіювати радіограми «Ультра». Усі дії, що розпочиналися на підставі інформації «Ультра», повинні були оформлятися бойовим наказом, наказом або рішенням без посилань на радіограми «Ультра» і з таким розрахунком, щоб не дати супротивнику приводу підозрювати, що його радіограми читалися.

Якщо доводилося розпочинати дії, що могли викликати підозри у супротивника (наприклад, систематичне затоплення восени 1942 року в Середземному морі німецьких конвоїв, що везли африканському корпусу Роммеля пальне), то застосовувалися ті або інші заходи маскування. Наприклад, англійські кораблі та літаки йшли в атаку лише після того, як над конвоєм пролетів розвідувальний літак, який

німці відмінно бачили.

Нерідко при поширенні інформації «Ультра» робилося посилання на якогось агента, що нібито мав доступ до цілком таємних матеріалів німців. Так, наприклад, один із середземноморських конвоїв був знищений у сильному тумані. Тому «маскування» літаком-розвідником здійснити було неможливо.

В результаті «міфічному» агенту в Неаполі була надіслана телеграма з вдячністю за цінні відомості та інформуванням про підвищення його платні. Зрозуміло, телеграма була зашифрована досить слабким шифром, який німці легко «розкрили» та «списали» загибель конвою на діяльність цього агента. За деякими даними, через цю телеграму начальник неаполітанського порту був відсторонений від посади за підозрою у шпигунстві.

Ось ще один приклад. У грудні 1943 року біля норвезьких берегів англійськими кораблями був потоплений німецький лінкор «Шарнхорст». В офіційному повідомленні про знищення «Шарнхорста» британці заявили, що лінкор випадково знайшов англійський катер, тоді як насправді місце розташування корабля вони визначили з перехоплень «Енігми».

Наказ маскувати джерело інформації при проведенні операції «Ультра» виходив особисто від Прем'єр-міністра Великобританії. Він також вимагав, щоб жоден одержувач інформації «Ультра» не мав права за власною ініціативою ставити себе в такі умови, коли з'являлася б найменша небезпека потраплення в полон до супротивника. Деяким старшим офіцерам, що одержували інформацію з дешифрованих повідомлень, забороняли особисту участь у бойових діях. Іноді виникали парадоксальні ситуації, коли для збереження таємності операції «Ультра» треба було поділитися цією інформацією з досить великою аудиторією.

Наприклад, про операцію було повідомлено співробітникам станцій радіоперехоплення. У Блетчлі-Парку побоювалися, що, працюючи «наосліп», ті могли поділитися з ким-небудь про активне перехоплення німецьких повідомлень і

про постійно зростаючий обсяг цієї роботи. Якщо ця інформація дійде до Німеччини, то там цілком могли правильно інтерпретувати цей факт – «Енігма» дешифрована. Однак співробітники станцій радіоперехоплення свято зберігали в таємниці відомості про свою роботу.

А ось приклад вдалого використання інформації «Ультра». У лютому 1941 року з розшифрованої радіограми стає відомо, що командувачем німецькими військами в Лівії був призначений генерал-лейтенант Роммель. З цього моменту всі пов'язані з його ім'ям радіограми одержали гриф особливої терміновості. В результаті більшість вантажів, адресованих генералу Роммелю, знищувалися британською авіацією в океані, причому німецьке командування навіть не уявляло причини загибелі своїх суден.

Як би ретельно не оберігалася таємниця «Ультра», Великобританія вела війну не одна, та деякими криптологічними секретами їй доводилося ділитися з союзниками. Хоча США вступили в Другу світову війну лише 7 грудня 1941 року, з самого початку бойових дій вони допомагали Англії, поставляючи їй озброєння та бойову техніку. Обмінювалися союзники і розвідувальною інформацією.

Вперше питання про надання американцям інформації «Ультра» постало наприкінці 1940 року, але, незважаючи на готовність Черчилля надати цю інформацію, керівники британських спецслужб категорично заперечували проти цього. Нарешті, було прийняте рішення надати за океан мінімум відомостей про машину «Енігма» та результати роботи з її дешифрування і не повідомляти нічого про зміст дешифрованих повідомлень.

Обмін матеріалами, розшифрованими криптоаналітиками, США і Великобританія розпочався ще у 1940 році, що продемонструвало значний успіх британців у «зломі» німецьких кодів, а їх американських колег - японських. Це привело до безпрецедентного рівня співпраці у сфері радіоелектронної розвідки між двома країнами під час Другої світової війни. Делегація відвідала Блетчлі-Парк - штаб-квартиру британських криптологів, а також обмінялася інформацією про німецькі та японські системи кодів.

У відповідь британці все ж таки відкрили факт дешифрування «Енігми». При цьому з американців були узяті особливі зобов'язання: ні при яких обставинах не розголошувати отриману інформацію. Її було дозволено передати тільки керівникам дешифрувальних служб американської армії та флоту. Місія була в цілому успішною та сприяла подальшому розвитку співпраці британських і американських криптологів.

Надалі, в 1941–1942 роках, британці вкрай неохоче інформували США про додаткові дані з криптоаналізу «Енігми», побоюючись витоку інформації, однак співробітництво продовжувалося. Вірність союзницьким обов'язкам взяла гору, і обмін інформацією у сфері криптоаналізу з американцями набув повноцінного характеру. Цьому сприяли два фактори. По-перше, на тісному співробітництві зі США наполягав

Черчилль, а по-друге, американці самі збиралися розгорнути роботу з криптоаналізу «Енігми». Технічні й фінансові можливості Сполучених Штатів були набагато вище британських, і у кінцевому успіху американців сумніватися не доводилося.

Змушувати ж союзників знову вирішувати ті ж проблеми, що уже з успіхом були вирішені в Блетчлі-Парку, британці вважали неправильно. Приблизно з кінця 1942 року в США стала передаватися вся наявна у британців інформація про розкриті ключові установки «Енігми». Мало того, вони ділилися з союзником своєю головною таємницею: інформацією про електромеханічну обчислювальну машину Тюрінга. Незабаром американці налагодили виробництво цих машин у себе та за їх допомогою змогли розкривати німецькі ключі самостійно.

Ще до початку Другої світової війни між британською й американською розвідками існував неофіційний пакт про обмін розвідданими. Ця практика стала приводом для укладання у 1943 році офіційного союзу розвідок, відомого як «Угода *BRUSA*». Однак вже до кінця 1940-х років у рамках підготовки до «холодної» війни з Радянським Союзом, протокол «*BRUSA*» застарів і був замінений «Угодою *UKUSA*», що була ратифікована США і Великобританією у 1947-1948 роках.

До речі, занепокоєння британців відносно збереження таємниці «Ультра» американцями виявилося даремним. У США цим питанням займалися на найвищому рівні, включаючи президента Рузвельта. Так, головнокомандувач союзними військами на Заході генерал Ейзенхауер не інформував про одержані матеріали навіть своїх найближчих соратників. Цікаво відзначити, що серед іншої інформації, отриманої з дешифрування «Енігми», генерал ознайомився з украй невтішними думками німців про здібності деяких заокеанських воєначальників. У своїх спогадах він шкодував, що через необхідність дотримувати таємність не

було можливості ознайомити американських генералів з оцінкою їхньої діяльності супротивником.

Англо-американське співробітництво в сфері криптології не обмежувалося машиною «Енігма». Спільна робота йшла й в інших напрямках. Так, наприкінці 1942 року Алан Тюринг був відряджений до США для консультацій з оцінки криптостійкості апаратури телефонного засекречування вокодерних станцій «*SIGSALY*».

Стали вже відомими численні приклади агентурного проникнення у криптологічні таємниці супротивника. Ці методи давали дуже цінну інформацію для криптоаналітиків. З іншого боку, нерідко результати криптоаналізу приводили до провалу агентів. Приведемо ряд успішних прикладів діяльності союзників у роки Другої світової війни, коли у викритті німецьких агентів британцям і американцям «допомагала» «Ультра».

Так, 8 грудня 1941 року в Блетчлі-Парку дешифрували першу криптограму, зашифровану на спеціальній модифікації «Енігми», що використовувалась абвером. Завдяки інформації, отриманої дешифрувальниками, був викритий ряд німецьких агентів, частину з яких удалося перевербувати. Після цього була розпочата радіогра з німцями в інтересах британської контррозвідки.

В результаті перехоплення й дешифрування німецьких радіопередач англійці виявили німецького агента Е.Сімоеса, португальця за національністю. Було вирішено дозволити йому якийсь час вільно діяти на британській території в надії «виходу» на інших німецьких агентів. Однак незабаром Сімоеса все-таки заарештували. На допиті він пояснив, що його метою було не шпигунство, а бажання добратися з Португалії до Великобританії і там заробляти гроші.

Він видав британцям усі відомі йому дані, включаючи інструкції, мікрокрапки тощо, отримані ним у Лісабоні від вербувальників. Деякі його свідчення були перевірені за іншими джерелами. Слова Сімоеса підтвердилися, тому німецький агент був покараний дуже м'яко.

Під час війни за допомогою дешифрувальників був виявлений інший німецький агент, клерк МЗС Португалії, направлений для роботи до Лондона. Агентом виявився якийсь де Менезес. Його ім'я виявилося на конверті, захованому в дипломатичній пошті. Арешт агента спровокував серйозну проблему, адже основне джерело інформації про нього знаходилося у дипломатичній пошті. Однак посол Португалії в Англії обмежився лише співчуттям із приводу допущеної британцями «нескромності». Менезес був засуджений.

29 листопада 1944 року на атлантичне узбережжя США з німецького підводного човна «*U-1230*» висадилися два диверсанти з метою радіокомандного наведення на Нью-Йорк експериментальної міжконтинентальної балістичної ракети, що розроблювалася знаменитим Вернером фон Брауном. Підозрілих осіб

помітили місцеві жителі та повідомили про них у поліцію, а звідти ця інформація потрапила до ФБР. Подібних повідомлень під час війни були тисячі і на нього просто могли не звернути увагу.

Однак до ФБР також надійшла інформація з дешифрованих перехоплень «Енігми» про те, що підводний човен «*U-1230*» виконує спеціальне завдання в районі, звідки надійшло повідомлення місцевих жителів. У результаті було проведене прочісування місцевості. І хоча спочатку німецьким диверсантам удалося уникнути арешту та добратися до Нью-Йорка, врешті-решт, їх затримали. Пошуки продовжувалися кілька тижнів і стали найбільшою спецопераціею у США під час війни.

Приведемо також приклад, коли інформація «Ультра» не спрацювала. У 1944 році британський фельдмаршал Монтгомері, вчасно попереджений про наявність у районі голландського міста Арнем двох німецьких танкових з'єднань, усе-таки наказав викинути полки 1-ої парашутно-десантної дивізії саме в цьому районі. В результаті вони майже повністю були знищені.

Тепер розглянемо ситуацію з іншим союзником Великобританії з антигітлерівської коаліції – СРСР. Напередодні початку Великої Вітчизняної війни за розпорядженням Черчилля радянському керівництву передали інформацію про підготовку нападу Німеччини на СРСР, отриману англійцями в результаті дешифрування «Енігми». При цьому було заявлено, що вона отримана з агентурних джерел. На жаль, цю інформацію, як і повідомлення на дану тему з інших джерел, Сталін належним чином не оцінив. Він вважав, що англійці бажають втягти СРСР у війну з Німеччиною лише для того, щоб відволікти від себе німецьку агресію.

Керівники операції «Ультра» були категорично проти надання СРСР даних з її матеріалів. У якості одного з аргументів висувалася теза про слабкості радянських шифрів (матеріали щодо «Енігми» могли бути зашифровані на них, перехоплені й дешифровані німцями). У Блетчлі-Парку існували щодо цього докази: з матеріалів «Ультра» було відоме, що напередодні війни німці читали шифровані повідомлення радянських морських суден і одного з авіаційних з'єднань, дислокованого в районі Ленінграда. Однак Черчилль розпорядився передавати до СРСР розвідувальні матеріали, добуті в рамках операції «Ультра», під виглядом

агентурних даних із джерел у нейтральних країнах, свідчень полонених тощо. Будь-які деталі, що могли б свідчити про те, що інформація отримана в результаті дешифрування «Енігми», виключалися.

Наведемо як приклад початок одного з таких повідомлень. У.Черчилль – Й.Сталіну (30.09.1942): «З того ж джерела, що було використане мною для того, щоб попередити Вас про майбутній напад на Росію півтора року тому, я одержав наступну інформацію. Я думаю, що це джерело заслуговує абсолютної довіри. Будь ласка, нехай це буде тільки для Вашого відома». Далі викладалися дані про плани німців на Північнокавказькому фронті. Англійців дуже турбувала можливість проникнення німців до нафтових джерел у Баку, і вони були зацікавлені в тому, щоб радянська армія не допустила цього.

Співробітництво продовжувалося до кінця 1942 року, після чого британці його майже припинили. Винятки робилися під час Сталінградської та Курської битв, однак з 1944 року матеріали «Ультра» офіційним шляхом повністю перестали надходити до СРСР.

У 1941 році мав місце цікавий обмін криптологічними таємницями. Великобританія передала СРСР коди люфтваффе та інструкції з розкриття ручних шифрів німецької поліції в обмін на захоплені нашими військами німецькі шифрувальні документи. Пізніше нашій країні були передані матеріали з розкриття ручних шифрів абверу, але, нічого не одержавши взамін, британці припинили співробітництво із СРСР.

Восени 1941 року США і Великобританія відкрили свої військові місії в містах радянської півночі, що відразу ж потрапили під пильну увагу радянської контрозвідки. Серед іншої важливої інформації контррозвідниками була виявлена наявність у структурі цих місій постів радіоперехоплення. В одному з добутих документів відзначалося, що отримані в результаті перехоплення англійцями «ворожі повідомлення направляються в Адміралтейство з метою розшифровки кодів супротивника». Також було встановлено, що союзники ведуть радіоперехоплення не тільки на німецьких, але і на радянських лініях зв'язку. У 1943 році за допомогою агента, впровадженого в обслуговуючий персонал англійської місії, радянській контррозвідці вдалося добути дані про англійські шифри.

Іноді матеріали, що надходили від британців, не завжди оцінювалися належним чином. Так, улітку 1942 року англійці надали СРСР матеріали, що свідчили про підготовку наступу німців під Харковом. Однак на них не звернули уваги, і радянські війська зазнали важких втрат.

Однак були й інші приклади. На початку лютого 1942 року британці дешифрували наказ верховного німецького командування, у якому військам, що відступали на Східному фронті, пропонувалося не допустити отримання супротивником новітнього озброєння, особливо секретних бронебійних снарядів нової

конструкції. Цю інформацію передали до СРСР. Дійсно, після закінчення битви під Москвою, радянські війська захопили багато німецької техніки й озброєння. Серед трофеїв виявилися і нові снаряди.

З'ясувалося, що їхній сердечник був виготовлений із найміцнішого в ті часи матеріалу – карбіду вольфраму. Родовищ вольфраму на території Німеччини та її союзників не було, отже, він поставлявся з нейтральних країн. Цю інформацію передали англійцям і американцям, їхні спецслужби провели ряд оперативних заходів і зуміли перекрити канали постачання вольфраму до Німеччини, позбавивши її військову промисловість важливої сировини.

А ось як оцінив допомогу англійців Радянському Союзу У.Донован, що керував під час Другої світової війни американською військовою розвідкою в Європі. У своїй доповіді Президенту США Ф.Рузвельту про операцію «Ультра» він відзначив: «Якби англійці пересилали до Кремля перехоплені німецькі військові накази, Сталін, мабуть, усвідомив би справжній стан речей. Однак англійці вважають апарат Блетчлі цілком таємним. Вони використовують перехоплену інформацію у власних цілях».

Однак інформація з матеріалів дешифрування «Енігми» попадала до СРСР не тільки офіційним шляхом. Найбільш повні матеріали надходили завдяки радянській розвідці.

У 1940 році відомий радянський розвідник Кім Філбі (1912-1988) спробував стати співробітником криптослужби Великобританії, однак йому це не вдалося. Пізніше, ставши одним з керівників британської розвідки, Філбі передав радянській розвідці важливі відомості, що, зокрема, висвітлювали діяльність британської криптослужби.

У 1935 році на радянську розвідку почав працювати співробітник МЗС Англії Джон Кернкрос (1913-1995), що передавав до СРСР важливі розвідувальні дані. У березні 1942 року він був переведений на роботу в британську дешифрувальну службу в Блетчлі-Парку для спостереження за розшифруванням британськими криптоаналітиками повідомлень, що зашифровувалися «Енігмою». Кернкросс як знавець німецької мови був призначений редактором матеріалів перехоплення. Протягом майже 3-х років він щотижня передавав радянській розвідці матеріали дешифрувальної служби Великобританії.

Так, 30 квітня 1943 року британці офіційно відправили до СРСР лише попередження про підготовку німецького наступу на Курській дузі (операція «Цитадель»), а також матеріали німецької розвідки про радянські війська у цьому районі, отримані за матеріалами «Ультра». Кернкросс же передав повні тексти перехоплення з указанням частин і з'єднань, що завжди вилучалися з матеріалів «Ультра», коли передавалися до СРСР.

Він повідомив про подробиці майбутньої операції, кількість і номери заді-

яних дивізій (в офіційних англійських повідомленнях номери не вказувалися), дані щодо напрямку ударів, укомплектованості німецьких частин озброєнням, боєприпасами тощо. Ця інформація мала особливу цінність, тому що радянське командування припускало, що німці завдадуть удару в напрямку Великих Лук, а не Курська. Надалі інформацію Кернкроса підтвердили інші джерела.

Особливо він пишався тим, що передані їм шифри позивних німецьких ВПС, розкриті британськими спецслужбами, допомогли радянському командуванню знищити напередодні бою на Курській дузі значну частину німецьких літаків безпосередньо на аеродромах.

Побоюючись, що німецький наступ почнеться 10 травня (хоча насправді почався лише 5 липня), радянське командування 6 травня завдало по 17 німецьких аеродромах у смузі довжиною 1200 кілометрів від Смоленська до Азовського моря попереджувального бомбового удару, підготовленого у режимі надзвичайної таємності. Багато німецьких літаків були пошкоджені на землі. Масовані удари по німецьких аеродромах були проведені також 7 і 8 травня, хоча елемент несподіванки був уже втрачений. Було зроблено 1400 літако-вильотів та знищено 500 німецьких літаків.

Цікаво відзначити, що інформацію Кенкроса підтвердили й наші криптоаналітики. Напередодні Курської битви буквально за добу до початку бою вони «розкрили» шифрований наказ Гітлера про наступ. Перехопивши радіограму, зв'язківці впізнали почерк радиста ставки головнокомандувача супротивника, а за характером передачі зробили висновок, що вона містить важливий наказ.

Дешифрувальники знали, що мова могла йти про великий наступ і припустили, що наприкінці документа знаходився підпис Адольфа Гітлера. За допомогою атаки «відкритий-шифрований текст» криптограма була дешифрована. Наказ Гітлера військам говорив: «Цьому наступу надається вирішальне значення. Воно повинно завершитися швидким і вирішальним успіхом...»

Матеріали «Ультра», передані Кернкросом, помітно доповнювалися даними від співробітника британської розвідки Лео Лонга. З грудня 1940 року він працював у британському міністерстві оборони у відділі військової розвідки «*MI-14*», де займалися аналізом розвідувальної інформації. Лонг регулярно мав доступ до дешифрованих документів. Крім того, радянська розвідка через свого агента Антоні Фредеріка Бланта, який служив у британській контррозвідці «MI-5», мала ще одну можливість знайомитися з матеріалами британської дешифрувальної служби, що за час війни перехопила й розшифрувала понад 15 тисяч німецьких шифровок.

Що стосується радянських фахівців, то дешифрувати «Енігму» у СРСР так і не вдалося. Але це було закономірно, тому що вони не володіли тією вихідною інформацією, що була в англійців. Проте наприкінці 1942 року група військової

дешифрувальної служби виявила теоретичну можливість «розкриття» німецьких телеграм, зашифрованих «Енігмою». Так було сказано в поданні до нагородження орденами 14 офіцерів дешифрувальної служби військової розвідки, що було підписано начальником Головного розвідуправління (ГРУ) генералом І.Іллічовим 29 листопада 1942 року.

Німці досить високо оцінювали можливості радянських дешифрувальників. У січні 1943 року фахівці Управління зв'язку вермахту дійшли висновку про розкриття «Енігми» радянськими криптоаналітиками, тому що в розташуванні оточеного під Сталінградом угруповання німецьких військ знаходилося 26 шифраторів цього типу. Підтвердити факт їхнього знищення в умовах оточення було неможливо, а тому існувала ймовірність захоплення «Енігми» росіянами. Крім цього, серед тисяч полонених, захоплених радянськими військами під Сталінградом, могли виявитися шифрувальники. Виходячи з цього, надалі німці застосовували вже удосконалений варіант «Енігми».

Дійсно, у ході бойових дій під час Другої світової війни до радянських фахівців потрапило декілька шифромашин «Енігма», ключі до них, а також потрапили в полон і зв'язківці-шифрувальники. Так, 2 шифрувальники були захоплені ще в 1941 році, ще 3 – при ліквідації Сталінградського «котла» (як бачимо, підозри німців не були даремними). 28 серпня 1943 року радянським підводним човном «С101» був потоплений німецький човен «*U639*», в результаті чого була отримана майже неушкоджена кодова книга.

А 30 липня 1944 року був одержаний морський варіант «Енігми» з піднятого з дна Фінської затоки німецького підводного човна «*U250*». Однак ефективно скористатися цими трофеями нашим фахівцям не вдалося, в основному, через відсутність достатніх людських і матеріальних ресурсів, а також слабкого розвитку «машинних» засобів обробки інформації.

Найвищим тріумфом «Ультра» було оточення німецьких армій у серпні 1944 року в Нормандії під Фалезом. Повна попередня інформація про німецькі плани, викладені Гітлером, у поєднанні з даними про чисельність всіх німецьких з'єднань, берущих участь у бойових діях, сприяла найкращому виконанню творчих планів генералів Ейзенхауера та Паттона. Завдяки високому рівню таємності операція «Ультра» продовжувалася до закінчення війни. Її внесок у справу перемоги британці й американці оцінили дуже високо.

Прем'єр-міністр Черчиль вважав, що «Ультра» була найважливішим і найтаємнішим джерелом інформації». Він також відзначав, що «Ультра» – це те, чим ми виграли війну». Маршал британських ВПС Слессор писав: «Ультра» – неймовірно цінне джерело розвідувальних даних, що робило майже казковий вплив на стратегію, а іноді навіть і на тактику союзників». Верховний головнокомандувач західними союзними військами генерал Д.Ейзенхауер назвав операцію «Ультра» «вирішальним

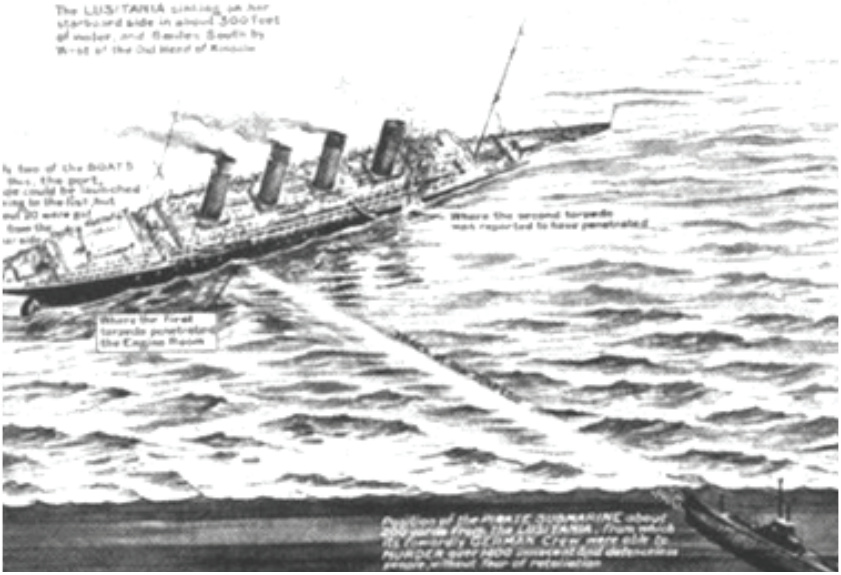
фактором перемоги союзників».

А от думка з «протилежного» боку. Німецький військовий історик Ю.Ровер так оцінив вплив дешифрування «Енігми» на хід військових дій: «Якщо розподілити усі фактори, що зробили вплив на результат битви в Атлантиці, у порядку зменшення важливості, то на вершині виявиться операція «Ультра». У зв'язку з вищесказаним цікавий ще один історичний епізод, що мав місце під час Першої світової війни.

Черчиль, у той час військово-морський міністр Англії, з перехопленого та дешифрованого листування німців довідався про їхній намір потопити в Атлантичному океані лайнер «Лузітанія». Час для вживання превентивних заходів ще залишався: можна було повідомити капітана «Лузітанії» про загрозу та запропонувати йому змінити курс, вислати кораблі прикриття тощо. Однак нічого цього не відбулося, і 7 червня 1915 року лайнер був потоплений німецьким підводним човном «*U-20*».

Загинуло 1198 осіб, у тому числі 115 громадян США. Неприйняття заходів для порятунку «Лузітанії» Черчилль пояснював небезпекою розкриття німцям успіхів англійських криптоаналітиків, хоча багато істориків вважають, що метою Черчилля було схилити Америку до вступу у війну на боці Антанти.

Таємниця операції «Ультра» зберігалася й після закінчення війни. Так, Черчиль у своїх спогадах, присвячених Другій світовій війні, не написав про «Енігму» жодного рядка. Тут слід зазначити, що протягом тривалого часу після війни англійці постачали закордон шифротехніку, в основу якої були покладені принци-



пи «Енігми».

Офіційно ж факт дешифрування «Енігми» був визнаний ними лише 12 січня 1978 року. Лише з цього моменту співробітникам Блетчлі-Парку дозволялося відкрито говорити про свою причетність до розкриття основного німецького шифратора Другої світової війни. Однак їм, як і раніше, заборонялося розповідати які-небудь подробиці своєї роботи з криптоаналізу. Цікаво, що й після війни у Західній Німеччині (ФРН) були настільки упевнені в стійкості «Енігми», що використовували її практично аж до 50-х років.

До речі, свої можливості з криптології приховували не тільки Великобританія, а й усі країни. Японське прислів'я говорить: «Мистецтво полягає в тому, щоб сховати мистецтво». Якщо цим керуватися, то криптологію можна визнати одним з найвищих мистецтв. Англійці посилено поширювали чутки про розгалуженість своєї агентурної мережі та колосальних успіхів радіолокації, американці ж на сторінках своїх чисельних газет запевняли довірливих читачів у тому, що ледве не кожну квадратну милю Тихого океану в них патрулює окремий літак.

Справа доходила до абсурду. Так, наприкінці війни американський шпигун, дезінформований щодо можливостей своєї криптослужби, викрав японську шифромашину. Він так і не зрозумів, чому машина таємно та дуже спішно була повернута на місце, а сам він потрапив у немилість, не одержавши ніяких нагород. Таким чином були суворо покарані німецькі солдати, що захопили при окупації однієї з країн Європи мішки з шифрованим таємним дипломатичним листуванням. Японські шифри, крім американців, розкрили ще й у Берліні, читаючи шифровану кореспонденцію посланця Окамото зі Швейцарії.

Завершуючи цей розділ, треба також відзначити, що британською розвідкою «*MI-5*» для читання зашифрованих повідомлень супротивника використовувався метод перехоплення на відстані сигналів шифрувальних машин за рахунок їхніх побічних електромагнітних випромінювань і наведень (далі – ПЕМВН). Застосування цього методу було описано співробітником «*MI-5*» Пітером Райтом у своїй книзі «Шпигунський улов» (англ. *Spycatcher*) у 1986 році. Цей метод, який був названий кодовим ім'ям «Енгольф» (англ. *Engulf* - захоплення, кидок) був використаний британцями у 1956 році у єгипетському посольстві в Лондоні. Фахівці спецслужби під виглядом зв'язківців розмістили в телефонному апараті шифробюро малопомітний електронний пристрій, що повинен був уловлювати коливання корпусу шифромашини під час її роботи. Через кілька днів із британської спецслужби надійшло перше підтвердження розшифрування єгипетських шифротелеграм.

Так «Енгольф» був прийнятий на озброєння британських спецслужб, що застосували його потім проти чехословацького посольства, потім французького та західнонімецького. Завдяки «Енгольфу» британська спецслужба змогла за-

безпечити надходження своєму уряду повної інформації щодо суецької кризи шляхом читання повідомлень, що надходили до єгипетського посольства в Лондоні, яке Каїр інформував про хід розвитку кризи, у тому числі, й про переговори Єгипту з СРСР, що проводилися єгипетським посольством у Москві. Тобто це дозволило британському уряду бути цілком у курсі радянських позицій у цей критичний період.

Наприкінці 1960-х років Великобританія вела переговори про вступ до Європейського економічного співтовариства, і для англійського уряду дуже важливою була інформація про позицію Франції з цього питання. Тому британська розвідка здійснила перехоплення зашифрованих повідомлень французької дипломатії з проводових каналів зв'язку, захищених французькою дипломатичною шифрувальною машиною за рахунок ПЕМВН з використанням високочастотного нав'язування.

Пітер Райт при аналізі випромінювань помітив, що поряд з основним сигналом присутній і інший дуже слабкий сигнал. Інженерам удалося налаштувати апаратуру на цей сигнал і демодулювати його. На їх подив, це було відкрите незашифроване повідомлення. Виявилося, що шифрувальна машина французів, утім, як і будь-яка інша електрична машина, мала ПЕМВН, що модулювалися інформаційним сигналом ще до моменту його кодування.

Таким чином, шляхом перехоплення й аналізу ПЕМВН французької шифрувальної машини британський уряд, навіть не маючи ключ для розшифровки кодованих повідомлень, одержував всю необхідну інформацію.

1.10. Комп'ютеризація криптології

Працюючи під час Другої світової війни в англійській урядовій криптологічнй школі у Блетчлі-Парку, інженер Алан Тюринг всерйоз захопився створенням електронно-обчислювальної машини (далі - ЕОМ) для розкриття шифрів німецької шифромашини «Енігма». Нічого подібного у той час ще не робили, оскільки для такої машини було потрібно 1200 електронних ламп-тиратронів, і мало хто вірив, що цей «монстр» узагалі буде працювати.

Тільки у 2000 році, коли уряд Великобританії зважився, нарешті, опублікувати 500-сторінковий технічний опис своєї першої ЕОМ «Колос», стало відомо, що британці не відставали від американців. На думку багатьох фахівців, ця машина була не тільки безпосереднім попередником післявоєнних цифрових комп'ютерів, але й першим практичним додатком великомасштабних і програмно керованих обчислень. При цьому Великобританія була першою державою, що використала ЕОМ для «розкриття» кодів і шифрів.

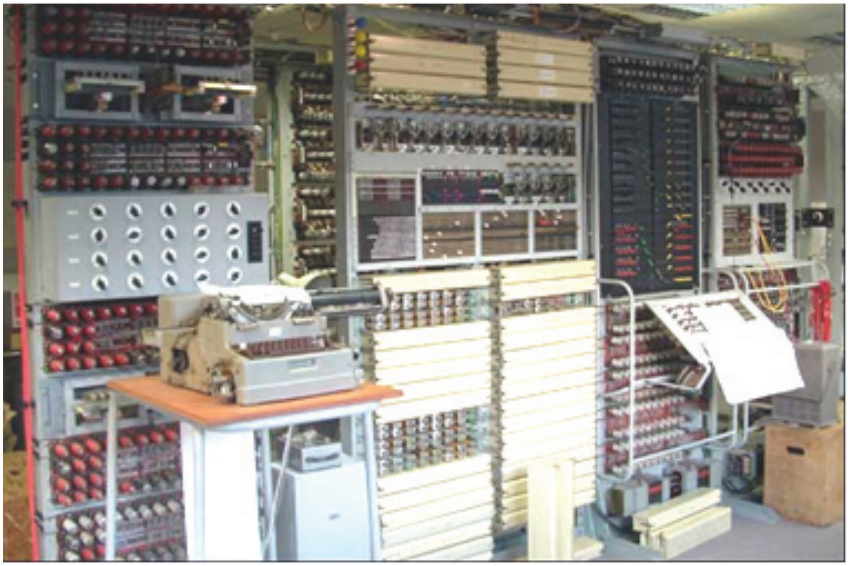
Це була вже програмувальна машина, що виконувала арифметичні та логічні операції над двійковими числами. Вона була обладнана зчитувачем з перфостріч-

ки та електричною друкарською машинкою. За допомогою цих ЕОМ удалося різко прискорити математичні операції при дешифруванні німецьких радіограм вищого німецького керівництва, переданих шифромашинами «Енігма».

Також у розсекреченому документі містився опис і машини «Колос II», досить істотно модифікованої версії ЕОМ, що почала роботу в перших числах червня 1944 року. Характеристики саме цієї моделі дозволили деяким експертам стверджувати, що загальноприйнята історія комп'ютерів потребувала серйозного коригування. Ці ЕОМ щомісяця забезпечували дешифрування близько 300 шифротелеграм командування вермахту. Саме за їхньою допомогою вдалося «зламати» шифр навіть таких складних шифрувальних машин, як німецькі «*Geheimschreiber*» і «*Schlüsselzusatz*».

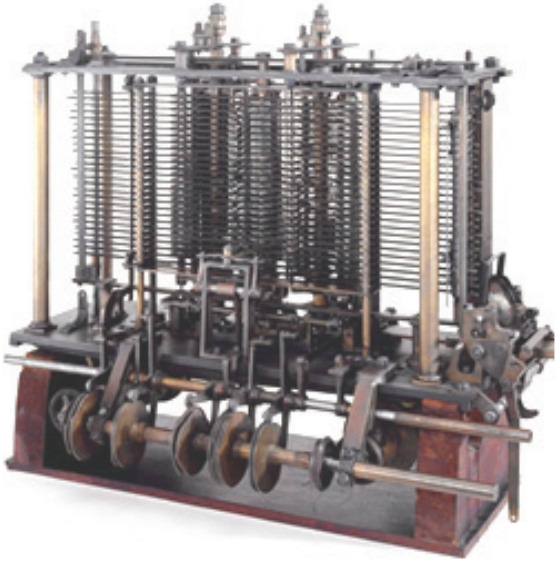
«Колос II» уже мав функціональність і незрівнянно більш значну продуктивність в обробці даних. Так сказав 76-літній професор Единбурзького університету Дональд Мічі, ветеран-криптолог і один з авторів розсекреченого звіту ШКУЗ, підготовленого у 1945 році відразу після перемоги над Німеччиною.

За словами Мічі, якому нарешті було дозволено широко поділитися спогадами про свою надтаємну роботу в роки війни, «можливо, хтось буде вражений, довідавшись, що до Дня перемоги Британія вже мала машинний парк з 10 високошвидкісних електронних комп'ютерів, що працювали цілодобово в тризмінному режимі». Комп'ютер «Колос II» на відміну від його попередника «Колос» уже можна було до визначеного ступеня перепрограмувати, що, без-



умовно, було найважливішим досягненням для того часу. Звідси ж деким і був зроблений висновок, що саме «Колос» проклав міст до створення цілком програмувальних машин кілька років по тому.

Правда, в британській історії був інший надзвичайно вражаючий комп'ютерний предок – розроблена близько 150 років тому обчислювальна машина Чарльза Бебіджа. У свій час недобудована, вона була відтворена лондонським Музеєм науки у відповідності до креслень конструктора. Обчислювальна машина Бебіджа, яка була названа «Різницева машина № 2» (англ. *Difference Engine*) і важила 3 тонни, продемонструвала публіці бездоганну роботу. Таким чином, якщо б фінансові справи Бебіджа «пішли вгору», людство цілком могло вступити в комп'ютерну еру на 100 років раніше.



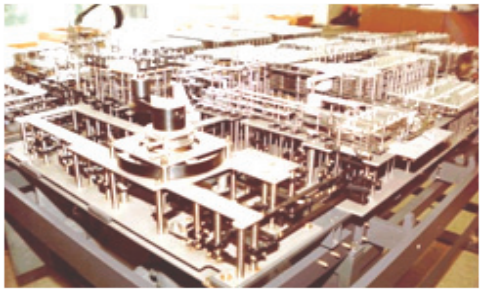
Цікаво, що у Німеччині до створення ЕОМ приступили задовго до Другої світової війни, але це було більш пов'язане з ініціативою ентузіаста-одинака, ніж з державним замовленням. Ще в 1934 році 23-літній студент Вищої технічної школи Конрад Цузе придумав новий пристрій, архітектура і принципи роботи якого загалом збігалися із сучасними цифровими комп'ютерами. Цей пристрій мав (тоді ще теоретично) керуючий блок, обчислювач (об'єднуючий арифметичні й логічні операції, тобто процесор) і пам'ять.

Саме Конрад Цузе першим зрозумів, що основою комп'ютерної обробки даних повинен бути двійковий знак «біт» (він назвав його «так/ні статус»). Це означало, що будь-які обчислення можна робити, ґрунтуючись на елементах, що мали два фізичні стани (замкнутий і розімкнутий). Цузе також увів поняття умовних суджень для формул двійкової алгебри і придумав «машинне слово».

У 1935 році Цузе одержав диплом і почав трудитися в авіабудівельній фірмі «Хеншель», де займався аеродинамічними розрахунками. Вони вимагали великого обсягу обчислень, тоді як допомогти в цьому могли тільки механічні арифмо-

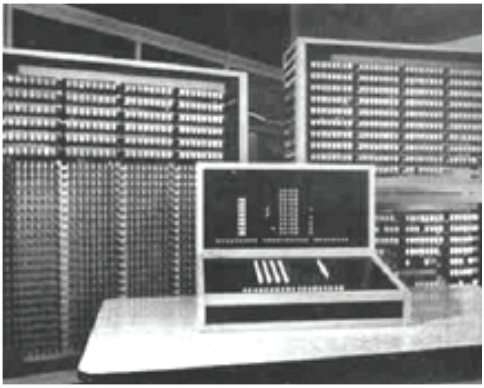
метри лише з арифметичними операціями. Усе це стимулювало продовження «комп'ютерного проекту» учорашнього студента. Він вирішив самостійно виготовити програмувальний пристрій, що працював з двійковими числами, у якому блок керування і процесор відділені від блоку пам'яті.

Цузе пішов з «Хеншеля» і цілком присвятив себе створенню нового обчислювального приладу. У 1936 році ним був зроблений і запатентований механічний запам'ятовуючий пристрій, заснований на двійкових елементах (рухомих металевих планках). У тому ж році в невеликій кімнаті квартири своїх батьків Цузе почав будувати свій перший комп'ютер «*V-1*» (нім. *Versuchsmodell* - дослідна модель), пізніше названий «*Z1*» – на честь конструктора.



У 1938 році «*Z1*» був готовий. Але цей експериментальний або демонстраційний зразок не мав здатності вирішувати серйозні практичні задачі через невеликий обсяг пам'яті та ненадійного механічного процесора. Незважаючи на усю свою недосконаліть, «*Z1*» дозволив Цузе одержати посаду і підтримку в Німецькому авіаційно-дослідному інституті. Використовуючи ту ж пам'ять, Конрад до квітня 1939 року побудував наступну модель комп'ютера «*Z2*», що мала процесор на електромеханічних телефонних реле (довелося купити в телефонних компаній 600 списаних реле).

Після цього успіху конструктора на рік призвали в армію. Відслуживши, він повернувся в інститут. У той час реле були доступні Цузе у великій кількості, і він вирішив зібрати з них серйозну машину, з тією ж архітектурою, що і «*Z1*». Ця машина – «*Z3*» – була офіційно «здана» 5 грудня 1941 року, і автор одержав на неї патент.



«*Z3*» був першим універсальним вільно програмувальним цифровим комп'ютером з ідеологією, що використовується понині. Тактова частота складала приблизно 5,3 Гц. Програма набивалася на перфострічці, що представляла собою кіноплівку, з використанням дев'яти

8-бітних команд (введення, виведення, читання з пам'яті, запис у пам'ять, квадратний корінь і 4 арифметичні операції).

На виготовлення ЕОМ «*Z3*» пішло близько 2600 реле, у тому числі 1800 на пам'ять і 600 на процесор. Вона виконувала 3-4 операції додавання в секунду і множила два числа за 4-5 секунд, споживаючи при цьому потужність приблизно 4 кВт. За тих часів вона (як і всі машини Цузе) могла вважатися портативною: важила близько тонни, її розміри були в десятки разів менше англійських і американських аналогів. Слід зазначити, що Цузе не застосовував у своїх машинах вакуумні лампи тільки через нестачу вільного місця і недостатнє фінансування.

Через невеликий обсяг пам'яті на «*Z3*» однак не можна було вирішувати, зокрема, системи лінійних рівнянь, а інституту це було потрібно (адже йшла війна й обсяг робіт істотно виріс, а терміни їхнього виконання, навпаки, зменшилися), і Цузе вирішив створити більш могутній комп'ютер. Прекрасно розуміючи, що головне – це великий обсяг оперативної пам'яті, він вирішив, що вона повинна мати ємність хоча б 1024 біта. Передбачалося, що новий комп'ютер буде оснащений двома перфораторами і 6 зчитувачами перфострічки (у тому числі для підпрограм), а також автоматичним друкувальним пристроєм.

На жаль, керівництво нацистської Німеччини не фінансувало довгострокові

наукові розробки. Ось чому «*Z4*» вдалося запустити лише під самий кінець війни (на той час при бомбуванні був зруйнований «*Z3*»). До того ж Цузе зумів побудувати кілька менших спеціалізованих комп'ютерів, що застосовувалися для розрахунків різних параметрів реактивних літаків і ракет (для визначення траєкторій польоту ракет, для математичного моделювання їхніх систем керування тощо).

Через складну військову обстановку «*Z4*» доводилося перевозити з місця на місце. 28 квітня 1945 року в підземному спорудженні в горах Гарца Цузе продемонстрував його провідним німецьким аеродинамікам. Зрештою «*Z4*» удалося врятувати тільки завдяки співробітникам Вернера фон Брауна, що сховали його в сараї в одному з альпійських сіл так, що американці його не знайшли.

«*Z4*» мав процесор з 2200 реле, механічну пам'ять з 64 32-розрядних слів (планувалася пам'ять на 500 слів), два пристрої для перфорації/зчитування перфострічки, десяткову клавіатуру, пристрій виведення у вигляді електричної друкарської машинки «*Mercedes*». Він працював на частоті 30 Гц, а важив і споживав енергії приблизно як «*Z3*». Фактично це був персональний комп'ютер, тому що його обслуговування було простим і, головне, він легко програмувався одною людиною. Для програмування «*Z4*» на вирішення типової задачі було потрібно близько 3 годин.

«*Z4*» набагато пережив країну, для якої був створений, – перетерпівши після війни кілька незначних модифікацій, у 1950 році він був встановлений у Вищій технічній школі у Цюриху, де пропрацював майже без перерв протягом 5 років над цілком реальними проектами (це був один із 2 комп'ютерів, що працювали тоді в Європі, другим була радянська «*МЭСМ*» Сергія Лебедєва). Потім він був перевезений у Францію, де працював ще приблизно стільки ж. В даний час «*Z4*» можна побачити в Мюнхенському музеї «*Deutsche Museum*».

Таким чином, закладених Цузе ідей виявилося цілком достатньо для 10 післявоєнного років, коли технічний прогрес (а особливо розвиток комп'ютерів) аж ніяк не стояв на місці.

Що стосується Радянського Союзу, то у 1931 році в Ленінградському електротехнічному інституті була відкрита перша кафедра приладів керування стрільбою, що готувала фахівців з обчислювальних пристроїв (у 1938-1939 роках у Ленінграді й Москві були утворені ще дві аналогічні кафедри). У 1941 році під керівництвом Акушського була організована перша в СРСР обчислювальна лабораторія – прообраз майбутніх обчислювальних центрів. Таким чином, до війни СРСР мало чим поступався іншим країнам у сфері ЕОМ, але війна призупинила подальші роботи.

Лише у 1945 році майбутній академік АН СРСР Сергій Олександрович Лебедєв утворив електронний аналоговий обчислювальний прилад для вирішення пов'язаних з енергетикою завдань, а у 1947 році з'явилася електронна аналогова машина «*ЭДА*», що дозволяла вирішувати диференціальні рівняння 20-го поряд-

ку.

Більш того, одержавши інформацію з відкритих публікацій західних радіотехнічних журналів, у 1947 році академік Михайло Лаврентьєв виступив з доповіддю про відставання СРСР у створенні ЕОМ. З доповіді зробили висновки – восени 1948 року Лебедєв переорієнтував свою лабораторію моделювання регулювання на конструювання ЕОМ, а 4 грудня того ж року Ісаак Брук і Башир Рамеєв одержали авторське посвідчення на винахід «Автоматичної цифрової машини» – фактично першого радянського комп'ютера.

Наприкінці 1948 року в секретній лабораторії у містечку Феофанія під Києвом під керівництвом Лебедєва (у той час - директора Інституту електротехніки АН України та за сумісництвом керівника лабораторії Інституту точної механіки й обчислювальної техніки АН СРСР) розпочались роботи з утворення Малої електронної рахункової машини (рос. скор. *МЭСМ*).

4 січня 1951 року приймальній комісії був продемонстрований діючий макет «*МЭСМ*», а 25 грудня вона була введена в експлуатацію: у той день на ній було отримане вирішення реального завдання – обчислення функцій розподілу ймовірностей, – за 2,5 години було виконано 250 тисяч операцій і отримано 585 значень з точністю до 5-го знака. У той час це був наймогутніший комп'ютер у континентальній Європі.

Що стосується США, то у січні 1941 року в американській газеті «Де Мойн Трибюн» з'явилася замітка про те, що Джон Атанасов і Кліфорд Беррі з Університе-

ту штату Айова побудували ЕОМ «*ABC*» (англ. *Atanasoff-Berry Computer*), «яка за принципом своєї роботи ближче людському мозку, ніж будь-яка інша». Роботи фінансувалися експериментальною сільсько-господарською станцією Університету, що планувала використовувати машину для вирішення сільсько-господарських завдань.

На замітку звернув увагу Джон Моучлі, що також займався конструюванням ЕОМ. Він виїхав на місце робіт і в липні 1941 року 5 днів гостював в Атанасова, спостерігаючи, як той зі своїм помічником Кліффордом Бері працював над комп'ютером з 300 електронними лампами. Через рік Моучлі написав пропозицію щодо створення швидкодіючого комп'ютера на електронних лампах, яким згодом зацікавилася Армія США з метою розробки нових балістичних таблиць, створення яких вимагало величезного обсягу обчислень (до 750 операцій множення для обчислення однієї траєкторії, а на кожну з таблиць було потрібно не менш 2000 операцій).

В результаті 9 квітня 1943 року Армія уклала з Вищим технологічним училищем Пенсильванського університету контракт на будівлю комп'ютера «ЕНІАК» (англ. *Electronic Numerical Integrator and Computer, ENIAC* - електронний цифровий інтегратор і обчислювач).

Але поки Моучлі працював, у серпні 1944 року була створена ЕОМ «*Mark I*» – машина для розрахунку балістичних таблиць, яку за контрактом з компанією «*International Business Machines*» (*IBM)* побудував математик Говард Ейкен. Основними її елементами були зубчасті колеса (для подання чисел) і електромеханічні реле (для керування процесом обчислень). Вона важила 5 тонн і, будучи 17 метрів довжиною і 2,5 метрів у висоту, займала в Гарвардському університеті площу у декілька десятків квадратних метрів.

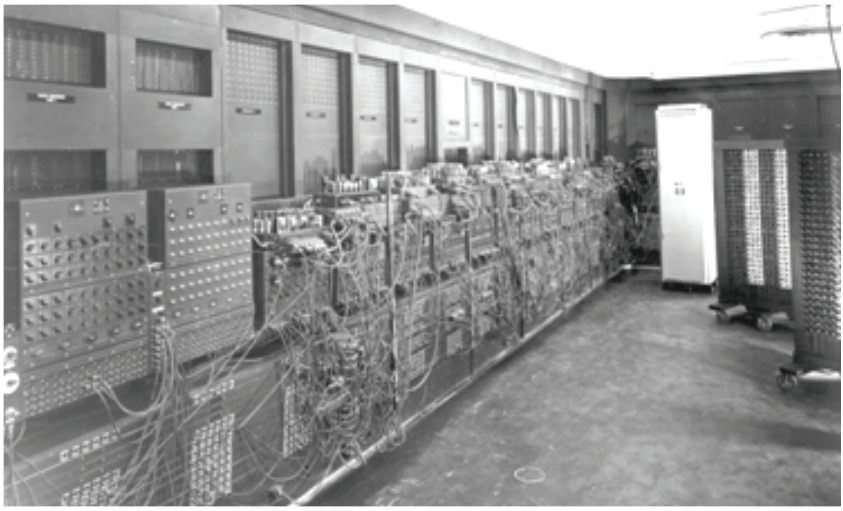
Машина мала 72 регістри, кожний з яких являв собою пристрій з 24 зубчастих коліс з механізмом передачі десятків до іншого регістру. 23 колеса служили для подання числа, одне – для його знака. Окремо для констант була передбачена механічна пам'ять з 60 регістрів. Для операцій множення і розподілу, а також для обчислення синуса, натурального логарифма і показника ступеня, використовувалися окремі обчислювальні блоки. Гарвардський «*Mark I*» працював за програмою, яку зчитував з перфорованої стрічки. Власне, це був не стільки комп'ютер, скільки удосконалений арифмометр, що заміняв працю приблизно 20 операторів

зі звичайними ручними арифмометрами.

Наприкінці 1945 року був зібраний і підготовлений до проведення першого офіційного іспиту «ЕНІАК». Він являв собою гігантське спорудження – 30-тонну машину з 17 468 електронними лампами, 26 метрів у довжину і 6 метрів у висоту. Правда, війна, заради якої створювався «ЕНІАК», уже встигла закінчитися, але завдання, що було поставлено на першому іспиті, – розрахунки для підтвердження можливості створення водневої бомби – доводило, що необхідність у комп'ютерах не зникла.

Після Другої світової війни криптоаналітики всіх країн розпочали розвивати комп'ютерні технології та застосовувати ЕОМ для розкриття будь-яких видів шифрів. Тепер вони могли використовувати швидкодію та гнучкість програмувальних комп'ютерів для перебору всіх можливих ключів, поки не буде знайдений правильний ключ. Але час йшов, і вже криптографи почали користуватися всією міццю комп'ютерів для створення усе більш і більш складних шифрів. Коротше кажучи, комп'ютер зіграв вирішальну роль у післявоєнному двобої між шифрувальниками та дешифрувальниками країн-супротивників.

Застосування комп'ютера для зашифровування повідомлення багато в чому нагадує звичайні способи шифрування. І справді, між шифруванням з використанням комп'ютерів і шифруванням з використанням механічних пристроїв, як наприклад, «Енігми», існує усього лише три основні відмінності. Перша відмінність полягає в тому, що можна побудувати механічну шифрувальну машину тільки обмежених розмірів, у той час як комп'ютер може імітувати гіпотетичну шифромашину величезної складності.



Так, наприклад, комп'ютер міг би бути запрограмований так, щоб відтворити дію сотень шифраторів, частина з яких обертається за годинниковою стрілкою, а частина – проти, деякі шифратори зникають після кожної десятої букви, а інші у ході шифрування обертаються усе швидше й швидше. Таку механічну машину в реальності виготовити неможливо, але її віртуальний комп'ютеризований аналог давав би винятково стійкий шифр.

Друга відмінність полягає просто у швидкодії: електроніка може працювати набагато швидше механічних шифраторів. Комп'ютер, запрограмований для імітування шифру «Енігми», може вмить зашифрувати довге повідомлення. З іншого боку, комп'ютер, запрограмований на використання істотно більш складного способу шифрування, як і раніше, здатний виконати своє завдання за прийнятний час.

Третя і, мабуть, найбільш істотна відмінність – це те, що комп'ютер виконує зашифровування чисел, а не букв алфавіту. Комп'ютери працюють тільки з двійковими числами – послідовностями одиниць і нулів, що називаються «бітами». Тому будь-яке повідомлення перед зашифровуванням повинне бути перетворене у двійкові знаки, після чого здійснюється його шифрування.

Разом з тим, зашифровування, як і раніше, виконується за допомогою традиційних способів заміни й перестановки, при яких елементи повідомлення замінюються іншими елементами, чи елементи повідомлення змінюються місцями, чи обидва способи застосовуються разом. Будь-який процес зашифровування можна уявити як сполучення цих двох простих операцій.

У той час комп'ютерне шифрування обмежувалося тільки тим колом осіб, у кого малися комп'ютери: спочатку це були урядові та військові установи. Однак ряд наукових відкриттів і інженерно-технологічних досягнень зробили комп'ютери та комп'ютерне шифрування набагато більш доступними. Так, у 1947 році американською компанією «*AT&T Bell Laboratories*» був створений транзистор – дешева альтернатива електронній лампі.

Використання комп'ютерів для вирішення промислових і комерційних завдань стало реальністю у 1951 році, коли компанія «Феррранті» розпочала виготовляти комп'ютери на замовлення. У 1953 році компанія «IBM» виготовила свій перший комп'ютер, а через 4 роки вона ж створила мову програмування «Фортран» (англ. *Fortran* - скорочення від «*Mathematical Formula Translating System*» - система трансляції математичних формул), що дозволила пересічним громадянам «писати» комп'ютерні програми. А поява у 1959 році перших інтегральних схем взагалі визначила початок нової ери світової комп'ютеризації.

Усе більше й більше комерційних компаній і промислових підприємств могли дозволити собі придбати комп'ютери та використовувати їх для зашифровування важливої інформації, наприклад, переказів грошей або проведення торгі-

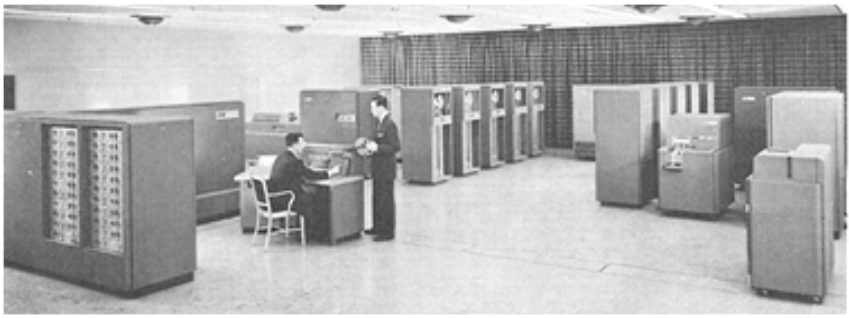
вельних переговорів. Однак по мірі зростання кількості таких компаній і підприємств та у зв'язку з тим, що шифрування між ними поширювалося, криптологи зіштовхнулися з новими складностями, яких не існувало, коли криптологія була прерогативою урядів і військових.

Бурхливий розвиток комп'ютерних технологій і мереж кардинально змінив сталі способи розвитку держави та ведення бізнесу. Вимоги часу при всій суперечливості інтересів різних державних і комерційних структур та організацій потребували доступні для всіх і абсолютно надійні методи захисту інформації від несанкціонованого доступу і, зокрема, алгоритми шифрування даних і захисту від фальсифікації переданих комп'ютерними мережами та каналами електрозв'язку електронних документів (повідомлень).

Одним із першочергових питань було питання стандартизації систем комп'ютерного шифрування. В результаті 15 травня 1973 року Американське Національне бюро стандартів США вирішило розв'язати цю проблему та офіційно запросило пропозиції щодо стандартної системи комп'ютерного шифрування, яка б дозволила забезпечити таємність комп'ютерного зв'язку між різними компаніями.

Одним із найбільш відомих і визнаних алгоритмів комп'ютерного шифрування та кандидатом на стандарт був продукт компанії «*IBM*», відомий як «Люцифер» (лат. *Lucifer* - світлоносець). Він був створений Хорстом Файстелем, німецьким емігрантом, що приїхав до Америки у 1934 році. Файстель вже ось-ось повинен був одержати громадянство США, коли Америка вступила у війну, що означало, що він знаходився під домашнім арештом аж до 1944 року. Після цього він ще кілька років замовчував свій інтерес до криптології, щоб не викликати підозри в американської влади.

Коли ж він зрештою почав займатися вивченням шифрів у Кембріджському науково-дослідному центрі ВПС США, то незабаром виявився під пильною увагою Агенції національної безпеки (далі – АНБ) – організації, що відповідає за забезпечення безпеки військового й урядового зв'язку та займається також перехо-



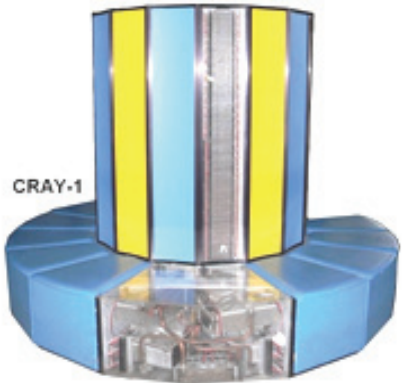
пленням і дешифруванням іноземних повідомлень. АНБ хотіла мати монополію в сфері криптологічних досліджень, і, вочевидь, саме вона влаштувала так, що дослідницький проект Файстеля був закритий.

У 1960-х роках Файстель перейшов у компанію «*Mitre Corporation*», але АНБ продовжувало «тиснути» на нього та знову змусило його покинути свою роботу. Зрештою Файстель виявився в дослідницькій лабораторії Томаса Уотсона компанії «*IBM*» неподалік від Нью-Йорка, де протягом декількох років міг без перешкод продовжувати свої дослідження. Там на початку 1970-х років він і створив криптоалгоритм «Люцифер».

Національним Бюро Стандартів США «Люцифер» був офіційно прийнятий 23 листопада 1976 року (патент США № 3958081) як перший у світі відкритий національний стандарт криптоалгоритму для внутрішнього застосування під назвою «*DES*» (англ. *Data Encryption Standard* - стандарт шифрування даних). Він був «блоковим шифром» (коли інформація обробляється блоками фіксованої довжини) і мав ключ (тобто елемент забезпечення таємності шифру) – число довжиною 56 біт, що дає 255 варіантів ключів.

Дотепер практично найбільш ефективними методами дешифрування алгоритму «*DES*» у його повному варіанті є метод, заснований на повному переборі всіх можливих варіантів ключа до одержання варіанта, який дасть можливість розшифровувати зашифровану інформацію. Звичайно, якщо шифр допускає методи «розкриття» істотно меншої складності, ніж тотальний перебір, то він не вважається надійним.

Гарантією стійкості алгоритму «*DES*» був час послідовного перебору комбінацій ключа довжиною 56 біт не менш 100 років безперервного машинного рахування суперкомп'ютером «*Cray-1*». Однак за час, що пройшов після створення «DES», комп'ютерна техніка розвилася настільки швидко, що виявилося можливим здійснювати вичерпний перебір ключів і тим самим «розкривати» шифр. Вартість цієї атаки постійно знижується. Так, у 1998 році була побудована машина вартістю близько 100 тисяч доларів, здатна по парі [вихідний текст – шифрований текст] відновити ключ за середній час у 3 доби.



Останнього разу «*DES*» був розкритий 9 січня 1999 року за 22 години 15 хвилин. З тих пір, наскільки відомо, спроби не повторювалися, але зрозуміло, що кількість витраченого часу може тільки зменшуватися. Тому в даний час симе-

тричний шифр вважається стійким, тільки якщо довжина його ключа не менш 128 біт. Через експонентний характер росту кількості ключів збільшення довжини ключа усього в два рази дає неймовірний ріст криптостійкості шифру. Досить сказати, що «злом» шифру з 128-бітним ключем займе не менш 1020 років.

Таким чином, «*DES*» при його стандартному використанні, уже став далеко не оптимальним вибором відповідності вимогам захищеності даних. Тому була висунута велика кількість пропозицій щодо його удосконалення, які частково компенсували зазначені недоліки. У 1984 році Рон Рівест запропонував розширення «*DES*», яке було назване «*DESX*» (англ. *DES eXtended*). Цей алгоритм, який сполучався з «*DES*» та ефективно реалізовувався апаратно, міг використовувати існуюче апаратне забезпечення «*DES*». Крім того, було доведено, що він збільшив стійкість до атак, заснованих на переборі ключів.

У 1989 році був розроблений та опублікований альтернативний алгоритму «*DES*» проект національного стандарту шифрування даних Японії, що одержав назву «*FEAL*». Він також був блоковим шифром, який використовував блок даних з 64 біт і ключ довжиною 64 біта. Потім, в 1990 році К.Лей і Дж.Месі (Швейцарія) запропонували проект міжнародного стандарту шифрування даних, що одержав назву «*IDEA*» (англ. *International Data Encryption Algorithm* - міжнародний алгоритм шифрування даних).

За останні роки цей шифр зусиллями міжнародних організацій із стандартизації (насамперед, європейських) активно просунувся до межі перетворення в офіційний загальноєвропейський стандарт шифрування даних. «IDEA» витримав всі атаки криптологів таких розвинутих країн, як Англія, Німеччина та Ізраїль, тому він вважається більш стійким, ніж традиційний «DES».

Не бажаючи відставати від американців, у 1989 році державний стандарт шифрування даних для мереж ЕОМ прийняли також і в СРСР. Він одержав назву «*алгоритм ГОСТ 28147-89*» і мав гриф обмеження доступу «Для службового користування» до кінця існування СРСР. Однак практично він не використовувався через відсутність у СРСР самих мереж ЕОМ.

У Росії він був прийнятий як офіційний стандарт шифрування даних із 1992 року поряд з іншими колишніми стандартами СРСР шляхом простого визнання їх надалі до прийняття чого-небудь нового свого, і був формально оголошений повністю «відкритим» у травні 1994 року. Стандарт «*ГОСТ 28147-89*» так само, як і «*DES*», був блоковим шифром. Довжина блоку інформації становить 64 біти, довжина ключа становить 256 біт, і ні про яку практичну можливість перебору всіх припустимих варіантів ключа тут уже не може бути й мови.

Можете спати спокійно...

Частина 2.

Історія американської криптології

2.1. Американська криптологія до XX ст.

За океаном, у Північній Америці, у XVIII столітті не було ні «чорних кабінетів», ні будь-яких криптослужб. Разом з тим, відомо, що американські делегати у Франції та державний секретар під час скандальної справи «Ікс-Ігрек-Зет» (англ. *X-Y-Z*) у 1737 році, повязаної з вимаганням французькими посадовими особами грошових «подарунків» від американців, шифрували своє листування за допомогою номенклатора.

Наприкінці XVIII століття розпочалася війна за незалежність США (1775-1783) між королівством Великобританії і лоялістами (прибічниками британської корони) з одного боку та революціонерами 13 англійських колоній (патріотами) з іншого, які проголосили свою незалежність від Великобританії, як самостійна союзна держава. 29 листопада 1775 року патріоти утворили такий державний орган як Комітет для секретної кореспонденції з друзями колоній у Великобританії, Ірландії та інших частинах світу. Наприкінці 1977 року він був реорганізований у Комітет закордонних справ (з 1789 року – Держдепартамент) США.

Повстанці як могли боролися з англійськими шпигунами, однак перехоплювати криптограми англійців їм вдавалося дуже мало. І лише коли війна наближалася до свого завершення та була захоплена достатня кількість шифрованих повідомлень, були організовані «разові групи» з дешифрування. В одну з таких груп входив май-

бутній віце-президент США Елбрідж Джеррі. Головним напрямком роботи цих груп було виявлення англійських шпигунів і дешифрування листування англійських військ. Більшість з криптограм було дешифровано Джеймсом Ловелєм (1737-1814), якого можна по праву назвати «батьком» американського криптоаналізу.

У 1777 році Ловель був обраний депутатом Конгресу, членом Комітету закордонних справ і незабаром став відомий завдяки своїй запопадливості та працьовитості. Одним з перших обов'язків Ловеля була розшифровка листів Чарльза Дюма, американського дипломата, що жив в Нідерландах і пізніше представляв інтереси США в Європі. Саме Дюма винайшов перший дипломатичний шифр Континентального Конгресу, який використовувався американським дипломатом у Франції Бенджамином Франкліном для листування з агентами а Європі.

Восени 1781 року американський командувач на півдні Натаніель Грін направив Конгресу кілька перехоплених англійських криптограм, які у його штабі ніхто не міг прочитати, додавши їх до свого загального повідомлення. Ця шифрована англійська кореспонденція виявилася листуванням між заступником головнокомандувача англійських військ в Америці Корнуолісом і його підлеглими.

Повідомлення Гріна було зачитано в Конгресі 17 вересня. Чотирма днями пізніше Ловель розшифрував додатки до повідомлення. На жаль, через швидкий розвиток подій добута ним інформація не принесла багато користі. Але знайдені Ловелєм ключі цілком могли згодитися коли-небудь у майбутньому. У своєму листі Вашингтонувін написав: «Не виключено, що супротивник має намір і далі зашифровувати своє листування... Якщо це так, то ваше превосходительство, можливо, побажає отримати для себе користь, давши вашому секретарю вказівку зняти копію ключів і зауважень, що я через вас направляю...»

Більш проникливим Ловель бути не міг. Розкритий ним шифр дійсно служив також і для зв'язку між Чарльзом Корнуолісом і генералом Генрі Клінтоном, що знаходився в Нью-Йорку. На той час Корнуоліс відступив до Йорк-Тауна, щоб дочекатися підкріплень від Клінтона. До речі, Клінтон зашифровував свої повідомлення, використовуючи номенклатор, алфавітну таблицю, ряд замін і решітку.

Але Вашингтон з 16-тисячним військом оточив місто, а французький адмірал граф де Грасс із 24 кораблями заблокував допомогу англійцям з моря. 6 жовтня Вашингтон писав Ловелю: «Мій секретар зняв копії з шифрів і за допомогою одного з алфавітів зумів розшифрувати параграф недавно перехопленого листа лорда Корнуоліса серу Клінтону». Ця інформація допомогла Вашингтону оцінити реальний стан справ в англійському таборі.

Тим часом для зв'язку з Корнуолісом Клінтон спорядив два невеликі судна, які він відправив з Нью-Йорка 26 вересня і 3 жовтня. Однак вони були захоплені повстанцями. При цьому одне з них прибило до берега, де англієць, який віз пачку шифрованих депеш, сховав їх під великим каменем, перш ніж його захопили в по-

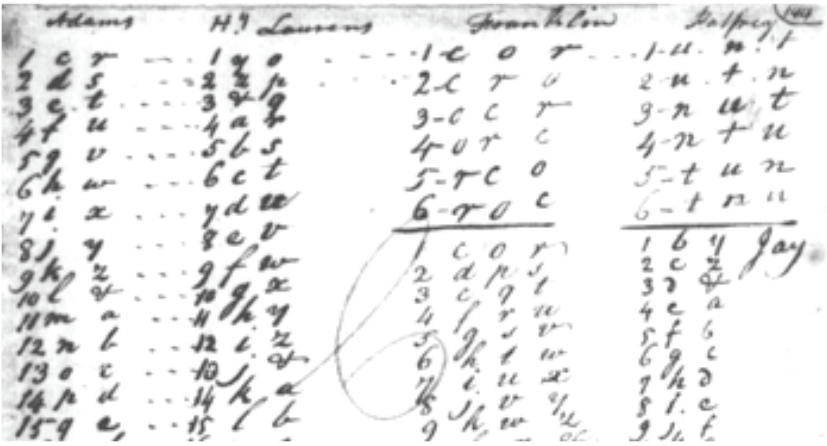
лон. Потім, як висловився один з очевидців, «у результаті нетривалої бесіди, пообіцявши прощення», повстанці умовили англійця віддати заховані депеші.

Ловель одержав ці депеші 14 жовтня та відразу приступив до справи. Успіх не змусив себе довго чекати, тому що він з'ясував, що вони були зашифровані тим же шифром, що й інше листування Корнуоліса. Через п'ять днів після того, як Ловель закінчив дешифрування, Корнуоліс капітулював.

Але перемога повстанців була не зовсім повною. Вашингтон зрозумів це, коли наступного дня він нарешті одержав від Ловеля копії дешифрованих депеш. Не втрачаючи ні хвилини, Вашингтон переправив їх де Грассу, кораблі якого повинні були перешкодити спробі надання допомоги Корнуолісу Грейвсом і Клінтоном. Будучи попередженим, французький адмірал ґрунтовно підготувався до нападу англійців. 30 жовтня він змусив англійський флот відступити й тим самим наблизив остаточну перемогу американців у війні за незалежність.

Пізніше Ловель винайшов власний поліалфавітний шифр. Цей шифр активно використовувався Ловелєм в його листуванні. Проте, як з'ясувалося пізніше, шифр став відомий тим, що постійно заплутував кореспондентів Ловеля. У його шифрі кореспонденти формували таблицю замін з узгодженого ключового слова. Спочатку в стовпець записувалися числа від 1 до 27, потім поряд з ним записувався стовпець з 27 букв алфавіту (a-z і &), починаючи з першої букви ключового слова. Потім аналогічний стовпець, що починався з другої букви ключового слова, і так далі. При шифруванні стовпці використовувалися по черзі, і кожна буква шифрувалася числом. Як видно, якщо при шифруванні допущена помилка, тобто наприклад один стовпець використовувався двічі підряд, процес розшифрування відразу ж заплутувався.

У цілому, ефективність дешифрування повстанців виявлялася досить високою завдяки тому, що англійські шифри й ключі не мінялися тривалий час. Крім того,



мережа шифрованого зв'язку Англії в США мала істотний недолік: усі командири військових підрозділів використовували для зв'язку між собою та Лондоном ті ж самі шифри й ключі. У цих умовах дешифрування повідомлень одного з абонентів приводило до компрометації листування всіх абонентів мережі. В результаті американцям вдавалося одержувати інформацію, досить важливу для проведення своїх військових операцій.

Посланець США у Франції, член Комітету закордонних справ, учений, дипломат, філософ Бенджамін Франклін (1706-1790) для зв'язку з Конгресом розробив свій власний шифр багатозначної заміни. Цікавий був сам спосіб складання шифру. Він узяв відрізок французького тексту (682 букви), пронумерував у ньому знаки і кожній букві латинського алфавіту додав безліч позначень (чисел) у пронумерованому тексті. При шифруванні кожна буква замінялася на довільно обране число з безлічі позначень.

У сучасному розумінні він використовував шифр пропорційної заміни, у якому кількість можливих шифропозначень пропорційна частоті повторюваності букв у відкритому тексті. При використанні такого шифру знаки шифрованого тексту з'являлися приблизно з однаковими частотами. Розробивши власний шифр пропорційної заміни, Франклін відтворив ідею шифру, запропонованого Габріелем де Лавінда ще в XV столітті.

На жаль (для американців), один із помічників Франкліна – генеральний секретар американської місії у Франції Едуард Банкрофт – був англійським шпигуном. В результаті Франклін часто відправляв в Америку дезінформацію, надану йому Банкрофтом. Інший помічник Франкліна, Артур Лі, користувався своєрідним книжковим шифром. Відкритий текст шифрувався не по буквах, а словах. Ключем шифру був заздалегідь обговорений словник, а всі слова мінялися на відповідні номери сторінок і слів на сторінці. Однак цей шифр виявився досить незручним у застосуванні.

У 1779 році конгресмен і офіцер континентальної армії Бенджамін Толмадж (1754 -1835) розробив для зв'язку з Вашингтоном номенклатор, який складався з одного розділу та 760 елементів. Для цього він використав найбільш уживані слова з «Нового орфографічного словника» Джона Ентіка. Виписавши у стовпець обрані слова, Толмадж привласнив кожному з них визначене число, а географічні назви та імена людей помістив у окремий розділ. Слова у номенклаторі були розташовані у буквено-цифровій послідовності, а крім того, номенклатор містив також перемешаний алфавіт для кодування слів і чисел, що не увійшли у список.

У 1781 році Секретар закордонних справ США Роберт Лівінгстон (1746-1813) розробив номенклатор, який містив упорядковану за алфавітом групу слів і складів на одному боці та числа від 1 до 1700 на іншому. Скориставшись системою Лівінгстона, майбутні держсекретарі та президенти США Томас Джеферсон (1743-1826) і

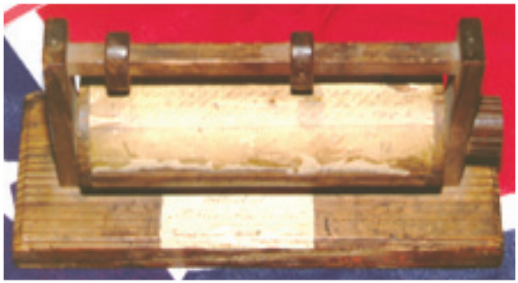
Джеймс Медісон (1751-1836) розробили свою власну систему захисту листування. Вона виявилася зручнішою, оскільки дозволяла вставляти букви або числа у відкритий текст при будь-яких обраних відправником і адресатом кодових комбінаціях.

Крім того, Медісон як член віргінської делегації на Континентальному конгресі користувався номенклатором, який складався приблизно з 846 елементів, щоб надсилати приватні листи губернатору штату Віргінія Бенджаміну Гарісону. Його система складалася щз перечня чисел, букв, складів і географічних назв, таких як Відень тощо. З 1801 року Медісон, перебуваючи на посаді державного секретаря США, для листування з Лівінгстоном, який у той час був послом у Франції, користувався номенклатором, що мав 1700 елементів. З 1803 року Медісон листувався зі своїми представниками Лівінгстоном і Джеймсом Монро вже новим кодом, який отримав назву «шифр Монро». Хоча ця система була названа шифром, вона вмала усі властивості номенклатора, 1600 елементів якого були розташовані у алфавітному порядку.

У 1790-х роках американська криптологія збагатилася чудовим винаходом. Його автором був державний діяч, перший державний секретар, а потім і президент США Томас Джеферсон. Свою систему шифрування він назвав «дисковим шифром». Цей шифр реалізовувався за допомогою спеціального пристрою, що згодом назвали «шифратором Джеферсона». Конструкція шифратора може бути коротенько описана таким чином.

Дерев'яний циліндр розрізався на 36 дисків (у принципі, загальна кількість дисків може бути й іншою). Ці диски насаджувалися на одну загальну вісь таким чином, щоб вони могли незалежно обертатися на ній. На окружності кожного з дисків виписувалися всі букви англійського алфавіту в довільному порядку. Послідовність букв на різних дисках була різною. На поверхні циліндра виділялася лінія, рівнобіжна його вісі. При шифруванні відкритий текст розбивався на групи по 36 знаків, потім перша буква групи фіксувалася положенням першого диска по виділеній лінії, друга – положенням другого диска й так далі. Шифрований текст утворювався шляхом зчитування послідовності букв по будь-якій рівнобіжно виділеній лінії.

Зворотний процес здійснювався на аналогічному шифраторі: отриманий шифротекст виписувався шляхом повороту дисків по виділеній лінії, а відкритий текст відшукувався серед рівнобіжних їй ліній шляхом прочитання осмисленого можливого варіанта. Хоча теоретично цей метод дозволяв припустити появу різних варіантів відкри-



того повідомлення, але, як показав накопичений того часу досвід, це було малоймовірно: осмислений текст читався тільки по одній з можливих ліній. Шифратор Джеферсона реалізовував раніше відомий шифр багатоалфавітної заміни. Частинами його ключа був порядок розташування букв на кожному диску та порядок розташування цих дисків на загальній осі. Загальна кількість ключів була величезна.

Цей винахід став провісником появи так званих дискових шифраторів, що знайшли широке поширення в розвинутих країнах у XX столітті. Шифратор «*M-94*», який був аналогічний шифратору Джеферсона, використовувався в армії США під час Другої світової війни. Однак при житті Джеферсона доля його винаходу склалася невдало. Будучи держсекретарем, сам Джеферсон продовжував використовувати традиційні коди (номенклатори) та шифри Віженера. Він дуже обережно відносився до свого винаходу та вважав, що його потрібно ґрунтовно проаналізувати. З цією метою він тривалий час підтримував зв'язок з математиком Р.Патерсоном.

В результаті обміну інформацією Патерсон запропонував свій власний шифр, який, на його думку, був більш надійним, ніж шифр Джеферсона. Він являв собою шифр вертикальної перестановки з уведенням «пустишок». За своєю стійкістю він значно поступався шифру Джеферсона, однак той прийняв доводи свого опонента та визнав його шифр більш прийнятним для використання. Таким чином, Джеферсон сам не оцінив усієї значимості свого власного винаходу.

У 1817 році полковник американської армії, начальник артилерійсько-технічної служби армії США Д.Уодсворт також запропонував свій механічний шифратор. Основними елементами пристрою були два шифрувальні диски. По окружності першого з них (верхнього), що реалізовував алфавіт відкритого тексту, за абеткою були розташовані 26 букв англійського алфавіту. На другому (нижньому) диску з алфавітом шифрованого тексту в довільному порядку розташовувалися ці ж букви та цифри від 2 до 8. Таким чином, він містив 33 знаки. Літери на диску були зйомними, що дозволяло змінювати алфавіт шифрованого тексту. Диски були з'єднані між собою шестерною передачею з числом зубів 26 х 33.

При обертанні першого диска (за допомогою кнопки) на один крок другий диск обертався також на один крок в інший бік. Оскільки числа 26 і 33 були взаємно простими, то при покроковому обертанні першого диска обидва диски поверталися у початковий стан через 26 х 33 = 858 кроків. Диск відкритого тексту обертався тільки в один бік. Диски містилися у футлярі, у якому були прорізані вікна. За допомогою

спеціальної кнопки шестірні роз'єднувалися, що дозволяло незалежно один від одного повертати диски в початкове для шифрування положення (за допомогою додаткових кнопок). Довгостроковим ключем був алфавіт шифрованого тексту (їхня кількість була 33), а разовий ключ складався з двох букв (верхнього та нижнього диска) і встановлювався у вікнах при незалежному повороті дисків. Кількість разових ключів була: 26 х 33 = 858.

Шифрування вироблялося таким чином. Перед початком шифрування диски ставилися в початкові умовні положення (наприклад, *LB*). Потім шестірні з'єднувалися, і за допомогою кнопки диск повертався доти, поки у верхньому вікні не з'являлася перша буква відкритого тексту. З вікна під ним списувалася перша буква шифрованого тексту. Інші букви шифрувалися аналогічним чином. Якщо букви повторювалися (наприклад, *AA*), то диск робив повний оберт, тому в шифротексті цій парі відповідали пари з різних знаків (наприклад, *8B*).

Розшифрування робилося зворотним чином. Букви шифрованого тексту встановлювалися по нижньому вікну, а з верхнього списувалася відповідна буква відкритого тексту. Даний шифр мав такі особливості:

- кількість знаків в алфавіті шифрованого тексту (33) була більше кількості букв в алфавіті відкритого тексту (26);

- шифрування букви відкритого тексту залежало від того, якою була попередня їй буква, що шифрувалася.

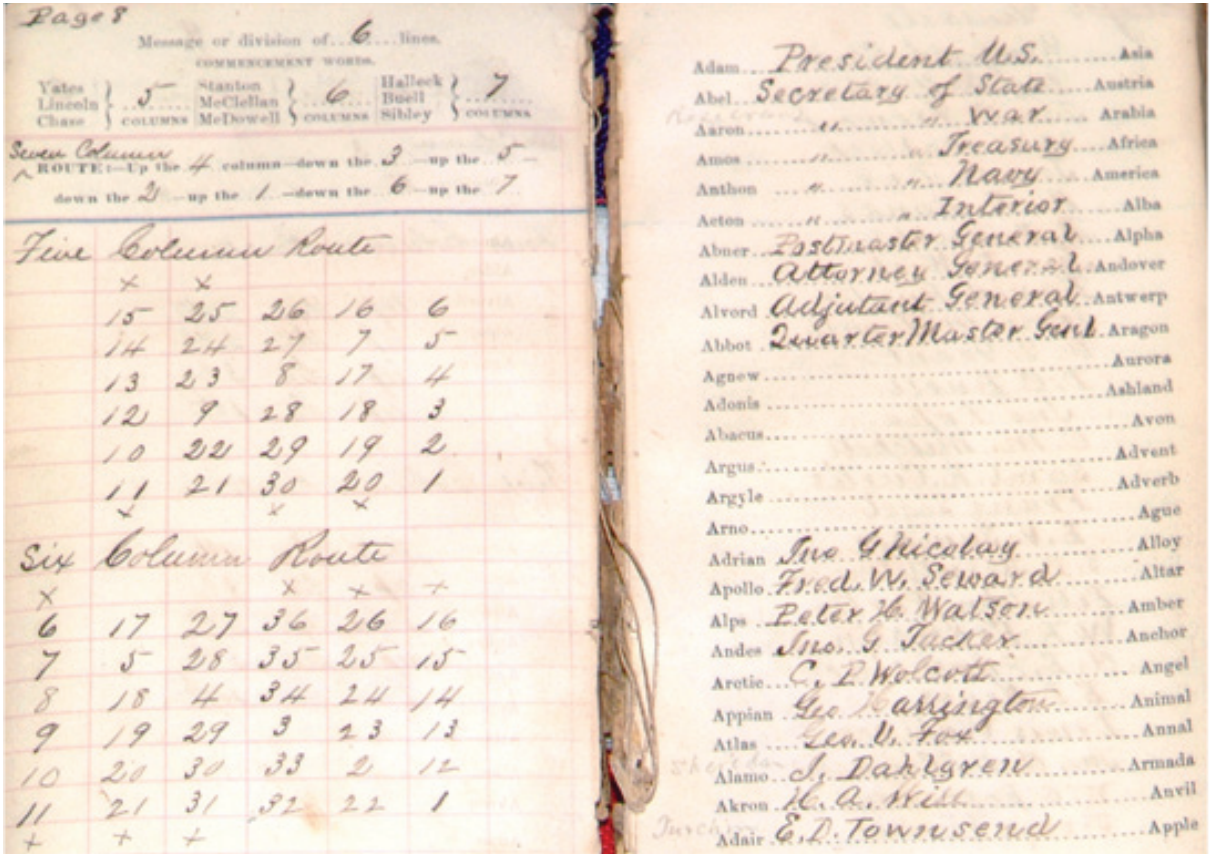
Пропозиція Уодсворта заслуговувала на увагу, незважаючи на те, що недоліком шифру була його особлива чутливість до неточностей (типу заміни та пропуску знаків у шифрованому тексті). Перекручена або пропущена буква робила весь наступний текст при розшифруванні незрозумілим. Однак історична відмова від запропонованої системи шифрування була пов'язана з іншими обставинами. В ці роки панували так звані «ручні шифри», застосування яких не вимагало спеціальних пристосувань. Ці шифри були добре засвоєні, їм вірили та їх добре знали, у зв'язку з чим пропозиція Уодсворта породжувала зайві «турботи».

Всередині XIX століття американець П.Е.Чейз запропонував модифікацію відомого шифру Полібія:

	1	2	3	4	5	6	7	8	9	0
1	X	U	A	C	O	N	Z	L	P	ф
2	B	Y	F	M	@	E	G	J	Q	ω
3	D	K	S	V	H	R	W	T	I	λ

Ключем шифру був порядок розташування букв у таблиці. При шифруванні координати букв виписувались вертикально. Наприклад, слово «UKRAINE» можна записати як такий дворядковий цифровий шифротекст:

1 3 3 1 3 1 2



Page 8

Message or division of 6 lines.

COMMENCEMENT WORDS.

Yates / Lincoln / Chase	5 columns	Stanton / McClellan / McDowell	6 columns	Halleck / Buell / Sibley	7 columns

Seven Column
ROUTE:—Up the 4 column—down the 3—up the 5—down the 2—up the 1—down the 6—up the 7

Five Column Route

×	×			
15	25	26	16	6
14	24	27	7	5
13	23	8	17	4
12	9	28	18	3
10	22	29	19	2
11	21	30	20	1
↙		×	×	

Six Column Route

×				×	+
6	17	27	36	26	16
7	5	28	35	25	15
8	18	4	34	24	14
9	19	29	3	23	13
10	20	30	33	2	12
11	21	31	32	22	1
+	+	+			

Adam	President U.S.	Asia
Abel	Secretary of State	Austria
Aaron	" War	Arabia
Amos	" Treasury	Africa
Anthon	" Navy	America
Acton	" Interior	Alba
Abner	Postmaster General	Alpha
Alden	Attorney General	Andover
Alvord	Adjutant General	Antwerp
Abbot	Quarter Master Genl	Aragon
Agnew		Aurora
Adonis		Ashland
Abacus		Avon
Argus		Advent
Argyle		Adverb
Arno		Ague
Adrian	Jno. G Nicolay	Alloy
Apollo	Fred. W. Seward	Altar
Alps	Peter H. Watson	Amber
Andes	Jno. T. Tucker	Anchor
Arctic	C. P. Wolcott	Angel
Appian	Geo. Harrington	Animal
Atlas	Geo. V. Fox	Annal
Alamo	J. Dahlgren	Armada
Akron	H. A. Wise	Anvil
Adair	E. D. Townsend	Apple

2 2 6 3 9 6 6

Чейз запропонував ввести ще один ключ: заздалегідь обговорене правило пребудови нижнього рядка цифр. Наприклад, число, визначене цим рядком, помножувалося на 9: 2263966 x 9 = 20375694, після чого отримувався новий шифротекст:

1 3 3 1 3 1 2
2 0 3 7 5 6 9 4

Цей дворядковий запис знову перетворювався у букви згідно з вищезазначеною таблицею, при цьому перше число (2) визначало букву першого рядка. В результаті отримуємо такий шифротекст: UфSWORPM.

Шифр Чейза був більш стійким за шифр Полібія, однак розповсюдження він не мав. Його недоліками були значне ускладнення процесу шифрування-розшифрування та особлива чутливість шифру до помилок (перекручування у шифротексті).

В другій половині XIX століття відбулася революція у військовій справі. З'явилися нові засоби збройної боротьби (парові кораблі, нарізні артилерія та стрілецька зброя), комунікацій (залізниця) та зв'язку (телеграф). Поява телеграфу змістовно вплинула на розвиток криптології.

Однією з війн, у якій широко застосовувалися перераховані новинки, стала громадянська війна в США (1861-1865) між мешканцями Півночі (далі – федерали) та Півдня (далі – конфедерати). Перемогу в цій війні одержали федерали, що в результаті привело до створення США в їхньому сучасному вигляді. У цій перемозі помітну роль зіграла перевага федералів у криптологічних методах. При цьому федерали часом «винаходили» заново шифри, що були добре відомі в Європі.

У той час для передачі повідомлень вже широко використовувався телеграф. Щоб телеграфіст міг легко читати переданий текст, шифротексти повинні були бути максимально наближеними до звичайних відкритих текстів. При передачі шифротекстів, що представляли собою хаотичний набір букв, телеграфісти робили численні помилки, що істотно ускладнювало наступне розшифрування. Крім того, помилки виникали через збої при роботі телеграфних апаратів. Наприклад, для американського апарата «Морзе» були характерні помилки при передачі, за результатом яких у тексті одна буква виявлялася зайвою, або навпаки, однієї букви не вистачало. У випадку «хаотичних» шифротекстів такі перекручування нерідко приводили до неможливості розшифрування.

Крім телеграфу застосовувалися й інші способи передачі інформації, зокрема, «прапорцеві» коди. У 1856 році офіцер медичної служби Альберт Джеймс Майер (1828-1880) запропонував метод зв'язку з використанням сигнальних прапорців - прапорцевий семафор (англ. *wig-wag*). Для представлення різних букв використовувалися різні положення прапорця, і в такий спосіб солдати передавали повідомлен-

ня. «Прапорцеву» систему Майера застосовували як солдати північної коаліції, так і конфедерати. Для цього використовувалися природні височини. Якщо таких не виявлялося, то будувалися спеціальні вишки.

Тепер розглянемо шифри, якими користувалися федерали та конфедерати під час Громадянської війни в США. Найбільше поширення у федералів мав шифр, що включав елементи кодування та перестановки слів. Найбільш таємні слова тексту попередньо замінювалися за допомогою довгострокового коду. Наприклад, слово «*COLONEL*» замінювалося на «*VENUS*». Аналогічно, фраза «*PRESIDENT OF USA*» замінювалася на слово «*ADAM*» тощо. Заміна на позначення, що легко читалися, полегшувала роботу телеграфістів, які передавали шифровані повідомлення.

Потім кодований текст виписувався за словами порядково в прямокутник, що містив визначену кількість стовпців. Кількість стовпців у відкритому вигляді передавалося в шифрованому тексті у вигляді якого-небудь слова. Наприклад, слово «*GUARD*», яке стояло на початку телеграми, означало, що в прямокутнику 5 стовпців (кількість букв у слові). Потім з отриманого прямокутника слова виписувалися, наприклад, за таким правилом: перший стовпець – зверху донизу, другий – знизу нагору, третій – зверху донизу тощо. Виходив остаточний шифрований текст, що й передавався телеграфом.

Цей шифр був запропонований у 1861 році Ансоном Стейджером, першим керівником компанії «Вестерн Юніон телеграф». Після мобілізації він був призначений керівником управління військового телеграфу в Огайо. Ще до війни Стейджер запропонував такий шифр для губернатора штату Огайо, що з успіхом використовувався останнім у листуванні зі своїми колегами – губернаторами штатів Індіана й Іллінойс.

У 1862 році завдяки першому масштабному використанню телеграфа у військових цілях шифр Стейджера почав застосовуватися всією армією Півночі. Досвід роботи Стейджера на телеграфі, вочевидь, привів його до системи, у якій шифротекст складався, як і в нових телеграфних кодах, зі звичайних слів, що значно менше піддавалися перекручуванням, ніж групи довільно набраних букв. У ході війни до системи були введені деякі елементарні ускладнення, що її помітно підсилили. До написаного тексту вставлялися «пустишки». Виписка стала робитися по діагоналях і змінних стовпчиках у прямокутниках, що усе більше і більше збільшувалися.

С.Беквіт, шифрувальник командувача військами федералів Уіліса Гранта, запропонував, щоб важливі терміни передавалися кодовими позначеннями, які він ретельно вибирав, щоб звести до мінімуму телеграфну помилку. Цікаво відзначити, що крім військових цим шифром користувався й керівник розвідки Алан Пінкертон,

майбутній засновник знаменитого детективного агентства.

Також використовувалися прості словникові перестановки. У цьому шифрі слова відкритого тексту переставлялися за визначеним законом (ключем). Цей шифр був досить слабким. Використовувався ще один вид шифрів – багатоалфавітні системи (стосовно алфавіту шифрованого тексту), у якому будувалася таблиця розміром 26х26 (число букв латинського алфавіту).

Стовпці таблиці позначалися буквами латинського алфавіту в порядку їхнього звичайного проходження (*A, B, C, ..., Z*). Рядки таблиці були довільними перестановками цих букв. Це був алфавіт відкритого тексту, що визначав верхній рядок підстановки, за яким набиралися букви відкритого тексту. Рядки таблиці використовувалися в природному порядку (перший, другий тощо) і визначали нижній рядок підстановки. Перша буква тексту шифрувалася по першому рядку, друга – по другому тощо. Правило повторювалося циклічно (27-а буква тексту шифрувалася знову по першому рядку, 28-а – по другому тощо).

У липні 1865 року сержант Е.Хоулі запропонував використовувати для цього шифру віяло, що складалося з 26 дерев'яних дощечок, на яких були записані алфавіти шифрованого тексту (рядки таблиці). Це віяло виявилося настільки ефективним у практичному застосуванні, що вперше в історії США його автору був виданий патент на шифропристрій.

У той час як федерали прийняли централізовану організацію системи зв'язку, конфедерати поширили принцип прав штатів і на сферу шифрувальної справи. Кожен командир міг за своїм розсудом вибирати власні коди та шифри. Це привело до істотних негативних наслідків, оскільки місцеві командири практично не розбиралися в шифрувальній справі.

Конфедерати використовували примітивні шифри аж до шифрів простої заміни. Наприклад, перед битвою в Шайлоу 6 квітня 1862 року генерал Джонстон домовився зі своїм заступником генералом Борегаром використовувати як військовий шифр заміну Цезаря. Зрідка вживалися книжкові шифри. Книжковим шифром користувався президент конфедерації південних штатів Джефферсон Девіс. Перед битвою під Шайлоу він послав генералу Джонстону словник для його використання як кодової книги. Додатком до словника була інструкція, в якій вказувалося, що слово «з'єднання» буде виражатися як «146.Л.20», що означало, відповідно, номер сторінки, лівий стовпчик і номер слова.

Словники використовувалися як кодові книги також у ВМФ конфедерації. Його міністр Стефан Мелорі особисто розпорядився, щоб командири кораблів здобули ідентичні примірники різних словників.

Поширені у той час були шифри типу Віженера. Збереглися, навіть, зразки таких шифрувальних пристроїв у вигляді мідних шифрувальних циліндрів. Шифрування здійснювалося за допомогою двох покажчиків (на верхній планці пристрою) на бук-

ви відкритого тексту та відповідні їм букви шифрованого тексту.

Як уже було сказано раніше, при шифруванні допускалися численні помилки. Помилками конфедератів успішно користувалися федерали для дешифрування перехоплених повідомлень. Зокрема, при використанні книжкових шифрів у якості вихідних шифровеличин вибиралися не букви, а слова й цілі вирази. При цьому конфедерати часто використовували загальнодоступні комерційні кодові книги, згідно з якими і робили заміну шифровеличин. Федералам не складно було перебирати обмежене число комерційних кодових книг і знаходити ключ. Для посилення кодування конфедерати вводили прості правила типу: якщо слово, що шифрувалося, знаходилося на 18-му місці 29-ї сторінки книги, то воно замінялося 18-м словом на 19-ій сторінці. Однак подібні модифікації не бентежили федералів.

Шифрований зв'язок федералів здійснювався через Управління військового телеграфу, при якому була шифрувальна служба. Начальником військового телеграфу був майор Томас Екерт, який пізніше став головою правління компанії «Вестерн Юніон телеграф». Управління військового телеграфу розміщалося в будинку військового міністерства, що знаходилося поруч з Білим Домом. Президент Авраам Лінкольн приділяв велику увагу організації шифрованого зв'язку та часто спілкувався з трьома молодими телеграфістами-шифрувальниками: Девідом Бейтсом, Чарльзом Тінкером і Альбертом Чендлером. Ці люди були основними криптоаналітиками Півночі.

Криптоаналітична служба федералів досягла досить серйозних успіхів. Так, наприклад, у грудні 1863 року начальник поштового відділення Нью-Йорка Абрам Уейкман, переглядаючи кореспонденцію перед відправленням, наткнувся на лист, адресований Олександру Кейту до міста Галіфакс у Новій Шотландії. Про Кейта було відомо, що той часто листувався з агентами Півдня. Тому, розкривши конверт та встановивши, що лист зашифрований, Уейкман передав його військовому міністру.

Протягом двох днів співробітники Військового міністерства марно намагалися розгадати таємничі знаки перехопленої криптограми. Потім вона була передана шифрувальникам президента Лінкольна, що взялися її прочитати. Вони швидко встановили, що невідомий автор листа використовував для його зашифрування як звичайний алфавіт, так і 5 різних шифроалфавітів. Але він вчинив нерозсудливо, розділивши слова листа комами та обмеживши одним алфавітом у межах кожного слова.

Дешифрувальники знайшли слово, що складалося з шести букв, у якому друга й шоста букви повторювалися. Потім випливало слово з чотирьох букв, за яким у свою чергу йшла фраза, послана клером: «reaches you». Вони вирішили, що за цією послідовністю шифрознаків повинна ховатися фраза «before this». Бейтс припустив, що в листі використано шифр, подібний тому, що застосовувався для позначення цін у магазині в Пітсбурзі, де він колись давно працював посильним.

Цей здогад дозволив значно просунути вперед процес дешифрування криптограми. Допомогло й виявлення знаків, що позначали місце відправлення і дату

– «Нью-Йорк, 18 грудня 1863 р.». Діючи таким чином, три шифрувальники у присутності президента Лінкольна, що нетерпляче очікував результати, за чотири години прочитали шифрований лист, у якому було написано:

«Нью-Йорк, 18 грудня 1863 р. ...Два пароплави відбудуть звідси приблизно на Різдво... 12 тисяч нарізних мушкетів прийшли точно за адресою та відправлені в Галіфакс відповідно до інструкцій. Ми зможемо захопити ще два пароплави, як намічено... перш ніж це дійде до вас. Ціна 2000 доларів. Нам потрібно більше грошей... Пишіть як колись...»

Два дні по тому була перехоплена та швидко дешифрована ще одна криптограма, адресована Кейту. У ній говорилося: «Передай Меміджеру, що в Хілтона усі верстати знаходяться в зібраному вигляді та всі матриці будуть готові до відправлення 1 січня. Гравірування друкованих форм чудове».

Таким чином, з листа стало відомо, що форми для друкування грошей конфедератів виготовлялися в Нью-Йорку. Гравера Хілтона легко знайшли в Манхеттені. 31 грудня 1863 року поліцейські відвідали його помешкання, де захопили друковані верстати й матриці, а також уже видрукувані гроші на суму в кілька мільйонів доларів. Тим самим конфедерація позбавилася устаткування для виготовлення паперових грошей, яких їй бракувало. Головну роль у всій цій справі зіграли криптоаналітичні здібності, виявлені трьома молодими шифрувальниками Лінкольна. За це кожний з них одержав збільшення до зарплатні розміром у 25 доларів на місяць.

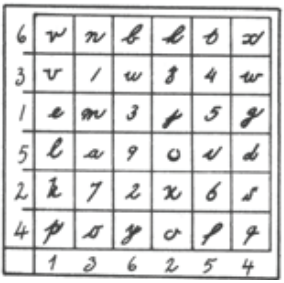
Усього за час війни Північ передала приблизно 6,5 мільйона телеграм. Конфедерати здійснювали перехоплення їхніх телеграфних повідомлень, багато з яких, зазвичай, шифрувалися. Їхня кавалерія робила нальоти на пункти зв'язку, що приводило до компрометації систем шифрування федералів та дозволяло конфедератам одержувати ключі й інформацію про відкриті тексти, що відповідали відомим шифрованим текстам. Крім того, шифри федералів мали слабкості. Незважаючи на все це, конфедерати так і не навчилися розкривати шифровані повідомлення федералів.

Вони іноді, навіть, не могли правильно розшифрувати свої власні повідомлення, не дивно, що їм не вдалося прочитати жодного шифрованого повідомлення федералів. Цьому факту було б важко повірити, якби конфедерати самі не визнали його, надрукувавши у своїх газетах кілька шифрованих повідомлень із проханням їхнього дешифрування.

Федерали також захоплювали шифри Півдня та здійснювали перехоплення кур'єрів із шифрованими повідомленнями. Так, наприклад, у 1863 році під час облоги міста Віксберга війська У.Гранта захопили вісім повстанців і в одного з них знайшли криптограму. Її відправили до Вашингтона криптоаналітикам Президента, які успішно справилися з черговим завданням. Хоча дешифрування цієї телеграми не допомогло Гранту «взяти» Віксберг, але воно дало федералам один з ключів, якими

конфедерати користувалися під час війни.

Шпіони як федералів, так і конфедератів зашифровували свої повідомлення дуже простими шифрами. Так, прихильниця Півночі Елізабет Ван Лью захищала свої агентурні донесення за допомогою буквено-цифрового шифру, основаного на квадраті Полібія. А прихильниця Півдня Роза Грінхоу захищала свої агентурні донесення за допомогою шифру випадкової заміни.



Шифр Розы Гринхоу

Із закінченням громадянської війни та перемогою федералів розробкою кодів і шифрів став займатися Державний департамент США. У 1867 році держсекретар Уільям Генрі Сьюард (1801-1872) розробив код Держдепартаменту на 148 сторінках. Однак процес кодування та декодування виявився для дипломатів дуже складним. Тому у 1871 році начальник корпусу зв'язку полковник Альберт Майер розробив для Держдепартаменту код на 88 сторінках, що складався з однієї частини. Книга містила коди для часу діб, днів, місяців і - вперше в історії кодів - років. Вона стала першим кодом Держдепартаменту, в якому одному кодовому слову відповідала довга фраза або ціле речення. Для позначення часу доби як кодові сдова використовувались жіночі імена, а днів місяця - чоловічі. Назви міст і країн замінялися цифрами.

Наступну книгу державних кодів розробив у 1876 році завідувач бюро каталогів і архівів Держдепартаменту Джон Генрі Хасвел (1841-1899), який до цієї справи підійшов дуже змістовно та прискипливо. Багато років він займався питаннями стійкості кодів і дорожнечі телеграм, вивчав методи шифрування Майера і Стейджера часів Громадянської війни та комерційні коди, зокрема: телеграфний код Слейтера 1870 року. В результаті книга Хасвела, яка мала назву «Шифр Держдепартамента (1876)», містила найкращі риси кодів того часу та мала одну частину на 1200 сторінках. Оскільки вона мала червону обкладинку, пізніше код був названий «червоним» (англ. *red*). Для підвищення стійкості свого коду Хасвел розробив також «Доповнення до шифру Держдепартаменту: код, що не піддається декодуванню». У цьому доповненні перераховувались 50 правил, або

способів перешифрування, які могли застосовуватися до закодованих повідомлень.

У 1878 році вперше в історії США вирішальну роль в американській політиці був вимушений зіграти криптоаналіз. Все почалося з сенсаційної статті, надрукованої 7 жовтня газетою «Трибуна Нью-Йорка» (англ. *The New York Tribune*). У замітці, розміщеній під заголовком «Перехоплені шифровані телеграми», приводився відкритий текст декількох криптограм.

Справа в тому, що в результаті підрахунку голосів, поданих на виборах президента в 1876 році, першим виявився кандидат від Демократичної партії Самуель Тілден, що одержав на чверть мільйона голосів більше, ніж його суперник від Республіканської партії Рутерфорд Хейс. Але як розподіляться вирішальні голоси виборців – це залежало від того, які із суперечливих результатів голосування, проведеного двічі у Флориді, Луїзіані, Південній Каролініі й Орегоні, будуть визнані дійсними. Конгрес створив спеціальну комісію для вирішення цього питання, яка постановила віддати всі спірні голоси виборців Хейсу. Це забезпечило йому більшість усього в один голос у колегії виборців і посаду Президента США.

На сесії Конгресу, що відбулася після виборів Президента, була призначена ще одна спеціальна комісія для розслідування поширених демократами слухів про «купівлю» республіканцями голосів вибірників. У ході розслідування комісія конфіскувала більше 600 шифротелеграм, що були послані різними політичними діячами та їх довіреними особами під час виборчої кампанії в чотирьох штатах. Інші американська телеграфна компанія «Вестерн Юніон» на той час уже встигла знищити, щоб показати, що гарантує таємницю довіреного їй листування.

У 1875 році 27 шифротелеграм були таємно передані до прореспубліканської газети «*The New York Tribune*» у надії на те, що будучи дешифровані, вони поставлять демократів у скрутне становище. Цікаво, що редактор газети Уайтлоу Рейд вирішив не обмежуватися публікацією шифротелеграм своїх політичних супротивників. Він особисто взявся за «розкриття» шифролистування демократів із метою оприлюднення їхніх відкритих текстів.

Багато читачів, спонукувані редакційними статтями газети, пропонували свої варіанти дешифрування опублікованих шифротелеграм, але при перевірці усі вони виявилися невірними. Тим часом газета «Детройт пост» зуміла вивідати в одного з демократів, яким саме шифром користувалися його партійні соратники під час передвиборчої кампанії в Орегоні. Шифрувальник відшукував потрібне слово в «Домашньому англійському словнику», що був виданий у Лондоні в 1876 році, визначав порядковий номер цього слова на сторінці, відраховував 4 сторінки назад і брав на ній відповідне слово як кодове позначення. Для розшифрування отриманого повідомлення його адресат робив навпаки.

4 вересня 1878 року один з редакторів «*The New York Tribune*» Джон Хассард, ґрунтуючись на інформації газети «Детройт пост», опублікував кілька відкритих тек-

стів дешифрованих криптограм, з яких випливало, що в Орегоні демократи прагнули підкупити одного республіканського виборця, однак угода не відбулася тільки через затримку з передачею йому грошей.

Але «Домашній англійський словник» мало допомагав у дешифруванні повідомлень демократів, надісланих з інших трьох штатів. Не розраховуючи більше на сторонню допомогу, Рейд запропонував своїм співробітникам зайнятися їхнім дешифруванням. За справу взялися Джон Хассард і Вільям Гросвенор, економічний оглядач «*The New York Tribune*». Причому Хассард працював над криптограмами настільки завзято, що застудився, занедужав туберкульозом і наступні останні десять років свого життя думав лише про своє одужання.

Пізніше Рейд згадував: «Обоє вони трудилися надзвичайно добре, працювали незалежно один від одного, чесно порівнюючи результати, чудово співробітничали разом... Хассард трохи раніше почав працювати в цій сфері та заслужив особливої похвали. Гросвенор був також здібним і, як я зараз пригадую, досяг майже такого ж успіху. Іноді він і Хассард підходили до дешифрування однієї і тієї ж криптограми з різних боків і після кількаразових невдач, нарешті, знаходили вірне рішення в той самий вечір...»

Одночасно з Хассардом і Гросвенором над читанням криптограм, оприлюднених у редакційних статтях «*The New York Tribune*», працював молодий математик з військово-морської обсерваторії США у Вашингтоні Едвард Холден. У своїх мемуарах Холден написав з цього приводу: «До 7 вересня 1878 року я відкрив закономірність, за допомогою якої можна було безпомилково знайти будь-який ключ до найважчих і хитромудрих із цих телеграм». Він звернувся до газети «Нью-Йорк трибюн», якій сподобалася ідея найняти професійного математика. Хассард вислав Холдену велику кількість криптограм. Однак на той час Хассард і Гросвенор незалежно від Холдена розробили свої криптоаналітичні методи та зуміли випередити його в читанні деяких криптограм. Рейд стверджував, що жодної з дешифрованих Холденом криптограм «*The New York Tribune*» не одержала раніше, ніж ці ж самі криптограми були прочитані Хассардом і Гросвенором. Тому результати роботи Холдена розглядалися лише як підтвердження правильності дешифрувань Хассарда і Гросвенора.

Результат перевершив усі сподівання. Громадськість була обурена з приводу непорядності демократів і захоплена винахідливістю дешифрувальників. Тисячі читачів розшифровували криптограми за допомогою ключів, опублікованих у «The New York Tribune», із задоволенням відзначали правильність їхнього розшифрування. До того ж до виборів у Конгрес залишалося усього кілька тижнів. На них республіканці здобули значну перемогу.

Частина дешифрованих телеграм була на адресу Тілдена – його племіннику У.Пептону. І хоча Тілден клявся, що зовсім не знав, чим займався його племінник і що все було зроблено без його дозволу, репутація Тілдена була назавжди

заплямована. Це викриття поклало кінець його надіям стати президентом. Навіть біограф Тілдена, що мав до нього велику симпатію, визнав, що в результаті дешифрування телеграм демократів республіканці одержали перевагу, яка забезпечила їм перемогу на президентських виборах у 1880 році. Ось так криптоаналіз допоміг обрати американського президента.

У листопаді 1899 року «червоний» шифр Держдепартаменту був замінений на новий - «блакитний» (англ. *blue*), який знову був розроблений Джоном Хасвелом і названий за кольором своєї обкладинки. Книга була більш докладною, містила найбільш уживані терміни та фрази з кореспонденції посольств і консульств, тому мала вже 1500 сторінок. Для підвищення стійкості свого коду Хасвел розробив також «Доповнення до шифру Держдепартаменту: код, що не піддається декодуванню» на 16 сторінках. У цьому доповненні перераховувались додатково ще 25 правил, або способів перешифрування, які могли застосовуватися до закодованих повідомлень, крім вказаних у доповненнях до «червоного» шифру.

У 1910 році Держдепартамент прийняв на озброєння «зелений шифр» (англ. *green*) , який складався з двох частин (кодування і декодування) і мав 1418 сторінок. У березні 1918 року був введений в дію «сірий» (англ. *grey*) код, в якому для позначення стандартних термінів і фразів використовувались 5-буквені групи. У травні 1919 року «зелений шифр», який реально був тільки кодом, отримав відповідну йому назву «Код Держдепартаменту А-1». Ці коди разом використовувались американськими державними службовцями навіть до Другої світової війни, коли було потрібно здійснити зміни в дипломатичних і військових криптосистемах з метою підвищення їхньої стійкості. Так, наприклад, ще у 1940 році ще «сірим» кодом «закривалася» трансатлантичне листування, навіть між керівниками США і Британії.

30 грудня 1937 року був введений в дію «коричневий» (англ. *brown*) код Держдепартаменту, який містив розділ для кодування обсягом 954 сторінки та розділ для декодування обсягом 938 сторінок. Подібно А-1 та іншим сучасним на той час кодам «коричневий» код мав багаточисельні варіанти заміни для часто уживаних слів. Він також поклав початок системі кодування дат і часу, що стало нововведенням наприкінці 1930-х років. Місяці позначалися першою буквою, дні - другою та третьою, час - четвертою, а за допомогою п'ятої букви уточнювалася половина дня - перша чи друга. І хоча цей код у 1939 році був викрадений з американського консульства у Загребі (Югославія), ним продовжували користуватися навіть під час Другої світової війни.

Кодом американських військових атташе у той час був «чорний» (англ. *black*), отримавший назву за кольором своєї палітурки. На початку 1940 року він вважався невразливим, оскільки додаткову стійкість йому забезпечували шифрувальні таблиці. Але насправді вже на початку війни він був скомпрометований: його «зламала» німецька служба радіоперехвату та криптоаналізу.

2.2. Винахід «лінійного» шифрування

В історії криптології спрощення процедури ручного шифрування шляхом механізації цього процесу здавна цікавило багатьох фахівців. Допитливі розуми винахідників неодноразово намагалися вирішити цю проблему. Спроб було багато, але лише деякі змогли залишити в історії помітний слід і закласти фундамент для майбутньої механізації, а потім і автоматизації шифрувальної справи.

Поштовхом до необхідності автоматизувати процес шифрування послужили технічні досягнення кінця XIX століття, такі як телеграф, телефон і радіо, при використанні яких для передачі криптограм удалося істотно підвищити оперативність шифрованого зв'язку. Слідом за змінами у зв'язку змінювалася й криптологія, яка стала спочатку електромеханічною, а потім електронною. Швидкість передачі інформації дуже зросла та все більші обсяги її були піддані перехопленню та прочитанню. Шифрувальники, що вручну заміняли букви та склади спеціальними символами, уже не могли упоратися з постійно зростаючим потоком інформації.

Радіозв'язок виявився дешевшим та мобільнішим за проводовий. З'явилася можливість активізувати повідомлення між військовими підрозділами, установлювати зв'язок з рухомими об'єктами (автомобілями, літаками, кораблями). Однак при цьому спростилося перехоплення переданих таким чином повідомлень, що, зокрема, підтвердила практика Першої світової війни.

Незважаючи на те, що всі учасники бойових дій постійно розробляли нові коди та вдосконалювали старі, забезпечити їхнє збереження вдавалося далеко не завжди. В результаті супротивники нерідко були цілком поінформовані про все, що було в таємному листуванні ворога. З цим були пов'язані і деякі трагічні події, з яких згадаємо у третій частині лише розгром двох російських армій – Раненкампа та Самсонова в Східній Пруссії в серпні 1914 року. Причиною їхнього розгрому була погана організація «закритого» зв'язку, у результаті чого переговори по радіо велися взагалі без усякого шифрування.

Під час війни головним (і найчастіше єдиним) засобом засекречування було кодування. Коди часто застосовували не тільки для того, щоб забезпечити таємність переданої інформації, але й щоб скоротити довжину повідомлення або зробити його більше зрозумілим. Найчастіше код являв собою набір символів (цифр або букв), що заміняли конкретні назви.

До речі, розвиток технічного шпигунства й, зокрема, радіоперехоплення, буквально ні на крок не відставав від розвитку систем передачі повідомлень, освоюючи нові діапазони та способи модуляції. Проте основна маса телеграфних та телефонних повідомлень передавалася або після їх закриття шифрами простої заміни, або просто відкритим текстом.

Різке розширення обсягів зашифрованих передач і порівняльна простота радіоперехоплення повідомлень підштовхнули дешифрувальників до думки про те, що дослідження окремої перехопленої криптограми необхідно зв'язати з аналізом усього масиву перехоплення, у якому з'явилася ця криптограма. Цей шлях виявився досить плідним. Як справедливо відзначає Д.Кан, «телеграф створив сучасну шифрувальну справу, радіо – сучасний криптоаналіз».

Шифрований текст, переданий по радіо, був доступний кожному, хто мав у своєму розпорядженні нескладний приймач. І навіть, якщо цей текст не можна було розшифрувати відразу, його можна було використовувати при аналізі наступних повідомлень. У цей період одержали розвиток методи дешифрування, засновані на парах відкритих і шифрованих текстів; на декількох шифровках, створених за допомогою одного ключа; на переборі ймовірних ключів. Саме ці методи застосовувалися англійцями для читання секретного листування німців під час Першої світової війни.

Телеграф і радіо почали поступово витісняти кодування з метою захисту інформації на користь застосування шифрів. Громіздкі та малозручні при використанні секретні кодові книги могли стати і ставали здобутком супротивника, а їхня зміна породжувала серйозні проблеми. Шифри виявилися набагато мобільнішими та дешевшими. Секретне кодування почало зменшуватися, але не зникло зовсім. Коди стали застосовуватися разом із шифрами. Таке сполучення виявилося досить ефективним і дійшло до наших днів. Підкреслимо, що при компрометації шифру досить лише змінити його ключі, а не всі кодові книги. Відзначимо також, що коди дуже чуттєві до лексики та словникового запасу мови спілкування. Поява нових термінів і понять приводила до необхідності поновлення кодових книг. Шифри в цьому плані набагато важливіші, тому що їхнє застосування не пов'язане зі змістом відкритого тексту.

До речі, у 1881 році була запатентована перша ідея телефонного шифратора Д.Х.Роджерсом. Ідея складалася в передачі телефонного повідомлення декількома (у найпростішому випадку – двома) лініями за допомогою почергових імпульсів у деякій послідовності, яка швидко змінювалася та нагадувала телеграфне повідомлення. Пропонувалося рознести такі лінії на значну відстань одна від одної для того, щоб усунути можливість підключення відразу до всіх одночасно. Підключення ж до однієї з них дозволяло б чути лише окремі нерозбірливі сигнали.

У XIX столітті застосовувалося, в основному, так зване, попереднє шифрування повідомлень. У цьому випадку відправник зашифровував передане повідомлення (у якому шифротекст задовольняв вимогам телеграфної передачі), після чого відносив шифроване повідомлення на телеграф. У XX столітті таке уповільнення в передачі повідомлень часто виявлялося неприйнятним. Треба було розробити методи так званої лінійної передачі шифрованих повідомлень, при якій апарат шифрування (шифратор) знаходився би безпосередньо в апаратурі передачі послань. Таким чином, передача шифрованого повідомлення в принципі не відрізнялася би від пере-

дачі нетаємного повідомлення.

Таку ідею автоматичного шифрування телеграфних повідомлень у грудні 1917 року запропонував американець Жильбер Вернам (1890-1960), молодий інженер компанії «Американський телефон і телеграф» (англ. *American telephone and telegraph, AT&T*) та талановитий винахідник. Він працював у телеграфному відділенні науково-дослідного відділу компанії, де займалися розробкою «телетайпу» – букводрукуючого телеграфного апарату.

Ще влітку, через кілька місяців після того, як Сполучені Штати оголосили війну Німеччині, в компанії почалася робота над секретним проектом щодо можливості зберігання в таємниці повідомлень, переданих телетайпом. Під час досліджень виявилося, що коливання струму в лінії зв'язку могли бути записані за допомогою осцилографу та потім легко перетворені в букви переданого повідомлення. Тому було вирішено внести зміни в з'єднання дротів друкуючого механізму телетайпу. У результаті текст повідомлення шифрувався методом одноалфавітної заміни. У телеграфному відділенні розуміли, що такий захист був занадто слабким, однак нічого іншого придумати не змогли та припинили займатися цією проблемою до тих самих пір, поки Вернам не повідав їм про свою ідею.

Він запропонував використовувати особливості телетайпного коду Бодо, в якому кожний знак складався з п'яти елементів. Кожний з цих елементів символізував наявність («+») чи відсутність («–») електричного струму в лінії зв'язку. Таким чином, було 32 різні комбінації «+» і «–». 26 з них повинні були відповідати буквам, а ті, що залишилися, позначали «службові комбінації» (пробіл між словами, перехід з букв на цифри та розділові знаки, зворотний перехід з цифр і розділових знаків на букви, повернення каретки друкуючого пристрою, перехід на новий рядок і холостий хід).

Наприклад, буква «А» позначалася комбінацією «++---», а перехід на цифри та розділові знаки позначався комбінацією «++-++». Закодоване повідомлення набивалося на перфострічці: «+» були дірками, а «–» – їхньою відсутністю. При зчитуванні перфострічки металеві щупи проходили через дірки, замикали електричне коло та посилали імпульси струму по дротах. А там, де на перфострічці знаходився «–», папір не дозволяв цим щупам замкнути коло, і в результаті струмовий імпульс не передавався.

Вернам запропонував готувати перфострічку з випадковими знаками (так звану «гаму») заздалегідь і потім електромеханічно складати її імпульси з імпульсами знаків відкритого тексту. «Гама» – це секретний ключ, що хаотичним набором букв того ж самого алфавіту. Отримана сума являла собою шифротекст, призначений для передачі по лінії зв'язку. Вернам установив таке правило підсумовування: якщо відразу обидва імпульси були «+» чи «–», то підсумковий імпульс буде «-», а якщо ці імпульси різні, то в результаті вийде «+».

Додавання, за сучасною термінологією, здійснюється «за модулем 2» («0»

означає знак «–», а 1 – «+»): 0 + 0 = 0; 0 + 1 = 1; 1 + 0 = 1; 1 + 1 = 0. Нехай, наприклад, знак «гами» має вигляд: «+-+--» (10100). Тоді буква «А» – «++---» (11000) при шифруванні переходить у двійкову комбінацію «-++--»: (01100) = (11000)х(10100). При розшифруванні ту ж операцію необхідно повторити у зворотньому порядку: (01100) х(10100) = (11000) - «++---» – буква «А».

Щоб підсумовувати електроімпульси при шифруванні, Вернам сконструював спеціальний пристрій, що складався з магнітів, реле та струмознімних пластин. А оскільки процедура розшифрування була аналогічна процедурі зашифрування, цей же прилад міг бути використаний і при розшифруванні. Імпульси надходили в пристрій підсумовування з двох зчитувачів: один зчитував «гаму», а інший – відкритий текст. «Плюси» й «мінуси», що отримували на виході, можна було передавати як звичайне телетайпне повідомлення. На прийомному кінці пристрій, винайдений Вернамом, додавав імпульси, що зчитувалися з ідентичної стрічки з «гамою», і відновлював вихідні імпульси відкритого тексту.

Важливість винаходу Вернама полягала в тому, що більше не потрібно було здійснювати зашифрування й розшифрування секретних повідомлень у вигляді окремих операцій. Відкритий текст входив в апарат, що знаходився у відправника повідомлення, і такий же відкритий текст виходив з апарата, що належав одержувачу цього повідомлення. А якщо хто-небудь перехоплював це повідомлення на шляху проходження від відправника до одержувача, то в його розпорядженні виявлялася нічого не значуща послідовність «плюсів» і «мінусів». Тепер, щоб зашифрувати, передати, прийняти та розшифрувати повідомлення, було потрібно прикласти не набагато більше зусиль, ніж при відправленні повідомлення відкритим текстом.

Основна перевага винайденого Вернамом методу засекречування повідомлень полягала не в механічному шифруванні відкритого тексту з наступною печаткою результату на папері, що було здійснено ще на початку 70-х років XIX століття французами Емілем Вінеєм і Жозефом Госсеном. Вернам уперше зумів поєднати два процеси – шифрування та передачу повідомлення. Він створив те, що згодом назвали лінійним шифруванням, щоб відрізняти його від традиційного попереднього шифрування. Вернам звільнив процес шифрування від кайданів часу й помилок, виключивши з цього процесу людину. Видатний внесок, зроблений Вернамом у практику шифрування, полягає саме в тому, що він привніс у шифрувальну справу автоматизацію, що вже встигла до початку XX століття послужити людям у багатьох сферах їхньої діяльності.

Навколо ідеї, висловленої Вернамом у колі колег, моментально розгорнулася активна діяльність. Спочатку Вернама змусили викласти цю ідею в короткій записці, яка була датована 17 грудня 1917 року. Компанія «*AT&T*» повідомила про винахід Вернама американське військово-морське відомство, з яким вона підтримувала тісне співробітництво. 18 лютого 1918 року відбулася нарада, у якій взяли участь

Вернам і інші інженери з телеграфного відділення компанії «*AT&T*», з одного боку, і військові моряки, з іншого.

27 березня ці ж інженери зустрілися зі своїми колегами з американської компанії «Вестерн електрик», виробничої філії «*AT&T*», і домовилися з ними про виготовлення перших двох лінійних шифраторів із використанням якомога більшої кількості стандартних деталей. У лабораторії «Вестерн електрик» виготовлені шифратори були приєднані до телетайпів і здійснені перші іспити процесу, що назвали «автоматичним шифруванням». Усі пристрої, що входили до його складу, працювали без збоїв. Компанія «*AT&T*» проінформувала про цей факт майора Джозефа Моборна (1881-1971), що займав тоді посаду начальника відділу науково-дослідних і конструкторських розробок військ зв'язку Армії США.

Невирішеним залишалося всього одне питання – звідки брати «гаму». Спочатку «гама» для пристрою Вернама являла собою склеєні петлею короткі перфострічки, на які були набиті знаки, витягнуті навмання з різних відкритих текстів. Інженери компанії «*AT&T*» майже відразу звернули увагу на істотні вади такого процесу «автоматичного шифрування», пов'язані з недостатньою довжиною «гами». Тому, щоб ускладнити криптоаналіз, вони зробили перфострічки з «гамою» більш довгими. Але тоді ці перфострічки стало занадто важко використовувати.

Вернам запропонував підсумовувати дві короткі, що мають різну довжину «гами» таким чином, начебто б одна «гама» шифрувала іншу. Отримана в результаті так звана вторинна «гама», яка мала значно більшу довжину, ніж дві вихідні первинні «гами», що були використані для її генерації, була застосована для зашифрування відкритого тексту. Наприклад, якщо одна закільцьована стрічка мала 1000 знаків, а інша – 999, то дане розходження в довжинах усього в один знак давало 999 000 комбінацій, перш ніж результуюча послідовність повторювалася.

Однак Моборн розумів, що навіть удосконалена система Вернама дуже вразлива для криптоаналізу. У свої 36 років майбутній начальник військ зв'язку США Моборн був неабияким криптоаналітиком. Він ґрунтовно вивчив криптоаналіз в армійській школі зв'язку та був добре обізнаний з останніми досягненнями в цій сфері. Більш того, за кілька років до описуваних подій Моборн сам брав участь в одній науково-дослідній роботі, у ході якої фахівці з армійської школи зв'язку зробили висновок про те, що єдиною стійкою «гамою» була така, що порівняна по довжині з самим повідомленням. Будь-яке повторення в «гамі» піддавали величезному ризику отримані за її допомогою криптограми та, скоріше за все, привели би до їх розкриття.

Проведений Моборном аналіз системи «автоматичного шифрування» ще більше переконав його в цьому. Він зрозумів, що не має ніякого значення, чи знаходяться повторення в межах однієї криптограми чи вони розподілені по декількох, чи виходять вони шляхом комбінування двох первинних «гам», чи в результаті простого повторення в єдиній довгій «гамі». Важливим було те, що в «гамі» повторень не

повинно бути ні за яких умов. Необхідно, щоб вона була зовсім унікальна й максимально хаотична.

Усвідомивши це, Моборн об'єднав властивість хаотичності «гами», на що спирався Вернам у своїй системі «автоматичного шифрування», із властивістю унікальності «гами», виробленою криптографами армійської школи зв'язку, у системі шифрування, що нині прийнято називати «одноразовим шифроблокнотом». Одноразовий шифроблокнот містив випадкову «гаму», що використовувалася тільки одного разу. При цьому для кожного знака відкритого тексту передбачалося використання абсолютно нового знака «гами», який не піддавався прогнозуванню.

Це була стійка шифросистема. Переважна більшість систем шифрування були абсолютно стійкими лише на практиці, оскільки криптоаналітик міг знайти шляхи їхнього розкриття при наявності в нього визначеної кількості шифротексту та достатнього часу для його дослідження. Одноразовий же шифроблокнот був абсолютно стійким як у теорії, так і на практиці. Яким би довгим не був перехоплений шифротекст, скільки б багато часу не приділялося на його дослідження, криптоаналітик ніколи не зможе розкрити одноразовий шифроблокнот, використаний для одержання цього шифротексту. І ось чому.

Розкриття багатоалфавітного шифру означало об'єднання всіх букв, зашифрованих за допомогою одного шифроалфавіту, у єдину групу, яку можна вивчати на предмет виявлення її лінгвістичних особливостей. Методи такого об'єднання могли бути різними в залежності від виду «гами». Так, метод Казиського полягав у виділенні ідентично «гамованих» букв відкритого тексту при повторюваній «гамі». Зв'язна «гама» могла бути розкрита шляхом взаємного відновлення відкритого тексту та «гами». А «гама», використана для зашифрування двох чи більше повідомлень, піддавалася розкриттю шляхом одночасного відновлення відкритих текстів цих повідомлень, причому правильність прочитання одного тексту контролювалася читаністю іншого. Майже для всіх різновидів багатоалфавітних шифрів був розроблений свій метод розкриття, заснований на їхніх відмінних рисах.

Зовсім іншою була ситуація з одноразовим шифроблокнотом. У цьому випадку криптоаналітик не мав відправної крапки для своїх досліджень, оскільки в одноразовій шифросистемі «гама» не містила повторень, не використовувалася більше одного разу, не була зв'язним текстом і не мала внутрішніх структурних закономірностей. Тому всі методи дешифрування, тією чи іншою мірою засновані на цих характеристиках, не давали ніяких результатів. Криптоаналітик заходив до тупика.

Залишався лише метод тотального випробування. Адже прямий перебір усіх можливих ключів, у кінцевому рахунку, обов'язково приводив криптоаналітика до відкритого тексту. Однак успіх, досягнутий цим шляхом, був ілюзорним. Тотальне випробування дійсно дозволяло одержати вихідний відкритий текст. Але воно також давало й кожен інший можливий текст тієї ж довжини, тому сказати, який з них

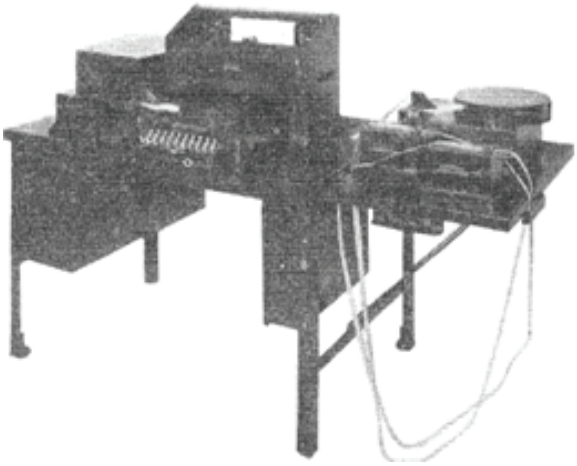
є правильним, було неможливо.

Разом із тим, цей досконалий шифр не знайшов широкого застосування через величезну кількість «гам», що потребуються при його використанні. Проблеми, що виникають при виготовленні, розсиланні та знищенні «гами», людині, не обізнаній в усіх тонкостях організації шифрозв'язку, можуть здатися дріб'язковими, однак у воєнний час обсяги листування стають дуже великими. Протягом доби може знадобитися зашифрувати сотні тисяч слів, а для цього потрібно виготовити мільйони знаків «гами». І оскільки «гама» для кожного повідомлення повинна бути єдиною та неповторною, то її загальний обсяг буде еквівалентний обсягу всього листування за час війни.

Таким чином, практичні проблеми не дозволили застосовувати одноразові шифроблокноти у ситуаціях, які швидко змінюються, наприклад, у ході проведення військових операцій. Цих проблем не існувало в більш стабільних умовах: у генеральних військових штабах, дипломатичних представництвах або агентурному листуванні одноразові шифроблокноти були досить практичними та знайшли застосування. Однак і тут виникали нездоланні труднощі, якщо обсяг листування був занадто великим.

Це саме й відбулося, коли Моборн, улаштувавши перший великий іспит шифросистеми Вернама, установив його машини відразу в трьох містах. Навіть, при порівняно невеликому обсязі листування (до 135 коротких повідомлень щодня) виявилося неможливим виготовити достатню кількість якісної «гами». Тому, не знайшовши іншого виходу зі скрутного становища, Моборн став комбінувати з двома відносно короткими «гамами» з метою одержання з них більш довгої «гами», як це спочатку й пропонував робити сам Вернам.

У вересні 1918 року Вернам відправився до Вашингтона та подав там заявку на патент. Перша світова війна встигла закінчитися скоріше, ніж шифросистема Вернама зуміла хоч якось виявити свої достоїнства на практиці. Проте 22 липня 1919 року на неї був виданий патент № 1310719 – найважливіший в історії криптології. Експерти з вашингтонського патентного бюро визнали можливу корисність цього винаходу й у мирний час.



Хоча прилад, утворений Вернамом, безсумнівно був цінним результатом творчої інженерної

G. S. VERNAM.

SECRET SIGNALING SYSTEM.

APPLICATION FILED SEPT. 13, 1918.

1,310,719.

Patented July 22, 1919.

2 SHEETS—SHEET 1.

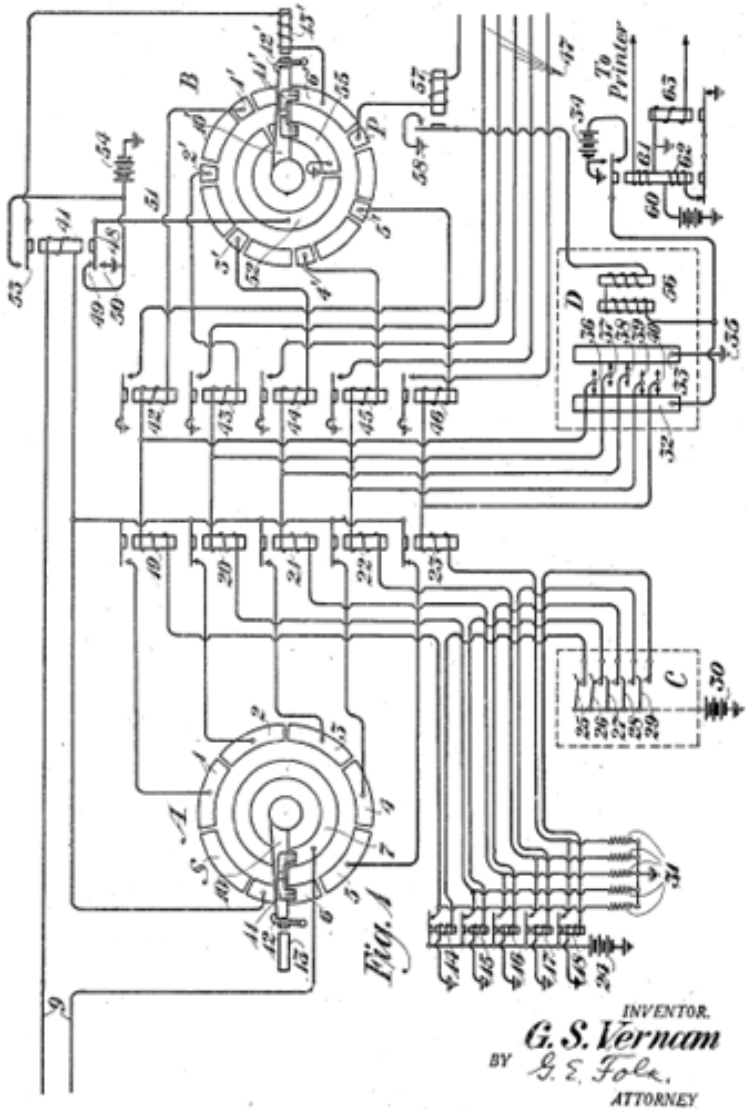


Fig. 1

INVENTOR.

G. S. Vernam

BY G. E. Folz.

ATTORNEY

думки талановитого винахідника, у комерційному плані він зазнав повного «провалу». Телеграфні компанії та комерційні фірми, що, на думку «*AT&T*», повинні були масово закуповувати запатентовані шифроприставки Вернама до своїх телетайпів, віддавали перевагу старомодним кодам, що істотно знижували довжину повідомлень, тим самим зменшуючи телеграфні витрати й одночасно забезпечуючи хоч якусь, навіть невелику, безпеку листування. Після закінчення Першої світової війни бюджети збройних сил усіх країн були скорочені до мінімуму. Недолік засобів і недостатність матеріальних ресурсів змусили армійських зв'язківців знову повернутися до комбінування двох відносно коротких стрічок з «гамою», а продемонстрована військовими криптоаналітиками слабка стійкість такої системи генерації «гами» призвела до того, що шифросистема Вернама на якийсь час була забута.

Стосовно ж самого Вернама, то він продовжував займатися науково-дослідною роботою в компанії «*AT&T*». Учений удосконалив свою шифросистему, а також винайшов прилад для автоматичного шифрування написаного від руки тексту під час його передачі фототелеграфом. У 1929 році Вернама зі значним підвищенням перевели в одну з філій компанії «*AT&T*». Однак через чотири місяці в США вибухнула фінансова криза, і, оскільки Вернам ще не встиг заробити достатній виробничий стаж на новому місці, його незабаром звільнили. Він перейшов на роботу в іншу велику компанію, але різка зміна в його особистій долі, певно, подіяла на нього гнітюче. З кожним роком про Вернама було чути усе менше і менше, поки нарешті 7 лютого 1960 року людина, що автоматизувала процес шифрування, не вмерла практично в повному забутті.

2.3. «Чорний кабінет» Ярдлі

У 1912 році у Держдепартаменті у якості шифрувальника почав працювати Герберт Ярдлі (1889-1958), один із видатних американських криптоаналітиків. На початку своєї кар'єри Ярдлі звернув увагу на слабкість шифрів, які використовувались американським урядом. Він був приголомшений, дізнавшись, що президент Вудро Вільсон користується кодом, який використовується впродовж більше 10 років. Так, коли Президенту США Вудро Вільсону було передане закодоване повідомлення з 500 слів від його радника Хауза, Ярдлі був уражений тим, що прочитав це повідомлення усього за кілька годин.

Досягнутий успіх ще більше підвищив інтерес Ярдлі до криптоаналізу, і він У травні 1916 року написав 100-сторінковий меморандум «Розкриття американських дипломатичних кодів», який передав своєму керівництву. Заглибившись у проблему можливого розкриття чергового коду, він першим поставив діагноз явищу, що з тих пір відомо серед американських криптоаналітиків як «симптом Ярдлі»: «Просинаючись, я відразу починаю про це думати. Засинаючи, я все одно продовжую

думати про це».

6 квітня 1917 року американський Конгрес оголосив про вступ США у Першу світову війну проти Німеччини. А 28 квітня у складі Управління військової інформації «*MID*» (англ. *Military Information Division*) Генштабу Військового департаменту (англ. *War Department General Staff*) була створена кабельно-телеграфна секція (англ. *Cable and Telegraph Section*), яка отримало кодову назву «*MI-8*» (англ. *Military Information, Section 8*).

Для участі в бойових діях Першої світової війни на територію Франції було перекинуто морем експедиційне з'єднання американських військ під командуванням генерала Джона Першинга чисельністю більше 175 тисяч осіб. Ярдлі був направлений в Американський експедиційний корпус у якості офіцера-шифрувальника. Вже в перші місяці роботи Ярдлі на практиці продемонстрував свої видатні криптоаналітичні здібності. Участь у війні дала йому можливість переконати «батька» американської військової розвідки «*MID*» майора Ральфа ван Демана в необхідності створити спецпідрозділ для «злому» шифрів інших країн. Він домігся успіху не тільки тому, що американській армії були потрібні криптоаналітики, але й завдяки винятковому таланту переконувати людей у своїй правоті. В результаті у червні 1917 року Ярдлі у званні другого лейтенанта вже очолив «*MI-8*».

Навчальний підрозділ «*MI-8*», що займався підготовкою криптоаналітиків, очолив доктор Джон Менлі. 52-літній філолог, який був деканом факультету англійської мови в Чиказькому університеті, а також давнім і палким шанувальником криптоаналізу, Менлі став одним з кращих криптоаналітиків «*MI-8*». Очолюваний ним підрозділ був розташований та проводив заняття з криптоаналізу у військовому коледжі армії США.

«*MI-8*» читала дипломатичне шифролистування Аргентини, Бразилії, Німеччини, Іспанії, Коста-Рики, Куби, Мексики, Панами і Чилі. Служба американської цензури надсилала до «*MI-8*» перехоплені шифровані листи. Більшість із них на перевірку виявлялася любовними посланнями, у яких застосовувалися дуже прості шифри. Хоча багато з них були настільки компрометуючими, що Ярдлі часто повторював: «Мене дратує той факт, що чоловіки й дружини довіряють своє таємнє листування таким слабким методам шифрування».

Найважливіша з розробок «*MI-8*» привела до звинувачення Лотара Вітцьке – єдиного німецького шпигуна, засудженого в США до страти під час Першої світової війни. 25 січня 1918 року при обшуку в його багажі був виявлений шифрований лист, датований 15 січня. Він потрапив до «*MI-8*» тільки навесні і пробув там протягом ще декількох місяців, поки криптоаналітики безуспішно намагалися його дешифрувати. Зрештою цей лист вдалося прочитати Менлі, який у з'ясував, що він був надісланий німецьким послом у Вашингтоні Еккардтом німецькому консулу в Мексиці. Відкритий текст листа був таким:

«Пред'явник цього є підданим Німецької імперії, що подорожує під ім'ям Павла Ваберського. Він є німецьким секретним агентом. Якщо він звернеться до вас із проханням, будь ласка, забезпечте йому захист і надайте допомогу. Також видайте йому до тисячі песо золотом і посилайте його шифровані телеграми до нашого посольства в якості офіційних консульських депеш».

Коли Менлі зачитав цей текст у залі суду на закритому процесі за обвинуваченням Вітцьке в шпигунстві, сумнівів у його винності ні в кого не залишилося. Шпигун був засуджений до страти через повішення. Однак Вільсон замінив смертний вирок довічним ув'язненням. У 1923 році Вітцьке був помилуваний та випущений на волю.

9 лютого 1918 року «*MID*» було реорганізоване в Управління військової розвідки (англ. *Military Intelligence Division*). У листопаді того ж року «*MI-8*» нараховувала 18 офіцерів, 24 цивільних криптографів, 109 друкарок і стенографісток. Однак до травня наступного року її штатна чисельність скоротилася до 15 офіцерів, 7 цивільних криптографів і 55 технічних службовців.

Після участі Ярдлі в 1919 році в Паризькій мирній конференції в якості головного криптографа американської делегації керівництво розвідки оголосило про майбутнє згортання дешифрувальної роботи через утрату її актуальності. Ярдлі категорично заперечував і підготував доповідь під назвою «Вивчення та розкриття кодів і шифрів», у якій вказував, що Сполучені Штати мають досить ворогів у всьому світі, тому розкриття їхніх шифросистем дозволить уряду завчасно одержати інформацію про можливі загрози національній безпеці.

Ярдлі пропонував не припиняти цю роботу, а реорганізувати «*MI-8*» у криптослужбу мирного часу з подвійним підпорядкуванням Держдепартаменту та Генштабу Військового департаменту. Ця аргументація настільки вразила начальника розвідки генерала Мальборо Черчиля, що він умовив держсекретаря зберегти «Бюро шифрів» і фінансувати його роботу з таємного фонду.

Це «Бюро шифрів», що пізніше стало відомим як «американський чорний кабінет» (англ. *american black chamber*) (далі – АЧК), повинно була спільно фінансуватися двома департаментами на суму приблизно в 100 000 доларів у рік, але її фактичні витрати ніколи не досягали цієї суми. За законом платежі Держдепартаменту, що почали надходити в червні 1919 року, не могли бути на законних підставах витрачені в межах Вашингтона, і тому Ярдлі разом з підібраним зі складу «*MI-8*» персоналом АЧК незабаром переїхав до Нью-Йорка. Військовим департаментом АЧК був уперше профінансований лише 30 червня 1921 року. Первісний бюджет Бюро склав 45 тисяч доларів замість запитаних 96 тисяч, а до 1929 року знизився до 19630 доларів.

Кінцевим продуктом криптослужби був бюлетень, що надсилався до Відділу військової розвідки та Держдепартаменту, у який включалися усі факти, що заслуговували уваги, природно, без посилань на справжнє походження інформації.

Усі повідомлення починалися стереотипно: «Із джерел, що заслуговують довіри, встановлено, що:». При цьому ніякого інформаційно-аналітичного підрозділу в «Бюро шифрів» не існувало, матеріали відбирав особисто його керівник, часто за суб'єктивними ознаками.

Післявоєнне дешифрування АЧК німецького листування базувалися на отриманих у Нідерландах у 1919 році ключах, що запропонував американським представникам ініціативник, відомий під агентурним псевдонімом «Дачмен». Як часто траплялося в подібних випадках, «Дачмена» обдурили: коли він залишив кодові таблиці для вивчення, їх сфотографували і повернули, нібито через непотрібність. На підставі його даних американці зуміли розкрити німецькі коди з позначеннями «2500», потім «2970», «9700», «5300» і «1219». Усього АЧК прочитав 20 німецьких кодів і шифрів, однак на післявоєнний період з них припало лише 9, що фактично являли собою варіації двох базових систем.

Одним з основних завдань, поставлених перед АЧК, було «розкриття» кодів Японії, напруженість у відносинах з якою зростала з кожним днем. У пориві ентузіазму Ярдлі пообіцяв домогтися їхнього «розкриття» протягом року або піти у відставку. Він пошкодував про свою обіцянку відразу, як тільки приступив до цієї справи, оскільки моментально заплутався у відкритих текстах японською мовою, не говорячи вже про самий шифротекст.

Після тривалого попереднього аналізу Ярдлі з'ясував, що для своїх телеграфних повідомлень, що передавалися буквами латинського алфавіту, японці використовували трохи видозмінену форму ієрогліфічної писемності, іменованої як «катакана». Але, незважаючи на ретельне вивчення перехоплених шифротелеграм, прочитати їх так і не вдавалося. Він писав:

«До цього часу я так довго працював з кодованими телеграмами, що кожен їхній рядок, навіть кожне кодове позначення назавжди викарбувалося в моїй голові. Я міг лежати на ліжку з відкритими очима та займатися своїми дослідженнями в повній темноті... І ось одного разу я прокинувся опівночі, тому що пішов з роботи рано, і звідкись із темряви прийшло переконання, що визначена послідовність двобуквених кодових позначень повинна абсолютно точно відповідати слову «Ірландія». Потім переді мною затанцювали, швидко змінюючись, інші слова – «незалежність», «Німеччина», «крапка»... Велике відкриття! Серце моє завмерло, я не міг рушити з місця. Чи було це зі мною уві сні або наяву, чи не зійшов я з розуму? Рішення? Нарешті, після всіх цих місяців! Я зістрибнув з ліжка та у поспіху (оскільки тепер уже точно знав, що не сплю) майже скотився по сходах. Тремтячими руками я відкрив сейф, схопив папку з паперами і квапливо почав робити замітки».

Протягом години Ярдлі перевіряв свої гіпотези, а потім, переконавшись, що початок успішному розкриттю покладено, повернувся до себе додому та напився. Однак його радість була трохи передчасною. Ярдлі зустрівся з несподіваними

труднощами, намагаючись підшукати перекладача з японської мови. Зрештою він знайшов добродушного місіонера, що у лютому 1920 року зробив для Ярдлі перші переклади відкритих текстів японських шифротелеграм. Через півроку місіонер-перекладач звільнився, усвідомивши шпигунський характер своєї праці. Однак на той час один із підлеглих Ярдлі зробив воістину нечуваний подвиг, вивчивши у цей термін дуже важку японську мову.

У 1920 році Ярдлі доповів про розкриття 4-х японських кодів, але це ствердження було не цілком коректним, оскільки розкриті системи були не кодами, а шифрами, причому досить невисокого рівня стійкості. Однак незабаром після цього «Бюро шифрів» дійсно досягло вражаючих успіхів. Усього з 1917 по 1929 роки американці зуміли скомпрометувати 31 японську шифросистему (умовні позначки від «*JA*» до «*JZ*» і від «*JAA*» до «*JEE*») і прочитати 10000 текстів, 1600 з яких відносилися до Вашингтонської конференції. Це було дуже високим показником, особливо з урахуванням гострої нестачі співробітників зі знанням мови.

Улітку 1921 року АЧК прочитав японську шифротелеграму від 5 липня, яка була направлена до Токіо послом Японії в Лондоні та містила перші згадування про конференцію з роззброєння, що повинна була відбутися в листопаді у Вашингтоні. Після цього читання японського дипломатичного шифролистування стало настільки регулярним, що за кілька місяців до відкриття конференції були введені щоденні поїздки кур'єрів між АЧК і Держдепартаментом. Одна офіційна особа в уряді США з посмішкою помітила, що керівники Держдепартаменту відносилися до роботи криптоаналітиків з АЧК із замилуванням і щоранку читали дешифровані ними японські криптограми, попиваючи при цьому апельсиновий сік або каву.

Метою Вашингтонської конференція з роззброєння було обмежити тоннаж великих військових кораблів. По мірі того, як переговори наближалися до свого головного результату – договору п'яти держав, який встановлював визначене співвідношення тоннажу для Англії, Італії, США, Франції і Японії, персонал Ярдлі читав усе більшу кількість секретних шифрованих інструкцій, що призначалися для країн, що брали участь у переговорах. Він писав: «Американський чорний кабінет, глибоко захований за надійними запорами, усе бачить й усе чує. Хоча віконниці закриті й вікна ретельно зашторені, його гострий зір спостерігає за тим, що діється на секретних нарадах у Вашингтоні, Женеві, Лондоні, Парижі, Римі і Токіо. Його чутливі вуха чують навіть найслабший шепіт у столицях іноземних держав».

Кожен учасник переговорного процесу у Вашингтоні прагнув домогтися найбільш сприятливого для себе тоннажного співвідношення. Найагресивнішою виявилася Японія, що виношувала широкомасштабні задуми, пов'язані з експансією в Азії, але побоювалася викликати невдоволення своїми діями з боку США. У самий розпал конференції, коли Японія зажадала встановити для себе співвідношення 10 до 7 у порівнянні зі США, АЧК прочитав японську шифротелеграму від 28 листопада,

яку Ярдлі пізніше назвав найважливішою з дешифрованих ним криптограм.

«Вам слід подвоїти зусилля для досягнення поставлених цілей відповідно до проведеної нами політики, уникаючи при цьому будь-яких зіткнень з Америкою з питання про обмеження озброєнь, — телеграфувало японське МЗС своєму послу у Вашингтоні. — Ви повинні домогтися прийняття пропозиції про співвідношення тоннажу 10 до 6,5. Якщо ж, незважаючи на всі ваші зусилля, через сформовану ситуацію й у інтересах нашої політики виникне потреба піти на поступки, вам необхідно заручитися згодою всіх сторін на обмеження права концентрації Військово-морських сил і проведення маневрів на Тихому океані в обмін на нашу гарантію зберегти там статус-кво. У прийнятій угоді вам також варто зробити відповідне застереження, з якого було б зрозуміло, що саме в цьому складається наш намір, коли ми приймаємо співвідношення 10 до 6».

Зменшення тоннажу Військово-морських сил Японії на 0,5 умовних одиниць, про що йшла мова в цій японській шифротелеграмі, приблизно відповідало двом великим бойовим кораблям. Оскільки представники США на переговорах вчасно одержали з АЧК інформацію про те, що у випадку натиску японці погодяться на збільшення тоннажного співвідношення між Америкою і Японією, залишалося тільки зробити цей натиск на практиці. Що і зробив держсекретар Чарльз Х'юз.

10 грудня Японія «капітулювала». У шифротелеграмі, яка була прочитана АЧК, японська делегація на переговорах у Вашингтоні отримала інструкцію з Токіо про те, що необхідно прийняти співвідношення, запропоноване США. У результаті договір, підписаний п'ятьма державами, встановив для США та Японії співвідношення тоннажа великих військових кораблів у розмірі 10 до 6. Японці сподівалися на більше. Однак домогтися бажаного їм перешкодив АЧК.

За час проведення конференції в АЧК було прочитано та перекладено більше 5000 шифроповідомлень. Внаслідок перенапруження декілька його співробітників занедужали на нервовому ґрунті: один почав щось незв'язно бурмотіти, інший став присвячувати весь свій вільний час ловлі бродячого собаки, у якого на боці нібито був записаний японський дипломатичний код, а третьому уявлялися жахіття, і він постійно носив при собі величезну сумку з камінням, зібраним на морському березі. В результаті усі троє були змушені піти з роботи. Сам Ярдлі також виявився на межі нервового розладу та у лютому 1922 року одержав чотиримісячну відпустку для відновлення свого здоров'я.

Крім стану здоров'я співробітників, предметом постійної турботи з боку держави стало також забезпечення безпеки функціонування АЧК. Його пошта направлялася на підставну адресу. Прізвище Ярдлі не значилося в телефонному довіднику міста Нью-Йорк. Замки на дверях мінялися якнайчастіше. Проте відомості про діяльність АЧК усе-таки просочилися за кордон, тому що була здійснена спроба підкупити Ярдлі. Коли вона провалилася, на службове приміщення АЧК був зроблений напад,

після якого зі столів зникли важливі документи.

Щоб не допустити нової пропажі, були прийняті додаткові заходи з безпеки. Тепер кожен аркуш паперу замикався на ніч у сейф, щоб нічого не залишалося в столах, хоча співробітникам АЧК усе-таки дозволялося брати додому матеріали, над розкриттям яких вони працювали.

Через якийсь час Ярдлі разом зі своїми підлеглими переїхав в інший службовий будинок. Як надійне прикриття для них була створена «Компанія зі складання кодів» (англ. *Code Compilation Company*). А щоб «легенда» виглядала цілком правдоподібною, Ярдлі склав «Загальний торгівельний код», яким компанія зі складання кодів стала торгувати разом з іншими розповсюдженими комерційними кодами.

У 1924 році асигнування АЧК були різко скорочені. У результаті Ярдлі довелося звільнити половину персоналу, і штат співробітників АЧК скоротився приблизно до 12 осіб. Однак, незважаючи на це, за словами Ярдлі, «у 1917-1929 роках АЧК вдалося прочитати більше 45 тисяч шифротелеграм Англії, Аргентини, Бразилії, Німеччини, Домініканської Республіки, Іспанії, Китаю, Коста-Рики, Куби, Ліберії, Мексики, Нікарагуа, Панами, Перу, Сальвадору, Радянського Союзу, Франції, Чилі і Японії, а також проробити попередній аналіз багатьох інших кодів, включаючи коди Ватикану».

У 1929 році плідній діяльності АЧК зненацька прийшов кінець. Справа в тому, що до Ярдлі тексти іноземних шифротелеграм надходили від американських телеграфних компаній, які передавали їх йому з великим небажанням. Коли посаду Президента США зайняв Герберт Гувер, Ярдлі вирішив врегулювати питання про шифроперехоплення з новим урядом раз і назавжди. Він задумав зробити доповідь безпосередньо Президенту з викладом характеру діяльності АЧК, а також необхідних кроків, що повинні бути розпочаті, якщо уряд США бажає цілком використовувати майстерність своїх криптоаналітиків.

Після того як Генрі Стімсон, держсекретар при Гувері, пробув на своїй посаді кілька місяців, що, як вважав Ярдлі, було необхідно для придбання деякого досвіду практичної дипломатії, АЧК направив йому серію важливих дешифрованих криптограм. Однак на відміну від колишніх держсекретарів, на яких ця тактика завжди робила належний вплив, Стімсон, довідавшись про існування АЧК, обурився та суворо засудив його діяльність. Він обізвав її «підлим різновидом шпигунського ремесла» та розцінив як віроломне порушення принципу взаємної довіри, якого він неухильно дотримувався як у своїх особистих справах, так і у своїй зовнішній політиці.

Все сказане Стімсоном було справедливим, якщо, звичайно, відкинути точку зору, відповідно до якої будь-які засоби виправдані, коли вони корисні для інтересів батьківщини. Зробивши акт моральної мужності та припинивши усяку фінансову підтримку АЧК з боку Держдепартамента, Стімсон тим самим затвердив верховенство принципу над інтересами.

Оскільки гроші, що виділялися Держдепартаментом, складали головне джере-

ло утримання АЧК, це означало його неминуче закриття. Невитрачені 6666 доларів і 66 центів, а також всі архіви АЧК були передані армійській службі зв'язку. Його співробітники швидко розбрелися хто куди (служити в армію ніхто з них не пішов), і 31 жовтня 1929 року АЧК (*MI-8*) перестав існувати. Десять років його дешифрувальної роботи обійшлися американській скарбниці в 300 000 доларів, при цьому Державний департамент надав дві третини цієї суми, а Військовий - одну.

Ярдлі не зміг підшукати собі роботу і повернувся додому, в рідний Уортінгтон. Там він написав книгу «Американський чорний кабінет» на 375 сторінках, яка була надрукована 1 червня 1931 року. У книзі була викладена історія американської радіотехнічної розвідки та діяльності «*MI-8*» під час Першої світової війни, а також АЧК у 1920-х роках і проілюстровані основні принципи радіорозвідки. Ця книга відразу ж стала популярною.

Критики прийшли до висновку, що це був «найсенсаційніший внесок в таємну історію війни, а також післявоєнного періоду, який до цих пір не написана американцем». У США відразу ж було продано 17 931 примірників книги, 5480 - у Великобританії, вона була перекладена на французьку, шведську, японську і китайську мови. Японське видання вийшло безпрецедентним тиражем у 33119 примірників. Ця книга була неприємним сюрпризом для уряду США і скомпрометувала ряд джерел, використаних Ярдлі. Завдяки цій роботі 19 країн було попереджено, що їхні коди були «зламані».

«Батько» американської криптології Уільям Фрідмен, прочитавши книгу, «ошаленів», оскільки визнав, що Ярдлі розкрив джерела і методи роботи криптологів і непомірно прикрасив свої заслуги. Ярдлі, можливо, вважав, що публікація цієї книги змусить уряд відновити програми радіорозвідки, але добився прямо протилежного ефекту. Уряд США намагався почати судове переслідування Ярдлі, але він формально не порушив чинне законодавство відносно захисту урядових документів. До 1933 року були внесені поправки в Закон про шпигунство 1917 року, відповідно до яких було заборонено розкриття іноземних шифрів і шифрованих повідомлень. Друга книга Ярдлі «Японські дипломатичні коди, 1921-1922» була арештована та ніколи не публікувалася, а рукопис був розсекречений тільки у 1979 році.

Пізніше Ярдлі вступив на службу до китайського диктатора Чан Кайши з окладом 10 000 доларів у рік, щоб займатися дешифруванням японських криптограм. У 1940 році він повернувся з Китаю, щоб відправитися до Канади. Там Ярдлі організував дешифрувальне бюро. Однак незабаром його вислали назад до США, де у 1958 році він помер від серцевого нападу. Ще одна книга його мемуарів «Китайський чорний кабінет» (англ. *The Chinese Black Chamber*) була розсекречена та опублікована тільки у 1983 році.

За значний вклад у криптологію ім'я Герберта Ярдлі увічнене в Залі слави АНБ (англ. *NSA Hall of Honor*) та військової розвідки США (англ. *Military Intelligence Hall of*

Fame). У бібліотеці Національного музею криптології США (англ. *National Cryptologic Museum*) зберігається 16 шаф із його особистими документами.

2.4. Армійська криптослужба

До початку Першої світової війни завдання забезпечення криптозахисту військових повідомлень у Армії США були покладені на три військові відомства:

1) Управління військової інформації «*MID*» Генштабу Військового департаменту відповідало за розробку армійських кодів і шифрів;

2) Генерал-ад'ютантський департамент (англ. *Army Adjutant General's Department*) забезпечував виготовлення кодових книг і шифродокументів та їхнє розсилання в підрозділи;

3) Війська зв'язку (англ. *Army Signal Corps*) відповідали за експлуатацію шифрувальної апаратури та забезпечення нею підрозділів армії. У той час на озброєнні Армії був кодовий диск, який був заснований на пристрої, зробленому Дж.Хіксом у Лондоні ще у 1893 році.

Підготовка фахівців з криптоаналізу для Армії США була розпочата за декілька років до початку Першої світової війни і спочатку здійснювалася у Школі військ зв'язку (англ. *Army Signal School*), розташованої у Форт-Лівенворт (штат Канзас). Пізніше всі питання, пов'язані з підготовкою таких фахівців, були передані у ведення «*MID*». Підготовка офіцерського і рядового складу почала здійснюватися у знов утвореній армійській школі криптології, яка розмістилася в містечку Рівербенк, недалеко від м.Женева (штат Ілінойс). Керівництво школою було покладене на фахівця в області криптології полковника Джорджа Фабіана, якому вдалося привернути до викладання в школі ряд цивільних професорів і учених. Серед них був і Уільям Фрідмен, в подальшому один з керівників і провідних фахівців армійської криптослужби.

Під час Першої світової війни завдання з організації надійного та безпечного зв'язку частин американського експедиційного з'єднання у Франції, розробки та розсилки кодових книг і шифродокументів, а також керівництво підрозділами радіорозвідки з добування відомостей про супротивника були покладені на начальника зв'язку з'єднання бригадного генерала Едгара Рассела. Підпорядкований йому невеликий за чисельністю спеціальний підрозділ займався складанням польових кодів. Оформлені у вигляді таблиць коди призначалися для перетворення відкритих текстів команд, розпоряджень і донесень в еквівалентних їм умовні групи буквено-цифрових символів. Кодові книги, що розсилалися в бойові підрозді-

ли, мали малий формат, були зручні для використання в польових умовах і містили близько 30 тисяч слів (фраз) і відповідних їм кодових значень.

Очолював ці роботи капітан Говард Барнс, що мав 10-річний досвід роботи з кодами Держдепартаменту. Уважно ознайомившись з існуючим британським кодом і вивчивши обстановку на полях битв, Барнс зі своїми помічниками склав «Американський код для окопів». Цей код призначався для передачі повідомлень у роти діючої армії, проте дійшов він лише до штабів полків, оскільки існували побоювання, що його може захопити супротивник. Весною 1918 року була підготовлена та випущена 1 тисяча примірників «окопного» коду в паперовій обкладинці – книжечка поміщалася в нагрудній кишені.

У березні 1918 року було підготовлене та поширене 500 примірників книги телефонної коди. Він служив для приховування імен командного складу, офіцерів штабу і назв організацій. Спочатку передбачалося використовувати його тільки для телефонних переговорів, але він почав застосовуватися також і в інших засобах зв'язку. Оскільки для приховування змісту служив список жіночих імен, то дуже скоро він отримав прізвисько «Жіночий код».

24 червня 1918 року була введена в дію перша з кодових книг серії «Річкових кодів» - «Потомак». Це була книга на 47 сторінках, яка містила 1800 фраз і слів, складалася з двох частин і призначалася для використання в батальйонах. Спочатку було випущено 2 тисячі примірників. Як і у разі інших кодів, номер і час складання повідомлення, закодованого «Потомаком», передавалися відкритим текстом, але місце відправлення і адресат були закодовані. Повідомлення великого об'єму ділилися та пересилалися двома або декількома частинами.

Після «Суоні» та «Уобаша» четвертим з серії «Річкових кодів» став «Мохаук». У серпні 1918 року було випущено для використання в батальйонах 3200 примірників кодової книги «Мохаук», що складалася з двох частин. Вона відрізнялася від своїх попередниць тим, що її коди складалися з груп по 4, а не по 3 цифри. У неї, як і у «Потомака», були варіанти для часто уживаних букв і чисел.

Роль експедиційного з'єднання американських військ зросла, коли в бойові дії вступила Друга армія. Для забезпечення захисту її зв'язку були розроблені коди, що отримали назву «Озерних кодів», тоді як Перша армія продовжувала користуватися діючим кодом «Колорадо» з серії «Річкових кодів». Назва коду «Шамплейн» на обкладинці була надрукована червоним кольором, щоб відрізнити його і наступні коди від «Річкових кодів», назви яких друкувалися чорним кольором. Цей код був триграфным і складався з двох частин.

У жовтні 1918 року був введений в дію другий з «Озерних кодів» - «Гурон». Цей код, що складався з двох частин, був примітний тим, що був першим в історії США кодом, призначеним для кодування телефонних переговорів у повному обсязі. Оскільки тепер до всього іншого ще і потрібно було забезпечити безпеку розмов по

телефонах, які були украй уразливі для підслуховування, то для передачі відкритим текстом слів застосовувався фонетичний алфавіт. Такі слова вимовлялися по телефону по буквах, при цьому для приховування кожної букви використовувалися різні кодові слова.

Також у жовтні був підготовлений та випущений «Американський службовий радіокод № 1». Він складався з двох частин і приблизно 1 тисячі слів і фраз. 2 тисячі примірників книг з цим кодом було передано в бригади та артилерійські частини. Кодові групи були триграфи без варіацій. У 6 розділах частини, призначеної для кодування, були представлені типові, впорядковані за абеткою слова і фрази, серед яких були ті, що використовувалися при радіопередачах, а також словник з радіомереж та радіоапаратури.

Робота підрозділу була достатньо складною, особливо у разі компрометації кодів. Один з таких випадків відбувся з кодом «Потомак», який потрапив до рук німців через місяць після надходження кодових книг в підрозділи експедиційного з'єднання американських військ. У жовтні 1918 року те ж саме трапилося з кодом «Мохаук» і його наступником «Аллегейні». Було потрібно декілька діб напруженої роботи особового складу підрозділу для їх повної заміни. Всього за 10 місяців бойових дій підрозділом було складене, віддруковане та розіслане у війська більше 80 тисяч кодових книг. Після цього на обкладинці кодової книги «Колорадо» - останньої з серії «Річкових кодів» - було надруковано: «Запам'ятай цю групу: *DAM* - Код втрачений».

Крім того, під час Першої світової війни для шифрування повідомлень під час бойових дій армія США використовувала також і мову індійців. Так, у вересні 1918 року у складі 30-ї Піхотної дивізії, що діяла в координації з британськими військами і під британським командуванням, знаходилося декілька загонів індійців-зв'язківців «черокі», які брали участь у Другій битві на річці Сомме. У жовтні 14 індійців-зв'язківців «чокто» у складі 36-ї Піхотної дивізії допомогли експедиційним військам США виграти ряд боїв у ході Мюс-аргонської кампанії у Франції. Протягом доби після того, як мова «чокто» почала використовуватися в бойових умовах, у діях відбувся поворот не на користь німців, а менш ніж через 3 доби війська Союзників вже переслідували відступаючі німецькі війська.

Характерною ознакою Першої світової війни, крім застосування воюючими сторонами нових видів озброєння - літаків, танків, підводних човнів, стала поява нового виду військової розвідки - радіорозвідки. Її успіху і широкому розвитку сприяли інтенсивне застосування засобів радіозв'язку, численні порушення радистами правил радіооб-

міну, передача по радіо секретних розпоряджень і наказів, зашифрованих з використанням нескладних код і шифрів. Разом з російською, англійською, французькою, німецькою і австро-угорською арміями радіорозвідка в роки Першої світової війни велася і підрозділами експедиційного з'єднання американських військ.

Пости підслуховування, до складу яких входили підготовлені військовослужбовці, які володіли німецькою мовою, розміщувалися в безпосередній близькості від районів розташування німецьких військ. Підключивши телефонні апарати до дротових ліній зв'язку супротивника, вони здійснювали прослуховування та запис передаваних по ним телеграфних і телефонних повідомлень. Пости радіоперехоплення, розташовані, як правило, на значному видаленні від лінії фронту, дозволяли без безпосереднього зіткнення зі супротивником здобувати цінні відомості про його угрупування, дії та наміри. Можливості американської радіорозвідки істотно підвищувалися завдяки використанню постів радіопеленгації, що визначали місця розташування військових радіостанцій супротивника.

Зашифровані повідомлення супротивника з постів підслуховування та радіоперехоплення поступали у відділ військової розвідки експедиційного з'єднання, де фахівці з дешифрування намагалися «зламати» коди і шифри, якими користувалися німецькі військові. Криптоаналітичною роботою у відділі в основному займалися випускники та колишні викладачі армійської криптологічної школи, які були мобілізовані на військову службу після вступу США у війну з Німеччиною.

Серед них був і Уільям Фрідмен, який у липні 1918 року в чині лейтенанта був направлений до французької штаб-квартири Американського експедиційного корпусу. Там він очолив розкриття німецьких шифрів у безпосередній близькості від фронту. Після швидкого закінчення війни Фрідмен повернувся у Військове міністерство у Вашингтоні, плануючи завершити своє 6-місячне перебування в армії. Але замість цього його служба у подальшому затяглася ще на 35 років.

1 січня 1921 року обов'язки з розробки армійських кодів і шифрів були передані з Управління військової розвідки до Управління начальника військ зв'язку (англ. *Office of the Chief Signal Officer*) Армії США. З цією метою у складі останнього була створена Секція коду і шифру **«***CCS*» (англ. *Code and Cipher Section*), керівником якої був призначений Фрідмен. Основним завданням, покладеним на новий підрозділ, стала не тільки розробка кодів, а й засобів і методів криптозахисту армійських систем зв'язку.

Завдяки зусиллям **«***CCS*» у 1922 році на озброєння американської армії поступив малогабаритний ручний шифрувальний пристрій роторного типу «*M-94*», а на озброєння ВМФ - під назвою «*CSP-488*» у 1926 році. В основу його роботи був покладений принцип дії шифрувального пристрою XVIII століття Томаса Джеферсона, що складався з декількох десятків обертових дисків, по окружності яких були вигравірувані букви й цифри.

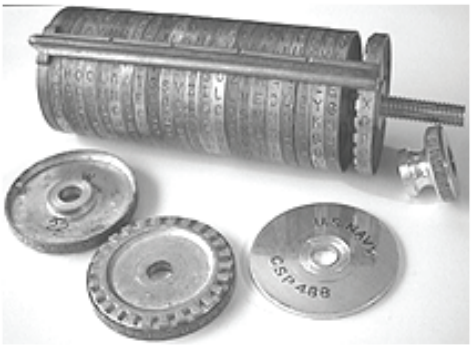
Історія його створення була такою. На початку 1917 року начальник відділу науково-дослідних і конструкторських розробок військ зв'язку майор Джозеф Моборн удосконалив смужковий шифратор «*M-138*», розроблений інструктором школи військ зв'язку капітаном Паркером Хітом у 1914 році. Моборн знову застосував диски, завдяки яким алфавіти могли розташовуватися значно різноманітніше, ніж у пристрої Хіта.

Цей пристрій під назвою «*M-94*» був призначений для використання в польових умовах і прийшов на заміну застарілого зразка, що знаходився на озброєнні армійських частин дуже багато років. В наступні роки він широко використовувався для шифрування інформації, переданої в тактичній ланці зв'язку, зокрема, при веденні бойових дій підрозділами американських військ у Китаї та Бірмі, аж до середини Другої світової війни.

«*M-94*» виготовлявся з алюмінієвого сплаву: на 4,25-дюймовій вісі встановлювалося 25 дисків, схожих на срібні долари. Уся ця конструкція закріплювалася з одного боку вісі гайкою-баранчиком. На металеві диски були нанесені букви від «*b*» до «*z*» і числа від 1 до 25. По зовнішньому краю дисків були відштамповані різні послідовності букв алфавіту. При обертанні диски утворювали безліч алфавітів, завдяки чому «*M-94*» ставав багатоалфавітним пристроєм, що дуже нагадував циліндр Базері.

Шифрувальник встановлював диски в заздалегідь визначеній послідовності, після чого, обертаючи їх, виставляв по горизонталі перші 25 букв повідомлення. У будь-якому іншому рядку виходив безглуздий набір букв, який і служив шифротекстом. Процес шифрування групами по 25 букв тривав до тих пір, поки не виявлялося зашифрованим усе повідомлення. Розшифрування виконувалося за відомою ключовою послідовнітю розташування дисків. Диски встановлювалися на вісі, а потім оберталися, поки не виходив такий самий рядок букв шифртекста. Після цього шукався рядок букв, що мав сенс, який і був рядком повідомлення.

Для оцінки криптостійкості нового шифру фахівцям з криптоаналізу було надано 25 повідомлень, зашифрованих з використанням одного і того ж ключа. Не дивлячись на тривалі спроби, зламати шифр не вдалося. У подальші роки пристрій «*M-94*» широко використовувався для шифрування інформації, передаваної в тактичній ланці зв'язку, зокрема при веденні бойових дій підрозділами американських військ в Китаї і Бірмі, аж до середини Другої світової війни. Ним також користувалися військові аташе, морські аташе і берегова



охорона США. З 1921 по 1941 роки було зроблено близько 10 тисяч пристроїв.

10 травня 1929 року у зв'язку з закриттям АЧК Ярдлі (*MI-8*) Військовий департамент вирішив об'єднати всі армійські шифрувальні та дешифрувальні служби в рамках військ зв'язку. В результаті відповідальність за криптологічну діяльність в Армії США була покладена на Начальника військ зв'язку. Щоб краще виконувати ці нові обов'язки, «*CCS*» у квітні 1930 року була реорганізована у розвідувальну службу зв'язку «*SIS*» (англ. *Signals Intelligence Service*), керівником якої став Фрідмен.

Новій службі були поставлені завдання з розробки армійських кодів і шифрів, перехоплення повідомлень, що передавалися по проводових і радіолініях зв'язку супротивника, пеленгації його радіостанцій, криптоаналізу кодів і шифрів і, нарешті, лабораторні дослідження в області тайнопису. Частину з вказаних функцій передбачалося виконувати тільки у разі ведення армією бойових дій.

Також у 1929 році в США був отриманий патент № 1845947 на шифр, який дозволяв шифрувати одразу 3 і більше символів, тобто «*N*» кількість букв («*N*»-грами). Криптосистема була винайдена Лестером Хіллом і здійснювала шифрування з використанням математичних перетворень: обчислень за допомогою прийомів лінійної алгебри. Зокрема, біграмний шифр був варіантом цього шифру при *N=2*.

Що стосується смужкового шифратора Хіта «*M-138*», то він розпочав використовуватися у військах лише з 1934 року. Метод Хіта грунтувався на використанні шифратора, створеного ще Етьєном Базері у XIX столітті. Правда, Хіт не користувався циліндрами; він розгорнув диски з буквами і записав ці букви на 25 вузьких паперових смужках у різному порядку. На кожній смужці знаходився перемішаний алфавіт, повторений двічі. Усі смужки нумерувалися та кріпилися в утримувачі розміром 18х8 см. Ці ключові числа визначали розташування смужок в утримувачі.

Зашифровування виконувалося шляхом переміщення смужок вгору та вниз, поки в якому-небудь з рядків не з'являлися перші букви повідомлення. Як шифротекст використовувався інший, обраний довільним чином рядок букв. Процес повторювався до тих пір, поки не виявлялося зашифровано усе повідомлення. Одержувач повідомлення встановлював смужки з алфавітом відповідно до ключового числа, яке було погоджено з посилачем, після чого виконував усі дії в зворотному порядку. Цей процес здобув популярність як «смужкова система».

У 1939 році пристрій був удосконалений, внаслідок чого в Сухопутних військах з'явилася модифікація «*M-138A*». Вона також діяла за принципом перемішаних алфавітів на пересувних паперових смужках. «*M-138A*» мав 100 паперових смужок, причому одночасно використовувалися лише 30 з них. Ці смужки з алфавітом вставлялися відповідно до ключа в горизонтальні пази панелі, закріпленої на шарнірах.

Зашифровування здійснювалося таким чином. Букви відкритого тексту вирівнювалися по вертикалі за допомогою прикріпленої лінійки. Далі вибирався який-небудь інший стовпець, лінійка пересувалася та встановлювалася поряд з ним, даючи можливість без зусиль виписати букви цього стовпця, які ставали шифротекстом. Ця операція повторювалася до тих пір, поки усе повідомлення не виявлялося зашифрованим. При розшифруванні смужки розташовували відповідно до заздалегідь заданого ключа, після чого для переходу від безглуздих груп букв до осмислених слів виконували ті ж дії, що і при зашифровуванні, але в зворотному порядку. Коли розпочалася Друга світова війна, «*M-138A*» використовували Держдепартамент і ВМФ як пристрій «*CSP-845*». З 1935 по 1944 роки було зроблено близько 17 тисяч пристроїв.

У 1930-і роки в Америці нелегальне добування розвідувальної інформації було дуже нелегким завданням. Розділ 605 Федерального акта про зв'язок 1934 року забороняв підслуховування, а також перехоплення послань між іноземними державами та Сполученими Штатами. Начальник штабу армії в період з 1937 по 1939 роки суворо виконував інструкції та перешкоджав спробам перехоплення японських дипломатичних послань, що надходили до США. Однак для генерала Джорджа Маршала, який його замінив, вимоги національної безпеки були найбільш важливими.

У зв'язку з цим військові підрозділи радіорозвідки з'явилися в США тільки у 1938 році - саме тоді було створено 1-у роту у Форт-Монмаут, а також утворені окремі підрозділи при 5 ротах зв'язку, розташованих у Панамі, на Гавайських островах, Філіппінах, в штаті Техас і районі Сан-Франциско. У 1939 році з метою вдосконалення керування створеними підрозділами на їх базі у Форт-Монмаут була сформована 2-а рота радіорозвідки у складі 101 військовослужбовця рядового складу і одного офіцера - командира роти. Для зарахування на службу в роту військовослужбовці проходили суворий професійний і морально-психологічний відбір, а перевагою користувалися ті з них, хто прослужив на військовій службі певний термін і виразив згоду на проходження подальшої служби на військових базах США, дислокованих за кордоном.

Перед початком Другої світової війни рота мала у своєму розпорядженні 6 постів радіоперехоплення: № 1 - Форт-Хенкок, штат Нью-Джерсі; № 2 - Сан-Франциско; № 3 - Форт-Шафтер, Гавайські острови; № 6 - Форт-Мілс, Маніла, Філіппіни; № 7 - Форт-Хант, штат Вірджинія; № 9 - Ріо-де-Жанейро. Перехоплені постами шифротелеграми прямували для їх криптоаналізу у «*SIS*», фахівці якої працювали в будівлі Військового департамента у Вашингтоні.

Спочатку доставка матеріалів радіоперехоплення до Вашингтона здійснювалася авіапоштою або морем, тому часто у зв'язку з поганими погодними умовами відбувалися значні затримки у відправці матеріалів. Для виправлення ситуації перехоплені і заздалегідь зашифровані американським військовим шифром повідомлення почали передаватися в столицю по каналах радіозв'язку.

Наприкінці 1930-х років американській розвідці в результаті успішної проведеної операції вдалося проникнути в таємницю побудови нової японської шифрувальної машини, яку спеціальні кур'єри таємно перевозили морем з Токіо до свого посольства у США. Після ретельного вивчення наданих в їх розпорядження креслень і інших матеріалів групі армійських криптоаналітиків на чолі з Фрідменом вдалося виготовити декілька копій японської шифромашини. Одна з них була передана до ВМФ, а останні залишилися у розпорядженні Армії. У серпні 1940 року, після більш ніж півтора років напруженої роботи, «*SIS*» вдалося розкрити ряд японських дипломатичних кодів і шифрів, що дозволило американському військово-політичному керівництву бути в курсі всього секретного радіолистування МЗС Японії з його посольством у США.

Потік повідомлень японського МЗС, перехоплюваних підрозділами армійської і флотської радіорозвідок, був достатньо великий. Восени 1941 року він складав від 50 до 75 радіограм на добу, при цьому обсяг окремих повідомлень досягав 15 сторінок надрукованого тексту. У зв'язку з великим завантаженням фахівців з дешифрування та з метою впорядкування їх роботи командуванням Армії і ВМФ США було ухвалено рішення, згідно якому дешифровка повідомлень, прийнятих по парних днях місяця, здійснювалася криптоаналітиками Армії, а по непарних днях - криптоаналітиками ВМС.

Робота підрозділів радіоперехоплення та криптоаналізу напередодні вступу США у війну з Японією була достатньо напруженою. З 227 повідомлень по питаннях японо-американских відносин, якими обмінялися МЗС Японії і його посольство у Вашингтоні в період з березня по грудень 1941 року, американській радіорозвідці вдалося перехопити 223 повідомлення та лише 4 радіограми були пропущені.

До початку Другої світової війни «*SIS*» налічувала всього 7 співробітників. Не дивлячись на свою нечисленність, у 1930-х роках їй вдалося виконати великий обсяг робіт в області вдосконалення армійських кодів і шифрів, підготовки фахівців і створення нової апаратури шифрування та радіорозвідки. У серпні 1934 року їй були передані функції виготовлення і розсилки кодових книг і шифрдокументов, внаслідок чого всі питання, пов'язані з криптографічним захистом повідомлень, опинилися у веденні Управління начальника військ зв'язку Армії США.

У березні 1941 року у зв'язку з відставкою Фрідмена начальником «*SIS*» був призначений підполковник Рекс Мінклер. А Фрідмен став у Мінклера цивільним заступником і головним технічним консультантом. Станом на 7 грудня «*SIS*» на-

раховувала 181 одиницю офіцерів, рядових і цивільного персоналу у Вашингтоні та 150 одиниць – на станціях радіоперехоплення. «*SIS*» містила в собі Школу розвідки зв'язку, у якій навчали криптології кадрових офіцерів і резервістів, другу роту зв'язківців, що поєднувала штат станцій перехоплення, та вашингтонські підрозділи самої служби.

Напад Японії 7 грудня 1941 року на Перл-Харбор став причиною для вступу США в Другу світову війну. Після нападу японців на Філіппінські острови генералу Д.Макартуру було наказано покинути Філіппіни та створити базу для Армії США в Австралії. Він, розуміючи необхідність дешифрувальної служби, своїм наказом 15 квітня 1942 року створив Центральне бюро радіорозвідки в Мельбурні (згодом воно було перебазоване у Брісбен).

У липні 1942 року капітан «*SIS*» Абрахам Сінков (1907-1998) прибув до Мельбурну як керівник американського підрозділу Центрального бюро. Його формально очолював генерал С.Ейкін, але насправді він рідко з'являвся в цій організації, фактично керівництво бюро здійснював Сінков, який проявив хороші організаторські здібності та зумів в короткий термін сформувати єдину команду з американців і австралійців. Діяльність бюро сприяла успіху дій американської армії в повітряній війні проти японців і дозволила одержати ряд перемог в операціях на Новій Гвінеї та Філіппінах.

Після початку війни обсяг роботи «*SIS*» стрімко зріс. Чисельність служби за попередні два роки збільшилася з 19 до 181 особи і продовжувала рости, у зв'язку з чим у серпні 1942 року особовий склад служби перебрався з Вашингтона до Арлінгтон-Холу – просторого будинку колишньої приватної школи, розташованого в одному з передмість штату Віргінія на узбережжі ріки Потомак. Практично одночасно з переїздом відбулися організаційні зміни в Управлінні начальника військ зв'язку Армії США.

«*SIS*» була перетворена в Напрямок безпеки зв'язку «*SSB*» (англ. *Signal Security Branch)*. До її складу увійшли батальйон радіорозвідки, школа радіорозвідки та криптології і 4 секції, які мали літерні позначення: «*A*» – адміністративна, «*B*» – радіорозвідки та криптоаналізу, «*C*» – безпеки зв'язку та криптографії, «*D*» – тайнопису. З метою координації діяльності польових постів радіоперехоплення у складі «*SSB*» була сформована секція «*E*», а у грудні 1942 року – секція «*F*», основним призначенням якої стала організація робіт зі створення нової шифрувальної апаратури для Армії США.

Основними «постачальниками» матеріалів радіоперехоплення для криптоаналітиків Арлінгтон-Холлу були підрозділи 2-го батальйону радіорозвідки, який був створений 2 квітня 1942 року в результаті збільшення чисельності та зміни структури 2-ої роти. За участю особового складу батальйону у вересні того ж року був створений новий стаціонарний пост радіоперехоплення у Вінт-Хілл Фармс (штат Вірджинія),

а трохи пізніше - ще 2 пости, в штаті Каліфорнія і на Алясці. В період Другої світової війни чисельність батальйону істотно зросла та у свій час досягала приблизно 5 тисяч осіб.

До середини Другої світової війни підрозділи батальйону знаходилися на території США, Аляски, Алеутських і Гавайських островів, а також в Австралії, Індії та Африці. Пости радіоперехоплення та радіопеленгації, що знаходилися за кордоном, входили до складу військ зв'язку відповідних армійських командувань. Окремі підрозділи батальйону, наприклад пости, розташовані в Беллморі (острів Лонг-айленд) і Тарзані (штат Каліфорнія), використовувалися тільки для радіоконтроля за роботою армійських радіостанцій на території США і до ведення радіорозвідки не притягувалися.

У березні 1943 року «*SSB*» стала називатися Службою безпеки зв'язку «*SSS*» (англ. *Signal Security Service*). У липні того ж року після відповідного збільшення чисельності особового складу всі секції були перейменовані у відділи, а Служба перетворена в Агенцію безпеки зв'язку «*SSA*» (англ. *Signal Security Agency*) Армії США.

Криптоаналітичному успіху «*SSA*» в чималому ступені також сприяло широке застосування обчислювальної техніки – спочатку простих табуляторів, а згодом і обчислювальних машин типу «*RAM*» (англ. *Rapid Analytical Machine* - швидка аналітична машина), створених на основі електронно-вакуумних ламп і логічних схем. Така машина, завдяки її швидкодії, дозволяла заміняти ручну працю багатьох тисяч криптоаналітиків.

На початку війни криптослужба мала всього 13 найпростіших машин фірми «*IBM*», що обслуговувалися 21 оператором з відділу «А». Нестача фахівців з криптоаналізу на цей час складала близько тисячі осіб. Вихід з такого положення керівництво Служби бачило в більш широкому використанні засобів обчислювальної техніки при вирішенні завдань з дешифрування. Тому влітку 1944 року в складі «*SSA*» був створений новий підрозділ – відділ «G» (обчислювальної техніки), який до весни 1945 року нараховував уже 407 машин та 1275 операторів. Збільшилась також чисельність відділу «*B*» до 2574 осіб, 82 % з яких було зосереджено на дешифруванні повідомлень японської армії. Загальна чисельність Агенції на той час складала близько 10 тисяч осіб.

Протягом усієї війни найбільш чисельним серед підрозділів Агенції був відділ «*B*» (радіорозвідки і криптоаналізу). Розвіддані, підготовлені фахівцями відділу на підставі аналізу перехоплених відкритих та зашифрованих радіоповідомлень супротивника, направлялися до Управління військової розвідки для їхньої наступної оцінки та використання. Висока цінність даних, що доповідалися, була обумовлена тим, що за роки війни американським криптоаналітикам удалося розкрити багато кодів і шифрів супротивника: у 1942 році ними був розгаданий шифр ВМС Японії, а у 1943 - армійські японські шифри.

Важливим напрямом в діяльності відділів «*B*» і «*G*» вважалося також взаємодія з Урядовою школою коду і шифру Великобританії з дешифрування повідомлень німецьких військ, які використовували шифромашину «Енігма». «Злом» шифрованих повідомлень «Енігми» в перші роки війни проводився в Блетчлі-Парку та йшов достатньо важко. Але після того, як з 1942 року англійські криптоаналітики почали використовувати спеціалізовані швидкодіючі машині «Колос», процес дешифрування значно прискорився.

З появою у американських фахівців обчислювальних машин «*RAM*», що перевершували за своєю швидкодією англійську машину «Колос», між Арлінгтон-Холл і Блетчлі-Парк був установлений спеціальний канал зв'язку, яким з Великобританії передавалися перехоплені англійською радіорозвідкою шифровки «Енігми». Тільки за період з липня 1943-го по січень 1945-го в Арлінгтон-Холл надійшло 1357 німецьких шифровок, з яких 413 були успішно дешифровані.

В 1943 році було розпочате будівництво великого лампового комп'ютера – «*ENIAC*» (англ. *Electronic Numerical Integrator And Computer* - електронний числовий інтегратор і комп'ютер). Закінчений через три роки, «*ENIAC*» важив 30 тонн, складався з 18 тисяч електронних ламп, мав продуктивність п'ять тисяч операцій у секунду. Тільки зовсім недавно стало відомо про те, що успіх спецслужб США в операції «Венона» (англ. *Venona*) багато в чому був пов'язаний з використанням цього комп'ютера, який розроблявся спочатку для проведення розрахунків атомної бомби. Комп'ютер прожив дев'ять років і останній раз був включений у 1955 році.

У зв'язку з широким застосуванням усіма воюючими країнами засобів радіорозвідки важливим напрямком діяльності Арлінгтон-Холлу було забезпечення безпеки зв'язку частин і підрозділів американських сухопутних військ. Вирішення зазначеного завдання досягалося за рахунок розробки нових кодів і шифрів, створення нових зразків шифрувальної апаратури, проведення заходів щодо радіомаскування та контролю за дотриманням радіодисципліни операторами армійських радіостанцій.

Відділ «*C*» був другим за чисельністю серед підрозділів «*SSA*» і відповідав за своєчасне постачання у війська шифрапаратури, кодових книг і шифродокументів, розробку правил і інструкцій з безпеки зв'язку військ. Важливе місце в діяльності відділу займали організація радіоконтроля за дотриманням правил радіообміну у військах, а також оцінка практичної криптостійкості шифрів, що використовувалися підрозділами зв'язку Армії США. Фахівці відділу розробляли спеціальні інструкції, що виключали можливість утрати шифротехніки, а також ретельно аналізували всі випадки, пов'язані з утратою шифродокументів і апаратури.

Завершальний етап війни ознаменувався для «*SSA*» новими організаційними змінами. На початку 1944 року в результаті проведеної реорганізації в ньому були створені чотири відділи: розвідувальний, безпеки зв'язку, допоміжний, комплекту-

вання та підготовки особового складу. У грудні того ж року Агенції було передано в оперативне підпорядкування Управління військової розвідки, при цьому адміністративне керівництво Агенцією залишилося за Начальником військ зв'язку Армії США.

2.5. Перші шифрувальні машини

Першим розробником шифрувальних машин у США був Едвард Хеберн (1869-1952). Після того, як йому у 1906 році виповнилося 40 років, він виявив велику цікавість до криптології. З 1912 по 1915 рік Хеберн подав декілька патентних заявок на різні шифрувальні пристрої. Спочатку Хеберн створив шифросистему, до якої входили дві електричні друкарські машинки, з'єднані між собою 26 дротами.

Коли натискалася яка-небудь клавіша на одній машинці, це приводило до того, що на іншій друкувалася буква шифротекста. Оскільки дроти залишалися приєднаними до тих самих контактів упродовж усього періоду часу, протягом якого набирався відкритий текст, то шифрування здійснювалося методом простої одноалфавітної заміни. Незважаючи на явні недоліки цього методу шифрування, винахід Хеберна був дуже значимий тим, що перетворення відкритого тексту в криптограму здійснювалося за допомогою струмових імпульсів, що посилалися по електричних дротах.

У 1917 році Хеберн сконструював більш складний дисковий шифрувальний пристрій, у якому для перемішування алфавітів використовувалися шифрувальні роторні колеса (диски). Роторне колесо являло собою невеликий диск, зроблений з електроізоляційного матеріалу. На кожному боці цього диска розташовувалися по окружності на рівній відстані один від одного 26 електричних контактів, кожний з яких відповідав однієї з 26 букв латинського алфавіту. Кожний контакт на одному боці колеса був з'єднаний проводом (більш-менш випадково) з одним із контактів на іншому боці колеса.

Коли електричний імпульс надходив до контакту, що відповідав букві «А» на одному боці колеса та з'єднувався з контактом букви «М» на іншому його боці, це можна було розглядати як заміну букви «А» на букву «М». Для введення букв, як правило, використовувалася клавіатура звичайної друкарської машинки, а результат шифрування або відтворювався друкувальним пристроєм, або засвічувався на світловому табло, що містило 26 буквених символів.

Якщо після шифрування першої букви ротор провертався на один крок від своєї початкової позиції, то підсумковий результат простої заміни цілком мінявся, тому що на один крок зрушувалися й всі проводи в роторі (у першій машині Хеберна ротор при шифруванні кожної букви зрушувався на один крок). Оскільки кроків (позицій) було всього 26, то по мірі обертання колеса при шифруванні перших 26 букв тексту породжувалося 26 різних шифрувальних алфавітів.

Після того, як перші 26 букв були зашифровані, ротор знову повертався у початкове положення та послідовність алфавітів повторювалася. З криптографічної точки

зору, таке повторення було недоліком, тому що воно наставало після зашифровування занадто невеликої кількості букв вихідного тексту. Щоб ускладнити процес шифрування, стали з'єднувати в ряд кілька роторів.

Якщо, наприклад, використовували три ротори, то електричний імпульс проходив при шифруванні по черзі через кожний із них, і на кожен ротор припадало по 26 можливих позицій, трироторний пристрій був здатний створити 26x26x26=17576 різних шифрувальних алфавітів. Після того, як була зашифрована кожна буква вихідного тексту, можна було вибрати новий алфавіт шляхом пересування одного або більш наявних роторів так, щоб змінити переплетення проводів, через які проходив струм. Хеберн побудував машини з чотирма і п'ятьма роторами. Один з роторів вступав у роботу при шифруванні кожної букви. Цей ротор вважався «швидким» ротором.

Інший ротор вступав у роботу тільки один раз протягом кожного обороту «швидкого» ротора і називався «середнім» ротором. «Повільний» же ротор вступав у роботу один раз за період обертання «середнього» ротора. Таким чином, машина Хеберна могла породжувати величезну безліч шифрувальних алфавітів, причому для шифрування кожної нової букви вихідного тексту використовувався цілком новий алфавіт. Більш того, ротори в машині могли, при бажанні, вийматися та переставлятися у довільному порядку. Ще одною змінною величиною при шифруванні того чи іншого повідомлення цією машиною було початкове положення роторів.

На початку 1921 року Хеберн прибув до Вашингтона, зв'язався з представниками служби зв'язку американського ВМФ і продемонстрував їм власний винахід, одночасно направивши свою першу заявку на шифродиск у вашингтонське патентне бюро. «У нас довгий час безуспішно намагалися, – згадував пізніше тодішній начальник служби зв'язку ВМФ, – внести радикальні зміни в систему забезпечення таємності військових комунікацій. І ось з'явився пан Хеберн із Західного узбережжя та приніс нам свою машину. Ми були вражені, коли він продемонстрував те, що вона може робити, та відразу ж захотіли замовити кілька таких машин для нашого флоту».

У 1921 році Хеберн заснував фірму «Хеберн електрик код» (англ. *Hebern electric code* - електричний код Хеберна), що стала першим виробником дискових шифраторів у США. Одержавши необхідну підтримку від ВМС, а також думаючи (цілком справедливо), що його винахід є шифрувальним пристроєм майбутнього, він став активно продавати акції своєї фірми, щоб зібрати необхідний капітал. Оскільки «Хеберн електрик код» володіла десятками патентів по усьому світі (не тільки на дисковий шифратор, але й на багато інших передових для свого часу пристроїв, таких як електричні друкарські машинки та покажчики напрямку руху для автомашин), Хеберн без особливих зусиль продав акції своєї фірми на астрономічну у ті часи суму приблизно в 1 мільйон доларів.

Sept. 30, 1924 **1,510,441**

E. H. HEBERN

ELECTRIC CODE MACHINE

Filed March 21, 1921 11 Sheets-Sheet 1

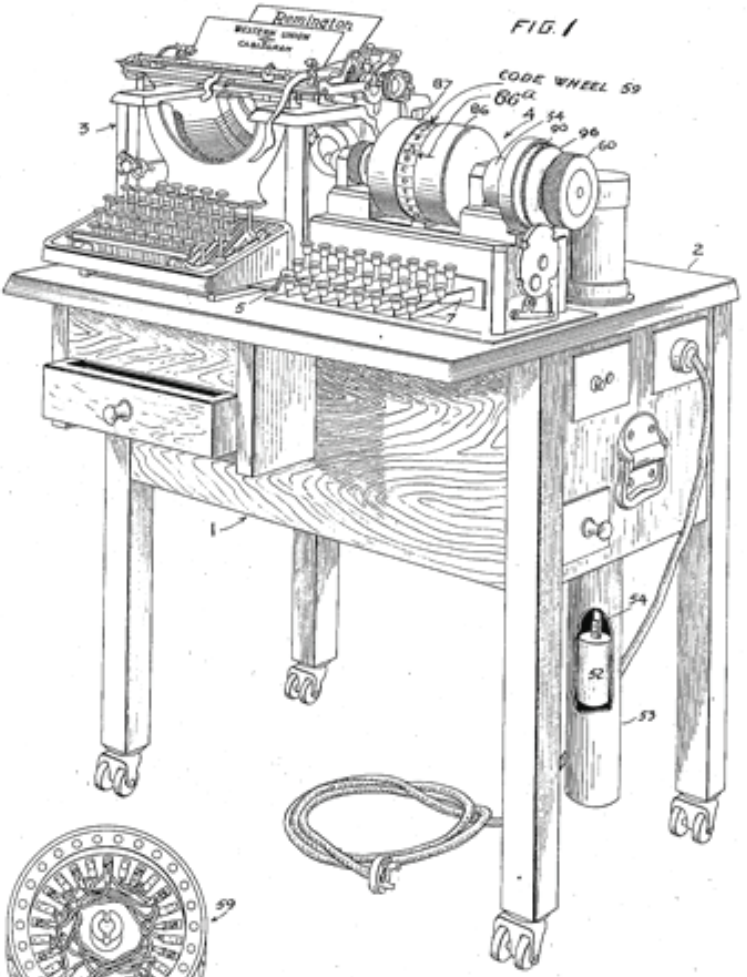


FIG. 2

INVENTOR
E.H. HEBERN

BY Francis M. Wright

У 1922 році на гроші, виручені від продажу акцій, Хеберн придбав механічні майстерні, щоб налагодити в них виробництво штампів, ливарних форм і шаблонів для дискових шифраторів. Виступаючи перед співробітниками своєї фірми, Хеберн заявив: «Ми дуже близькі до великого фінансового успіху завдяки нашим винаходам у сфері шифрувальних машин, і тому необхідно підготуватися до того, щоб зайнятися цим бізнесом на постійній основі». 21 вересня почалося будівництво триповерхового будинку. Відповідно до планів Хеберна, під дахом цього будинку повинні були згодом розміститися полірувальний, інструментальний та збірний цехи, а також ряд інших виробництв, необхідних для налагодження масового випуску дискових шифраторів.

До кінця 1922 року було нарешті закінчене будівництво грандіозного підприємства з виробництва дискових шифраторів. Його вартість перевалила за 380 тисяч доларів, що в півтора разу перевищило первісний кошторис. Спочатку керівництво американського ВМС із великою увагою поставилося до досягнень Хеберна, однак під час випробування стійкості запропонованого шифру криптологу Вільяму Фрідману вдалося «зламати» його.

У 1923 році була створена авторитетна комісія кваліфікованих експертів-криптологів ВМФ для розгляду дискового шифратора Хеберна. Після недовгих міркувань ця комісія одноголосно порекомендувала прийняти машину на озброєння, але тільки після її удосконалення.

Незважаючи на це, доходи «Хеберн електрик код» виявилися значно нижче витрат на будівництво, і навесні 1924 року фірма не змогла розрахуватися по своїх боргових зобов'язаннях. У ході реорганізації, що розпочалася, Хеберн був знятий з посади президента. 30 квітня відбулися збори розлючених акціонерів, що зажадали притягнути Хеберна до кримінальної відповідальності за те, що він торгував акціями своєї фірми по 3-5 доларів за штуку замість встановленої американським законом ціни в 1 долар.

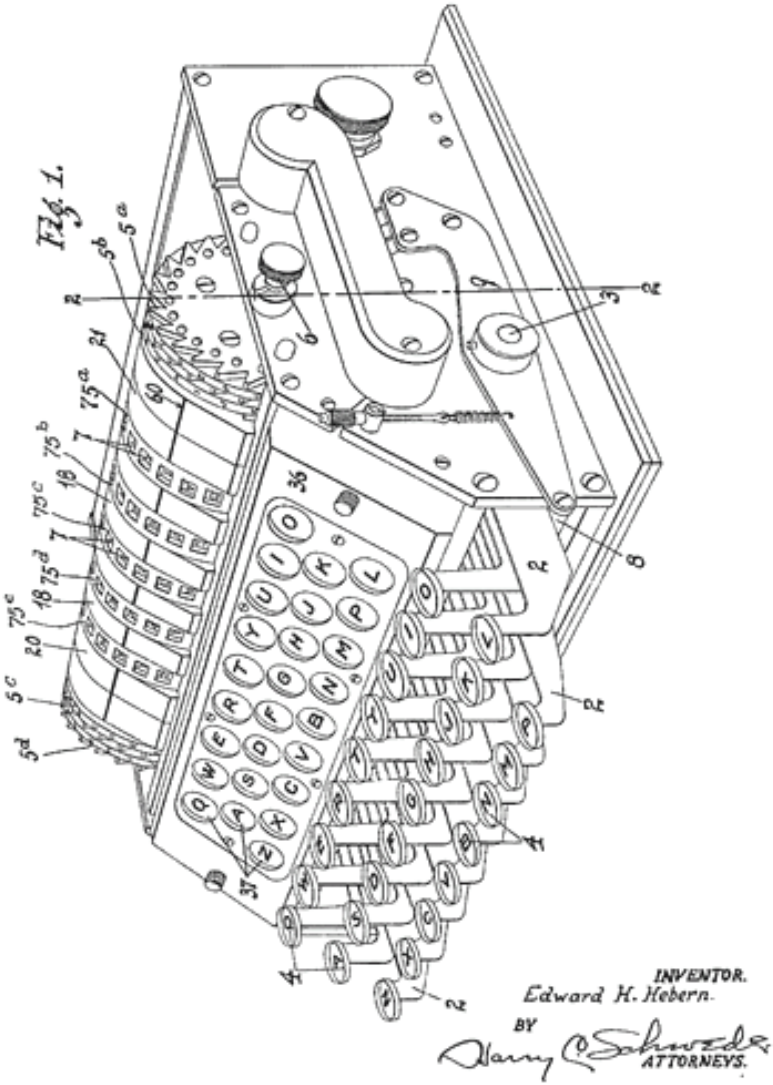
Почалося розслідування, що продовжувалося з 1924 по 1926 рік. За цей час ВМФ США замовив у «Хеберн електрик код» два дискові шифратори, заплативши за них по 600 доларів за кожен, а армія перерахувала Хеберну 1000 доларів ще за два шифратори. Велика судноплавна компанія «Пасифік стимшип» купила сім дискових шифраторів Хеберна за ціною 120 доларів за кожний (така різниця в ціні була пов'язана з різною кількістю шифродисків у машинах, виставлених на

Sept. 4, 1928. 1,683,072

E. H. HEBERN

ELECTRIC CODE MACHINE

Original Filed Nov. 20, 1923 4 Sheets-Sheet 1



продаж) для використання на пароплавах і у філіях цієї компанії. Нарешті, італійський уряд придбав ще один дисковий шифратор виробництва «Хеберн електрик код».

Тим часом тиск з боку власників акцій все зростав. Вони скаржилися на недостатні обсяги продажів, регулярно проводили мітинги протесту проти неправильної, на їхню думку, політики керівника фірми. Зрештою 1 березня 1926 року в суді вищої інстанції почалося слухання справи Хеберна за обвинуваченням у порушенні закону штату Каліфорнія про корпоративні цінні папери. Після чотириденного розгляду суд розпочав нараду. Повернувшись через 12 хвилин, судді визнали Хеберна винним. І хоча виконання вироку було відкладено, усі ці події звели до нуля всякі шанси залучити до «Хеберн електрик код» додатковий капітал, щоб розрахуватися з боргами та продовжити виробництво дискових шифраторів. В результаті через три місяці фірма збанкрутувала.

Але Хеберн не бажав сидіти склавши руки. Пов'язуючи свої надії з ВМФ, він заснував у штаті Невада нову фірму за назвою «Інтернешнл код машин» (англ. *International Code Machine* - Міжнародна кодова машина). У 1928 році її справи пішли на лад, коли їй вдалося продати американському ВМФ 4 електричні шифрувальні машини, які мали назву «*Electric Cipher Machine Mark I*» (*ECM Mark I*), по 750 доларів за штуку та одержати ще по 20 доларів за кожен шифродиск до них. «*ECM Mark I*» мала 5 роторів (дисків з електричними проводами), кожен з яких управлявся цевочним колесом з 25 штифтами. З їх допомогою встановлювався або активний, або пасивний режим, тобто ротори або поверталися, або ні. Використовувалася також додаткова штепсельна, або комутаційна, панель для передачі управління від одного ротора до іншого.

Хеберн із декількома своїми співробітниками зумів виготовити ці машини практично вручну та потім особисто доставив їх у штаб 12-го військово-морського округу в Сан-Франциско. Одна машина залишилася там, а інші були розіслані у Військово-морське міністерство та головнокомандувачу флотом США. У ВМФ, у першу чергу, хотіли на практиці переконатися в їхній механічній надійності, а не в криптографічній стійкості, що тоді вважалася цілком задовільною.

З 1929 по 1930 рік ці машини забезпечували секретність значної частини офіційного листування вищого командування американського ВМФ. Справи Хеберна пішли ще краще: через рік ВМФ купив у нього 31 дисковий шифратор на загальну суму 54480 доларів для повсякденного використання в якості шифросистеми командування вищої ланки.

Однак, коли в 1934 році Хеберн запропонував ВМФ придбати новий, удосконалений варіант своєї шифрувальної машини, у відповідь він несподівано одержав дуже різкий лист із категоричною відмовою. Оскільки інших замовників у Хеберна практично не було, ця відмова змусила Хеберна припинити діяльність з виробництва

шифрувальної техніки. І хоча куплені в Хеберна дискові шифратори не були зняті з експлуатації після розриву відносин з ним, незабаром у результаті інтенсивної роботи вони остаточно зносилися та у 1936 році були замінені на нові, зроблені вже іншою американською фірмою. Цікаво відзначити, що ці машини були потім відремонтовані та встановлені на берегових станціях, де продовжували використовуватися аж до 1942 року. А дві з них, навіть, були захоплені японцями як військові трофеї.

Переконаний, що Збройні сили скористалися його основними ідеями, не сплативши йому за це відповідну компенсацію, у 1947 році Хеберн пред'явив усім трьом видам Збройних сил США позов на загальну суму в 50 мільйонів доларів. Так і не дочекавшись закінчення бюрократичної тяганини, 10 лютого 1952 року Хеберн помер. На початку 1953 року Армія, ВМФ і ВПС США відкинули позов Хеберна. Через кілька місяців його спадкоємці знову пред'явили американському уряду позов на суму в 50 мільйонів доларів.

Використавши дрібні юридичні зачіпки, позовний суд США обмежив час відшкодування збитку періодом з 1947 по 1953 роки, а порушення прав позивача було зведено до дуже вузького питання про незаконне використання одного спеціального пристрою для керування рухом шифродисків. Було проігнороване основне питання, що стосувалося того, чи дійсно Збройні сили США запозичили в Хеберна основні принципи роботи дискового шифратора та потім використали ці принципи в сотнях тисяч стійких шифрувальних машин під час Другої світової війни без справедливої компенсації автору, що їх винайшов.

Спираючись на букву закону, американський уряд з усіх сил прагнув не заплатити Хеберну та його спадкоємцям ні цента. У 1958 році він зрештою погодився віддати їм якісь жалюгідні 30 тисяч доларів, проте аж ніяк не з почуття справедливості, а оскільки побоювався, що відстоюючи свої права в суді, йому доведеться розкрити деякі секрети.

Оскільки аналіз принципів кодування роторних шифромашин Хеберна, здійснений Уілямом Фрідменом, привів до швидкого виходу цих машин із застосування в США, криптослужбам потрібно було знайти більш надійні шифромашини. З цією метою наприкінці 1930-х років армійська криптослужба «*SIS*» придбала і випробувала доставлені з Європи 50 комерційних зразків малогабаритної шифромашини шведа Бориса Хагеліна «*C-36*». У 1942 році, коли Хагелін прибув у США, була створена компанія, що випускала до 400 модернізованих шведських шифромашин «*C-38*» на день, які одержали в Армії назву «*Converter M-209*», а у ВМФ - «*CSP-1500*». Всього було випущено більше 140 тисяч таких шифромашин.

«*M-209*» використовувалася у військових підрозділах від дивізії до батальйону, оскільки забезпечувала лише середній рівень криптостійкості. Досить широко вона використовувалися також під час війни у Кореї 1950–1953 років. Крім того, після закінчення Другої світової війни безліч країн у різних регіонах світу закупили та три-

валий час використовували на своїх лініях зв'язку значну кількість шифраторів типу «*С-36/38*» і їхніх модифікацій.

Розглянемо докладніше конструкцію «*М-209*». Шифратор реалізовував шифр модульного гамування (модуль шифрування 26). Його пристрій і схема функціонування повторювали принципи, закладені в шифраторі «*С-35*», але мали декілька особливостей. Також, як і «*С-35*», шифромашина «*М-209*» складалася з трьох основних частин: набірно-друкуючого блоку, блоку ключових коліс і барабана з комбінаційними лінійками.

Набірно-друкуючий блок був призначений для встановлення (набору) букв відкритого тексту на індикаторному диску та друкування відповідних букв шифротекста на паперовій стрічці. Букви відкритого тексту набиралися навпроти спеціально нанесеної риски, інша риска дозволяла вважати букву шифротекста з відтворюючого диска. Кінематично набірно-друкований блок був розташований цілком на окремій вісі, пов'язаної шляхом шестірневої передачі з барабаном, що ніс комбінаційні лінійки. Нумерації букв на індикаторному та відтворюючому дисках були взаємнозворотними, що дозволяло реалізувати шифр Бофора.

Шифромашина приводилася в дію мускульною силою людини шляхом провертання спеціально призначеної для цього рукоятки на один оберт. Рукоятка знаходилася на одній вісі з барабаном (забезпеченим розташованими на ньому запрограмованими рухомими комбінаційними лінійками), що при шифруванні однієї

букви робив повний оберт. Під час обертання барабана спеціальний зуб приводив до обертання блоку ключових коліс на одну позицію.

Блок ключових коліс складався з 6 коліс з такими періодами обертання:

- 26 символів з кутовими положеннями, що відповідали буквам латинського алфавіту від *A* до *Z*;
- 25 символів - від *A* до *Z*, за винятком *W*;
- 23 символу - від *A* до *X*, за винятком *W*;
- 21 символ - від *A* до *U*;
- 19 символів - від *A* до *S*;
- 17 символів - від *A* до *Q*.

Так само, як і в попередніх моделях, на кожному колесі розташовувалися штифти. Але, на відміну від «*C-35*» і «*C-36*», висунутий вправо штифт був «робочим», а вліво – «неробочим».

Барабан з лінійками складався з 27 лінійок із двома рейторами на кожній лінійці. Аналогічно шифромашині «*C-38*», рейтори були рухомими та могли бути або «робочими», або «неробочими». Функціонування американської шифромашини «*M-209*» повторювало логіку роботи шведської «*C-35*». Повідомлення, що шифрувалися за допомогою «*M-209*», роздруковувалися на паперовій стрічці у вигляді п'ятизначних груп. Потім вони передавалися по радіо та розшифровувалися на прийомному кінці за допомогою іншої такої ж машини.

У червні 1935 року керівник «*SIS*» Уільям Фрідмен і криптолог Френк Роулет розробили концепцію каскадного з'єднання груп роторів. Обертання одного ротора після зашифровування чергового символу, робило вплив на рух решти роторів. Інші ротори були заздалегідь встановлені так, щоб характер їх обертання, після того, як перший ротор з групи повертався, був переривистим. Таким чином, в результаті попередньої дії електричного струму та регулярних/преривістих рухів створювалася серія варіацій замін букв в остаточному шифротексті.

Тим часом криптослужба ВМФ «*Op-20-G*» також займалася пошуком шифромашини, в якій використовувався б дротовий шифрувальний ротор Хеберна, але яка була би більше пристосована до суворої погоди, бойових умов і інших несприятливих чинників. Тому у жовтні 1935 року Фрідмен передав подробиці каскадного процесу криптологу ВМФ лейтенанту Джозефу Венджеру. Без відома Фрідмена і Роулета Венджер і керівник «*Op-20-G*» Лоуренс Сеффорд приступили до обговорення, чи зможе ВМФ виготовити багатороторний пристрій. До кінця 1930-х років, після консультації з компанією «*Teletype Corporation*», електрична шифрувальна машина «*ECM Mark II*» стала реальністю.

Машина мала 15 роторів, розміщених трьома групами: 5 шифруючих роторів (у задньому ряду), 5 управляючих (у середньому ряду) і 5 індексних (у передньому ряду). Набрані на клавіатурі букви відкритого тексту перетворювалися на імпульси

електричного струму. Імпульси поступали на управляючу групу (середню), а потім через ряд контактних точок на індексну (передню). Ці 2 групи роторів управляли обертанням шифруючих роторів у задньому ряду. 5 шифруючих і 5 центральних роторів були більші за розміром і мали по 26 електричних контактів на кожному боці, причому кожен контакт представляв букву алфавіту. 5 індексних роторів були менші і мали на кожному боці всього по 10 контактів.

Три з п'яти управляючих шифрувальних роторів, що знаходилися у центрі (№ 2, 3 і 4), рухалися із заданою швидкістю. Управляючий ротор № 3 називався швидким ротором; при введенні з клавіатури якої-небудь букви він повертався на один крок вперед. Ротор під номером 4 називався середнім, і він переміщався на одну позицію вперед лише після того, як ротор 3 робив повне обертання. Управляючий ротор № 2 був найповільнішим і повертався на один крок вперед, тільки коли повне обертання робив ротор № 4 (26 оборотів для 26 контактних точок). Управляючі ротори № 1 і № 5 не рухалися. Передні 5 індексних роторів встановлювалися тільки в отворах індексної групи в заздалегідь обумовленому порядку один раз на день (наприклад, 4, 1, 5, 2, 3).

Для передачі імпульсів струму від клавіатури могли бути записані тільки 4 контакти на першому управляючому роторі. Контакт між останнім дротовим ротором з управляючої групи та першим індексним ротором здійснювався за допомогою 9 груп з'єднань, причому кожна група включала від 1 до 6 проводів. У деяких модифікаціях один з контактів індексного ротора не використовувався. 10 вихідних контактів останнього індексного ротора приєднувалися попарно до 5 електромагнітів, які записувалися для приведення в дію шифруючих роторів, і від 1 до 4 шифрувальних роторів рухалися при наборі на клавіатурі кожної букви.

В інструкції з експлуатації «*ECM*», озаглавленої «*SIGQZF*», а також її виправлених і перероблених редакціях під номерами 2 і 3, для «*Mark II*» були вказані списки ключів і розташувань роторів для дешифрування. Шифрувальник і дешифрувальник повинні були враховувати, що один раз в день індексні ротори встановлювалися в новому положенні (змінювався порядок роторів) - так відбувалося впродовж всієї Другої світової війни. Адресат також отримував щоденний секретний список ключів, що містив порядок розташування (обертання) індексних роторів. Їх розміщення мінялося залежно від можливих змін ступеню криптостійкості конкретних повідомлень, які могли мати гриф «таємно», «конфіденційно» або «для обмеженого користування». Для особливо секретних донесень потрібно було змінити індексні ротори.

Під час Другої світової війни управляючі та шифруючі ротори також переставлялися щодня. Їх порядок задавався секретним списком ключів, проте обидва ці види роторів завжди змінювалися з кожним отриманим повідомленням. Для розшифрування повідомлення адресату була потрібна вся необхідна інформація. Від «*ECM Mark II*», яка отримала також кодову назву «*CSP-888/889*», ВМФ відмовився лише у 1959 році, оскільки вона вже не могла задовольняти потребам сучасного зв'язку.

У лютому 1940 року флотська криптослужба «*Op-20-G*» передала технічний опис шифромашини «*ECM Mark II*» армійській криптослужбі «*SIS*». В результаті сухопутні війська США прийняли її на озброєння як шифромашину «*M-134C*», або «*SIGABA*». Букви «*SIG*» означали «війська зв'язку», а «*ABA*» відповідали позначенню одного з видів зашифровиванія. Під час Другої світової війни «*SIGABA*» стала для армії США основною системою захисту повідомлень. Був навіть розроблений спеціальний сейф, що мав кодове позначення «*CH-76*», куди машину поміщали в тривалих поїздках, і особливий дерев'яний ящик для перевезення її на короткі відстані.

До моменту вступу Сполучених Штатів у війну з Японією «*SIGABA/ECM*» була встановлена в штабах всіх основних частин і з'єднань Армії і ВМФ. Використовувалася вона також на лінії урядового зв'язку під умовним найменуванням «*POTUS-PRIMER*» (англ. *President of the United States - Prime Minister*) для забезпечення шифрованим зв'язком Президента США з Прем'єр-Міністром Великобританії.

Модифікація машини, названа «*M-134A*» (*SIGMYK*), забезпечувала безпеку з використанням одноразової стрічки, схожої на ту, що була придумана для телетайпів Гілбертом Вернамом. Така стрічка з комбінаціями міток і пропусків (наприклад, «є контакт», «немає контакту») допомагала управляти роторами. Союзники, щоб поліпшити зв'язок між собою під час війни, розробили та виготовили адаптери для забезпечення сумісності між «*SIGABA*» і британськими пристроями, зокрема «*Typex*». Один з таких адаптерів, розроблений ВМФ і отримавший назву «*CSP-1600*», сприяв створенню гібридного пристрою з 5 роторами, який почав позначатися як «*CSP-1700*».

На подальших етапах війни «*SIGABA/ECM*» була вдосконалена і мала вже 15 роторів, 5 з яких дозволяли змінювати положення інших шифруючих 10 роторів. «*SIGABA/ECM*» знаходилась в експлуатації до 1950-х років, залишаючись при цьому власністю США, хоча інші машини передавалися союзникам по різних військових блоках, зокрема НАТО.

Разом з шифромашиною «*SIGABA/ECM*» фахівцями «*SIS*» була розроблена і досконаліша модель «*M-228*» (*SIGCUM*), яка почала поступати у війська, починаючи з 1943 року. Машина являла собою літеродрукувальний апарат, що забезпе-

чував шифрування тексту, який набирався на клавіатурі, з одночасною передачею його в лінію зв'язку. Застосування нового принципу дії дозволило істотно підвищити швидкість передачі та прийому шифрованих повідомлень, що було досить важливо в зв'язку зі значним ростом потоків інформації в період проведення великих військових операцій.

Так, у середині 1943 року при проведенні військами союзників десантної операції з захоплення острова Сицилія обсяг шифрованого листування штабу 5-ої армії США досягав 23 тисяч кодових груп на добу, а у період Південно-італійської операції – до 40 тисяч груп. Завдяки наявності шифромашин «*SIGCUM*» штабу армії вдавалося вчасно одержувати необхідну інформацію від підлеглих частин, а також передавати їм необхідні розпорядження, дотримуючи при цьому вимоги з прихованого керування військами.

Поряд із своїми достоїнствами технічна конструкція машини мала й істотний недолік – при неуважності оператора виникали передумови до порушення безпеки зв'язку. Особливість «*SIGCUM*» полягала в тому, що вона дозволяла здійснювати передачу тексту як у відкритому, так і зашифрованому вигляді, для чого оператор повинний був перед початком роботи установити перемикач режиму у відповідне положення. За роки Другої світової війни мали місце принаймні два випадки, коли через неуважність операторів «*SIGCUM*», які забули перевести перемикач у необхідне положення, в ефір були передані секретні повідомлення в незашифрованому вигляді.

2.6. Криптослужба Фрідмена

Ще одним талановитим американським криптоаналітиком був Уільям Фрідмен (1891-1969). Він народився в Кишиневі (Молдова), а у 1892 році його родина емігрувала до США. 1 червня 1915 року Фрідмен почав працювати в приватній криптоаналітичній лабораторії, яка належала багатому торговцю Джорджу Фабіану та знаходилася у його маєтку Рівербенк біля міста Женева в штаті Іллінойс.

Ця лабораторія була потрібна Фабіану для того, щоб довести, що не Уільям Шекспір, а Френсіс Бекон написав всесвітньо відомі п'єси, тому шукав в них криптограми, які б засвідчили авторство Бекона. Так Фрідмен уперше довідався про «дешифрування» п'єс Шекспіра, яке повинно були довести те, що їх написав Бекон. Це розбудило у Фрідмена жвавий інтерес. Потроху він почав займатися криптоаналізом, усемогутні чари якого, подібно дурману, поступово заволоділи його розумом. «Коли справа доходила до криптоаналізу, - згадував Фрідмен через багато років, – щось у мені пробуджувалося».

Жагуче захоплення криптоаналізом не пройшло непоміченим для Фабіана, і незабаром він довірив Фрідмену керівництво криптоаналітичною лабораторією. Пристрасть до криптоаналізу підсилювалася ще тим, що йому подобалася одна зі своїх підлеглих – дотепна і весела міс Елізабет Сміт (1892-1980). У травні 1917 року вони одружилися, ставши найзнаменитішою подружньою парою в історії криптоаналізу.

Коли Сполучені Штати оголосили війну Німеччині, у Рівербенку фактично почала працювати національна криптослужба, а молодята Уільям і Елізабет Фрідмени стали розкривати шифри Німеччини і Мексики для армії США, а також допомагати Скотланд Ярду у виявленні антибританських агентів у Північній Америці.

Рівербенк почав неофіційно одержувати криптограми для дешифрування від різних урядових закладів. Найважливішою з них була шифрована кореспонденція групи змовників-індусів, які не без допомоги німців спробували скористатися сприятливою ситуацією, коли Англія була поглинена війною в Європі, щоб домогтися незалежності для Індії. Перехоплені шифротелеграми індусів передавалися для дешифрування Фрідмену, який швидко «розкрив» застосований ними шифр.

В результаті індуси були засуджені за спробу закупити в Сполучених Штатах зброю для організації повстання проти Англії. У ході масових процесів у Чикаго та Сан-Франциско Фрідмен виступив з показаннями, які по суті виглядали як викриття змовників з їх же власних вуст. На процесі в Сан-Франциско відбулася одна з найдраматичніших сцен, що коли-небудь, розігрувалися в американських судах: один з підсудних індусів встав і двома пострілами з револьвера убив наповал співвітчизника, який свідчив проти своїх соратників, а потім був убитий поліцейським, що вистрілив поверх голів людей з публіки. Суд визнав більшість обвинувачуваних винними.

Через декілька місяців після прочитання шифрованого листування індусів англійці направили в Рівербенк п'ять коротких криптограм. Вони були зашифровані за допомогою шифрувального пристрою, сконструйованого співробітником криптоаналітичного бюро Військового міністерства Англії Дж.Плеттсом. Англійці настільки високо цінували й оберігали цю машину, що один з аргументів, які висувалися проти її несанкціонованого використання, полягав у тому, що якби німцям удалося захопити хоч один її примірник і використовувати у своїх цілях, то союзники більше не змогли б читати шифроповідомлення супротивника!

Однак Фрідмен моментально розкрив ключ «*CIPHER*» до однієї з надісланих через океан криптограм. Але він ніяк не міг одержати інший ключ і, зайшовши в тупик, скористався своїм досвідом у сфері «психологічного криптоаналізу». Уільям звернувся до своєї дружини та попросив її «звільнитися» від усяких думок. «Тепер, – продовжував він, – я хочу, щоб ти вимовила перше випадкове слово, що прийде тобі на розум, коли я назву тобі інше слово». Фрідмен витримав паузу. «Шифр», – сказав він. «Машина», – відповіла вона.

Слово «*MACHINE*» виявилося другим ключем. Через три години після того як Фрідмен одержав криптограми для криптоаналізу, їхні відкриті тексти були телеграфовані назад у Лондон. Перший з них містив досить утішну для гордого англійського винахідника фразу: «Цей шифр є таким, що абсолютно не розкривається». Після такого конфузу більше до розгляду питання про використання шифропристрою Плетса союзники американців не поверталися.

Крім криптоаналітичної роботи Фрідмен займався викладацькою діяльністю з групою, підібраною з армійських офіцерів, що були прислані восени 1917 року в Рівербенк для вивчення криптоаналізу. Коли американська армія створила, нарешті, власне шифробюро, перші 84 співробітники якого пройшли курс навчання у Фрідменів у Рівербенку.

Для викладання на цих курсах Фрідмен підготував серію монографій. Відомі як «Рівербенкські публікації», вони з'явилися поворотним пунктом в історії криптоаналізу. В цих публікаціях був запропонований метод визначення періоду гами (довжини гасла) у шифрі Віженера, а також безключовий метод дешифрування при використанні нерівноймовірної гами. Майже в усіх з них викладався новий матеріал, оволодіння яким дотепер вважається необхідною умовою одержання вищої криптоаналітичної освіти.

Незабаром повний комплект «Рівербенкських публікацій» перетворився в необхідний атрибут колекції робіт із криптоаналізу, а тому що було надруковано усього лише 400 примірників, вони стали незабаром бібліографічною рідкістю. Найвідомішою серед «Рівербенкських публікацій» стала написана в 1920 році брошура за назвою «Індекс збігу та його застосування в криптоаналізі». У ній описувався процес розкриття двох складних шифрів. Однак Фрідмен менш за все був зацікавлений у

доказі вразливості цих шифрів і використовував їх, в основному, для розробки нових криптоаналітичних методів.

Таких методів Фрідмен створив два. Перший з них дозволив відновлювати шифроалфавіт, не будуючи ніяких здогадів у відношенні хоча б єдиної букви відкритого тексту. Інший метод зробив дійсну революцію в криптоаналізі. Фрідмен підійшов до тексту на будь-якій мові не просто як до сукупності окремих символів, що випадково стоять у визначеному порядку, а як до єдиного цілого – кривої, крапки якої пов'язані визначеною закономірністю. До цієї кривої він застосував статистичні концепції. Отримані Фрідменом результати можна охарактеризувати як прометеївські. Його геніальна ідея дала поштовх до використання численних статистичних інструментів, що є вкрай необхідними в сучасному криптоаналізі.

До Фрідмена криптоаналіз існував як чиста наука, яка нічого не запозичала з інших галузей знання та нічим їх не збагачувала. Підрахунки частоти зустрічальності букв, використання мовних характеристик, специфічні методи розкриття шифрів – усе це було характерним винятково для криптоаналізу. Фрідмен же вивів криптоаналіз із цього стану самотнього існування та поєднав його зі статистикою. Коли Фрідмен відніс криптоаналіз до категорії статистичних досліджень, він тим самим широко розгорнув двері в багатий арсенал засобів, якими криптоаналіз ніколи не користувався. Ці засоби ідеально підходили для вивчення статистичного поводження букв і слів. Криптоаналітики з вдячністю сприйняли нововведення Фрідмена і з тих пір з успіхом застосовують їх на практиці.

Найважливішим внеском Фрідмена в даній сфері варто вважати введення терміну «криптоаналіз» (англ. *cryptanalysis*), який він уперше використовував у 1920 році, щоб усунути постійне джерело плутанини в криптології – двозначність дієслова «розшифрувати», що означало тоді будь-яке перетворення криптограми у відкритий текст. А пізніше, у 1935 році він перший увів у споживання термін «криптологія» (англ. *cryptology*).

Наприкінці 1920 року Фрідмен і його дружина залишили Рівербенк. 1 січня 1921 року він уклав 6-місячний контракт з військами зв'язку на розробку шифросистем у Секції коду і шифру «*CCS*». Там Фрідмен застосував свої методи в роботі з шифрувальними машинами, що відразу ж висунуло Америку в перші ряди світової криптології. Коли цей контракт минув, він був призначений головним криптоаналітиком «*CCS*».

Одним із перших службових завдань Фрідмена стала викладацька діяльність у школі військ зв'язку. Для цього він написав підручник, у якому ліквідував плутанину, що панувала в криптологічній термінології. Крім викладацької діяльності в різних військових школах країни, Фрідмен в ці роки опублікував ряд дослідницьких робіт, методичних і навчальних підручників. Особливо значним став випущений ним

у 1923 році підручник «Елементи криптоаналізу», який став базою нової наукової дисципліни.

Досить значний внесок зробила в американську криптографію і дружина Уільяма Фрідмена. У той час як її чоловік працював на Збройні сили США, Елізабет Фрідмен займалася вирішенням досить схожих задач для міністерства фінансів, де в роки «сухого закону» розкривала коди бутлегерів. Коли ж це міністерство вирішило створити власну криптослужбу, місіс Фрідмен очолила її, залишаючись на даній посаді протягом 18 років. Після цього обдарована жінка створювала систему шифрозв'язку для Міжнародного валютного фонду, а також для спецслужби «*OSS*», з якої згодом утворилося Центральне розвідувальне управління.

Тим часом сфери діяльності Фрідмена постійно розширювалися. У 1924 році він виступив у комісії Конгресу з приводу прочитання деяких шифрованих повідомлень, пов'язаних із кримінальною справою щодо махінації з нафтоносними ділянками. А у 1927 році він написав статтю про коди і шифри для «Британської енциклопедії».

Коли у 1930 році Фрідмен став керівником розвідувальної служби зв'язку «*SIS*», він організував інтенсивну програму навчання криптології для цивільних службовців і залучив до роботи трьох молодих криптоаналітиків, кожному з яких було не набагато більше 20 років. Це були вчителі математики Френк Роулет (1908-1998), Абрахам Сінков (1907-1998) і Соломон Кульбек (1907-1994). Вони пройшли підготовку в тренувальних таборах у Форт-Мід, після чого отримали звання офіцерів запасу.

Після завершення навчання їм була доручена робота з розробкиі збірок шифрів для Армії США, а також тестування апаратури комерційного шифрування, яку виготівники пропонували уряду США. Так був покладений початок створенню солідної криптологічної організації, що існує в США й понині. Незважаючи на свою нечисленність, у 1930-х роках їй вдалося виконати великий обсяг робіт у сфері вдосконалення армійських кодів і шифрів, підготовки фахівців і створення нової апаратури шифрування та радіорозвідки.

Поступово, незважаючи на депресію та ізоляціонізм, група Фрідмена розширювалася та «ставала на ноги». У 1935 році вона «розкрила» дипломатичний код японської машини «*91-shiki O-bun In-ji-ki*», не маючи навіть перехоплених зашифрованих цим кодом повідомлень. Назва означала «алфавітна друкарська машинка 91». Число 91 було скороченим найменуванням 2591 року за японським календарем, що відповідав 1931 року. Вона також мала й іншу назву - шифромашина типу «*A*» (англ. *Type A Cipher Machine*), яку американські криптоаналітики назвали «червоною» (англ. *red*).

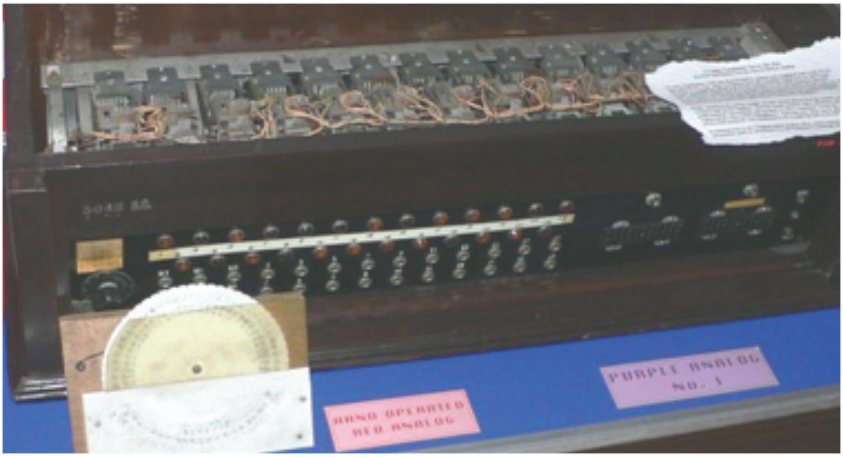
Цей успіх посприяв зростанню авторитету «*SIS*»,

а також збільшенню її фінансування урядом США та зростанню чисельності персоналу. У 1938 році японці почали використовувати для передачі дипломатичної кореспонденції шифромашину «*97-shiki O-bun In-ji-ki*» - «алфавітну друкарську машинку 97», тобто випуску 1937 року. Вона також мала й іншу назву - шифромашина типу «*B*» (англ. *Type B Cipher Machine*), яку американські криптоаналітики назвали «пурпурною» (англ. *purple*). Японці зазвичай посилалися на неї як на «машину» або «*J*». Ці назви були дані їй японським флотом, який адаптував німецьку шифромашину «Енігма» до своїх умов і потім позичив її МЗС, а той, у свою чергу, видозмінив її стосовно до своїх умов.

Повною мірою геній Фрідмена проявився в роботі з розкриття «пурпурної» машини. Він згадував, що «коли вперше з'явилася «пурпурна» машина, вона стала такою складною проблемою», що наш начальник зв'язку попросив нас усіх направити на її рішення всі зусилля. Після того як мої підлеглі не змогли домогтися значних успіхів, Моборн попросив мене особисто зайнятися цією справою. У той час я в основному здійснював адміністративні функцій, але на його прохання я залишив усе, що тільки було можна, і почав працювати разом із групою».

Прокладаючи дорогу за допомогою особисто розроблених методів, Фрідмен вів своїх криптоаналітиків крізь лабіринти «пурпурної» машини. Він організовував команди для дослідження різних припущень. Деякі виявлялися неплідними, та їхнім єдиним результатом ставало переконання, що таким шляхом йти не слід. Фрідмен і його колеги почали виділяти шифровані букви в цикли, що відповідали ротації дисків, – спочатку дуже повільно, а потім у міру нагромадження інформації усе швидше і швидше.

В роботі Фрідмена вирізняла постійна діяльність розуму, зайнятого цією складною головоломкою, постійні міркування над темою, навіть під час їди, хронічне



безсоння, твердий натиск на усіх, з ким працював, тому що він розумів значення своєї роботи для держави. Коли задача здавалася майже нерозв'язною, нелюдська робота розуму, величезне нервове напруження та пережиті розчарування, а також терміновість і таємність роботи безупинно тиснули на його мозок.

Прорив відбувся, коли криптологи спробували використати крокові шукачі, що застосовувалися в телефонії. За щасливим збігом вони працювали, ґрунтуючись на тому ж принципі, що й перемикачі «пурпурної» машини. Це відбулося в серпні 1940 року, коли Уільяму Фрідмену було 48 років. Наприкінці 1940 року криптослужба військово-морської контррозвідки змогла створити свій варіант «пурпурної» машини. Після цього криптоаналітики розкрили пристрої японських шифрувальних машин «*Jade*» і «*Coral*».

Незважаючи на завантаженість криптоаналітичною роботою, Фрідмен у 1936 році створив шифромашину «*M-325*» (*SIGFOY*), що було відповіддю німцям на машину «Енігма». Патент на машину був поданий 14 серпня 1944 року, але виданий тільки 17 березня 1959 року. Машина містила три проміжних та один відновлюючий диски. У період з 1944 по 1946 роки машин «*M-325*» було виготовлено 1100 штук. Однак через проблеми, пов'язані з їх недосконалістю, що призводили до шифрувальних помилок, виготовлення та використання «*M-325*» було припинено у 1946 році.

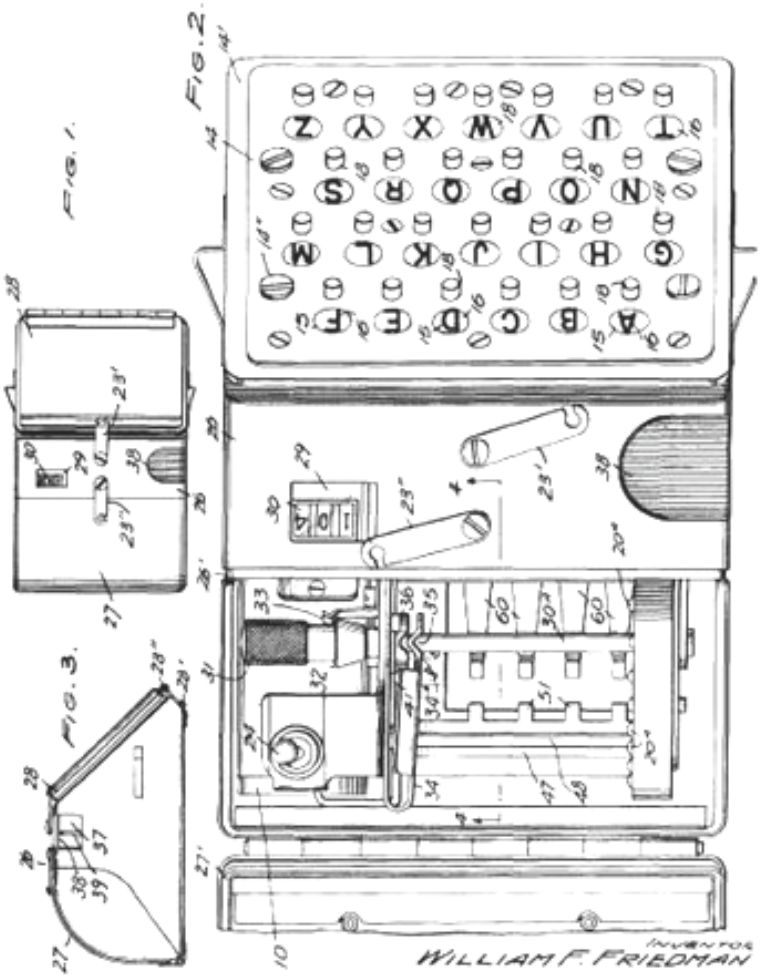
Разом з тим, геніальний криптоаналітик Фрідмен не витримав навантаження, пов'язаного з розкриттям японських шифрів, і 4 січня 1941 року був поміщений у госпіталь Уолтера Ріда у зв'язку з нервовим розладом. Виписався Фрідмен тільки 24 березня та був змушений піти у відставку за інвалідністю, але йому було дозволено залишитися у службі радіорозвідки у якості цивільної особи.

Крім того, згідно спільної угоди союзницькмх спецслужб члени групи Фрідмена брали участь у роботі з британськими криптоаналітиками та працювали у Школі коду й шифру у Блетчлі-Парку. Так, у січні-квітні 1941 капітан Сінков знаходився у складі делегації американських спецслужб у Великобританії для обміну інформацією щодо програми дешифрування кодів супротивників. А у травні 1942 року у відрядженні у Великобританії знаходився майор Кульбек. Незабаром

March 17, 1959 W. F. FRIEDMAN 2,877,565

ELECTRICAL CRYPTOGRAPH

Filed Aug. 11, 1944 4 Sheets-Sheet 1



INVENTOR
WILLIAM F. FRIEDMAN
BY William F. Friedman
ATTORNEY

після повернення до США він очолив японський напрям у службі дешифрування.

У 1944 році Фрідмен отримав Нагороду за виняткову цивільну службу (англ. *Commendation for Exceptional Civilian Service*). У 1946 році він був нагороджений президентською Медаллю за заслуги (англ. *Medal for Merit*), однією з вищих цивільних нагород США.

У 1947 році Фрідмен став директором комунікаційних досліджень Армійської агенції безпеки «*ASA*» (англ. *Army Security Agency*) та подав прохання про зняття грифа секретності з однією з винайдених ним, але не запатентованих шифрувальних машин. Комерційне використання таких машин могло швидко перетворити його на спроможну людину. Після того, як йому було відмовлено в проханні, Фрідмен подав до суду на федеральний уряд.

Зимою 1949-1950 року він був знову госпіталізований з повторним загостренням депресії, а у 1955 році переніс інфаркт міокарда. У тому ж році Фрідмен вийшов на пенсію за станом здоров'я і покинув АНБ, але продовжив консультувати НАТО з питань криптології до кінця 1950-х років. У 1955 році він був нагороджений Медаллю національної безпеки (англ. *National Security Medal*), вищою нагородою ЦРУ.

Лише у 1956 році Фрідмен виграв суд і отримав компенсацію у розмірі 100 тисяч доларів за ушкодження, нанесеного грифом секретності. У лютому 1963 року він був утретє госпіталізований з нападом важкої депресії, а у 2 листопада 1969 року помер після двох повторних серцевих нападів.

Колега Фрідмена Абрахам Сінков після війни служив в «*ASA*» , а у 1949 році, коли була створена Агенція безпеки збройних сил «*AFSA*» (англ. *Armed Forces Security Agency*) - перша централізована криптологічна організація в США, він став в ній керівником програми безпеки комунікацій і зберіг цю посаду при реорганізації агенції в АНБ у 1952 році. У 1954 році Сінков став другим співробітником АНБ, який закінчив Національний військовий коледж (першим був Л.Торделла). Повернувшись в АНБ, він став помічником директора, помінявшись місцями зі своїм старим колегою Роулетом. Сінков вийшов у відставку з АНБ у 1962 році у званні полковника. У 1966 році він написав книгу «Елементарний криптоаналіз: математичний підхід», яка була однією з перших книг із криптології, доступних для широкої громадськості.

Другий колега Фрідмена Френк Роулет у 1945 році став начальником «*ASA*», а у 1949 році після утворення «*AFSA*» - технічним директором її Оперативного директорату. Після реорганізації агенції в АНБ у 1952 році він перейшов на роботу в ЦРУ, а з 1958 року працював в

АНБ як спеціальний помічник директора. У 1965 році Роулет очолив Національний інститут криптографії, і в цьому ж році Президент США нагородив його Медаллю національної безпеки (англ. *National Security Medal*) за «злом» японського «пурпурного» шифру. У 1964 році Конгрес США виплатив Роулету 100 тисяч доларів як часткову компенсацію за його секретні винаходи. За заслуги в області захисту інформації Американська організація безпеки інформаційних систем (англ. *Information Systems Security Organization*) заснувала нагороду імені Роулета (англ. *Frank Byron Rowlett Award*).

Третій колега Фрідмена Соломон Кульбек з 1952 року працював у відділі криптоаналізу АНБ. Його співробітники першими освоїли такі види машинної пам'яті, як магнітні стрічки та магнітні барабани, а також багатозадачний режим роботи комп'ютерів і вели роботи в області кибербезпеки. Кульбек звільнився з АНБ у званні полковника у 1962 році, після чого викладав в університеті Джорджа Вашингтона і вів наукову роботу.

За значний вклад у криптологію імена Уільяма Фрідмена, Абрахам Сінкова, Френка Роулета і Соломона Кульбека увічнені в Залі слави АНБ і Залі слави військової розвідки США. У 1999 році в Залі Слави АНБ був встановлений також і бюст Фрідмена з написом «Глава американської криптології» (англ. *Dean of American Cryptology*).

2.7. Перша апаратура засекречування

Роботи зі створення засобів і методів засекречування телефонних переговорів були розпочаті американськими інженерами незабаром після закінчення Першої світової війни. Створений ними перший зразок апаратури закритого телефонного зв'язку отримав назву «скремблер» (англ. *scrambler* – шифратор) і використовувався при передачі повідомлень конфіденційного характеру по радіотелефону між Лос-Анджелесом і віддаленим від нього на 20 кілометрів островом Каталін.

«Закриття» каналу зв'язку досягалося в скремблері за рахунок частотної інверсії спектру мовного сигналу, в процесі якої здійснювалося перетворення низькочастотних складових спектру у високочастотні і навпаки. В результаті такого перетворення телефонне повідомлення ставало нерозбірливим у разі його прийому сторонньою особою за допомогою звичайного радіоприймача.

В той же час на приймальному боці радіолінії, обладнаної скремблером, здійснювалося відоме зворотне перетворення спектру прийнятого мовного сигналу, за допомогою чого відбувалося відновлення початкового повідомлення.

У 1920-і роки в США був розроблений новий скремблер на основі використання досконалішого методу закриття телефонних повідомлень. Відповідно до нього спектр мовного сигналу в результаті фільтрації підрозділявся на 5 частотних смуг рівної ширини, після чого здійснювалася їх частотна інверсія і перестановка за деяким правилом, яке мінялося кожні 20 секунд.

Вказаний метод був використаний при створенні першої американської апаратури телефонного засекречування, яка називалася «*А-3*». Вона була прийнята в експлуатацію у 1937 році та використовувалась Американською телефонно-телеграфною компанією для забезпечення засекреченим зв'язком вищих посадових осіб з числа політичного і військового керівництва США.

Принцип засекречування «*А-3*» складався з інверсії та перестановки 5 піддіапазонів частот. З 3840 можливих комбінацій ($5x2^5$) фактично використовувалися лише 6, що мінялися 36 разів за кожні 20 секунд. Криптографічна слабкість апаратури компенсувалася регулярною зміною частот передачі.

Хоча система «*А-3*» достатньо часто використовувалася президентом США Ф.Рузвельтом для телефонних переговорів з прем'єр-міністром Великобританії У.Черчиллем, а також з американськими послами в зарубіжних країнах, на думку американських військових фахівців, вона не забезпечувала повною мірою секретність радіопереговорів і дозволяла лише виключити їх випадкове підслуховування сторонньою особою. У разі ж систематичного радіоперехоплення телефонних повідомлень існувала достатньо висока вірогідність того, що дешифрувальній службі супротивника вдасться відновити їх зміст.

Через це окремі воєначальники відносилися до системи «*А-3*» з недовірою і вважали за краще користуватися радіотелеграфним зв'язком із застосуванням звичайної шифрувальної апаратури. До «обережних» відносився і генерал Д.Маршалл, який неодноразово рекомендував президенту Ф.Рузвельту відмовитися від використання системи «*А-3*» для ведення секретних переговорів з послами США за кордоном. Застереження генерала були небезпідставні.

Як з'ясувалося згодом, фахівці Поштового відомства фашистської Німеччини протягом тривалого часу здійснювали перехоплення і запис радіотелефонних переговорів, що засекречувалися «*А-3*», із станції радіоперехоплення, розташованої в Нідерландах. В результаті німецькій дешифрувальній службі вдалося у 1941 році розгадати принцип засекречування телефонних повідомлень в системі «А-3». Це дозволило німецькій розвідці регулярно отримувати дешифровані записи переговорів, які вели Президент США Ф.Рузвельт, Прем'єр-міністр Великобританії В.Черчилль, Міністр закордонних справ Великобританії А.Іден, помічник Президента США Р.Гопкінс, американський генерал М.Кларк та інші.

Перекладені з англійської на німецьку мову тексти дешифрованих переговорів високопоставлених осіб США і Великобританії доповідалися командуванням німецької розвідки безпосередньо Адольфу Гітлеру, а також іншим керівникам Третього рейху.

Крім того, відсутність у розпорядженні командування Збройних сил США надійного засекреченого радіотелефонного зв'язку, здатного без затримок довести до відповідних інстанцій наявну інформацію, була непрямою причиною найбільших

втрат, яких зазнали США в результаті раптового масованого удару японської авіації по найбільшій військово-морській базі США на Гавайських островах – Перл-Харбор.

До кінця 1941 року Японія розвернула підготовку до захоплення Індонезії, а також американських і британських володінь на Тихому океані. Тимчасовий японський уряд вів діалог з урядом США про врегулювання японсько-американских відносин. Ці переговори мали на меті приспати пильність США і виграти час для підготовки раптового удару по базах американського флоту на Тихому океані.

Недільним ранком 7 грудня 1941 року начальнику штабу Армії США Д.Маршаллу стало відомо про рішення японського уряду перервати японсько-американські переговори. Побоюючись, що його телефонна розмова за системою «*А-3*» з командуванням збройних сил на Гавайських островах може бути перехоплена й дешифрована японською розвідкою, Д.Маршалл розпорядився зашифрувати інформацію про можливий напад Японії на американські бази та передати її по радіотелеграфному каналу зв'язку.

Оскільки шифрування й дешифрування інформації здійснювалося вручну та вимагало значного часу, телеграма була отримана адресатом вже після того, як японська авіація завдала масованого удару по Перл-Харбору. В результаті з 8 лінкорів, що стояли на рейді Перл-Харбору, 5 були потоплені, а 3 пошкоджені. Всього з ладу було виведено 18 кораблів, флот втратив декілька тисяч осіб.

Реально оцінюючи недоліки і обмежені можливості системи «А-3», фахівці американської телефонної компанії «*Bell Telephone Laboratories*» ще з жовтня 1940 року приступили до проведення досліджень по створенню такої апаратури засекречування телефонних переговорів, яка б дозволяла вести секретні розмови, не побоюючись того, що вони можуть бути «розкриті» дешифрувальною службою супротивника. Як один із нових методів «закриття» розглядалося маскування мовних сигналів шумом.

Суть пропонованого методу полягав у тому, що на передавальному боці радіолінії аналоговий мовний сигнал змішувався з псевдошумовим сигналом, а на приймальному боці (в результаті віднімання з прийнятого сигналу точної копії псевдошумового сигналу) відбувалося відновлення початкового мовного повідомлення.

Основна складність практичної реалізації даного методу полягала в тому, що маскування мовного сигналу вимагало достатньо високого відношення шум/сигнал, що істотно ускладнювало його виявлення під час прийому.

Одночасно компанією «*Bell Telephone Laboratories*» проводилися дослідження за оцінкою можливості використання на користь засекречування телефонних розмов «вокодера» (англ. *vocoder - voice coder* – голосовий шифрувальник). Вокодер був створений американськими інженерами для стиснення смуги частот передаваного мовного сигналу. Цей пристрій визначав основні параметри сигналу, кодував їх і передавав модульований радіосигнал в ефір у вужчій в порівнянні із звичайним телефонним сигналом смузі частот.

На приймальному боці радіолінії здійснювалося декодування параметрів прийнятого сигналу та синтезування на їх основі спеціальним генератором початкового мовного повідомлення, але оскільки звучання синтезованої мови на приймальному боці лише віддалено нагадувало голос, що говорив на передавальному боці радіолінії, вокодерна телефонія на початку 1940-х років широкого розповсюдження не отримала.

Аналіз принципів функціонування вокодера наштовхнув американських інженерів на думку використовувати при створенні апаратури для захисту телефонних переговорів принципово новий метод, що полягав у шифруванні мовних сигналів, заздалегідь перетворених у цифрову форму.

Групою фахівців під керівництвом інженера Р.Поттера був розроблений експериментальний зразок апаратури засекреченого радіотелефонного зв'язку «X-system», в якому поєднувалися принципи дії вокодера і пристрою шифрування буквено-цифрової інформації. Вхідний мовний сигнал поступав на 10 смугових фільтрів і аналізатор збудливого сигналу (послідовність імпульсів із частотою основного тону мови для дзвінких звуків, або шумоподібна послідовність сигналів для глухих звуків).

В результаті аналого-цифрового перетворення значення амплітуди сигналу в кожному із смугових фільтрів кодувалося однією шестерічною цифрою, а частота і вид збудливого сигналу – двома шестерічними цифрами. Одночасно з визначенням цифрових параметрів мовного сигналу в розробленій апаратурі генерувалася ключова псевдовипадкова послідовність шестерічних цифр.

В результаті підсумовування за модулем 6 параметрів телефонного сигналу з ключовою послідовністю відбувалося автоматичне шифрування переданого повідомлення. Визначення параметрів мовного сигналу та генерація цифр ключової послідовності здійснювалися одночасно, з частотою 50 Гц.

Використання на приймальному боці радіолінії тієї ж ключової послідовності дозволяло розшифрувати параметри та синтезувати початковий телефонний сигнал. У зв'язку з особливостями функціонування вокодера звучання прийнятого повідомлення істотно відрізнялося від голосу того, хто говорив на передавальному боці радіолінії. Можливість розпізнати того, хто говорив, більше ґрунтувалася на його манері говорити, ніж на тембрі голосу.

Міністр оборони США Л.Стімсон, ділячись своїми враженнями після переговорів по апаратурі засекреченого радіотелефонного зв'язку з генералом Д.Маршаллом, розповідав, що в телефонній трубці він почув «роботоподібний голос, абсолютно не схожий на голос генерала Маршалла. Проте по характеру ведення розмови я міг зрозуміти, що говорю саме з ним».

Як показали випробування нової апаратури, розбірливість слів на приймальному боці радіолінії в цілому була достатньо хорошою і підвищувалася у міру звикання особи, що слухала, до особливостей формування звуків у вокодері.

І хоча окремі особи, що випробували новий пристрій, знаходили якість відтвореної мови незадовільною, проте у апаратури «X-system» з'явилося достатньо багато прихильників, які були готові пожертвувати якістю звучання в обмін на гарантію секретності телефонних переговорів.

Можливо, що роботи щодо створення нової апаратури зв'язку, які проводилися компанією «*Bell Telephone Laboratories*», так і не вишли б із стадії експериментальних досліджень, коли б не зустріч Президента США і Прем'єр-міністра Великобританії, що відбулася 14 січня 1942 року, в ході якої Ф.Рузвельт вказав на необхідність удосконалити засекречений радіотелефонний канал зв'язку між Вашингтоном і Лондоном.

І хоча присутні при зустрічі начальник штабу армії США і головнокомандувач військово-морськими силами спробували переконати Президента в тому, що наявні системи не дозволяють забезпечити необхідний рівень секретності, після закінчення зустрічі Президентом США було дано вказівку на активізацію робіт із створення надійної засекреченої лінії радіотелефонного зв'язку між Вашингтоном і Лондоном.

Ці роботи були доручені спеціальній групі фахівців компанії «Bell Telephone Laboratories» в кількості 30 чоловік на чолі з інженером Полом Блю. До участі в розробці нової апаратури, що отримала умовне найменування «*SIGSALY*», були залучені такі відомі в подальшому американські інженери, як К.Шенон, Х.Найквіст і провідний фахівець англійського криптоаналітичного центру Алан Тюрінг.

Перший зразок станції «*SIGSALY*» був виготовлений на початку 1943 року в Манхеттені. При її створенні в значній мірі були використані технічні ідеї та рішення, вироблені в процесі розробки експериментального зразка апаратури «*X-system*».

Достатньо складною проблемою, з якою зіткнулися розробники «*SIGSALY*», було отримання і подальше використання при роботі станції ключової послідов-

ності, що забезпечувала автоматичне шифрування телефонних переговорів. Для отримання такої послідовності було запропоновано використовувати спеціальну паророртутну лампу заввишки 35 сантиметрів і діаметром 10 сантиметрів, що генерувала шумовий сигнал з випадковим значенням амплітуди. В результаті періодичної вибірки (з інтервалом 20 мілісекунд) і квантування шумового сигналу відбувалося формування псевдовипадкової послідовності сигналів, які записувалися на вініловий диск з числом рівнів квантування за амплітудою, рівним 6.

Диск за своїм виглядом нагадував звичайну грамофонну пластинку, що використовувалася в студії звукозапису. Перші оригінали дисків, що виготовлялися в приміщенні компанії «*Bell Telephone Laboratories*», доставлялися під озброєною охороною в одну з будівель компанії «*World Broadcasting System*», де на їх основі виготовлялися два повністю ідентичні штамповані шифродиски діаметром 35 сантиметрів. Оригінал при цьому знищувався.

Подальша доставка дисків для станцій «*SYGSALY*» повинна була здійснюватися кур'єром і покладалася на центр шифрувальної служби Армії США.

Для ведення секретних переговорів на станціях «*SIGSALY*» заздалегідь потрібно було встановити ідентичні шифродиски, забезпечити однакову швидкість їх обертання та синхронність генерації ключових послідовностей на обох боках радіолінії. З цією метою включення механізму обертання дисків на станціях проводилося одночасно.

Час включення визначався обслуговуючим персоналом за сигналами точного часу, що передавалися радіостанцією військово-морської обсерваторії США, і заздалегідь узгоджувався операторами по відкритих каналах радіозв'язку.

Синхронність обертання дисків на двох станціях досягалася за рахунок передачі та прийому спеціальних сигналів синхронізації і фазового налаштування частоти обертання диска оператором однієї зі станцій. Висока стабільність частоти обертання дисків забезпечувалася за рахунок ускладнення схеми електроживлення механізму обертання та використання в ній опорних генераторів із кварцовою стабілізацією частоти, які поміщалися в спеціальні термостати.

Зчитування ключової послідовності з шифродиска здійснювалося при його обертанні в процесі переміщення головки звукознімача та перетворення механічних коливань голки в електричні сигнали з певною амплітудою.

Для забезпечення надійної розбірливості мови тимчасове невладнання

ключових послідовностей, що генерувалися шифродисками двох станцій, не повинно було перевищувати півсекунди. Кожна станція «*SYGSALY*» була обладнана двома механізмами обертання дисків.

Таким чином, у разі потреби після закінчення роботи одного диска вмикався інший, що забезпечувало можливість ведення достатньо тривалих переговорів. Відповідно до встановлених правил шифродиски використовувалися тільки один раз, після чого підлягали знищенню.

Розробники станції «*SYGSALY*» були повністю упевнені в тому, що їх апаратура здатна забезпечити секретність телефонних розмов. Керівник групи інженер Пол Блю вважав, що навіть у разі захоплення та доставки станції до Берліна дешифрування телефонних переговорів супротивником за відсутності у нього копій шифродисків буде неможливим.

Перша станція «*SYGSALY*» була встановлена в будівлі Міністерства Оборони США у березні 1943 року, а друга – у травні того ж року в Лондоні. Випробування працездатності станцій при веденні засекречених телефонних переговорів по трансатлантичному радіоканалу Вашингтон – Лондон були завершені 29 червня 1943 року. Офіційна церемонія введення «*SYGSALY*» в експлуатацію відбулася 15 липня 1943 року.

Всього за період Другої світової війни американською компанією «*Bell Telephone Laboratories*» було виготовлено близько 10 таких станцій, які і утворили урядову систему засекреченого радіотелефонного зв'язку США. Крім Вашингтона і Лондона, вони були встановлені в Алжирі, Брисбені (Австралія), на Гавайських островах (форт Шафтер), в Окленді (штат Каліфорнія), Парижі (після його звільнення від німецьких

військ), на острові Гуам (західна частина Тихого океану), в Берліні і Франкфурті (після їх окупації англо-американськими військами).

Окремі станції «*SYGSALY*» були обладнані засобами, що забезпечували проведення сеансів конференц-зв'язку, коли декілька осіб, що сиділи за спеціально обладнаним столом, могли одночасно слухати, що говорили на іншому кінці радіолінії. Проте говорити в мікрофон міг тільки один з присутніх.

У Вашингтоні і Лондоні приміщення, звідки велися секретні переговори, були територіально рознесені з приймально-передавальною та шифрувальною апаратурою станцій «*SYGSALY*». Встановлені в цих приміщеннях телефонні апарати під'єднувалися до станції по захищених дротових лініях зв'язку.

У разі підключення до таких ліній апаратури прослуховування на посту оператора «*SYGSALY*» спалахувала лампочка червоного кольору – сигнал тривоги. Одночасно в телефонну трубку поступав шумовий сигнал, застерігаючи особу, яка вела переговори, про можливе підслуховування.

Телефонні переговори між абонентами станцій «*SYGSALY*» велися по одному з каналів багатоканальної трансатлантичної радіомережі «*PL-60*» в короткохвильовому діапазоні хвиль. При перехопленні цих переговорів на звичайний радіоприймач вони сприймалися на слух як шум.

Технічне обслуговування й експлуатація всіх станцій «*SYGSALY*» (незалежно від місця їх розташування) були покладені на війська зв'язку Армії США. До складу обслуговуючого персоналу станцій набиралися, як правило, військовослужбовці, що мали спеціальну технічну освіту й досвід роботи в телефонних компаніях до військової служби. Для їх підготовки при компанії «Bell Telephone Laboratories» були створені спеціальні курси, де військовослужбовці вивчали пристрій станції, організацію й порядок її експлуатації та ремонту.

Перший випуск курсів складався з 6 офіцерів і відбувся 5 січня 1943 року. Всього навчання на курсах пройшли 186 військовослужбовців у складі 10 груп. Тривалість навчання складала від 28 до 44 робочих днів. Перші випускники курсів склали основу створеної 10 лютого 1943 року 805-ої роти зв'язку – спеціального підрозділу для обслуговування станцій засекреченого радіотелефонного зв'язку «*SYGSALY*». Командир роти майор Е.Ептід до служби в армії працював в одній з американських телефонних компаній, підпорядкована йому рота налічувала 81 офіцера і 275 військовослужбовців.

Технічне обслуговування та експлуатація станцій «*SYGSALY*» здійснювалися окремими підрозділами у складі 4-5 офіцерів і 6-8 військовослужбовців. Завдяки добрій підготовці персоналу станції в основному працювали справно. Разом з тим, протягом тривалого часу не вдавалося забезпечити ведення переговорів Прем'єр-міністра Великобританії В.Черчилля з телефонного апарату, встановленого в спеціальній кімнаті підземного бункера урядової будівлі в Лондоні.

З цієї причини В.Черчилль і інші високопоставлені особи з літа 1943 року по весну 1944 року були вимушені продовжити використання системи радіотелефонного зв'язку «*A-3*». У зв'язку з її слабкою криптостійкістю у вказаний період німецька розвідка продовжувала дешифровувати телефонні переговори та отримувати важливі відомості військового характеру, включаючи інформацію про діяльність військ і маршрути руху конвойних кораблів і судів торгового флоту союзників.

На початку 1944 року німецькому посту радіоперехоплення, розташованому в Нідерландах, вдалося перехопити телефонну розмову між Ф.Рузвельтом і В.Черчиллем, що тривала близько 5 хвилин. В результаті її дешифрування німецькій розвідці стали відомі важливі відомості про заплановану висадку англо-американського десанта до Європи.

Після того, як несправності в роботі станції «*SYGSALY*» в Лондоні були усунені, секретні переговори в системі зв'язку «*A-3*» були практично припинені, внаслідок чого керівництво Поштового відомства фашистської Німеччини, якому були підпорядковані пости радіоперехоплення, дійшло висновку, що між США і Великобританією встановлений новий канал засекреченого телефонного зв'язку.

Незважаючи на широкі можливості, що надавалися системою «SYGSALY», окремі військові і політичні керівники США ставилися до неї досить скептично. Так, командувач союзними військами в південно-західній частині Тихого океану генерал Д.Макартур сумнівався в надійності засекречування телефонних переговорів і вважав за краще використовувати букводрукувальну апаратуру радіозв'язку «*SYGTOT*» з попереднім шифруванням інформації.

Генерал Д.Ейзенхауер, верховний головнокомандувач експедиційними силами союзників у Західній Європі, вдавався до використання системи «*SYGSALY*» украй неохоче, також не покладаючись на її надійність. Крім того, генерал часто зазнавав труднощі в розумінні окремих слів, які вимовляли його співбесідники на іншому боці радіолінії.

У роботі системи траплялися збої, не завжди вдавалося достатньо швидко встановити зв'язок між станціями, в окремих випадках мова супроводжувалася сильними перешкодами, що ускладнювали її розуміння. Проте, не дивлячись на ці недоліки, урядова система засекреченого радіотелефонного зв'язку «*SYGSALY*» отримала визнання серед значного числа генералів і урядовців США і Великобританії.

Завдяки їй велика кількість різноманітних відомостей військового й політичного характеру своєчасно доводилася до зацікавлених осіб і разом із тим зберігалася в таємниці від супротивника. У числі цих відомостей була, зокрема, інформація про доставку двох атомних бомб на розташований в Тихому океані острів Тініан, звідки у серпні 1945 року був зроблений виліт американських літаків для бомбардування японських міст Хіросіма й Нагасакі.

Найбільш напружено використовувалася станція «*SYGSALY*» в Лондоні. Тільки за перший рік експлуатації з її допомогою було проведено 448 сеансів конференц-зв'язку, в процесі яких, як правило, обговорювалися питання, пов'язані з підготовкою союзних військ до ведення бойових дій в Європі.

Час від часу система «*SYGSALY*» використовувалася за своїм основним призначенням – для забезпечення секретних переговорів між Президентом США і Прем'єр-міністром Великобританії. Так, в один з травневих днів 1944 року начальник підрозділу 805-ої роти зв'язку, дислокованого в Лондоні, отримав наказ підготувати станцію для проведення таких телефонних переговорів. Після того, як радіозв'язок між Вашингтоном і Лондоном був встановлений, до телефонних апаратів були запрошені керівники країн-союзників.

Привітавшись і поговоривши небагато часу про собаку Ф.Рузвельта – шотландського тер'єра по кличці Фала, Президент і Прем'єр-міністр перейшли до розмови про раптовий наступ союзних військ, що заздалегідь планувався в ніч на 5 або 6 червня. Розмова тривала близько півгодини.

Після смерті Ф.Рузвельта 12 квітня 1945 року того ж дня до присяги як президент США був приведений Р.Труман. Одна з розмов між В.Черчиллем і новим Президентом США відбулася 25 квітня 1945 року. Під час бесіди Прем'єр-міністр повідомив, що йому передали пропозицію рейхсфюрера СС Г.Гіммлера про часткову капітуляцію німецьких військ на західному фронті при продовженні бойових дій з частинами Радянської Армії на східному фронті. В результаті розмови керівники країн-союзників прийшли до рішення відхилити пропозицію Гіммлера. Одночасно вони домовилися повідомити про цю бесіду керівнику СРСР Й.Сталіну.

Так, до самого закінчення Другої світової війни створена зусиллями декількох десятків американських інженерів система «*SYGSALY*», що експлуатувалася фахівцями військ зв'язку американської армії, забезпечувала збереження в таємниці планів і намірів вищого військово-політичного керівництва країн-союзників – США і Великобританії.

2.8. Військова радіорозвідка

Власну криптослужбу мав і ВМФ США, яка іменувалася Секцією коду і зв'язку **«***Op-58*» (англ. *Code and Signal Section*) та з жовтня 1917 року знаходилася у складі Управління військово-морських операцій (англ. *Office of the Chief of Naval Operations*). З січня 1920 року ця секція під кодовою назвою **«***Op-18*» була підпорядкована Начальнику зв'язку ВМФ (англ. *Director of Naval Communications*). 1 липня 1922 року вона під кодовою назвою **«***Op-20-G*» увійшла до складу 20-го відділу Управління зв'язку ВМФ (англ. *20th Division of the Office of Naval Communications, G Section*).

З січня 1924 року «*Op-20-G*» очолив лейтенант Лоуренс Сеффорд (1890-1973), який у подальшому став головним криптологом ВМФ США. Провідним криптоаналітиком секції була Агнес Дріскол (1889-1971), відома як Мадам «*X*», яка «злама-

ла» декілька японських ручних військово-морських кодів: «червоний» - у 1926 році та замінивший його «блакитний» - у 1931 році. На початку 1935 року вона успішно «зламала» код японської шифрувальної машини «*M-1*», що використовувалася для шифрування повідомлень японських військово-морських аташе по всьому світу, яку американські криптоаналітики назвали «оранжевою» (англ. *orange*).

11 березня 1935 року на «*Op-20-G*» були покладені всі питання криптозахисту військово-морських мереж і систем зв'язку, тому вона була реорганізована в Групу безпеки зв'язку (англ. *Communications Security Group*). З березня по жовтень 1939 року та з лютого по жовтень 1942 року «*Op-20-G*» працювала під назвою «Секція радіорозвідки» (англ. *Radio Intelligence Section*), а з жовтня 1939 року по лютий 1942 року - під назвою «Секція безпеки зв'язку» (англ. *Communications Security Section*).

Військовим підрозділам радіорозвідок: армійської «*SIS*» і флотської «*Op-20-G*» було дане «добро» на здійснення програм перехоплення. Всі матеріали, що були отримані в результаті перехоплення та дешифрування цими підрозділами, були суворо засекречені та отримали кодову назву «Магія» (англ. *magic*). Виняткова таємність, що оточувала їхню діяльність, дозволяла уникати викриття.

Вони сконцентрували свою увагу на радіограмах, оскільки компанії проводового зв'язку, усвідомлюючи значення заборони, відмовлялися надавати їм іноземну кореспонденцію. Відповідно, 95% одержуваної інформації були радіоперехопленнями. Тільки 5% інформації припадало на перехоплення проводового зв'язку та фотокопії послань, які зберігалися в архівах деяких компаній, що співробітничали з військовими.

Для перехоплення радіограм ВМФ, в основному, покладався на мережу постів радіоконтроля на Бейн-бридж-Айленді в Пагет-Саунді; Вінтер-Харборі в штаті Мен; Челтенхемі штату Меріленд; Хиейя в Оаху; Корехидорі, а також більш дрібні станції на Гуамі, в Імперіал-Біч у Каліфорнії; Амагансетті на Лонг-Айленді та Юпітері у Флориді. Кожний з них відповідав за визначені діапазони радіочастот. Станція на Бейнбрідж-Айленді, наприклад, контролювала радіообмін японського уряду з Токіо із Сан-Франциско.

Передача дипломатичних послань, як правило, здійснювалася каналами комерційного радіо з використанням латинського алфавіту. Військово-морські радіограми використовували спеціальний код Морзе. Моряки перехоплювали його за допомогою операторів, що знали японську морзянку, і фіксували на спеціальній машинці, яка перетворювала шифр у його латинські еквіваленти.

Спочатку всі станції направляли послання до Вашингтона авіапоштою. Але це проходило занадто повільно. Авіалайнер, що доставляв армійські перехоплення з Гаваїв на континент, у середньому літав раз у тиждень, а погода іноді приводила до скасування рейса, змушуючи посилати перехоплення морським шляхом. Буквально за тиждень до Перл-Харбора два армійські перехоплення з Ріо не могли добратися

до Вашингтона протягом одинадцяти днів.

Подібні затримки змусили флот установити в 1941 році радіотелетайпний зв'язок між Вашингтоном і станціями на території США. Станція набивала пачку перехоплень на телетайпну стрічку, з'єднувалася з Вашингтоном за допомогою телетайпного зв'язку та автоматично відправляла всі послання зі швидкістю 60 слів у хвилину, втричі знижуючи витрати в порівнянні з ручною передачею кожного окремого послання. Армія встановила телетайпний зв'язок зі своїми континентальними постами тільки з 7 грудня 1941 року.

Армійські та морські станції перехоплювали японські послання, зашифровували їх за американською системою та передавали по радіо до Вашингтона. Зашифрування робилося для того, щоб японці не довідалися про криптоаналітичну діяльність американців. До цієї досить дорогої системи радіоретрансляції були включені тільки три найбільш значні японські системи – «пурпурна», «червона» (її попередниця, що зберігалася у віддалених місіях, наприклад, у Владивостоці) та деякі інші.

Потік повідомлень японського МЗС, що перехоплювалися «*SIS*» і «*Op-20-G*» був досить великий. Восени 1941 року кількість перехоплень складала від 50 до 75 радіограм на добу, при цьому обсяг окремих повідомлень досягав 15 сторінок видрукуваного тексту. Криптослужби були змушені постійно прискорювати швидкість своєї роботи. Так, у 1939 році їм були потрібні три тижні для того, щоб всі перехоплення пройшли весь шлях до Держдепартамента. А у кінці 1941 року цей процес займав вже не більше чотирьох годин.

Служба радіоперехоплення працювала чітко. З 227 послань, які відносилися до японсько-американських переговорів та посилалися між Вашингтоном і Токіо з березня по грудень 1941 року, не були перехоплені тільки чотири. Вашингтон був просто завалений перехопленнями, що накопичувалися у секретній папці з назвою «*Magic*». Крихітний апарат криптологів фізично не міг справлятися з таким потоком.

Проблема була вирішена двома способами. По-перше, було скорочене дублювання в роботі. Спочатку обидві служби «*SIS*» і «*Op-20-G*» самостійно розшифровували всі японські перехоплення. Однак у 1940 році між ними була досягнута домовленість про розподіл обов'язків таким чином: повідомленнями з Токіо по непарних днях займалася «*Op-20-G*», а по парних днях - «*SIS*». Тим самим заощаджувався час для розкриття нерозшифрованих систем і ліквідації завалів. Іншим способом стало «розкриття», в першу чергу, важливих послань; інші повідомлення доводилося відкладати, принаймні, до закінчення роботи над більш важливим матеріалом. Вважали, що більш важливі послання «закривали» більш складною системою кодування.

Посилати всі повідомлення тим самим кодом було неможливим, тому що величезний потік інформації легко дозволив би криптоаналітикам його розкрити та дешифрувати. Тому держави установлювали свою ієрархію послань у залежності від ступеня важливості. Японія не була винятком. Хоча її МЗС і використовував воістину

приголомшливу розмаїтість кодів, час від часу звертаючись до послуг приватного коду Йокогамського банку та кодів на основі «катакани», в основному вони все-таки використовували чотири основні системи. Американські криптоаналітики виділили чотири ступені значимості цих передач, виходячи з заданої складності самого кодування та важливості змісту послань, що звичайно вказувалися спеціальними знаками. Дешифрування перехоплень здійснювалося у встановленій черговості.

Найпростішим кодом, який займав найнижче місце та дешифровувався в останню чергу (не рахуючи відкритого тексту), був код «*LA*», названий у такий спосіб через позначення, що випливали перед початком повідомлення. «LA» просто перекладав «катакану» на латинські букви для передачі телеграфом і використання скорочень з метою економії телеграфних витрат. При цьому «*ki*» замінявся на кодову форму «*CI*» тощо. Одним з самих типових послань цього виду могло служити повідомлення № 01250 від 4 листопада, спрямоване з Токіо до Нага-но Киті: «Нижченаведене затверджено як щорічну премію для друкарок, що служать у даній установі». Цей вид кодування називався «паспортним кодом», оскільки він звичайно застосовувавсія для адміністративних рутинних проблем консульства, наприклад, для видачі паспортів і віз. Цей вид кодування було особливо легко розкрити, тому що він діяв з 1925 року та мав визначену послідовність у його побудові.

Вище рангом знаходилася система, відома японцям за назвою «Ойте», а для американців як «*PA-K2*». Частина «*PA*» складалася з дво- і чотиризнакового коду, схожого на «*LA*», однак більш великого та з переплутаними кодовими номерами. Частина «*K2*» складалася з перестановки, заснованої на кодових номерах. Букви з кодування «*PA*» зображувалися під їхніми кодовими номерами ліворуч, а потім копіювалися в змішаному порядку, починаючи з букви під кодовим номером 1 і так далі до закінчення рядка. Потім це все повторювалося. Тому ця система не представляла особливої складності для досвідчених американських криптоаналітиків.

Вони вважали, що здатні «розколоти» послання «*PA-K2*» у термін від шести годин до шести днів, у середньому за три дні. Змішування піддавалося розшифруванню, тому що кожен рядок перемішувався аналогічно. Криптоаналітик розрізав криптограму на групи по 15, 17 або 19 частин і досліджував ці частини одночасно, поки на всіх криптограмах не виявлялися аналогічні сполучення голосних і приголосних. Потім кодування розкривалося, виходячи з уяви про те, що групи кодування, які найбільш часто зустрічалися, являли собою найбільш застосовувані сполучення. А оскільки ця система застосовувалася протягом багатьох років, американці вже давно її розкрили. Тому в кожному окремому випадку вирішення було в тому, щоб зрозуміти систему перестановки, що при удачі могло бути здійснене за кілька годин. Оскільки ця система привертала особливу увагу, термін від перехоплення до перекладу складав від двох до чотирьох днів.

Найміцнішим «горішком» була система перестановки. Подібно «*K2*» вона ви-

користовувала кодові номери, але відрізнялася тим, що копіювалася вертикально, а не горизонтально, і крім того, у блоках перестановки залишалися визначені «білі плями», що не заповнювалися при вписуванні у блоки кодових груп. При розшифруванні криптоаналітики насамперед розбивали криптограму на приблизно рівні сегменти, які, на їхню думку, являли собою стовпчики оригінальних блоків. Порожні місця значно ускладнювали цей важливий первісний етап роботи, оскільки вони змінювали розміри колонкових сегментів. Наступним етапом була спроба розташувати один сегмент поруч з іншим для того, щоб виявити визначену послідовність кодування. У цьому випадку «білі плями», які позначали пропуски в невідомих місцях між буквами сегмента, також значно ускладнювали роботу криптоаналітика.

Про труднощі розшифрування даної системи свідчив той факт, що вона була розкрита тільки через місяць після початку її застосування. Криптоаналітикам довелося в кожному окремому випадку проводити новий аналіз для кожної послідовності порожнеч і кожного ключа перестановки. Ключ мінявся щодня, послідовність порожнеч – три рази на місяць, звідси затримки з дешифруванням. Наприклад, ключ і послідовність послання 18 листопада змогли розкрити тільки 3 грудня, а послання від 28 листопада – тільки 7 грудня. З іншого боку, вирішення проблеми іноді досягалося за день або два. Успіх багато в чому залежав від якості перехоплення в даному ключі. Близько 10-15% цього коду так і не було взагалі дешифроване.

Це положення різко відрізнялося від «пурпурної» системи, яка вважалася найбільш секретною японською системою, де більшість послань розкривалося протягом декількох годин, а нерозкритими залишалося не більше 2-3 % передач. Пов'язано це з тим, що на той час «пурпурна» система була розкрита. Однак процес початкового розкриття системи виявився незрівнянно більш важким, ніж в інших системах. Тому розкриття шифру «пурпурний» можна вважати одним з найбільших світових досягнень криптоаналізу.

Оперативна частина «пурпурної» машини являла собою бокс розміром з висувну шухляду столу, яка була розташована між двома великими чорними електронними друкарськими машинками «Ундервуд», що були з'єднані одна з одною 26 дротами, підключеними до цілої низки розеток, які називалися «штепсельним комутатором». Для того, щоб зашифрувати послання, шифрувальник повинен був виконати дії у такій послідовності:

- подивитися у товстий довідник машинних ключів,
- зробити провідні з'єднання відповідно до порядку, обумовленому ключем на цей день,
- повернути чотири диски на боксі таким чином, щоб цифри на їхніх закінченнях відповідали вказівкам довідника,
- надрукувати відкритий текст.

Машина записувала відкритий текст, у той час як інша, одержавши імпульси від

кодуючого боксу, пропускала його через різні хитрі процедури та друкувала зашифрований текст. Процедура дешифрування була такою ж.

Алфавітна друкарська машинка працювала на латинському шрифті. Тому вона могла розшифровувати англійські та латинські тексти, подібні до кодів «*J*». Оскільки машина не могла зашифровувати номери або пунктуацію, то шифрувальник спочатку переводив їх у тризначкові буквені коди, позначені в короткому кодовому списку, які і зашифровував. Шифрувальник на прийомі спочатку відновлював пунктуацію, розбивку по параграфах і т.д., а потім друкував остаточний текст декодованого послання.

Серцем і душею машини були її штепсельний комутатор і кодуючі диски. Вони направляли рух відповідно до з'єднань у приймаючій машині до випускаючої машини таким чином, що якщо, наприклад, на панелі приймаючої машини був натиснутий ключ «*A*», то він міг бути надрукований на випускаючій машині. Відхилення починалися зі з'єднань панелі. Якщо не було кодуючого боксу, то проводка панелі одержувала електронні імпульси від ключа «*A*» друкарської машинки відкритого тексту і передавала його, наприклад, прямо на друкований пристрій «*R*» шифрувальної машини. Інші проводи також з'єднували ключі відкритого тексту з відповідними їм друкованими пристроями шифрованих текстів. Це негайно приводило до створення шифру, щоправда, досить примітивного. Щоразу, коли натискалася буква тексту «*A*», з'являлася буква шифротексту «*R*». Простота системи забезпечувала її безпеку. З'єднання на панелі можна було змінювати після кожного послання, навіть, у ході його передачі, але це не підсилювало помітно його ефективність.

Тепер у справу вступали чотири шифродиски. Розташовані між штепсельним

комутатором машинки відкритого тексту та шифрувальної машини, вони постійно переміщалися відносно один одного за допомогою сполучного пристрою. Процедура шифрування зводилася до формування безперервно змінюваних шляхів проходження сигналу від однієї машинки до іншої, а постійне обертання дисків безперервно виробляло різні сполучення. Таким чином, сигнали відкритого тексту, проходячи по різних шляхах, перетворювалися в зовсім відмінний від нього зашифрований текст. Зазвичай з'єднання на комутаторі мінялися щодня.

Усі разом ці фактори створювали шифр, який було дуже важко розгадати. Чим більше шифр відрізнявся від первісної форми, при якій одна зашифрована буква неминуче заміняла одну букву відкритого тексту, тим важче було прочитати текст. Шифр, наприклад, міг заміняти ту або іншу букву відкритого тексту п'ятьма різними зашифрованими буквами, причому робити це в порядку ротації. Але алфавітна машинка робила серії замінників довжиною в сотні тисяч букв. Її копіюючі диски, що змінювали положення після кожної букви, ніколи не поверталися в колишнє положення для створення тих же серій шаблонів і, отже, тих же серій послідовності, поки не закінчиться шифрування сотень тисяч букв.

Тому основною задачею криптоаналітиків було відтворення проводки і вимикачів кодуючих дисків, а щоденна зміна з'єднань на комутаторі робила її ще більш обтяжною. Коли ж ця задача виконувалася, криптоаналітикам було необхідно ще визначити первісне положення кодуючих дисків для кожного дня. Але це вже було легше тому, що «пурпурна» система замінила стару «червону», яку американці давно «розкусили».

Криптоаналітики відзначили деякі характерні риси «пурпурної» машини: частоту букв, відсоток порожніх місць (букв, що не друкувалися в потрібних місцях), кількість повторень. І тому вони побачили, що нова машина є набагато більш складною й удосконаленою в порівнянні зі своєю попередницею. Перші спроби розкрити принцип роботи нової машини були пов'язані з прагненням розпізнати характер шифру.

Попередні успіхи з «червоною» машиною та іншими менш складними системами дозволили американцям зрозуміти японські дипломатичні форми звертання один до одного, повсякденні фрази та стиль (наприклад, абзаци завжди нумерувалися). Це дало можливість криптоаналітикам скласти набори слів, які найчастіше траплялися у відкритому тексті, що зрештою дозволило їм вирішити завдання розкриття шифру. Вступні та заключні шаблони, такі як «Маю честь інформувати ваше превосходительство» або «На вашу телеграму», стали першими удачами. Крім того, газетна інформація наводила на думку про характер передбачуваних повідомлень. Державний департамент США іноді публікував повні тексти дипломатичних нот Японії до американського уряду, тим самим надаючи криптоаналітикам відкриті тексти (або їхні переклади) усього послання.

Японське МЗС найчастіше розсилало той самий текст у кілька посольств, не усі

з яких мали «пурпурну» машину, і шифрувальнику неминуче доводилося кодувати телеграми як на «пурпурній» машині, так і іншим кодом, що американські криптоаналітики вже могли читати. Відбувалося порівняння часу та довжини послання – і виникла ще одна ниточка на шляху до розгадки. Як завжди, істотну допомогу робили допущені помилки. Так, у листопаді 1941 року станція в Манілі повторила текст телеграми через помилку на «штепсельному комутаторі». А скільки ж однотипних помилок було зроблено в період, коли шифрувальники ще тільки училися працювати на новій машині. Передача того самого повідомлення двома різними кодами приводила до створення «ізоморфічних» телеграм, що являли собою дуже цінну інформацію для визначення побудови шифру.

Криптоаналітики «*SIS*» і «*Op-20-G*» порівнювали ці відкриті повідомлення зі своїми зашифрованими текстами і намагалися знайти повтори, з яких вони могли установити послідовність шифрування. Даний етап роботи, особливо на початку складного криптоаналізу, був, імовірно, найбільш болісний, дратівний розумовий процес, властивий людині. Година за годиною, день за днем, а іноді і місяць за місяцем криптоаналітик буквально «висушував» свій мозок, прагнучи знайти якийсь взаємозв'язок між буквами, змушуючи себе не піддаватися паніці в тупиковій ситуації та заплутуватися у власних протиріччях, щоб домогтися додаткових важливих результатів.

Як писав один із криптоаналітиків: «Велику частину часу він бродить у повній темряві. Іноді в ночі з'являлися слабкі відблиски просвіту, що подають йому болісну надію на те, що він знайшов послідовність. Він кидається з надією тільки для того, щоб очутитися знову в лабіринті. І лише знання того, що день змінює ніч, підтримує в ньому мужність продовжувати роботу, і він знову прагне туди, де, на його думку, повинні виникнути ранкові промені. Іноді, щоправда, він знову виявляється в обіймах безпробудної полярної ночі». Саме таке відчуття нескінченної північної ночі виникало в криптоаналітика, коли він приступав до розбору нової японської машини. Розшифровувачі спочатку просувалися далеко вперед для того, щоб потім протягом місяців не просунутися далі ні на крок.

Багатоалфавітна система шифрування, до якого належала «пурпурна» машина, ґрунтувалася на алфавітній таблиці розміром 26x26. Для реконструкції цих таблиць криптоаналітики застосовували прямі й непрямі симетрії положення – найменування були не менш складні, ніж безпосередньо самі методи. Помилки, що виникали через неточність перехоплення або ж просто помилок у криптоаналізі, приводили до безладу ці непрості методи та ускладнювали роботу. Дешифрувальник, який чаклував над покресленим листком паперу, що лежав на його столі, намагався знайти основу повтору в декількох розкиданих буквах та вставити в нього вже «розкритий» фрагмент.

Після цього він пробував з'єднати ці досягнення та потім виявляв, що сполучення дає прийнятний відкритий текст. Тоді він вставляв своє дослідження в проблему загального рішення та рухався далі. Японісти вставляли відсутні букви, математики

прив'язували один цикл до іншого та потім обидва цикли до таблиць. Будь-яка можлива зброя криптоаналітичної науки, що в основному, спиралася на математиків, які використовували теорію груп, конгруентність і таке інше, кидалася в «битву». Зрештою процес вирішення досягав визначеної вершини, коли криптоаналітики мали на папері досить точне відтворення «пурпурної» машини.

Тоді американці почали споруджувати машину, що автоматично могла робити те ж саме, що криптоаналітики ручним способом зі своїми циклами і таблицями. Вони збирали її зі звичайних запчастин, які використовувалися в засобах зв'язку. Це навряд чи можна було назвати прекрасним творінням, бо коли в ній щось не спрацьовувало, вона починала іскрити або запекло скрипіти. Хоча американці ніколи не бачили японську машину, її аналог зовні дивно походив на неї і, звичайно, цілком відтворював машину з криптологічної точки зору.

Криптоаналітики продемонстрували першу машину, створену своїми руками, у серпні 1940 року після 18-20 місяців напруженої роботи. Оглядаючись назад на всі ті зусилля, що привели до цього визначного криптологічного успіху всіх часів, Фрідмен великодушно писав: «Звичайно це був результат спільної роботи всіх тих, хто брав у ній участь. Не було ні однієї людини, на яку покладалася б честь цього відкриття, як не було і жодного, кому належала б вирішальна роль. Як я вже сказав, це була команда, і успіх виявився можливим тільки завдяки тісній командній роботі всіх учасників. Результат став видатним досягненням армійської криптоаналітичної служби, тому що, наскільки я знаю, криптологи Англії і Німеччини працювали над цією проблемою, але так і не змогли її вирішити».

Тим часом криптоаналітики спорудили другу «пурпурну» машину та віддали її ВМФ США. Третя машина була відправлена до Англії у січні 1941 року на найсучаснішому та великому британському лінкорі «Георг П'ятий». Машину супроводжували двоє армійських і двоє морських криптоаналітиків. У відповідь США одержали англійську криптоаналітичну інформацію, пов'язану з німецькими шифрами і кодами. Машина, врешті-решт, опинилася в руках англійської шифрувальної групи у Сингапурі. А потім, коли японці рушили в Малайзію, її евакуйовано в Делі. Четверта машина була відправлена на Філіппіни, а п'яту тримали як резервну в самій «*SIS*». До моменту нападу японців на Перл-Харбор конструювалася машина також і для Гавайських островів. Але через події, що відбулися, її, як і третю машину, передали англійцям.

Коли «*Ор-20-G*» уже зробила значний внесок у полегшення та швидкість щоденних розшифрувань машини, 27-літній лейтенант Френсіс Рейвен «розкрив» таємницю її ключів. Після того, як кілька послань машини було розшифровано, він помітив, що щоденні ключі протягом кожного третього циклу з десяти днів пов'язані один з одним, та незабаром прийшов до висновку, що японці просто перемішували ключі першого дня, щоб скласти ключі наступних дев'яти днів. Аналогічний порядок існував і для інших десятиденних циклів. Відкриття Рейвена дозволило американ-

ським криптоаналітикам передбачати ключі на дев'ять з десяти днів. Зазвичай, їм необхідно було окремо розшифровувати ключі першого дня, але потім робота значно полегшувалася. Більш того, криптоаналітикам, оскільки вони знали порядок перемішування, вдавалося читати всю листування даного періоду, навіть, якщо вони розпізнавали тільки один із щоденних ключів.

Через рік після спорудження першої «пурпурної» машини американці змогли розшифрувати послання, що було закодовано «найвищим ступенем таємності в класифікації, застосовуваної японським МЗС». Це послання було насамперед закодоване в системі «*AC*». Потім перемішано відповідно до системи «*K9*» (звичайно застосовуваного з кодом «*J19*»), а потім перемішаний кодований текст був знову зашифрований на «пурпурній» машині. Рішення, засноване на кількості сполучень, зайняло б цілу вічність, а в даному випадку на це треба було усього лише чотири дні.

Завдяки наявному аналогу «пурпурної» машини 2 грудня 1941 року американські криптоаналітики прочитали циркуляри №№ 2444, 2445 за кодом «*J19*» із Токіо для японських посольств і консульств у Вашингтоні, Лондоні, Гонконзі, Сингапурі та Манілі, де їх персоналу приписувалося негайно знищити «пурпурні» машини, всі телеграфні коди та системи, крім одного примірника, та всі таємні документи.

Процедура знищення шифрувальних машин була розписана у завчасно підготовлених інструкціях. Машини спочатку розгвинчувалися викруткою на частини, які потім викривлялися до невпізнанності ударами молотка та розчинялися в кислоті до їх повного зникнення. Це була явна ознака підготовки японців до початку війни з американцями.

6 грудня 1941 року криптослужби США отримали перехоплену зашифровану японську телеграму до Вашингтонського посольства та того ж дня її розшифрували. Вона складалася з 14 частин, але найважливіша остання частина, де говорилося про розрив переговорів Японії і США, була передана з Токіо лише вночі з 6 на 7 грудня. Завдяки напруженій роботі криптоаналітиків 14-а частина була розшифрована вже о 8-й годині ранку 7 грудня та відправлена Президенту США. Цікаво, що в японському посольстві остання частина була розшифрована лише о 13-ій годині, тобто американський уряд прочитав японську ноту у повному обсязі на декілька годин раніше за японське посольство у Вашингтоні.

На жаль, величезна та кропітка праця американських криптослужб не змогла попередити напад Японії на військово-морську базу на Перл-Харборі, який стався о 13-й годині (за Вашингтонським часом) 7 грудня 1941 року. По-перше, незважаючи на великий обсяг дешифрованого японського листування, ні в одній телеграмі не йшла мова про напад на Перл-Харбор. По-друге, американська військово-морська розвідка не мала ніякої інформації про місцезнаходження та рух японського флоту завдяки його радіомовчанню та іншим заходам з безпеки зв'язку.

До речі, на території бази працював підрозділ радіотехнічної розвідки, який

обслуговував Тихоокеанський флот США та складався з 30 офіцерів і рядових. Його начальником був Джозеф Рошфор (1900-1976), перед яким стояло завдання «розкриття» японських радіограм, зашифрованих військово-морським кодом «*JN-25*» (англ. *Japanese Navy code № 25*). Цей код був «зламаний» у 1939 році провідним криптоаналітиком «*Op-20-G*» Дріскол.

У 1942 році військово-морська радіорозвідка «*Op-20-G*» також була реорганізована, на базі якої була створена Організація розвідки комунікацій ВМФ (англ. *Communications Intelligence Organization*) під керівництвом капітана третього рангу Сеффорда, яка стала центром криптослужб ВМФ. Вона повинна була розробляти військово-морські коди та шифри, перехоплювати проводові та радіоповідомлення супротивника, пеленгувати його радіостанції, здійснювати криптоаналіз кодів і шифрів та, нарешті, лабораторні дослідження в галузі криптології. Частину зазначених функцій передбачалося виконувати тільки у випадку ведення армією бойових дій.

Ця організація була наділена широкими криптологічними функціями: складала та розсилала нові коди й шифри, а також вела переговори з фірмами щодо виробництва шифрувальних машин. Діяльність відділу розподілялася між підрозділами у Вашингтоні, на Гаваях і на Філіппінах. Тільки Вашингтону доручалася робота над дипломатичними та морськими кодами іноземних держав, що використовувалися на атлантичному театрі воєнних дій (в основному, Німеччини). Філіппінський підрозділ розміщувався в тунелі фортеці Корехидор і був оснащений 26 радіоприймачами, апаратурою для перехоплення передачі даних та автоматичного виробництва схем і таблиць. З 700 офіцерів і рядових військово-морських установ радіорозвідки дві третини були зайняті перехопленням повідомлень і тільки одна третина – криптоаналізом і перекладами.

Саффорд розподілив свій персонал таким чином: у Перл-Харборі служили найкращі офіцери, більшість з яких мали по 4-5 років досвіду радіорозвідки; команда в Корехидорі мала всього 3 або 4 роки досвіду; у Вашингтоні відповідали за загальне спостереження та навчання – тут служили найдосвідченіші зі стажем більше 10 років. Але до 90% співробітників не мали й річного досвіду. При Саффорді три підсекції займалися криптоаналітичною діяльністю: керівник першої, капітан другого рангу Джордж Уелкер займався радіоперехопленням і пеленгацією, другої – Лі Парк очолював криптоаналітичну підсекцію, третьої – Крамер займався перекладом і розсиланням матеріалів. Найпершим завданням підрозділу було добування матеріалу для обробки його криптоаналітиками.

Успіху організації посприяли навіть японці, що не змогли знайти для друкування своїх кодових книг типографську фарбу, яка б розчинялася у морській воді. У зв'язку з цим 29 січня 1943 року американцям вдалося захопити на пошкодженому японському підводному човні 200 кодових книг, серед яких були як діючі, так і резервні. Завдяки цим книгам та зусиллям американських криптоаналітиків 13 квітня того ж

року була отримана інформація про інспекційний політ командувача японського ВМФ адмірала Ямамото. В результаті цього 18 квітня літак Ямамото був збитий американськими льотчиками-винищувачами, що безумовно негативно вплинуло на моральний дух його підлеглих та японського суспільства.

Завдяки перехопленому та дешифрованому військово-морському шифролистуванню супротивника американське командування було в курсі японських військових планів наступу, в результаті чого вони були зірвані. А вищим тріумфом криптологів на Тихому океані було мистецтво, з яким адмірал Німіц використав інформацію «Магія» у битві біля атолу Мідуей - останній великій морській битві, де кораблі так і не побачили один одного та бій вели тільки літаки.

Треба також відмітити, що разом із шифротехнікою для шифрування повідомлень у 1942 році військове командування вирішили використати також і мову індіанців «навахо». Мова «навахо» ідеально підходила для цієї мети. Надзвичайно складна, вона, крім того, не мала писемності. Ніхто не зафіксував ні граматичні правила, ні навіть елементарний алфавіт. Тому людині, що не належала до племені «навахо», навчитися мові було практично неможливо.

Індіанці «навахо», що стали радистами в різних частинах морської піхоти, замість того, щоб шифрувати повідомлення, просто передавали їх один одному, використовуючи свою рідну мову. Японці, що розгадали майже усі військові шифри США, як не намагалися, так і не змогли зрозуміти «шифр», на якому передавалися повідомлення американської морської піхоти.

Процес шифрування здійснювався таким чином: кожна буква англійського слова передавалася як слово на мові «навахо», що у перекладі на англійській починалося з цієї букви. Так, буква «а» могла передаватися декількома словами, наприклад: «тсеніл» (*axe* – сокира), «вол-ла-чи» (*ant* – мураха) і «бе-ла-сана» (*apple* – яблуко). Для збільшення швидкості передачі деякі військові терміни визначалися одним словом. Найцікавіше у всій цій історії було те, що в мові «навахо» були відсутні військово-технічні терміни, яких там і бути не могло. Однак був придуманий дотепний вихід: неіснуючі в мові слова стали позначати за допомогою комбінації інших слів.

Слово	Мовою «навахо»	Дослівний переклад
Підводний човен	Беш-ло	Залізна риба
Головнокомандувач	Бих-ке-хе	Військовий лідер
Полковник	Атсах-беш-ге-лай	Срібний орел
Америка	Не-хе-мак	Наша мати
Китай	Цех-ехс-бесі	Косичка
Німеччина	Беш-бе-ча-хе	Залізна шапка
Японія	Бех-на-алі-тсосі	Косі очі
Росія	Сила-гол-чи-их	Червона армія
Літак-розвідник	Не-ас-джах	Сова
Есмінець	Ка-ло	Акула
Літак-винищувач	Да-хе-ті-хі	Птах грому
Взвод	Дебе-лі-зіне	Чорні вівці

У травні 1942 року перші 29 індіанців «навахо» прибули на спеціальну базу та зайнялася розробкою шифру. Їхнім основним завданням була передача бойової інформації та наказів по телефону та рації. Проведені іспити показали, що «навахо» могли зашифрувати, передати й розшифрувати 3-рядкове повідомлення англійською мовою за 20 секунд – у 90 разів швидше, ніж було потрібно машинам того часу.

У цілому, на тихоокеанському театрі військових дій проходило службу близько 400 індіанців-шифрувальників. Про це американською кінокомпанією «*Metro-Goldwyn-Mayer*» у 2002 році був знятий художній фільм «Ті, що говорять з вітром» (англ. *Windtalkers*). Їхнє вміння, швидкість і точність стали легендою,

тому й не дивно, що на їхню честь у місті Фенікс (штат Арізона) був встановлений пам'ятник, а Президент США Рональд Рейган оголосив 14 серпня Державним Днем радистів і шифрувальників «навахо».

6 вересня 1945 року, через чотири дні після закінчення Другої світової війни, військовим керівництвом було прийнято нове рішення, відповідно до якого «*SSA*» була цілком виведена з підпорядкування Начальника військ зв'язку та з 15 вересня разом з усіма своїми підрозділами та військовими установами зв'язку була реорганізована у Агенцію безпеки Армії «*ASA*» у складі Генерального штабу Військового департаменту США. Очолив її колега Фрідмена і криптолог Френк Роулет.

10 липня 1946 року всі підрозділи радіорозвідки та зв'язку ВМФ були об'єднані у 2-гу секцію 20-го відділу Управління зв'язку ВМФ «*Op-20-2*», яка була названа «Комунікаційною допоміжною діяльністю» (англ. *Communications Supplementary Activities of the 20th Division of the Office of Naval Communications, Section 2*). 23 червня 1948 року Військово-повітряні сили США також створили власну радіорозвідку - Групу безпеки «*AFSG*» (англ. *Air Force Security Group*), яку вже 20 жовтня перейменували у «*AFSS*» (англ. *Air Force Security Service*), яка повинна була займатися криптологічною діяльністю.

20 травня 1949 року військовим керівництвом США було прийняте рішення про об'єднання зусиль всіх військових радіорозвідок і криптослужб: «*ASA*», «*Op-20-2*» і «*AFSS*». В результаті була утворена об'єднана Агенція безпеки Збройних Сил «*AFSA*» у складі Міністерства оборони США, яку у 1951 році очолив генерал Ральф Джуліан Канін (1895-1969). Через рік, у 1952 році, коли «*AFSA*» була трансформована у Агенцію національної безпеки США, став її першим директором і знаходився на цій посаді до 1956 року.

2.9. Агенція національної безпеки

Агенція національної безпеки США (далі – АНБ) – *National Security Agency (NSA)* – датою свого народження зобов'язана Перл-Харбору. Після розслідування обставин раптового нападу Японії на США Конгрес порекомендував американському уряду створити централізовану криптологічну спецслужбу. Рекомендація була прийнята до уваги, і 24 жовтня 1952 року президент Гарі Трумен поставив свій підпис наприкінці семисторінкового меморандуму, відповідно до якого Агенція безпеки збройних сил поряд з аналогічними службами Військово-повітряних і Військово-морських сил увійшла до складу знову утвореного АНБ.

Утворення АНБ було суворо засекреченою інформацією. Аж до 1957 року про її існування взагалі не згадувалося в офіційних документах. Це дало привід жартів-

никам розшифровувати абревіатуру «*NSA*» як «*No Such Agency*» (Немає такої агенції), або «*Never Say Anything*» (Ніколи нічого не говори). Між собою співробітники АНБ жартівливо називають своє відомство «фабрикою печива» (англ. *cookie factory*). Лише в 1957 році у «Довіднику з урядових закладів США» уперше з'явився короткий опис Агенції в дуже розпливчастому формулюванні.

Через кілька років цей опис було злегка змінений та придбав стереотипну форму з трьох речень: «Агенція національної безпеки була створена в 1952 р. відповідно до директиви президента. Вона входить до складу Міністерства оборони, її діяльність направляється та контролюється міністром оборони. Агенція національної безпеки здійснює найвищою мірою спеціалізовані технічні та координаційні функції, пов'язані з національною безпекою».

Незважаючи на розпливчастість, цей опис абсолютно точний. Технічні функції АНБ складаються з перехоплення та криптоаналізу шифрованих повідомлень усіх держав, як дружніх, так і ворожих США. «Координаційні» функції містять у собі забезпечення безпеки зв'язку, тобто організацію, контроль і об'єднання зусиль усіх зацікавлених відомств (Міністерства оборони, Держдепартаменту, ЦРУ, ФБР тощо) в сфері розробки, виробництва й експлуатації засобів криптозахисту.

АНБ – ще більш мовчазна, таємна й похмура організація, ніж ЦРУ. Офіційні представники ЦРУ час від часу роблять заяви для засобів масової інформації, передають представникам преси сприятливу для себе інформацію. Офіційні особи з Агенції не займалися цим ніколи. Таким чином, АНБ залишається найбільш таємничою організацією серед американських спецслужб. Статут АНБ дотепер засекречений. Лише в 1984 році були віддані розголосу деякі його положення, з яких виявилося, що Агенція звільнена від всіх обмежень на ведення розвідки зв'язку.

В перші роки після свого утворення АНБ розміщалося в різних будинках, розкиданих по усьому Вашингтону. У 1954 році Міністерство оборони США уклало контракт на будівництво для АНБ спеціального великого будинку у Форт-Міді (штат Меріленд). Будівництво було в основному закінчено восени 1957 року, але тільки на початку наступного року новосілля справили останні співробітники АНБ.

І хоча цей «храм криптоаналізу», безсумнівно, став найграндіознішим із коли-небудь, побудованих для його «жреців», він виявився для них занадто малим

уже через п'ять років. Тому наприкінці 1965 року до нього був прибудований ще один дев'ятиповерховий корпус. Розширення було викликано небачено швидким ростом чисельності співробітників АНБ.

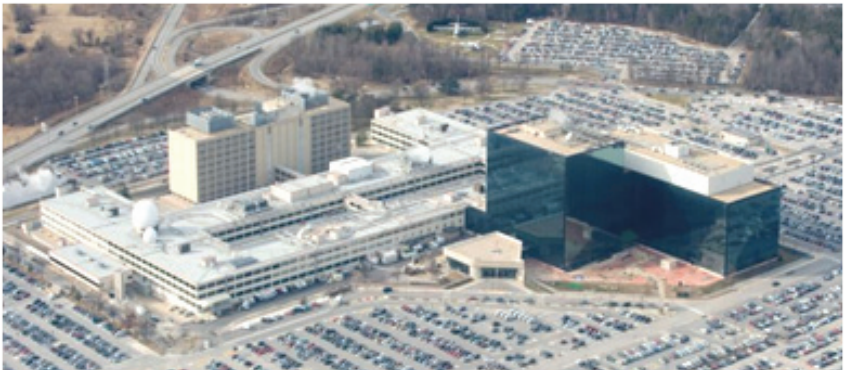
Як уже було сказано, АНБ займається радіоелектронною розвідкою та обробкою зібраної інформації, передачею отриманих даних зацікавленим відомствам для нестатків зовнішньої розвідки та контррозвідки, наданням розвідувальної підтримки операціям американських збройних сил, а також проведення наукових досліджень і впровадження розробок у сфері електронної розвідки.

З метою забезпечення доступу до телеграм, що пересилалися каналами зв'язку найбільших комерційних телекомунікаційних компаній США, з 1952 по 1975 роки в АНБ був запроваджений проект «Шемрок» (англ. *Shamrock* – трилистник). Одночасно з метою обмеження поширення інформації про те, що АНБ займається зібранням та обробкою інформації конфіденційного характеру, з 1969 по 1973 роки у США здійснювався комплекс заходів згідно з проектом «Мінарет» (англ. *Minaret* - ісламська башта).

Друга група завдань, що покладені на АНБ, пов'язана з виконанням контррозвідувальних функцій. Це забезпечення безпеки ліній секретного зв'язку, ведення зовнішнього шифролистування, розробка кодів і шифрів для передачі таємної інформації і спеціального устаткування зв'язку.

У 1978 році з метою забезпечення нагляду за діяльністю АНБ з боку американських правоохоронних органів у США був введений у дію Закон про контроль за збором розвідувальної інформації про закордонні країни (англ. *Foreign Intelligence Surveillance Act*). На його виконання були створені Судова інстанція (англ. *Foreign Intelligence Surveillance Court*) та Апеляційна судова інстанція з контролю за збором розвідувальної інформації про закордонні країни (англ. *Foreign Intelligence Surveillance Appeals Court*).

За своїм статусом АНБ є «особливою агенцією у складі Міністерства обо-



рони». Однак було б неправильно розглядати її як один з підрозділів американського військового відомства. Незважаючи на те, що АНБ організаційно входить у структуру Міністерства оборони, вона є при цьому самостійним членом Розвідувального співтовариства США.

Директор АНБ за своїм статусом повинен бути військовослужбовцем у званні тризіркового генерала (тобто, генерал-лейтенанта) або віце-адмірала, який раніше працював у розвідці. Він підпорядковується Міністру оборони та представляє АНБ у Розвідувальному співтоваристві США. Станом на кінець 70-х років структура АНБ виглядала таким чином. Найбільш важливими її підрозділами були Управління радіорозвідувальних операцій, безпеки інформаційних систем та наукових досліджень і техніки.

Управління безпеки інформаційних систем (англ. *Information Systems Security Directorate*) відомо також як організація «*S*». Воно постачає шифрувальне устаткування для всіх державних установ США (у 1993 році контракти АНБ тільки у штаті Меріленд оцінювалися в 700 мільйонів доларів), а також установлює процедури захисту ліній зв'язку для усіх відомств, що входять у Розвідувальне співтовариство США.

Це Управління складається з таких груп:

- група «*K*» - керує криптологічною роботою АНБ, надаючи теоретичну й іншу підтримку роботам із захисту ліній зв'язку Уряду США і перехопленню інформації з каналів зв'язку інших країн;
- група «*T*» - керує всіма роботами, що виконуються в сфері проектування, розробки, впровадження й експлуатації спеціальних комунікаційних розвідувальних мереж і систем, призначених для передачі даних, що збираються підрозділами технічної розвідки;
- група «*I*» - розробляє, впроваджує і контролює різні програми в сфері інформаційної безпеки, державної таємниці, організації та забезпечення режиму;
- група «*S*» - розробляє та впроваджує різні стандарти в сфері інформаційної безпеки, захисту державної таємниці, організації та забезпечення режиму, а також контролює їхнє дотримання. Група керує програмою забезпечення режиму на виробництві, займаючись експертизами і видачею дозволів при виконанні робіт, зв'язаних з державною таємницею. Вона також представляє інтереси уряду США при узгодженні контрактів, а також у різних технічних радах. Ця група здійснює контроль дотримання режиму за контрактами, пов'язаними з державною таємницею. Саме на цю групу покладається основне навантаження по розробці і сертифікації устаткування та процедур, що використовується для захисту комунікацій;
- група «*V*» - група розробляє, впроваджує та контролює різні програми в сфері безпеки комунікаційних мереж, а також відповідних виробничих питань.

Управління наукових досліджень і техніки, як виявляється з його назви,

зайнято різноманітними науково-технічними дослідженнями в сфері перехоплення радіосигналів, дешифрування та захисту ліній зв'язку, починаючи від математичних методів та закінчуючи розробкою нових технологічних процесів і устаткування. Управління складається з чотирьох відділів:

- математичних досліджень - займається математичними методами криптоаналізу;
- апаратури перехоплення (англ. *Intercept Equipment Division*) - розробляє устаткування для перехоплення й аналізу радіосигналів;
- криптографічного устаткування - розробляє нові види шифрувальної апаратури, яка потім запускається у виробництво Управлінням захисту комунікацій;
- комп'ютерної техніки - займається дослідженнями в сфері електронно-обчислювальної техніки.

Директор АНБ одночасно очолює і Центральну службу безпеки (англ. *Central Security Service, CSS*). При цьому, якщо сама АНБ виглядає надсекретною організацією, то «*CSS*» є надтаємною «у квадраті». Створена в 1972 році указом президента, «*CSS*» відповідає за криптоаналіз і криптобезпеку. Перед «*CSS*» стоять дві задачі: дешифрування іноземних кодів і шифрування офіційних матеріалів, що передаються засобами зв'язку. Як керівник «*CSS*» директор АНБ контролює дії підрозділів радіоелектронної розвідки армії, авіації та флоту.

Шифрувальні служби, що входять до складу видів і родів військ, із усіх питань, пов'язаних з відповідною діяльністю, підпорядковуються безпосередньо «*CSS*». При виконанні окремих завдань в оперативне підпорядкування «*CSS*» можуть передаватися й інші підрозділи МО, зайняті радіотехнічною розвідкою та перехопленням.

До складу «*CSS*» входять такі підрозділи:

- командування з розвідки та безпеки Армії США (англ. *Army Intelligence & Security Command, INSCOM*);
- командування групи безпеки ВМС (англ. *Naval Security Group Command*);

🗝 управління розвідки ВПС (англ. *Air Intelligence Agency*).

Підготовка кадрів для АНБ здійснюється в Національній школі криптології. Ця школа готує кадри не тільки для АНБ, але й для декількох інших підрозділів Міністерства оборони. Крім того, АНБ оплачує навчання своїх співробітників у провідних коледжах і університетах США, а деяких з них направляє у військові коледжі Міністерства оборони. Подібно багатьом спецслужбам світу, АНБ має власний музей — Національний музей криптології, розташований у колишньому мотелі неподалік від штаб-квартири Агенції.

Чисельність персоналу на об'єктах АНБ, включаючи прикомандированих військовослужбовців усіх видів збройних сил перевищує 120 тисяч осіб. При цьому 20-24 тисячі з них працюють у центральному апараті АНБ, інші ж, в основному військовослужбовці, – працюють на базах і станціях АНБ по усьому світі. Кількість таких об'єктів, за різними даними, – сьогодні понад 4 тисячі. Таким чином, з погляду чисельності співробітників, АНБ, безсумнівно, є найбільшою серед американських спецслужб.

Незважаючи на те, що формально АНБ підпорядковується Міністерству оборони, по суті ця організація має скоріше цивільний характер. Цивільні фахівці, що приходять на службу в АНБ, зобов'язані підкорятися суворому розпорядку цієї «закритої» установи. Щоб не бовкнути випадково таємну інформацію під наркозом, вони навіть ходять до «свого» перевіреного службою безпеки АНБ дантиста. Існують обмеження щодо виїзду закордон. У випадку одруження (або заміжжя) кого-небудь зі співробітників АНБ або його родичів з іноземним громадянином необхідно доповідати про це керівництву Агенції.

Протягом багатьох років співробітники АНБ не мали права розголошувати місце своєї служби — у відповідь на всі питання про те, де вони працюють, вони повинні були відповідати: «на федеральний уряд» або «у Міністерстві оборони». Навіть, сьогодні колишнім співробітникам АНБ заборонено писати мемуари або ділитися спогадами про свою роботу. Кількість же книг, що вийшли в США та присвячені АНБ, можна буквально перерахувати по пальцях. Надання гласності офіційних даних про Агенцію (бюджет, чисельність персоналу, структура) заборонено законом.

У відношенні вільнонайманих в АНБ діють найсуворіші критерії підбору. Майбутній співробітник повинен пройти всеосяжну перевірку, що включає тест на детекторі неправди. Потім його можуть прийняти для участі в програмі навчання, але остаточне оформлення на роботу відбувається тільки після скрупульозного вивчення його особистої справи. Обов'язково буде перевірений час і місце народження, освіта та послужний список. Друзям, сусідам, товаришам з попередньої служби та роботодавцям будуть задані питання щодо того, чи заслуговує кандидат довіри та наскільки зрілим є його поводження. Буде проведений аналіз його кредитоспроможності, а також послані запити на предмет можливої причетності до підривних організацій. Але навіть після проходження всіх цих перевірок і остаточного оформлення на роботу всі

співробітники АНБ регулярно піддаються новим перевіркам кожні чотири роки. Це потрібно для підтвердження дозволу на їхній доступ до таємних документів.

Співробітники АНБ працюють таким чином: якщо вони одержують кілька примірників того самого повідомлення, перехопленого різними радіостанціями, редактори намагаються усунути всі наявні в ньому перекручування. Потім криптоаналітики порівнюють і зіставляють місцезнаходження відправників і одержувачів повідомлень, маршрути їхнього проходження та службові позначки з метою інформування шифрувальників і операторів зв'язку. Це дозволяє відсортувати перехоплені повідомлення за принципом приналежності до однакових шифросистем. А вивчаючи картину листування у всій його повноті, можна виявити загальну структуру мережі зв'язку та одержати іншу корисну інформацію.

Криптоаналітики працюють групами. Складні сучасні шифри залишили роботу талановитих одинаків у минулому. Керівник групи тепер розподіляє завдання між підлеглими, проводить наради, вирішує, який саме метод є більш продуктивним.

Робота окремо взятого криптоаналітика в складі групи полягає у відшукуванні закономірностей, що дають значні відхилення від випадкового тексту. Ці закономірності часом дуже важко визначити, і трапляється, що окремі букви, у яких вони виявляються, повторюються через дуже великі інтервали. Тільки величезна кількість тексту може зробити ці закономірності помітними. І тільки наймогутніші суперкомп'ютери можуть поглинути потоки букв і перевірити немислиму кількість можливостей, щоб відшукати відкритий текст криптограми в реально припустимий проміжок часу, тобто до того, як вона втратить свою актуальність.

АНБ має дуже великий парк комп'ютерного устаткування порівняно з будь-якою іншою подібною установою у світі. Однак здобути повну перемогу в нескінченній боротьбі з шифрами за допомогою комп'ютера американським криптоаналітикам повною мірою так і не вдалося, оскільки теорія шифрувальної справи «йде в ногу» з досягненнями криптоаналізу. Також не виходить цілком автоматизувати працю криптоаналітика. Комп'ютер зміг тільки звільнити його від стомлюючої монотонної роботи. У криптоаналізі усе ще є багато можливостей для реалізації інтуїції, досвіду й індивідуальної обдарованості. Комп'ютери є лише знаряддями праці криптоаналітиків, а не їх заміною.

Як повідомили агенти радянської розвідки Мартін і Мітчел на прес-конференції у Москві в 1960 році, АНБ домоглося успіхів у «розкритті» шифрів багатьох країн світу. Агенція читала шифролистування більше 50 держав, у тому числі і ряду своїх союзників, що полегшувало США ведення переговорів з політичних, економічних, військових і інших проблем. Серед цих країн були Італія, Туреччина, Франція, Югославія, Єгипет, Індонезія, Уругвай.

АНБ, як і аналогічні спецслужби в інших країнах, активно користувалася допомогою інших спецслужб, зокрема ЦРУ і ФБР, у тих випадках, коли зіштовхува-

лася з незнайомим шифром, що вводився заново в яких-небудь державах. Так, у 1982 році, коли АНБ треба було добути французькі шифри, ЦРУ завербувало французького розвідника, який працював у посольстві Франції у Вашингтоні. За його допомогою агенти ФБР проникли в це посольство, вилучили та скопіювали всі шифрувальні документи та потім повернули їх на місце, не залишивши ніяких слідів. Таким чином АНБ одержала ключі до французьких шифрів.

Під час Фолклендської війни з Аргентиною в 1982 році АНБ розкрила аргентинський код, що дозволило постачати Англію важливою актуальною військовою інформацією.

Найважливіша проблема, що завжди стояла та стоїть перед професіоналами АНБ, – це розшифрування секретних кодів іноземних держав, насамперед радянських (а тепер – російських) дипломатичних представництв і органів військового управління. В американській пресі приводився факт, що звичайна шифрувальна система має близько 70 квадрильйонів (тобто, 7x1016) ключів. Персональний комп'ютер здатний перевірити 100 тисяч ключів у секунду, а для перевірки всіх можливих ключів йому буде потрібно 22652 роки. Суперкомп'ютери АНБ здатні здійснити цю операцію за кілька секунд.

Бюджет АНБ, як і інших спецслужб США, у даний час засекречений. Більш того, на відміну від ЦРУ або ФБР, він ніколи і не розсекречувався. Щодо його величини існують різні оцінки. Американська «Енциклопедія шпигунства» повідомляє, що «це цифра порядку трьох з половиною мільярдів доларів, не рахуючи обслуговування космічних супутників-шпигунів». Однак за іншими оцінками, бюджет АНБ складає близько 15 мільярдів доларів. У будь-якому випадку, всупереч розповсюдженій омані, саме АНБ, а не ЦРУ є найбільш фінансованою спецслужбою США.

АНБ, чисельність співробітників якої зараз складає близько 40 тисяч чоловік, напружено працює над тим, щоб засоби захисту інформації, які використовуються урядом США, зовсім не піддавалися злому. Агенція не шкодує грошей на сучасні криптологічні заходи та засоби щодо забезпечення секретного зв'язку.

АНБ розробляє рекомендації і стандарти з інформаційної безпеки та «закриття» технічних каналів витоку інформації з використанням побічних електромагнітних випромінювань і наведень (ПЕМВН) у власній країні. Одним з таких стандартів є серія нормативних документів з описом технічних умов експлуатації радіоелектронних пристроїв під абревіатурою «*TEMPEST*» (англ. Transient Electromagnetic Pulse Emanation Standard - стандарт на побічні електромагнітні імпульсні випромінювання).

Усі комп'ютери, на яких обробляється інформація у вищому ешелоні державного та військового керування США, мають захист від випромінювання за стандартом «*TEMPEST*». Цей же стандарт використовується для захисту найважливіших радіоелектронних систем від електромагнітного імпульсу, джерелом якого можуть бути

атмосферні електричні розряди як природного (грозового), так і штучного (від ядерного вибуху) походження.

АНБ постійно удосконалює національні криптографічні алгоритми, залучаючи для цього у відкритих конкурсах кращих фахівців у всьому світі. Прикладом такого міжнародного проекту був конкурс на розробку нового стандарту для так званої комерційної криптології «*AES*» (англ. *Advanced Encryption Standard*), переможцем у якому за підсумками двох раундів протягом чотирьох років серед 15 алгоритмів став бельгійський шифр «*Rijndalen*».

Уперше за всю сучасну історію криптології американці пішли на безпрецедентний крок, допустивши до участі в конкурсі на національний стандарт іноземних фахівців. Утім, у цьому немає нічого дивного, якщо взяти до уваги той факт, що Бельгія є союзником США по НАТО, і, крім того, однією з умов конкурсу була повна прозорість алгоритму з погляду математичних операцій, а також відсутність патенту на його винахід у США. Кращою нагородою та рекламою переможцям стали відгуки провідних криптоаналітиків АНБ, що перевіряли стійкість алгоритму на суперкомп'ютерах з використанням спеціальних математичних методів аналізу.

Важливим завданням АНБ є розробка нових видів шифрувальної техніки передачі даних та апаратури засекречування телефонних розмов. Першою шифромашиною, яка розроблялася як стандартна для всіх частин Збройних сил США з використанням електронних ламп і працювала зі стрічковими букводрукувальними апаратами, була електромеханічна 8-роторна машина «*KL-7*». У 1952 році вона була введена в експлуатацію в Армії, ВМФ і ВПС. «*KL-7*» також була відома як «*ADONIS*» (на вищому рівні) і «*POLLUX*» (на нижчому рівні) та широко застосовувалася у Збройних силах до середини 1960-х років. Її також використовували деякі країни-учасники НАТО, поки вона не була виведена з експлуатації у 1983 році.

Однак початок розробки цієї машини, названої тоді «*MX-507*», була ініційована «*ASA*» ще у 1945 році з метою заміни машин «*SIGABA/ECM*» і «*M-209*». З 1949 року над її розвитком продовжила роботу «*AFSA*», яка перейменувала машину у «*AFSAM-7*» (англ. *Armed Forces Security Agency Machine № 7*). На початку 1960-х років вона отримала уніфіковану назву «*TSEC/KL-7*» розроблених АНБ серії криптопристроїв «*TSEC*» (англ. *Telecommunications Security*). Перша буква в назві машини після черти позначала функцію пристрою: «*K*»

- криптологічна, «*H*» - криптологічна допоміжна, а друга - тип: «*G*» - генерація ключа, «*L*» - преобразування букв, «*O*» - багатоцільовий, «*W*» - телетайп, «*Y*» - розмова тощо.

У 1957 році новий електронний лінійний шифратор «*TSEC/KW-26*» був побудований на магнітній базовій логіці та працював з телетайпами рулонного типу на швидкості 74,2 бод. Машин «*KW-26*», також відомих як «*ROMULUS*», було побудовано з початку 1960-х років приблизно 14 тисяч для використання Збройними силами, Агенцією захисту комунікацій, Держдепартаментом і ЦРУ. Починаючи з середини 1980-х років, система «*KW-26*» була виведена з експлуатації та замінена цифровою системою шифрування «*TSEC/KG-84*», також відомою як «*Tri-Tac*». Вона, наприклад, входила до складу автоматизованого безпечного робочого місця «*ST-2000*» та забезпечувала шифрування даних і мови. Для цього до «*KG-84*» підключались такі захищені пристрої, як факсиміле, телефон, швидкісні принтери та модеми.

У 1950-х роках АНБ була розроблена система «*TSEC/KW-37*», відома також як «*JASON*», для захисту радіомереж ВМФ. Морська доктрина зобов'язувала військові кораблі у відкритому морі підтримувати радіомовчання як можна довше, щоб виключити можливість бути знайденими потенційним супротивником. Щоб кораблі отримували повідомлення та накази, штаб ВМФ передавав по радіо безперервний потік інформації

спочатку азбукою Морзе, а пізніше використовуючи радіотелетайп. Повідомлення передавались у цьому потоці та могли призначатися як для конкретних суден, так і для бойових груп або флоту у цілому. Радіорубка кожного судна постійно контролювала ефір та розшифровувала тільки ті повідомлення, які стосувались тільки свого судна. З метою автоматизації цього процесу була розроблена система «*KW-37*», яка складалася з двох головних компонентів: приймача «*KWR-37*», який встановлювався на судні, і передавача «*KWT-37*», який встановлювався на узбережжі. Наприкінці 1980-х років на заміну «*KW-37*» прийшла «*KW-46*», а експлуатація «*KW-37*» була припинена у 1990-х роках. «*KW-46*» мала кодову назву «*Vallor*» і складалася з таких же компонентів, як і «*KW-37*».

У 1960-х АНБ здійснило розробку апаратури дуплексного широкосмугового телефонного засекречування «*TSEC/KY-3*», яка мала розмір невеликого холодильника. Її використовували Збройні сили та уряд сполучених штатів з середини 1960-х до кінця 1980-х років.

Наприкінці 1960-х років АНБ розпочало проектування та розробку сімейства телефонних модулів безпеки «*STU*» (англ. *Secure Telephone Unit*) - пристроїв шифрування голосового зв'язку. Проблему розмовної якості вирішило використання системи кодування «*LPC*» (англ. *Linear Predictive Coding*) і алгоритма кодування «*SAVILLE*», що дуже поліпшило розмовну якість у вузькосмугових системах. Проблема розповсюдження ключів була вирішена створенням відповідних центрів «*KDC*» (англ. *Key Distribution Center*).

Перше покоління «*STU-I*» було дуплексною системою широкосмугового телефонного засекречування, також відомою як апарат засекречування

«*TSEC/KY-70*», з відносно хорошою розмовною якістю та швидкістю передачі даних 2,4 або 4,8 кбіт/сек. Вона була введена АНБ в дію у 1977 році з метою заміни громіздкого апарата засекречування «*KY-3*». Виробництво «*STU-I*» закінчилося вже у 1979 році, оскільки розмір і ціна обладнання (35 тисяч доларів) були дуже великими
.

Негайно після введення в дію «*STU-I*» АНБ розпочало створювати 2-е покоління системи «*STU-II*», що передбачало зменшення розміру та ціни обладнання. В результаті проведеної АНБ роботи «*STU-II*» стала дійсно дешевше - 13 тисяч доларів, але була все ще дорожче, ніж проектувалося (до 5 тисяч доларів). До того ж, система була все ще великою і громіздкою, для якої необхідно було використовувати окреме велике приміщення. У 1980 році розробка «*STU-II*» була завершена та запущена у виробництво. У період з 1982 по 1986 роки було вироблено приблизно 10 тисяч апаратів «*STU-II*», також відомоого як апарат засекречування «*TSEC/KY-71*».

Наступне покоління шифрувальної техніки та апаратури засекречування розвивалося протягом 1980-х років і було засноване на транзисторній логіці з використанням інтегральних схем. У 1984 році АНБ розпочало прискорену програму вдосконалення голосових шифраторів «*FSVS*» (англ. *Future Secure Voice System*), націлену на підвищення безпеки зв'язку та покращення якості мови. Вироблені у той час пристрої були значно меншими та використовували швидші і стійкіші криптографічні алгоритми. Ключі завантажувалися в апаратуру за допомогою спеціального ввідного пристрою. Спочатку вони розповсюджувалися на паперовій перфострічці, яку перед записом в апарат протягували через пристрій зчитування інформації «*KOI-18*», але пізніше перфострічку замінили електронні ключові пристрої «*KYK-13*».

У 1984 році АНБ розпочала розробку третього покоління «*STU-III*», що дозволяло здійснювати переговори з грифом обмеження «цілком таємно». Нова система була завершена у 1987 році, запущена у виробництво та вироблялася до середини 2000-х років. За розмірами та формою цей модуль мав вигляд звичайного телефонного апарату, та міг бути використаний, як і звичайний несекретний телефон. Відмінність полягала в наявності змінного ключового модуля пам'яті «*KSD-64A*» (англ. *Key Storage Device*), при підключенні якого ставало можливим безпечне, тобто засекречене, з'єднання, а також електронної систе-

ми управління ключами «*EKMS*» (англ. *Electronic Key Management System*).

Пристрій «*KSD-64A*», що за формою нагадував ключ, містив електронний чіп «*EEPROM*» (англ. *Electronically Erasable Programmable Read Only Memory* - електронна пам'ять для зчитування, що стирається та програмується), який міг зберігати 64 кілобіт інформації. Пристрій треба було вставити як ключ в спеціальний отвір «*STU-III*» і повернути, щоб чіп увійшов до контакту з електронними компонентами апарату. Більшість моделей «*STU-III*» також мали порт «*RS-232*» для безпечної передачі даних і факсів, тобто крім передачі мови могли бути використані для передачі зашифрованих даних по модемному каналу.

«*STU-III*» вироблялися такими компаніями, як «*AT&T*», «*RCA*» і «*Motorola*», для використання урядом Сполучених Штатів і їх союзниками. Сама система була заснована на криптографії з відкритими ключами. Більшість апаратів, яка вироблялася компанією «*Motorola*», мала назву «*SECTEL*» (англ. *Secure Telephone*), вигляд звичайного телефонного апарату, ціну 2 тисячі доларів та забезпечувала швидкість передачі даних до 9,6 кбіт/сек. На протязі 1990-х років апарати «*STU-II*» на території США були замінені маленькими та дешевими апаратами «*STU-III*».

Близько 400 тисяч апаратів «*STU-III*» було виготовлено станом на 1994 рік та багато хто все ще використовував їх у 2000-х роках. 31 грудня 2009 року став останнім днем використання системи «*STU-III*», після чого вона була виведена з експлуатації. Їй на заміну прийшло сучасніше обладнання «*STE*» (англ. *Secure Terminal Equipment*), що працює по лініях «*ISDN*». Нова система подолала багато проблем «*STU-III*», включаючи 15-секундну затримку та низьку швидкість передачі даних (128 замість 9,6 кбіт/сек).

Також АНБ багато уваги приділяє роботі з особовим складом із питань конспірації та пильності. Причому робиться це з нещадною наполегливістю доти, поки конспірація та пильність не стане для них більш ніж звичкою, більш ніж другою натурою, поки вона не трансформується в «основний інстинкт». Співробітники АНБ ніколи не розповідають своїм дружинам і дітям, що являє собою їхня робота. Однак, незважаючи на всі запобіжні заходи, АНБ виявилося причетним до найскандальніших провалів в історії американських спецслужб.

Перший провал АНБ був пов'язаний з Джозефом Петерсеном, коли 9 жовтня 1954 року на перших шпальтах двох найбільших щоденних газет було опубліковане повідомлення про його арешт за крадіжку таємних документів з АНБ. 39-літній

Петерсен вивчав криптоаналіз на заочних військових курсах у 1940—1941 роках, а потім був прийнятий на службу в армійську дешифрувальну службу. Після війни за власною ініціативою Петерсен зайнявся викладанням криптоаналізу на курсах підвищення кваліфікації Міністерства оборони. У 1953 році розроблена ним програма навчання стала базовою в АНБ. Після затримання Петерсен сказав у своє виправдання, що взяв усього два таємні документи для підготовки до проведення занять.

Під час слідства з'ясувалося, що у роки Другої світової війни Петерсен подружився з полковником Феркуілом, одним із кращих голландських криптоаналітиків. Разом із Феркуілом Петерсен займався розкриттям японського дипломатичного коду. У цій сфері у Феркуіла був значний досвід, набутий ним ще до війни. Через Феркуіла Петерсен познайомився з Джакомо Стуітом, офіцером зв'язку голландського посольства.

Після війни, коли Феркуіл повернувся зі США назад до Голландії, у своїх листах Петерсен ділився з ним методами викладання криптоаналізу, а також повідомляв інші деталі, що, на його думку, корисно було знати при створенні в Голландії власної криптоаналітичної спецслужби. Разом з тим, Стуіт працював в Америці, і Петерсен також підтримував з ним дружні стосунки.

У той час для захисту свого дипломатичного листування голландці застосовували шифромашини швейцарської фірми «Хагелін». У 1948 році Петерсен зняв копії з двох таємних документів, у яких говорилося про успіхи американців з розкриття голландських шифромашин. Крім того, він додав до цих копій оригінал ще одного документа за назвою «Криптоаналіз шифромашини «*B-211*» фірми «Хагелін» і показав їх Стуіту. Феркуіл вважав, що Петерсен не мав жодного наміру завдати шкоди Сполученим Штатам, а просто намагався допомогти своїм друзям захистити батьківщину від зазіхань інших держав.

Восени 1954 року під час обшуку квартири Петерсена співробітники ФБР знайшли обидві копії й оригінал. Це був перший серйозний випадок порушення закону співробітником АНБ. Імовірно, саме тому Міністерство юстиції та Міністерство оборони прийняли рішення передати справу до суду, замість того, щоб вирішити питання в адміністративному порядку всередині АНБ. Мабуть, вони хотіли зробити справу Петерсена показовою. Але, як сказав його адвокат, «прийнявши таке рішення, вони вскочили у халепу», тому що арешт набув занадто широкого розголосу в американській пресі.

На суді Петерсон визнав себе винним і отримав 7 років ув'язнення. Таким чином, АНБ вдалося довести до своїх співробітників – потенційних правопорушників, що розголос таємної інформації з криптологічних питань буде завжди суворо покараний.

Новий скандал, пов'язаний з діяльністю АНБ, розгорівся в США 15 грудня 2005 року, коли газета «*The New York Times*» опублікувала матеріал про те, що Джордж Буш дозволив після скоєння терактів 11 вересня прослухувати американських громадян з метою боротьби з тероризмом. Президент дозволив АНБ вести стеження за

будь-якою людиною, що знаходиться на території країни, без санкції судових органів. Відповідне розпорядження Буш підписав у 2002 році, дозволивши Агенції прослуховувати міжнародні телефонні переговори, а також читати повідомлення, що розсилаються електронною поштою. Агенція могла тримати «на мушці» від п'яти до семи тисяч підозрюваних у терористичній діяльності одночасно.

АНБ в обхід американських законів схилило фірму «*AT&T*» установити на вузлах її інфаструктури спеціальні відводи для тотального контролю розвідки за телефонними лініями та мережним трафіком. Головним доводом щодо захисту цих дій, коли таємне стало явним, була «турбота про загальну безпеку». Мовляв, навколо багато терористів, що виношують свої терористичні плани, а захистити від них громадян держава може лише взявши під повний контроль усі телефонні розмови та мережні комунікації...

Зрозуміло, що настільки вільне й широке трактування державою своїх повноважень викликає (принаймні, у США) у багатьох людей протести, через що «*AT&T*» сьогодні змушена відбиватися в судах від серйозних позовів, у яких компанію обвинувачують у протизаконному стеженні. Хоча ініціатива виходила зовсім не від «*AT&T*», її схилили до таємної і широкомасштабної шпигунської операції заради «загального блага».

17 січня 2005 року Американський союз громадянських свобод і Центр захисту конституційних прав подали в суд на президента США Джорджа Буша з вимогою припинити прослухувати американських громадян без санкції суду. Американське законодавство згідно «*FISA*» (англ. *Foreign Intelligence Surveillance Act of 1978* - акт 1978 року про закордонне розвідувальне спостереження) допускає прослуховування телефонних розмов без санкції суду тільки протягом 48 годин. Тим часом, законом 1978 року був створений спеціальний суд «*FISA*», який у разі потреби видавав санкцію на прослуховування протягом декількох годин. Насправді закон дозволяє уряду почати прослуховування, а потім у судовому порядку одержати санкцію заднім числом. З 1979 року суд «*FISA*» задовольнив десятки тисяч запитів на прослуховування, а відхилив всього чотири.

У січні 2006 року Джордж Буш під час відвідування штаб-квартири АНБ заявив, що він на «усі сто відсотків» підтримує надсекретну роботу співробітників АНБ. Підкресливши, що більшість досягнень АНБ залишаються таємницею, Буш назвав електронну розвідку, що здійснює Агенція, «життєво важливою» для США у війні з тероризмом. При цьому він знову виступив у захист програми прослуховування телефонних переговорів, що у рамках боротьби з тероризмом АНБ здійснює з дозволу «Білого дому», у тому числі на території США.

2.10. Мережі спеціального зв'язку США

У 1960-і роки Міністерство оборони США (далі – МО) стало фінансувати організа-

цію, що займалася найсучаснішими та перспективними дослідженнями – Управління перспективних досліджень «*DARPA*» (англ. *Defense Advanced Research Projects Agency*), і одне з завдань, що стояли перед Управлінням, полягало у тому, щоб знайти спосіб об'єднати комп'ютери військового призначення, що знаходилися на значних відстанях один від одного. Це дозволило б у випадку пошкодження або виходу з ладу якого-небудь комп'ютера передати завдання, що ним вирішувались, іншому комп'ютеру в мережі. Основною метою було створення більш надійної і стійкої до ядерного удару інфраструктури наявних у Пентагоні комп'ютерів, але ця мережа також дозволила б ученим пересилати один одному повідомлення та виконувати обчислення, використовуючи резервні потужності вилучених комп'ютерів. Мережа «*ARPANet*» була створена в 1969 році, а у 1982 році на її основі з'явилася мережа передачі даних «Інтернет» (англ. *Internet* від *Internet-working* - міжмережевий обмін).

Розвитку й удосконаленню систем спеціального зв'язку військове керівництво США приділяло дуже пильну увагу. За оцінкою американських військових фахівців, проведення робіт у даному напрямку протягом двох-трьох років еквівалентно включенню до складу угруповань Збройних Сил (далі – ЗС) від 15 до 20 дивізій. Основна мета цих робіт (у сухопутних військах) – оснащення штабів і пунктів керування засобами автоматизації й удосконалення систем зв'язку для передачі великих обсягів інформації в автоматичній системі керування військами, а також підвищення стійкості, скритності й безперервності їхнього керування.

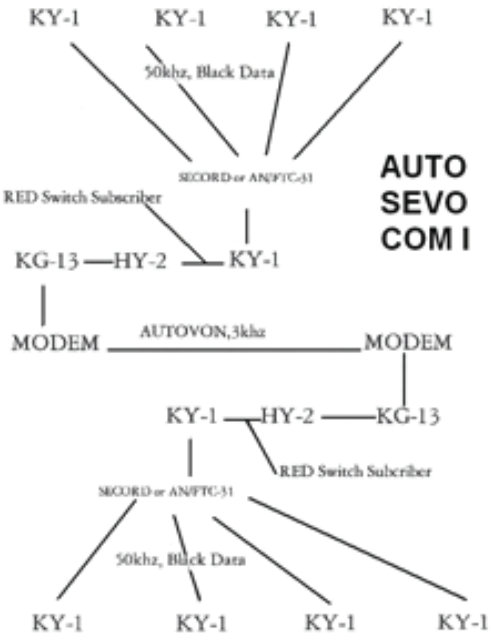
У середині 1960-х років американським урядом було прийняте рішення про створення захищеної системи передачі мовної інформації «*Autosevocom*» (англ. *Automatic Secure Voice Communications*). Армійська частина цієї системи була передана командуванню стратегічних комунікацій Армії США (*USASCC*), чия штаб-квартира знаходиться у Форті Хуачука у штаті Арізона. Підлегла йому 7-а Сигнальна команда Армії США, чия штаб-квартира знаходиться у Форті Річі у штаті Меріленд, відповідає за всі комунікації армії США в континентальних Сполучених Штатах (*CONUS*).

Кожен форт армії або об'єкт США має Управління телекомунікацій (англ. *Post Signal Office*), що відповідає за функціонування усіх видів телефонного зв'язку, радіозв'язку, комунікаційного центру тощо.

У липні 1967 року на території Штатів була утворена мережа «*Autosevocom-1*». До її складу входили вузькополосні (*NBST*) і широкополосні (*WBST*) абонентські термінали, а також вузькополосний транкінговий прилад (*NBTU*). До складу абонентського термінала мережі «*Autosevocom I*» входило таке устаткування:

- *TSEC/KY-1 - Wideband* (50 кГц) - напівдуплексна апаратура засекречування, захована в металевому сейфі;
- *TSEC/HY-2 - VOCODER* - мовний аналого-цифровий перетворювач;
- *TSEC/KG-13 - Key Generator* - генератор ключа, пристрій шифрування й сполучення з лінією;
- *SECORD - Secure Cord Board* - настільна шнурова панель ручного обслуговування;
- *AN/FTC-31 - Automatic Telephone Switch* - автоматичний телефонний комутатор;
- *RED Telephone Switches* - пристрій підключення телефонів.

Мережа «*Autosevocom I*» дозволяла абонентам обговорювати таємну або конфіденційну інформацію по телефону. Однак недостатня розбірливість мови, низька швидкість обслуговування, складність проведення телефонних конференцій й забезпечення заходів із безпеки підштовхнули чиновників США схвалити розробку у травні 1976 року удосконаленої системи «*Autosevocom II*» та призначити Армію відповідальною за її розробку. У системі «*Autosevocom II*», що вводилась в експлуатацію у період з 1980 по 1985 рік, були використані нові технологічні досягнення та високоякісне устаткування зв'язку для декількох тисяч абонентів. Зокрема, пристрої «*KY-1*» і «*HY-2*» були замінені на більш сучасні пристрої «*KY-3*» і «*HY-11*» тощо.

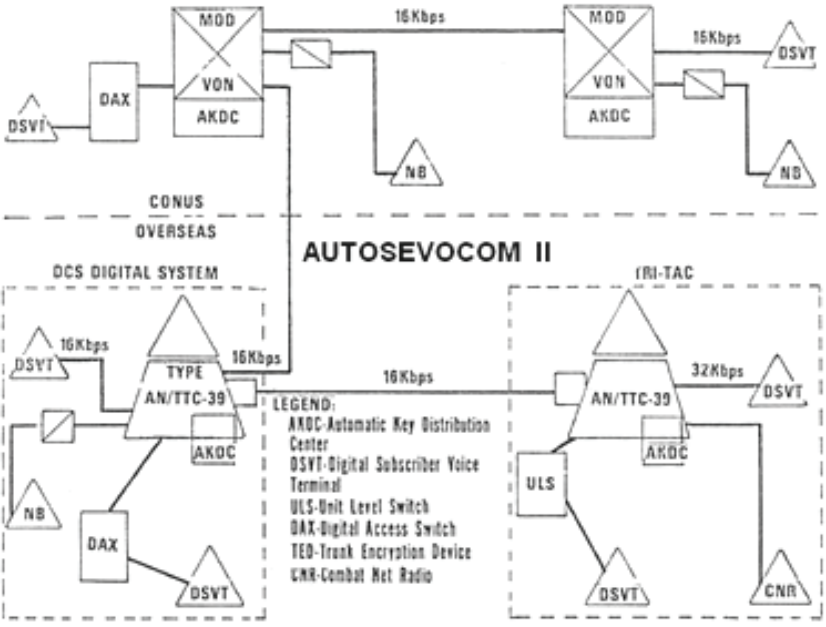


Однак система «*Autosevocom*», 1850 терміналів

якої вже було встановлено, виявилася дуже дорогою та незручною, тому в кінці кінців МО відмовилося від неї. Останній комутатор «*Secord/Autosevocom*» був вимкнений у Пентагоні в 1994 році. Єдиною захищеною мережею на сьогоднішній день залишається мережа «*Red Switch*», що з'єднує між собою командні пункти ЗС.

Для передачі службових повідомлень МО у 1960-х роках була створена багаторівнева захищена глобальна автоматична цифрова мережа «*AUTODIN*» (англ. *Automatic Digital Network*), що використовувала канали радіозв'язку, у тому числі супутникові, та підводні коаксіальні кабелі. На території Штатів було використано 4 наявних центра автоматичних електронних комутацій «*AESC*» (англ. *Automatic Electronic Switching Center*) і за кордоном створено 11 нових центрів автоматичних цифрових комутацій «*ADMSC*» (англ. *Automatic Digital Message Switching Center*). На даний час всі центри мають єдину назву - «*ASC*» (англ. *AUTODIN Switching Center*)

Штат більшості центрів «*Autodin*» на території Штатів передбачав 60 осіб військового персоналу: начальник, офіцер безпеки, 13 офісних співробітників, 15 технічних диспетчерів, 10 криптологічних техніків, і 20 комп'ютерних операторів. Більшість кінцевих користувачів були підключені до мережі за допомогою обладнання цифрових терміналів «*DSTE*» (англ. *Digital Subscriber Terminal Equipment*). У мережі щомісяця циркулювало близько 40 мільйонів повідомлень, при цьому комутація здійснювалася естафетним методом з ідентифікацією джерела й одержувача



на транзитних вузлах. Щоб здійснити передачу, користувач мережі спочатку набирав текст повідомлення на комп'ютері, записував його на дискету, а потім відносив на дивізіонний вузол зв'язку для шифрування та відправлення.

Мережа «*Autodin*» використовувалася під час операції «Буря в пустелі» у Перській затоці у 1991 році для обміну секретною інформацією. Але незважаючи на високу надійність, вона була предметом критики через нездатність працювати в умовах інтенсивного пульсуючого навантаження.

Тому в середині 1990-х років МО США розгорнуло роботи з модернізації мережі «*Autodin*» та її об'єднанню з мережею «*DDN*» (англ. *Defence Data Network*) для створення оборонної системи передачі повідомлень «*DMS*» (англ. *Defense Message System*). Ця система була призначена для оперативного закритого обміну інформацією між частинами, підрозділами й окремими екіпажами на марші (метеодані, розвідувальні повідомлення, накази тощо) на основі ресурсів глобальної мультимедійної мережі Пентагона «*DISN*» (англ. *Defense Information Systems Network*). Вартість системи «*DISN*» оцінювалася в 1,6 мільярда доларів.

На початку 1990-х років «*Autodin*» була замінена військовою мережею пакетної комутації «*MilNet Packet Switching network*». 15 вересня 2000 року «*Autodin*» замінила адміністративна система захисту «*DMS*» (англ. *Defence Management System*), але вона залишилася військовою мережею для обміну оперативних повідомлень з грифом обмеження «цілком таємно» і нижче. У 2000 році «*DMS*» була встановлена на 360 тисячах комп'ютерів і 7 тисячах сайтів у всьому світі. «*Autodin*» підтримала комунікації Департаменту захисту «*DoD*» (англ. *Department of Defense*) протягом тридцяти років. Служба «*DMS*» (англ. *Defense Message Service*) і мережа «*DISN*» (англ. *Defense Information Systems Network*) замінять

«*Autodin*» і його компоненти. DoD планує припинити використання «*Autodin*» 30 вересня 2003 року.

Для зручності користувачів формат повідомлень «*DMS*» був наближений до електронної пошти «*Outlook*» і дозволяв відправляти та одержувати повідомлення із вкладеннями, що мали гриф «Таємно» й «Цілком таємно». Для тих, хто ще не встиг засвоїти цю систему, була передбачена можливість відправлення звичайного поштового повідомлення з шифруванням на основі криптокартки «*FORTEZZA*» по каналах всесвітньої «павутини», що працювала з секретним протоколом обміну даними «*SIPRNET*». Всі вхідні повідомлення перевірялися на автентичність відправника.

До середини 1990-х років мовний трафік МО на материковій частині, в основному, як і раніше проходив через оборонну комутовану мережу «*Autovon*» (англ. *Automatic Voice Network*), яка з 1963 року була фактично мережею загального користування військового відомства. До кінця 1990-х років була побудована комерційна оборонна телекомунікаційна мережа «*DCTN*» (англ. *Defence Commercial Telecommunications Network*) для передачі мовної інформації комутованими та виділеними каналами зв'язку, передачі даних та проведення відеоконференцій. Канали зв'язку орендувалися у фірми «*AT&T*».

Головним телекомунікаційним проектом федерального уряду США в середині 90-х років минулого століття було розгортання телекомунікаційної мережі з інтеграцією служб «*FTS 2000*», що орієнтована на передачу невеликої частини трафіка МО. Трафік даних МО розподілений між декількома великими мережами загального користування і мережами спеціального призначення. Основна його частина передається глобальною оборонною мережею передачі даних з комутацією пакетів «*DDN*», що складається з чотирьох окремих мереж: «*Milnet*», «*Disnet*», «*Scinet*» і підсистем зв'язку «*WIN*». Найбільша з них – мережа «*Milnet*», що має 225 вузлів у США, Європі і Тихоокеанському регіоні.

Зараз «*DDN*» передає в середньому 4,6 мільйона повідомлень на добу, що включає дані з планування та тилових завдань, перевезення та обліку особового складу в інтересах об'єднаного командування. Мережа «*DDN*» побудова-

на на технологіях 80-х років і реалізує протоколи «*X.25*» і «*TCP/IP*». Трафік у мережі настільки напружений, що деякі служби МО, включаючи військово-повітряні сили (далі – ВПС), військово-морські сили (далі – ВМС) та службу тилу, розгорнули власні мережі для передачі додаткового трафіка. Так, у мережі тилової служби «*DLAnet*» і ВМС «*Navnet*» використовується комутаційне устаткування фірми «*Timeplex*» і канали зв'язку T1 зі швидкістю 1,544 Мбіт/с, орендовані у фірми «*AT&T*» за контрактом на мережу «*DCTN*». У мережі ВПС «*Afnet*» застосовані інтелектуальні мультиплексори класу T1 фірми «*N.E.T.*» і лінії зв'язку компанії «*AT&T*».

В новому тисячолітті МО серйозно зіштовхнулося з проблемою збільшення кількості своїх мереж, багато з яких надлишкові й не можуть ефективно взаємодіяти одна з одною. Крім того, вони створювалися 30-40 років тому і вже не здатні задовольнити вимоги користувачів щодо пропускної здатності та надання послуг. Тому був розроблений ряд перспективних програм розвитку як інформаційних, так і телекомунікаційних мереж. Ці програми припускають створення єдиної інформаційної інфраструктури МО, що базується на єдиній цифровій системі зв'язку.

Розроблена МО програма створення оборонної інформаційної інфраструктури «*DII*» (англ. *Defense Information Infrastructure*) є першим кроком в об'єднанні різних видів і принципів передачі інформації. Вона призначена для найшвидшого впровадження передових інформаційних і оборонних технологій. «*DII*» – це глобальне об'єднання всіх стаціонарних і мобільних інформаційних систем МО, що забезпечують збір, підготовку, збереження, передачу, обробку й відображення усіх видів інформації. Транспортною платформою для передачі інформації в «*DII*» повинна стати розроблена на початку 90-х років минулого століття мережа «*DISN*» (англ. *Defense Information Systems Network*).

«*DISN*» – це глобальна оборонна мережа передачі даних. Її призначення – надавати послуги з передачі різних видів інформації (мови, даних, відео, мультимедіа) для ефективного й захищеного керування військами, зв'язком, розвідкою та радіоелектронною боротьбою (далі – РЕБ). Вона відповідає усім вимогам національної безпеки та повинна реалізувати широкий спектр інформаційних потреб військового командування США у XXI столітті. «*DISN*» інтегрує всі елементи системи зв'язку МО: мережу військового супутникового зв'язку «*MILSATCOM*» (англ. *Military Satellite Communications*), проекти зі створення комерційного сегмента «*SATCOM*», орендовані зв'язні ресурси, мережі різних оборонних ві-

домств і мобільні мережі.

При розробці архітектури «*DISN*» основна увага приділялася розвитку транспортної підсистеми, що поєднує різні стаціонарні й мобільні мережі; підсистемі керування мережею, що забезпечує єдине керування «*DISN*» і мережами, що сполучаються; підсистемі надання додаткових послуг для підтримки єдиних адресних довідників, паперових каталогів, тактичних каталогів в електронній і паперовій формі; підсистемі засекреченого та безпечного обміну усіма видами інформації.

Стратегія розгортання «*DISN*» відповідно до планів Агенції оборонних інформаційних систем «*DISA*» (англ. *Defense Information Systems Agensy*) включає три основні етапи: короткостроковий етап (*Near Term, NT* – до 2000 року), етап найближчої перспективи (*Mid Term, MT* – 2000-2005 роки) і довгостроковий етап (*Far Term, FT* – до 2010 року). На кожному з етапів передбачається враховувати такі фактори, як виникнення локальних, регіональних і глобальних конфліктів та війн, зміна державної зовнішньої, внутрішньої й військової політики, тенденції розвитку нових мережних і інформаційних технологій, стан і тенденції розвитку інших цивільних, комерційних і військових телекомунікаційних і інформаційних мереж. Зараз завершена побудова мережі «*DISN-NT*» – об'єднання існуючих мереж МО в глобальну телекомунікаційну мережу загального призначення з єдиними архітектурою, принципами функціонування, бюджетом і мережним керуванням. Адміністративне керування мережею здійснює «*DISA*».

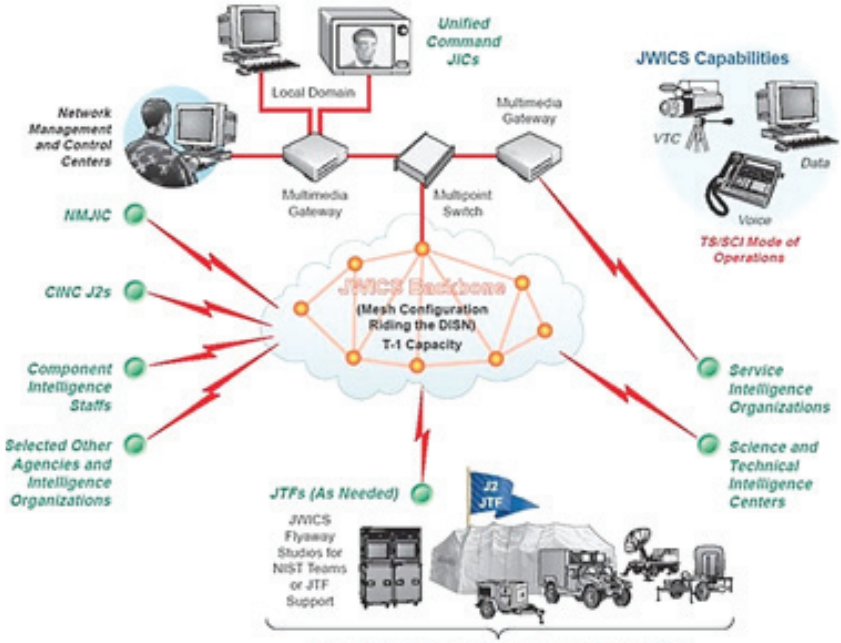
За планами «*DISA*» мережі, що підлягають включенню в «DISN-NT», були розбиті на три групи. До першої до кінця 1992 року ввійшли мережі «*DLAnet*», «*Afnet*», «*Navnet*», «*MCDN*» і «*CEAP*», а також мережі «*Milnet*», «*Pilot*», «*Internet*», «*DSIR*» (англ. *DCS Spain, Italy Reconfiguration*) і мережа сухопутних сил «*SISOCS*». Пізніше в цю групу ввійшли мережі: «*DDN/DMS*», мережа АНБ, телекомунікаційна система Оборонної картографічної агенції «*DMAIS*» (англ. *Defence Mapping Agency Telecommunications System*) і мережа «*Red Switch*». До другої групи (до 1996 року) увійшло більше 170 додаткових мереж, що не мали доступу до мережі «*DDN/DMS*». До третьої групи (до 2000 року) увійшли мережі спеціального призначення, основою яких називають об'єднану глобальну систему зв'язку розвідувальних служб «*JWICS*» (англ. Joint Worldwide Intelligence Communications System). Всіма цими мережами після завершення створення єдиної системи безпеки передбачалося передавати зашифровану інформацію.

«*DISN-NT*», типова змішана мережа, будується на базовому комунікаційному середовищі, що поєднує через виділені урядові й орендовані канали Т1 і Т3 різні фізичні природи мережі, що сполучаються, за допомогою швидкісних мультиплек-

сорів. Вузол комутації мережі «*DISN-NT*» включає комутатор пакетів «*X.25*» мережі «*DDN*» і маршрутизатор або концентратор доступу абонентів до ліній зв'язку базової мережі. Високошвидкісні маршрутизатори, об'єднані лініями базової мережі й утворюючу мережу швидкої комутації пакетів, поступово будуть заміняти низькошвидкісну мережу «*X.25 DDN*». Такий підхід дозволить поступово перетворити найбільшу у світі мережу «*X.25 DDN*» у найбільшу у світі мережу зі швидкою комутацією пакетів (мережа «швидких маршрутизаторів»).

Швидке розширення функціональних можливостей і розвиток мережі «*DISN-NT*» передбачалося забезпечити за рахунок використання оборонної супутникової системи зв'язку «*DSCS*» (англ. *Defence Satellite Communications System*), що повинна була стати комунікаційною основою глобальної системи супутникового зв'язку в рамках програми «*Global Grid*» – плану створення всесвітньої глобальної системи зв'язку, що включає стаціонарні і мобільні континентальні фрагменти, поєднані у єдину систему супутникового зв'язку.

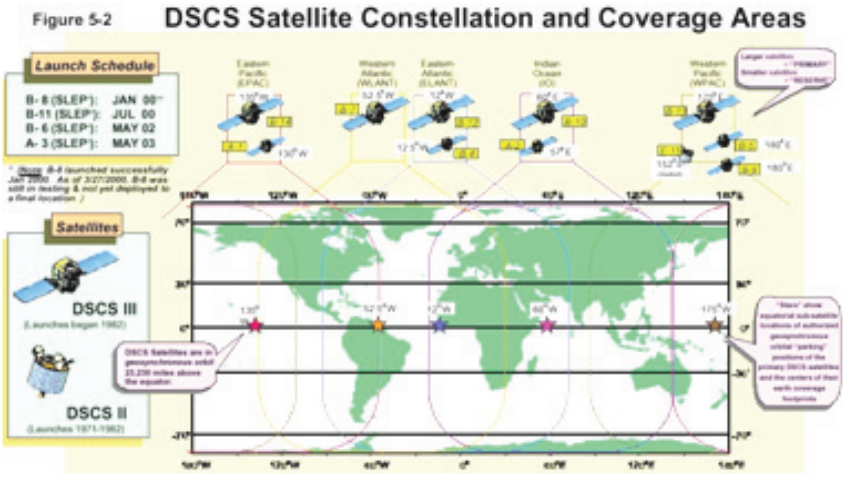
Однак вже у 1996 році агенція «*DISA*» відзначила ряд недоліків даної системи. Насамперед, це низький рівень інтеграції об'єднаних у складі «*DISN-NT*» мереж, що істотно обмежував взаємодію в рамках єдиної мережі та перешкоджав ефективному єдиному керуванню всіма її ресурсами. Зокрема, відзначалися складнос-



ті взаємодії стаціонарної та польової (мобільної) компонент базової мережі через розходження у використовуваних стандартах, типах каналів зв'язку (аналогових і цифрових), наданих послугах, пропускній здатності (у мобільної компоненти вона значно нижче, ніж у стаціонарної), у комутаційному та зв'язковому устаткуванні. Це породжувало додаткові труднощі матеріального забезпечення бойових сил, технічного обслуговування та підготовки фахівців.

Крім того, використані мережеві технології недостатньо масштабувалися та були не в змозі належним чином надавати пропускну здатність за вимогою. Система зв'язку «*DSCS*», на яку робилася ставка, та її система керування були не автоматизованими та орієнтованими на виділення фіксованого ресурсу, що виключало його динамічний перерозподіл у процесі роботи, тим більше дистанційно з єдиного центра керування. Через відсутність загальної архітектури та стандартів була ускладнена передача даних в інтересах розвідки та РЕБ. Несумісність устаткування ускладнювало застосування різних засобів засекречування та криптозахисту. У цілому, базова архітектура «*DISN-NT*» була недостатньо гнучкою, особливо для мобільних сил, що розгортаються оперативно в різних регіонах світу.

Тому при розробці принципів побудови другої черги мережі «*DISN-NT*» агенція «*DISA*» пішла шляхом використання готових комерційних продуктів у сфері нових інформаційних і мережних технологій. При цьому упор був зроблений на відкриті системи при оптимальному використанні національних стандартів і на новітні комерційні технології та послуги «*COTS*» (англ. *Commercial-Off-the-Shelf*). Добір технологій проводився на конкурсній основі за результатами дослідної експлуатації. Була розроблена програма «*DSSG*» (англ. *DISN Support Services Global*) – стратегія підтримки спільних контрактів із фірмами-виробниками та постачальниками теле-



комунікаційного устаткування і послуг. Вважалося, що якість наданих послуг будуть контролювати постачальники устаткування для «*DISN*» разом з агенціями «*DISA*» і «*DARPA*» (Управління перспективних досліджень МО).

Для реалізації стратегії «*DSSG*» з метою відпрацьовування перспективних мережевих технологій у національній мережі передачі даних МО був розгорнутий ряд експериментальних дослідних мереж. Так, агенція «*DISA*» ще в 1993–1994 роках створила широкополосну мережу передачі інформації на Гавайських островах. Вона з'явилася прототипом другого етапу «*DISN*» і будувалася на основі «*B-ISDN*» у сполученні з «*ATM*» і «*SONET/SDH*»-технологіями. Національна космічна агенція США «*NASA*» разом з фірмою «Rockwell International» спостерігали за експериментальною мережею на базі «SMDS»-технології, що була створена фірмами «*GTE*» і «*Packard Bell*» у Національному дослідному центрі МО. На цій же мережі компанія «*AT&T*» досліджувала можливості даної технології з передачі на велику відстань різних видів інформації. Міністерство енергетики США «*DoE*» (англ. *Departament of Energy*) запропонувало корпорації «*Sprint*» побудувати «*ATM*»-мережу, що спочатку повинна об'єднати п'ять дослідницьких центрів «*DoE*» з п'ятьма центрами «NASA» і лабораторією в Ліверморі. «*DoE*» мало намір передавати цією мережею дані й відеозображення, а «*NASA*» збиралося об'єднати ряд суперкомп'ютерів у різних містах. Надалі планувалося перетворити дану «*ATM*»-мережа в мережу «*Esnet*» (англ. *Doe's Energy Sciences Network*) і дві мережі «*NASA*» – «*SI*» (англ. *Sciences Internet*) і «*Aeronet*», а також підключити до неї національну наукову мережу «*NSFnet*».

Агенція «*DARPA*» і Національний науковий фонд «*NSF*» (англ. *National Scientific Fund*) для дослідження можливості побудови ліній передачі на швидкостях до 5 Гбіт/с планували створити мережу «VistaNet». Вилучених абонентів передбачалося об'єднати за допомогою технології «*ATM*». Результати цих робіт повинні були використовувати при створенні національної дослідної мережі «*NREN*» (англ. *National Research and Education Network*). Координувати зусилля «*NSF*», «*NASA*», «*DARPA*», «*DoE*» та інших агенцій зі створення цієї мережі в рамках загальнодержавної програми «*DII*» повинен був центр «*OSTP*» (англ. *Office of Science and Technology Policy*).

У результаті завершення робіт над «*DISN-NT*» була побудована стаціонарна мережа, що надавала послуги вузькополосного «*ISDN*» (*N-ISDN*) зв'язку, розробку «безпечних» кінцевих пристроїв «*N-ISDN*» і введення в дію тестової мережі «*DISN*». Були реалізовані такі експериментальні проекти, як використання комерційного сегмента супутникової системи «*SATCOM*» (перспективної широкополосної системи супутникового зв'язку, що підтримує технологію «*ATM*») і моделювання застосування «*Internet*» в інтересах МО (програма «*DSI*» – англ. *Defense Simulation Internet*).

Була здійснена заміна комерційної телефонної мережі МО «*DCTN*» (англ. *Defence Commercial Telecommunications Network*) цифровою мережею, що складається із широкополосних контролерів *(*англ. *Bandwidth Managers – BWMs*), з'єднаних магістралями «*SONET*».

На другому етапі (до 2005 року) була проведена подальша цифровізація мережі та розширення переліку наданих послуг, у тому числі створення інтелектуальної служби каталогів, уведення багаторівневого захисту обміну інформацією, реалізація розподіленого інтерактивного моделювання, оперативне конфігурування та надання послуг комерційного сегмента мережі «*SATCOM*» в інтересах стаціонарних і мобільних абонентів; надання послуг індивідуальної та групової передачі, персонального зв'язку/універсальної персональної передачі даних (англ. *Personal Communications Services/Universal Personal Telecommunications, PCS/UPT*), а також здійснений перехід на технологію «*ATM*» при побудові базового сегмента стаціонарної та мобільної компонент мережі.

Особливість другого етапу була в застосуванні «*ATM*»-технології в польовій/мобільній компоненті. При цьому поряд з рухомими «*ATM*»-комутаторами в оперативно-тактичній та тактичній ланках керування використовується й існуюче устаткування систем зв'язку армійського корпуса ЗС «MSE» (Mobile Subscriber Equipment) і тактичної ланки «*TRI-TAC*» (англ. *Tri-Services Tactical*). Для сполучення з ними була розроблена спеціальна архітектура рухомого «*ATM*»-комутатора, що підтримує ве-

ликий набір різноманітних інтерфейсів і стиків.

Третій етап побудови «*DISN*» (до 2010 року) припускає створення глобальної високошвидкісної широкополосної мережі, що буде ефективно передавати усі види інформації та надавати багато додаткових послуг, специфічних для військового застосування (передача закритої інформації, підключення до мережі абонентів мобільних сил за допомогою системи «*Global Grid*»). В основу архітектури мережі третього етапу покладені технології відкритих систем «*B-ISDN*» для елементів стаціонарної мережі і «*ATM*» у мобільній компоненті та супутниковому сегменті мережі. У єдину систему їх об'єднають високошвидкісні волоконно-оптичні, радіорелейні та супутникові канали зв'язку, що забезпечить ефективну взаємодію між багатьма військовими формуваннями (у тому числі мобільними групами) в усьому світі.

Ключове питання створення «*DISN*» – це побудова високошвидкісної широкополосної системи супутникового зв'язку, система керування якої цілком буде інтегрована в єдину систему керування «*DISN*». За планами розгортання третього етапу «*DISN*» перспективна система супутникового зв'язку «*SATCOM*» повинна буде включати, крім супутників зв'язку військового призначення, і комерційні супутники. Основне призначення супутникової мережі – це підключення мобільних користувачів у зонах конфліктів до континентальної частини єдиної мережі передачі даних.

Паралельно зі створенням транспортної підсистеми загальнонаціональної мережі МО «*DISN*» агенція «*DISA*» розробляє ряд програм, що повинні забезпечити надійний обмін через мережу «*DISN*» конфіденційною інформацією для нестатків різних військових і урядових відомств США. Це такі проекти, як «*TMP*» (англ. *Telecommunications Management Program*) – програма створення єдиної системи керування мережею «*DISN*» – «*TMS*» (англ. *Telecommunication Management System*) і програма побудови захищеної мережі передачі повідомлень «*DMS*» (англ. *Defense Message System*), цілком реалізуючої можливості діючої мережі «*Autodin*» МО з передачі таємної та відкритої інформації. Передбачається, що при об'єднанні з «*DISN*» мережа «*DMS*» збереже своє ядро адміністративного керування, що займе окреме місце в ієрархічній архітектурі керування «*DISN*».

Для інформаційного обміну між різними тактичними, а також стратегічними мережами планується розгорнути об'єднану тактичну та стратегічну польову мережу передачі даних «*ITSDM*» (англ. *Integrated Tactical/Strategic Data Network*), що буде використовувати ресурси «*DISN*». У рамках програми створення захищених оборонних інформаційних систем «*DISSP*» (англ. *Defense Information Systems Security Program*) проводяться роботи над єдиною архітектурою всіх оборонних систем. Передбачається створення архітектури систем захисту, її впровадження в «*DISN*» та інші оборонні мережі, розробка стандартів і протоколів захисту як систем у цілому, так і переданої інформації, що сформує технологію багаторівневого захисту МО.

Крім того, мережу «*DISN*» на другому етапі передбачається використовувати як

магістральну для дослідної ділянки імітаційної оборонної інтермережі «*DSI*» (англ. *Defense Simulation Internet*), яка створюється агенцією «*DARPA*». Мережа «*DSI*» повинна стати могутнім імітаційним засобом моделювання всього спектра бойових операцій на різних театрах воєнних дій, а також інструментом оцінки альтернативних телекомунікаційних технологій для «*DISN*».

З 2001 року американські ВМС разом із морською піхотою здійснюють грандіозну й безпрецедентну за своєю вартістю та масштабом програму створення глобальної інформаційної мережі «*NMCI*» (англ. *Navy Marine Corps Intranet*). За даними військово-морського відомства США вартість програми оцінюється в 7 мільярдів доларів. У ході її виконання у період з 2001 по 2008 роки було передбачено об'єднання близько 100 розрізнених у той час відомчих інформаційних мереж і ліквідація порядку 200 телекомунікаційних шлюзів, задіяних у системі оперативного планування й бойового використання кораблів, авіації й підрозділів морської піхоти США.

Загальна кількість комп'ютерів (серверів, настільних робочих станцій, портативних і кишенькових комп'ютерів) може досягти 360 тисяч одиниць, при цьому вони будуть розкидані по всій земній кулі на 300 військових базах (Аляска, Ісландія, Пуерто-Рико, Гуам, Окінава, Гавайи, Куба тощо), включаючи континентальну частину США.

За умовами контракту, що був укладений американськими військовими з однією з провідних американських компаній «*Electronic Data Systems Corp*», вартість

оплати робіт по роках була розподілена таким чином (у мільйонах доларів): 2001 – 146, 2002 – 667, 2003 – 1038, 2004 – 1116, 2005 – 1116 і з 2006 по 2008 – по 939 щорічно. Пік фінансування програми «*NMCI*» припав на 2003 рік, коли за планом захисту інформаційних систем США на всіх «критично важливих об'єктах національної інформаційної інфраструктури» були проведені заходи щодо забезпечення безпеки доступу до інформаційних ресурсів.

Вимога щодо забезпечення «гарантованої інформаційної безпеки» була одним з основних при проведенні всіх робіт у рамках даного контракту, а на заходи щодо захисту інформації виділялося від 5 до 10 мільйонів доларів щорічно. Головним виконавцем робіт у числі інших 25 субпідрядників став один з найбільших системних інтеграторів «*Raytheon Co*», що брав участь у таких великих військових проектах, як програма «*Land Warrior*» (комп'ютеризація керування військами на полі бою).

Передбачається, що будь-який користувач мережі «*NMCI*» залежно від рівня повноважень доступу до інформації зможе працювати на одній і тій же робочій станції як із секретними, так і несекретних даними практично всіх форматів (аудіо, відео, пошта, новини тощо), а при необхідності, використовуючи спеціальне устаткування «*CRAS*», підключатися до інформаційних ресурсів через мобільний телефон на швидкості 56 Кбіт/с.

В інтересах забезпечення інформаційної безпеки фахівцями ВМС разом з АНБ, Військово-космічним командуванням і Управлінням інформаційних систем МО США була розроблена так звана «стратегія глибокого захисту», що передбачала використання всього доступного арсеналу засобів захисту даних: міжмережевих екранів (firewalls), шифраторів, фільтрів пакетів даних, пристроїв виявлення вторгнення, смарт-карт, процедур розподілу ключів і новітніх криптоалгоритмів.

Таким чином, аналіз стану та тенденцій розвитку телекомунікаційних мереж спеціального призначення США показує, що відбувається стрімкий процес їхньої інтеграції в єдину мережу з використанням окремих спеціально розроблених протоколів забезпечення безпеки обміну даними на верхніх рівнях функціональної архітектури.

У транспортній мережі передбачається використовувати єдині технології та стандарти для всіх типів мереж – локальних, глобальних, стаціонарних і мобільних (польових). Особлива увага приділена питанням глобальних систем безпеки та керування, підтримки єдиної довідкової системи з опорою на високошвидкісну первинну мережу зв'язку, що в цілому, дозволяє говорити про створення єдиної глобальної інфраструктури для всіх існуючих інформаційних систем США.

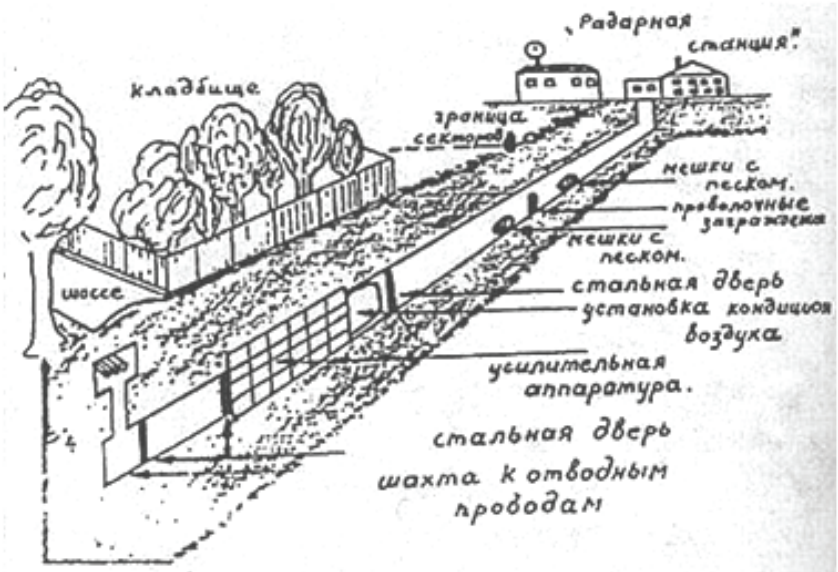
2.11. «Шпіонська» діяльність АНБ

З моменту свого створення західні спецслужби своїм вістрям були націлені на Радянський Союз, що ніколи й не приховувалося. На цьому головному напрямку були зосереджені кращі кадри та велика частина всіх технічних і фінансових засо-

бів. За довгі роки «холодної» війни АНБ і ШКУЗ записали мільйони повідомлень, розмов і бесід радянських політиків, дипломатів, військових, учених, суспільних діячів. У 1967 році апаратура АНБ записала останні слова радянського космонавта Володимира Комарова, що згорів в атмосфері при поверненні на Землю.

Головним полем технічних операцій британської розвідки з прослуховування радянських телефонних ліній секретного зв'язку спочатку стала Австрія. Ця операція отримала кодову назву «Сілвер» (Silver – срібло). Наприкінці 1952 року її співробітникам удалося підключитися до двох кабелів зв'язку радянських військ в Австрії. Правда, велика частина переговорів деяких високопосадовців йшла з використанням апаратури засекречування, яка не піддавалася розшифруванню. Це робило їхнє перехоплення зовсім безглуздим заняттям.

Незважаючи на це британська спецслужба запропонувала американським колегам повторити свій віденський досвід щодо ліній Групи радянських військ у Німеччині. Операцію назвали «Голд» (Gold – золото), адже треба було в буквальному значенні «зарити в землю» десятки мільйонів доларів. У грудні 1953 року в Лондоні



Берлинский туннель. Эскиз из архивов СВР

відбулася нарада представників обох розвідслужб, на якій обговорювалися технічні нюанси і перспективи операції «Gold».

Оскільки зв'язок радянських військ у Німеччині з Москвою здійснювався через Берлін, вирішено було спробувати підключитися до підземних ліній зв'язку під Східним Берліном, що йшли з радянського військово-розвідувального містечка в Карлсхорсті. Спокуса була велика: 113 телефонних кабелів пролягали усього в 300 метрах від кордону радянської зони окупації.

План операції був затверджений директором ЦРУ Алленом Даллесом, після чого почалося її здійснення. Як вихідну крапку для тунеля був обраний будинок поблизу кордону між американським і радянським секторами Берліна, у якому розміщався склад армії США. Для маскування робіт і приховання викопаної землі поруч був побудований величезний складський ангар. З метою дотримання таємності роботи велися тільки ночами, викопаний ґрунт виносився так, щоб не помітив супротивник. Усе це тривало сім місяців.

На початку 1955 року американські солдати вирили підземну галерею на глибині в 4,5 метра довжиною 450 метрів і діаметром 2 метри, що з'єднав під землею розділені на поверхні райони «Treptow» і «Rudow». Усередині галерея була викладена металевими пластинами, були проведені електрика, вода та вентиляція. Надзвичайно таємно в цю сталеву трубу доставили новітню прослуховуючу та звукозаписуючу апаратуру. Роботи зі спорудження тунелю велися день і ніч, і вже в травні того ж року цей ризикований проект вартістю 6 мільйонів доларів почав функціонувати.

150 магнітофонів цілодобово вели запис телефонних переговорів з Москвою. Інформація агентів КДБ, військові приготування, плани уряду – все потрапляло в руки ЦРУ... Але одного не знали західні спецслужби: радянська розвідка була добре інформована про те, що всі таємні переговори прослуховуються. Як часто це трапляється, допоміг радянський агент – співробітник британської розвідки Джордж

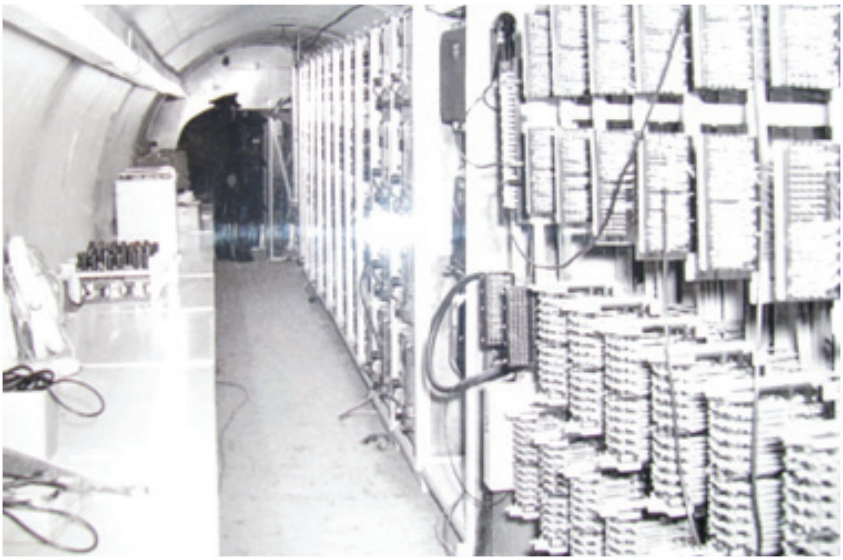
Блейк.

Він виявився учасником таємної наради в британській спецслужбі з планування цього проекту. Одержавши матеріали проекту, Блейк передав їх до Москви. Довідавшись про тунель, радянська контррозвідка вирішила не перешкоджати його прокладанню. Цим вирішувалося відразу кілька задач. По-перше, виводився з-під удару Блейк, який інакше неминуче потрапив би під підозру. По-друге, тим самим створювалася можливість для широкомасштабної дезінформації західних спецслужб. Нарешті, по-третє, це дозволяло в потрібний момент «випадково знайти» тунель і потім використовувати це в пропаганді як наочний доказ «шпіонської» діяльності ЦРУ та інших західних спецслужб.

Було вирішено припинити найбільш важливі переговори по визначених для перехоплення супротивником каналах зв'язку, переключивши їх на інші лінії зв'язку. Однак деякі конфіденційні переговори здійснювали по цих кабельних лініях, щоб не викликати підозру у західних спецслужб. Одночасно був визначений план широкомасштабної дезінформації з військових та політичних питань.

Західні спецслужби протягом восьми років, одержавши 500 тисяч записаних телефонних розмов і 400 метрів телекса, працювали цілодобово, обробляючи величезний потік інформації, що перехоплювався ними. Працювали сотні перекладачів з російської мови, фахівці високої кваліфікації аналізували ці матеріали, витрачаючи багато десятків мільйонів доларів.

І хто знає, як довго продовжувалася б ця недитяча гра, якби не втрутився його



величність Випадок. 22 квітня 1956 року після сильної зливи в районі шосе над прокладеним тунелем була ушкоджена німецька телефонна лінія. Нічого не підозрюючи німецькі техніки виїхали на усунення несправності, копнули землю, а там – гігантський суперсучасний комутатор. В результаті були організовані дипломатичні ноти протесту та «гнівні» статті в пресі. Тунель швидко розібрали та закопали. Західні спецслужби провели спільне розслідування причин виявлення тунелю та вирішили, що все дійсно відбулося випадково. У результаті вони продовжували вірити усьому, що одержали з цього перехоплення аж до арешту Блейка в 1961 році, тобто ще п'ять наступних років. Таким чином, майже вісім років «берлінський тунель» був джерелом дезінформації.

Зараз у берлінському музеї «Alliiertenmuseum» працює історична виставка «Шпигунський тунель». На ній представлена велика кількість документальних матеріалів, що розповідають про цю дивну історію, газетні статті й унікальні фотографії, що висвітлюють будівництво таємного об'єкта, докладні схеми та плани пристрою, а також розташування на місцевості. Також є кінохроніка розкриття тунелю та відвідування його радянськими військовими та журналістами. Але центральним експонатом виставки є справжня семиметрова ділянка тунелю. Він чомусь не був знищений. Знайшли його в 2005 році під час робіт із розширення того шосе, під яким він і був прокладений більше, ніж п'ятдесят років тому.

Крім методу безпосереднього гальванічного підключення до ліній зв'язку, технічна розвідка західних спецслужб також використовувала метод перехоплення на відстані таємних повідомлень супротивника за рахунок побічних електромагнітних випромінювань та наведень (далі – ПЕМВН) їхньої шифротехніки.

Так, у середині 1950-х років уряд США почав цікавитися питаннями ПЕМВН і за-

снував відповідну програму «Буря» (англ. *Tempest*). В результаті був розроблений перший американський «*Tempest*»-стандарт «*NAG-1A*». У 1962 році під час Карибської кризи АНБ з розвідувального судна «Оксфорд» (Oxford) спробувала обійти радянську систему шифрування, перехоплюючи ПЕМВН шифрувальних машин радянських радіостанцій на Кубі. Проводилися також спроби перехопити шумові викиди, що розкривали установки ротора в старих радянських шифрувальних машинах.

Наприкінці 1960-х – початку 1970-х років, незважаючи на всі труднощі з розкриттям таємних радянських кодів, АНБ провело успішну операцію за назвою «Гама Гупі». Американські фахівці прослуховували особисті розмови членів Політбюро ЦК КПРС, які розмовляли один з одним по радіотелефонах з урядових автомашин. Справа в тому, що з 1971 року засекречування цього зв'язку забезпечувалося апаратурою тимчасової стійкості. При визначених зусиллях, використовуючи сучасну комп'ютерну техніку, можна було розшифрувати окремі розмови. Для цієї мети, наприклад, був задіяний портативний комплекс радіотехнічного моніторингу «WG-1240», що керувався за допомогою звичайної ПЕВМ.

У 1976 році в КДБ для обслуговування керівництва держави була впроваджена нова система рухомого засекреченого радіозв'язку, що цілком виключала можливість розшифрування перехоплених розмов. Така апаратура використовувалася також на державних дачах у Криму, на Чорноморському узбережжі Кавказу, у Мінеральних Водах. Однак система рухомого зв'язку Міністерства зв'язку СРСР, якою користувалася основна маса урядових чиновників, починаючи від заступників Голови Ради міністрів і нижче, через високу вартість апаратури засекречування захисту не мала.

Прослуховування телефонних розмов вищого керівництва СРСР підтверджують і самі американці. У книзі Крістофера Ендрю «Президенту ТІЛЬКИ ЧИТАННЯ» наводяться дані з прослуховування телефонів в автомашинах керівництва СРСР:

«Серія повідомлень, перехоплених АНБ із радянського посольства на Шістнадцятій вулиці у Вашингтоні, – один із секретів Білого Дому в роки правління Ніксона, який найбільш суворо охороняли. Ні Ніксон, ні Кіссінджер навіть не згадують про них у своїх спогадах. Кажуть, вони приділяли величезну увагу цим перехопленням, імовірно, тому, що за їх допомогою можна було досліджувати роботу каналу зворотнього зв'язку та перспективи роззброєння. Президент був також особисто зацікавлений в Операції «Гама Гупі», що почалася незадовго до його перемоги у виборчій компанії. Ця Операція здійснювалася групою АНБ, що працювала під керівництвом АНБ у Посольстві США в Москві, і успішно перехоплювала мікрохвильові радіо й телефонні повідомлення між великими чорними лімузинами членів Політбюро, що їздили по Москві. За повідомленням одного зі старших аналітиків ЦРУ, що мали доступ до цих перехоплень, матеріали «Гама Гупі» читали не тільки в Білому Домі. Ми, аналітики, пильно вивчали ці повсякденні розмови (частіше між водіями членів Політбюро, ніж між самими членами Політбюро), відшукуючи значиму

інформацію, але знаходили мало. Згодом ми дізнавалися, хто з ким полював і рибалив. Ми складали разом інформацію і дізнавалися про існування близьких дружних відносин. Однак інформація була занадто конфіденційною, та на неї не можна було посилатися в повсякденних дослідженнях, пов'язаних із керівниками!»

До речі, чергова спецоперація американських спецслужб з прокладання підземного тунелю була знову здійснена з 1989 по 1991 роки, але вже під новим будинком радянського посольства у Вашингтоні. За взаємною домовленістю між СРСР і США тоді було прийняте рішення про будівництво нових посольських комплексів у Москві та Вашингтоні. Одразу ж американським спецслужбам спала на думку ідея вирішити раз і назавжди проблеми з прослуховуванням нового об'єкта, проклавши під ним тунель. А оскільки відповідно до діючого законодавства, ЦРУ не має права проводити операції на території США, сумнівна честь впровадити цей проект у життя була надана ФБР разом з АНБ.

Отже, одночасно з початком будівництва нового будинку радянського посольства почалися й роботи з прокладки під ним тунеля. З цією метою уряд США придбав житловий будинок поруч із майбутнім посольством. У підвалі цього будинку й розташовувався вхід у тунель. У ході його будівництва американцям довелося вирішити велику кількість технічних проблем, починаючи з таємного вивезення землі та закінчуючи налаштуванням спецобладнання, зокрема, фокусуванням лазерних променів, які необхідно було спрямувати вгору на будинок посольства. Не дивно, що цей проект обійшовся платникам податків у кілька сотень мільйонів доларів.

У 1979 році новий будинок посольства почав заселятися радянськими дипломатами. І тоді ж американці почали пропагандистську компанію, обвинувачуючи СРСР у використанні нового посольського комплексу, розташованого в одному з найвищих місць Вашингтона, для збору розвідувальних даних за допомогою радіоелектронного устаткування. Крім того, було заявлено, що КДБ установило підслуховуючі пристрої у новому будинку посольства США у Москві. У результаті цих скандалів остаточний переїзд радянського дипломатичного корпуса до нового будинку постійно відкладався, що дозволило американським спецслужбам без перешкод завершити будівництво тунеля та монтаж у ньому спеціальної апаратури.

Разом з тим, за словами колишнього офіцера ЦРУ у Москві Тоні Мендеса, який брав участь у здійсненні даної спецоперації, у 1989 році в підземному тунелі під московським Кремлем також були встановлені підслуховуючі пристрої на кабелях кремлівської системи зв'язку. Те, що під російською столицею існує підземне п'ятирівневе місто, підтвердив сам Мендес, який там побував: «Ці тунелі були там з найдавніших часів – ще Іван Грозний вирив частину з них. Але деякі тунелі мають зовсім недавню історію».

Одного разу ввечері агенти ЦРУ, озброївшись комп'ютерними системами керування, повітряними фільтрами та картами, ввійшли в тунель. Через колектор вони

потрапили в метрополітен, а потім і в тунелі під Кремлем. У той вечір Мендес був присутній у Кремлівському палаці на балеті. Там також був і американський шпигун у 16-му Управлінні КДБ, що займалося електронною розвідкою, майор Петро Леонов зі своєю дружиною. Двоє співробітників концертного залу також працювали на ЦРУ. В антракті подружня пара зайшла в туалет, переодяглася в одяг капельдинерів, а останні зайняли їхні місця в залі. Одягнені як працівники концертного залу, Леонови ввійшли в службові ліфти. Спустившись до тунелю, Леонов показав агенту ЦРУ, на яких кабелях зв'язку встановити підслуховуючі пристрої.

Через декілька днів Леонов утік із СРСР через Фінляндію. За інформацією Мендеса за допомогою встановлених підслуховуючих пристроїв ЦРУ попередило Бориса Єльцина про переворот, що готувався «ГКЧП» у серпні 1991 року і, по суті, допомогло його перемогти. Тодішній президент США Джордж Буш-старший і прем'єр-міністр Великобританії Джон Мейджор особисто повідомили Бориса Єльцина про переворот і поквапили його заручитися підтримкою армії.

Тим часом у 1992 році посольство тепер уже Російської Федерації остаточно переїхало в новий будинок у Вашингтоні. Відповідно, і можливості тунеля з перехоплення інформації стали використовуватися у повному обсязі. Адже це лише в теорії мешканці посольства зобов'язані вести розмови на конфіденційні теми тільки в спеціально захищених приміщеннях, а на практиці ці вимоги не завжди виконувалися. За інформацією газети «Вашингтон пост» (англ. *Washington Post*), керівники ФБР настільки пишалися своїм дітищем, що організовували екскурсії до тунеля для американських високопосадовців, що мали відповідний допуск до державної таємниці.

Однак незабаром в американської розвідки з'явилися сумніви у вірогідності інформації, що ними перехоплювалася. І не дивно, адже, зважаючи на все, у цей час російська розвідка вже знала про існування тунеля від свого агента у ФБР Роберта Хансена. Проте тунель знаходився в експлуатації аж до 1995 року, поки американці остаточно не зрозуміли, що їх постачали дезінформацією. Отже, в результаті й ця спецоперація завершилася повним провалом, як і аналогічна історія з «берлінським» тунелем.

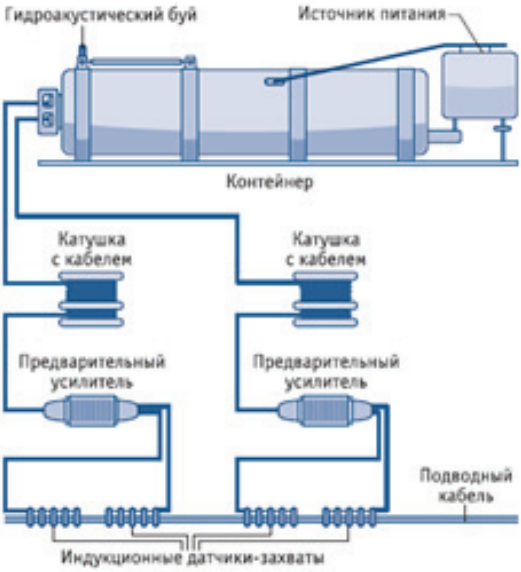
Після викриття Хансена інформація про існування тунеля просочилася в американську пресу. Перша публікація на цю тему з'явилася 4 березня 2001 року в газеті «Нью-Йорк таймс» (англ. *The New York Times*), потім про це написала і «*Washington Post*». Наступного дня віце-президент США Ричард Чейні, коментуючи публікацію в «The New York Times», ухильно заявив: «Таке спорудження, цілком можливо, було зведено, хоча інформацію треба перевіряти».

Розповімо ще про одну спецоперацію, але пов'язану вже не з підземним, а з підводним підслуховуванням. Так, у листопаді 1971 року АНБ розпочала таємну операцію під кодовою назвою «В'юнок» або «Дзвіночки плюща» (англ. *Ivy bells*). На схід

від радянського узбережжя глибоко на дні горловини затоки Шеліхова в Охотському морі АНБ і ВМС США з підводного човна «Палтус» (*Halibut SSN-587*) установили спеціальне устаткування, за допомогою якого знімалася інформація з глибоководного радянського кабелю, що з'єднував містечко Палана на західному узбережжі Камчатки та півострів Пьяшна на материку.

За твердженнями американців цей кабель зв'язував місто Петропавловськ-Камчатський, розташований поруч з островом Карпинський ракетний полігон «Кура» і базу підводних човнів «Крашеніково» з материком. У вересні 1972 року на підводному кабелі був встановлений найсучасніший та складний підслуховуючий апарат. Апарат мав спеціально облягаючий кабель пристрій, що дозволяв індукційно-електронними методами без фізичного контакту з проводами «знімати» з них інформацію. Його можна було розміщати над підводним кабелем та залишати для запису переговорів на тижні й місяці, а поті

«Кокон» – так назвали апарат для автоматичного знімання та запису інформації, що передавалася підводним кабелем. Він був створений компанією «Белл» за замовленням Відділу підводної розвідки Розвідувального управління міністерства оборони (РУМО) США. Перша модель довжиною у 6 метрів, діаметром у 1 метр і вагою у 6 тонн дозволяла безупинно знімати інформацію з двадцяти каналів протягом місяця. Тому у жовтні субмарина «Halibut» забрала «кокон» і повернула його розробникам.

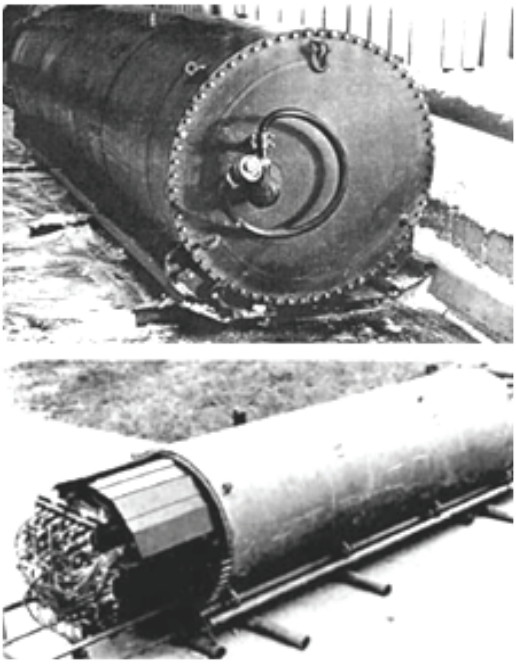


Спеціально обладнаний підводний човен повинен був регулярно з'являтися в Охотському морі. Військові аквалангісти за допомогою мінічовна та, навіть, підводного робота встановлювали місцезнаходження записуючого «кокона» та змінювали плівки, що потім надсилалися до

АНБ для розшифрування. Особливий інтерес представляли повідомлення, пов'язані з випробуваннями радянських балістичних ракет. Ракети завершували свій політ у районі Камчатського півострова, та вся інформація про ракети й випробування передавалася по цьому кабелю.

Восени 1973 року була розроблена нова модель «кокона». Основною відмінністю стала наявність акустоавтомату та програмування режиму й часу запису. Це дозволило збільшити час автономної роботи «кокону» до декількох місяців. Навесні 1978 року було прийняте рішення про установку ще одного «кокона» на підводному кабелі – але вже в Баренцевому морі. Підводна кабельна лінія зв'язку з'єднувала Северодвинськ із Мурманськом. У вересні 1979 року за участю підводного човна «Перч» (*Parche SSN-683*) «кокон» був встановлений на кабель зв'язку в Баренцевому морі.

Будучи впевненими, що підводні кабельні лінії зв'язку були абсолютно надійними, інформація, що по них передавалася, не засекречувалася. Однак незважаючи на успішний початок і отриману інформацію, операція знову «провалилася». Виявилося, що у 1980 році КДБ переграв американську розвідку, завербувавши колишнього співробітника АНБ Рональда Пелтона, який і розповів про прослуховування підводних кабелів.



Операція «*Ivybells*» успішно здійснювалася до серпня 1981 року, коли радянський уряд прийняв рішення оголосити про виявлення «кокону». У затоці Шеліхова (Охотське море) за 32 милі від західного узбережжя Камчатки з глибини в 65 метрів радянське кабельне судно підняло ділянку підводного кабелю, на якому моряки знайшли два дивні циліндричні предмети розміром з 250-літрову бочку.

Незрозумілий пристрій чіпко охоплював броньований кабель, встромивши в його покриття сталеве «жало». Циліндри зняли та передали до контррозвідки. В одному з герметичних контейнерів було

знайдено 32 міні-магнітофони. Інший являв собою мініатюрний ядерний реактор для енергоживлення підслуховуючої апаратури. Реактор був відправлений до Казахстану на семипалатинський ядерний полігон для його знешкодження, а контейнер з розвідувальною апаратурою - до Москви.

Для збереження в таємниці джерела інформації була проведена операція з дезінформації. Хоча аналітики ЦРУ засумнівалися в цій версії та припустили, що про операцію повідомив хтось зі співробітників АНБ, РУМО або екіпажа одного з підводних човнів. З цієї причини був відмінений плановий похід субмарини до місця установки другого «кокону» у Баренцевому морі. Пройшло кілька місяців, але СРСР не намагався демонтувати цей пристрій.

Тому у жовтні 1982 року модуль «кокону» у Баренцевому морі був замінений. Однак у кінці 1983 року у музеї КДБ з'явився незвичайний експонат, що був піднятий з дна Баренцева моря. Це була третя модифікація «кокону». Його технічні параметри були такими: вага – 7 тонн, довжина – 5 метрів, діаметр – 1200 мм, кількість контрольованих кабельних каналів – до 60. Вітчизняні фахівці назвали його «камбалою».

Для «зняття» сигналів із захищеного подвійною бронею із сталевої стрічки підводного кабелю використовувалися індукційні датчики-захоплення (магнітні антени). Сигнали з індукційних датчиків заздалегідь посилювалися антенними підсилювачами, а потім по кабелю поступали в спеціальний блок, де було змонтовано електронне устаткування для прийому, посилення, частотного ущільнення (демодуляції) і запису «знятих» з кабелю сигналів на магнітофони. Запис розмов здійснювався автоматично за наявності сигналу в телефонному каналі (режим акустопуску). Для запису використовувалося 60 магнітофонів, кожен з яких був розрахований на 150 годин запису, а загальний об'єм запису перевищував 3 тися-

чі годин. Касети із записаною інформацією з пристрою періодично вилучалися та прямували для аналізу в АНБ.

Не дивлячись на величезний ризик, пов'язаний з провалом операції «*Ivybells*», командування ВМФ США продовжило проводити розвідувальні операції з перехоплення інформації з підводних кабелів зв'язку у Баренцевому та Охотському морях. Від «золотої жили» США відмовлятися не збиралися. З урахуванням подій, що відбулися, в АНБ і ВМФ США були прийняті надзвичайні заходи з посилювання режиму секретності. Для позначення розвідувальних операцій підводних човнів в цілому почав застосовуватися термін «Манта», а операцій з перехоплення інформації з підводних кабельних ліній зв'язку - «Ацетон». Але й ці умовні найменування згодом стали неодноразово змінюватися.

У 1990-і роки розвідувальні операції «Ацетон» успішно продовжувалися, про що свідчать факти нагородження атомного підводного човна «Перч» у 1995, 1996 і 1997 роках нагородами президента США за успішне вирішення спеціальних завдань. Очевидно, ці операції продовжуються і в наші дні.

Для перехоплення інформації з кабельних ліній зв'язку, що проходили по суші, в 1970-х роках американські фахівці розробили пристрій «Кріт», що використовував той же принцип, що і «Камбала». Інформація з кабелю «знімалася» за допомогою спеціального індукційного датчика. Для його установки використовувалися кабельні колодязі, через які проходили телефонні магістральні кабелі спеціального зв'язку. Датчик в колодязі зміцнювався на кабелі і для ускладнення виявлення проштовхувався в трубу, що підводила кабель до колодязя.

Перехоплювана датчиком інформація записувалася на спеціальний магнітофон. Після заповнення котушка з магнітною плівкою замінювалася на нову. Пристрій дозволяв здійснювати запис інформації, що передавалася одночасно по 60 телефонних каналах. Тривалість безперервного запису розмови на магнітофон складала близько 115 годин. Обробка перехоплених розмов здійснювалася з використанням спеціальної апаратури в приміщеннях спецслужб в будівлях посольств і іноземних представництв. За відсутності такої апаратури плівки із записом відправлялися для обробки в АНБ.

Пристрої серії «Кріт» були забезпечені радіомаяками, змонтованими в їх корпусах. Агент, проїжджаючи або проходячи в районі установки пристрою, за допомогою портативного передавача пересилав спеціальний сигнал. Якщо пристрій залишався ніким

не зворушеним, радіомаяк передавав у відповідь кодований сигнал. В цьому випадку здійснювалася заміна диска магнітофона.

Наприкінці 1980-х років радянські контррозвідники виявили пристрій «Кріт» в пункті зосередження кабелів спеціального зв'язку. Американським розвідникам вдалося встановити його на значній відстані від Москви, під землею – в розподільному колодязі, де сходилися лінії урядового зв'язку та оперативного зв'язку КДБ. З цього приводу один із колишніх керівників КДБ Бобков Пилип Денисович писав: «Це був безперечний успіх американських спецслужб, що свідчив про професіоналізм співробітників розвідки, що працювали в Москві».

Вже пройшли роки «холодної війни», багато змін відбулося на політичній карті світу. Однак як і раніше тривають запеклі сутички на невидимих «фронтах». У бойовий склад американського флоту й зараз входить малошумний атомний багатоцільовий підводний човен класу «Морський вовк» (*Sea Wolf SSN-23*) водотоннажністю 9 тисяч тонн, на оснащення якої сучасною апаратурою радіотехнічної розвідки виробництва компанії «Дженерал Динамікс» (*General Dynamix*) Конгрес США за замовленням АНБ виділив майже 1 мільярд доларів. Субмарина-шпигун, хрещеним батьком якої став екс-президент Джимі Картер, оснащена спеціальним глибоководним автономним підводним апаратом для підключення до кабельних ліній зв'язку на дні океану.

АНБ у своїй «шпіонській» діяльності тісно співпрацює зі своїм британським аналогом – Штаб-квартирою урядового зв'язку (далі – ШКУЗ). Так, наприклад, коли вийшов з ладу на три дні комп'ютерний центр АНБ, що відповідав за електронну розвідку, то агенції довелося звернутися по допомогу до британських колег, і увесь цей час розвіддані для АНБ обробляв обчислювальний центр ШКУЗ.

Наприкінці січня 2003 року завдяки пресі «розгорівся» черговий скандал з прослуховування АНБ і ШКУЗ телефонних розмов. ШКУЗ отримав розпорядження посприяти США в організації прослуховування розмов членів Ради Безпеки ООН. Прохання США було викладене в доповідній записці, яка була складена АНБ. Її текст у березні 2003 року став відомий газеті «Спостерігач» (Observer), що відразу оприлюднила деякі її деталі.

Видання повідомило, що АНБ розгорнула кампанію з перехоплення телефонних розмов представників Анголи, Камеруну, Чилі, Болгарії, Гвінеї і Пакистану – країн Ради Безпеки ООН. Як випливало зі службової записки, США була потрібна допомога британських фахівців у встановленні «жучків», тобто радіомікрофонів, у квартирах і офісах представників цих країн.

Крім того, нещодавно в Європі розгорівся сканадал з приводу розкритих недавно зв'язків між шифрувальним підрозділом Євросоюзу та АНБ. Скандал вибухнув після того, як були оприлюднені свідчення британського керівника шифробюро Десмонда Перкінса, який визнав, що АНБ мала доступ до систем засекреченого зв'язку Євросо-

юзу. Такі свідчення були зроблені на слуханнях у Європарламенті, однак не так давно стенограму слухань опублікувала французька газета «Визволення» (Liberation), яка стала єдиним виданням, що довело цю інформацію до широкої громадськості.

Даючи показання в Європарламенті, 65-літній Перкінс без натяків повідомив, що «завжди мав дуже гарні контакти з АНБ, що зазвичай перевіряє системи Євросоюзу на предмет правильного звертання та недопущення зловживань». Коли трохи здивовані члени парламенту запитали, чому ж Перкінс ніколи не просив про це експертів Євросоюзу, а відразу звертався в АНБ, той відповів буквально так: «Тому, що в мене там працюють родичі. І взагалі, вам варто було б пам'ятати, що американці все одно усіх прослуховують... А коли вони після двох тижнів не змогли розкрити наш шифр, я був просто щасливий».

Підсумком цього неприємного розгляду стала офіційна заява Єврокомісії, яка повідомила, що все, що відбулося, – це «непорозуміння». Зі скандалу, щоправда, мала певну користь німецька компанія «Сіменс», яка поставляє шифротехніку для Євросоюзу та стала з гордістю заявляти, що її шифратори не «по зубах» навіть АНБ.

Крім того, ще в середині 40-х років у США була задумана глобальна система прослуховування та перехоплення радіоповідомлень. У зв'язку з цим у 1947 році англомовні країни поділили увесь світ на зони спостереження. У британську зону ввійшли Африка, Європа, а також територія колишнього СРСР до Уральських гір. Канада відповідала за північні та заполярні широти, а Австралія – за Океанію, Індокитай та Азіатсько-Тихоокеанський регіон. Сполученим Штатам «дісталися» обидві Америки, Карибський басейн і частина Тихого океану.

Разом із тим, вважається, що система споконвічно задумувалася та створювалася для тотального спостереження за телекомунікаціями СРСР та інших соціалістичних країн. Однак у єдину мережу всі вони були об'єднані лише в 70-і роки. Тоді ж з'явилася й назва всієї системи – «Ешелон» (англ. *Eshelon*). Вона була розроблена

Echelon
Echelon hört ungefiltert den gesamten eMail-, Telefon-, Fax- und Telexverkehr ab, der weltweit über Satelliten weitergeleitet wird.
Menwith Hill
Morwenstow
Bad Aibling
Misawa
Yakima Firing Center
Sugar Grove
Leitrim
Geraldton Station
Shoal Bay
Waihopai
Grafik: Landesamt für Verfassungsschutz Baden-Württemberg

АНБ у 1971 році як «Проект П-415» (англ. *Project P-415*) і використовувалася разом із ШКУЗ.

«Ешелон» у повному розумінні слова - це Мережа, яка має окремі підмережі, що розкидані по усьому світі та здійснюють загальні для мережі програми. Це «Клесікел Булзай» (англ. *Classical Bullseye* - класичне вічко) і «Пушер» (англ. *Pusher* - штовхальник) - перехоплення ВЧ-сигналів; «Стіплбуш» (англ. Steeplebush), «Ранівей» (англ. *Runway* - злітна смуга) і «Мунпені» (англ. *Moonpenny*) - перехоплення супутникового зв'язку; «Войскест» (англ. *Voicecast* - мовний зліпок) - розпізнавання голосових повідомлень, а також визначення особистостей, що говорять.

Основою мережі є наземні бази, оснащені чутливими антенами, подібними до радіотелескопів, і супутниковими тарілками. Крім того, є бази іншого роду, розташовані поблизу надземних, підземних і підводних телекомунікацій, призначені для зняття сигналу зі звичайних і оптоволоконних кабелів. Такі ділянки є не тільки у США і Великобританії, але також у Данії, Італії, Японії, Китаї, Туреччині, Пуерто-Ріко, Африці та на Близькому Сході.

Основне джерело розвідданих – міжнародні супутники зв'язку «Інтелсат» (Intelsat), розташовані на геостаціонарних орбітах, що використовуються більшістю телефонних компаній світу та служать ретрансляторами телефонних переговорів, факсів і електронної пошти. П'ять основних станцій спостереження займаються перехопленням інформації, переданої цими супутниками від одного до іншого.

Британська станція спостереження розташовується на території бази Королівських ВПС Великобританії в Моруенстоу (Morwenstow) на півночі Корнуельського узбережжя, на вершинах високих стрімчаків. Вона знімає сигнал із супутників, що висять над Атлантикою, Європою та Індійським океаном. Станція АНБ «Шугар Гров»

(англ. *Sugar Grove* - солодкий гай), у горах Західної Вірджинії, охоплює Атлантику обох Американських континентів.

Інша станція АНБ - у штаті Вашингтон, усередині армійського полігона «Якіма» (*Yakima*) - «читає» трафік «*Intelsat*» над Тихим океаном. Ті тихоокеанські комунікації «Intelsat», що недоступні станції «Якіма», і Індійський океан контролюють станції у Джеральдтоні (*Geraldton*) на Заході Австралії і на острові Вайхопай (*Waihopai*) у Новій Зеландії.

Крім того, до «Ешелону» входить інша мережа станцій, що «читає» регіональні супутникові орбіти, не приналежні «Intelsat», зокрема, російські. Це станція «Менвіт-Хілл» (*Menwith Hill*) у північній Англії, що шпигує за Європою і Росією, станція «Шоел Бей» (англ. *Shoal Bay* – бухта мілководдя) в австралійській провінції Дарвін, що стежить за Індонезією, станція «Лейтрім» (*Leitrim*) у канадській Оттаві, що стежить за Латинською Америкою, і база «Місава» (*Misawa*) у північній Японії.

Станція у Менвіт-Хіллі, яка була заснована у 1950-х роках і має кодове ім'я «Польова Станція Ф-83» (*F-83*), з її 25-супутниковими терміналами та більше, ніж 20 квадратними кілометрами, «нашпигованими» надсучасною електронікою будинків, є вузлом мережі «Ешелон». Спочатку «F-83» призначалася для перехоплення міжнародних комерційних комунікацій у мережі «ILC» (International Leased Carrier), що використовувалась банками і фірмами для платежів.

У 1970-х станцію перепрофілювали. У рамках програм «*Steeplebush I*» і «*Steeplebush II*» вона стала «знімати» інформацію з супутників. На «*F-83*» працює 1400 інженерів, фізиків, лінгвістів, математиків, інформатиків і 370 співробітників Міністерства оборони. «Скромна» станція «*F-83*» має штат, рівний усієї «*MI-5*» – службі держбезпеки Британської Імперії.

Вона не тільки виконує функцію найбільшого «вуха» у світі, але і служить порта-

лом зв'язку з угрупованням англо-американських супутників-шпигунів, включаючи головну мережу, що контролює Євразію. Щохвилини три супутники «Вортекс» (англ. *Vortex* – вир), що висять над екватором, повідомляють на «*F-83*» розвідувальну інформацію в режимі реального часу. Більш сучасні великі супутники «Магнум і Оріон» (англ. *Magnum & Orion*) також керуються з «*F-83*».

Але не варто думати, що «Ешелон» зайнятий тільки супутниковим перехопленням. «*F-83*» є одночасно і самим могутнім вузлом класичного радіошпигунства. Вона перехоплює повідомлення, що передаються мікрохвильовими лініями зв'язку, ультра- і короткохвильові сигнали, що утворюються військовими радіостанціями.

У другій половині минулого століття підвищену увагу АНБ приділяла лініям радіорелейного зв'язку, які використовувались двома радянськими міністерствами – оборони та зв'язку. Так, наприклад, з 1968 по 1977 роки 7 супутників системи «Каньон» (англ. *Kaniyon*) перехоплювали інформацію, що передавалася по лініях радіорелейного зв'язку, прокладених у Сибіру. Їм на заміну прийшли апарати системи «Шалет», а на початку дев'яностих років – «Меркурій» (англ. *Merkury*). А з 1994 по 1998 роки було виведено на навколоземну орбіту 8 супутників радіоелектронної розвідки.

Але найважливіша складова «Ешелону» – це комп'ютерна мережа АНБ, кодове ім'я «Платформа» (англ. *Platform*), що взаємно погоджує 52 окремі мережі суперкомп'ютерів, що знаходяться в інших частинах світу. Командний центр «Платформи» розташовується у штаб-квартирі АНБ. Комп'ютерні мережі місцевих мереж «Ешелону» шукають у мільйонах перехоплених повідомлень ті, що містять кодові слова. Завдяки високоорганізованому системному забезпеченню, керування даними цілком автоматизовано, і координація станцій у єдину мережу така, що центральні органи системи мають практично миттєвий доступ до всієї значимої інформації з усього світу.

У середині 1990-х років комп'ютери «Ешелону» ще не вміли автоматично розпізнавати та перетворювати мову в текст, тому фіксували телефонні переговори за визначеними параметрами та тривалістю. Але до початку 2-го тисячоліття проблема була вирішена, і у Менвіт-Хіллі з'явився підрозділ збору та аналізу отриманої інформації «*C/TAR*» (англ. *Collection/Transcription Analysis and Reporting division*), що має два відділи: 1) Росії і країн колишнього СРСР і 2) усіх інших країн.

Система «Ешелон» розвивалася дуже швидко, оскільки АНБ, яка володіла колосальними фінансовими засобами, не шкодувала для цього грошей. Прогресувала комп'ютерна техніка, удосконалювалися приймальні і передавальні антени, а також дешифратори. АНБ одержало можливість запускати власні супутники-шпигуни та ввести до свого штату велику кількість професійних програмістів.

В даний час в АНБ працюють до 10 тільки надпотужних комп'ютерів серії «Крей» (англ. *Cray*) вартістю в десятки мільйонів доларів кожний, створені за спецзамовленням АНБ компанією «Сілікон Графікс» (англ. *Silicon Graphics* - кремнієва

графіка). Наприклад, суперкомп'ютер «*Cray-1*» у 1976 році виконував 240 мільйонів арифметичних операцій та коштував від 4 до 11 мільйонів доларів у залежності від комплектації. Створений у 1988 році суперкомп'ютер «*Cray-YMP*» поєднував уже до 16 процесорів та коштував від 2,5 до 16 мільйонів доларів. Вартість таких обчислювальних систем ставала просто астрономічною, якщо до ціни устаткування додавалися витрати на виготовлення програмного забезпечення.

Хоча номенклатура, кількість і характеристики встановлених у цьому відомстві суперкомп'ютерів засекречені, за розрахунками фахівців їхня сумарна продуктивність складає величину порядку 156 Гфлоп. АНБ належить одна із наймогутніх за кількістю процесорів (1024) моделей суперкомп'ютер «*Cray-T3D*». За останні 10 років загальна кількість суперкомп'ютерів у світі, зв'язаних із секретними проектами (у тому числі й у сфері криптоаналізу), за офіційною статистикою коливалася в межах від 19 у 1993 році до 46 у 1998 році та складає в даний час 25 одиниць. Враховуючи це, неважко оцінити в першому наближенні кількість ЕОМ цього класу й в АНБ, узявши за основу частку США в їхній загальній масі (46%) – 12 одиниць.

Для перехоплення інформації на території країн СНД (колишнього СРСР) АНБ був створений спеціальний центр радіо- і радіотехнічної розвідки, розташований недалеко від Аугсбурга (Німеччина). Це найбільший центр перехоплення АНБ: його головна антена діаметром 300 м і висотою 30 м, а службові приміщення центра розташовані під землею на глибині 25 м на 12 поверхах. Не будемо забувати і супутників-шпигунів. З 1996 року над територією країн СНД висять 3 супутники високодетальної видової розвідки «Кіхоул» (англ. *Keyhole* – свердловина).

Орбітальна побудова супутників забезпечує мінімум два щоденні прольоти над будь-якою крапкою цих країн. Крім того, інформацію в нічний час і хмарну погоду забезпечують супутники «Лакрос». Ці супутники виконують радіоперехоплення повідомлень, переданих по космічних, тропосферних, радіорелейних і інших лініях радіозв'язку.

У функціонуванні «Ешелону», крім США і Великобританії, сьогодні також беруть участь спеціальні технічні служби таких країн, як Канада (англ. *Communications Security Establishment* - Міністерство безпеки комунікацій), Австралія (англ. *Defence Signals Directorate* - Директорат захисту зв'язку) і Нова Зеландія (англ. *Government Communications Security Bureau* - Бюро безпеки урядових ко-

мунікацій).

У вкрай спрощеному вигляді «Ешелон» працює приблизно таким чином. Джерелами інформації служать Інтернет, електронна пошта, телефон і телефакс. Повідомлення, передані цими шляхами, скануються надпотужними комп'ютерами, так званими словниками «Ешелону», за ключовими словами, виразами, тембром голосу (наприклад, зі 100 мільйонів перехоплених повідомлень відбирається 10 тисяч).

Як тільки суперкомп'ютери окремої мережі виявляють ключове слово – ім'я, назва, номер телефону або телефаксу, електронна поштова адреса (англ. *e-mail*), «відбиток» голосу, що у кожної людини індивідуальний, як відбитки пальців, то дане повідомлення шифрується та відправляється на базу. Перед відправленням комп'ютер автоматично записує подробиці повідомлення – час/місце перехоплення, адресат/відправник, тип зв'язку.

Ці ключові слова та вирази постійно поновлюються. Принцип схожий на той, який використовують пошукові системи мережі «Інтернет» (англ. *Internet*), але на відміну від них «Ешелон» працює в реальному часі та вже в процесі, наприклад, телефонної розмови вирішує: цікаве йому це повідомлення чи ні.

«Ешелон» знає безліч мов, знайомий із професійним «сленгом» (наприклад, торговців наркотиками або зброєю) і спеціальною лексикою, знає «клички» або прізвиська великих політичних діячів провідних країн світу. До того ж АНБ навчилася одержувати «відбиток голосу», що так само унікальний, як і відбиток пальця. За наявним у пам'яті комп'ютера зразком голосу можна швидко ідентифікувати будь-який голос у потоці звуків. Іншими словами, якщо «Ешелон» один раз зареєстрував голос якоїсь людини, то потім може відстежити її розмову з будь-якого телефонного апарату у світі.

Що ж стосується мережі «*Internet*», то АНБ одержало від «Майкрософт» (англ. *Microsoft*), «Нетскейп» (англ. *Netscape*), «Лотус» (англ. *Lotus*) та інших фірм-виробників комп'ютерних програм ключі або так звані «закладки», що дозволяють зацікавленим особам ідентифікувати всі, навіть анонімні, повідомлення. В результаті «Ешелон» здатний відслідковувати практично весь інформаційний потік (трафік) у світі.

На другому етапі повідомлення, відібрані скануючими комп'ютерами з усього світу, потрапляють

у блок накопичення інформації. Там вони записуються, сортуються по темах (наприклад, «військові справи», ракетні або ядерні технології, тероризм, політика, зброя, наркотики, контрабанда тощо) та направляються для подальшого аналізу. Потім спеціально розроблені для кожної теми програми аналізують отриману інформацію з заданих тем. З відібраних на першому етапі 10 тисяч повідомлень залишається тільки 100-200 дійсно важливих.

Четвертим етапом, після якого матеріали, як правило, попадають на стіл посадовців в адміністрації США, стає вже експертна оцінка співробітників профільних відділів АНБ у штаб-квартирі спецслужби у Форт-Міді по кожному з отриманих 100-200 повідомлень. Сумнівні випадки залишаються в пам'яті комп'ютерів АНБ, а оскільки ця пам'ять практично нескінченна, то усе більше людей (а отже, й урядових структур, фірм, компаній, концернів тощо) у світі потрапляють у поле зору «Ешелону».

Якщо в АНБ одержують декілька примірників того ж самого повідомлення, перехоплених різними радіостанціями, редактори намагаються усунути в ньому всі наявні перекручування. Потім здійснюється порівняння і зіставлення місцезнаходження відправників і одержувачів повідомлень, маршрути їхнього проходження і службові позначки, що наявні у цих повідомленнях для шифрувальників і операторів зв'язку. Це дозволяє відсортувати перехоплені повідомлення за принципом приналежності до однакових шифросистем. Загальна картина листування у всій її повноті дозволяє виявити загальну структуру мережі зв'язку та одержати іншу корисну інформацію.

Експерти стверджують, що система здатна проаналізувати та запам'ятати до 3 мільярдів повідомлень у день. На їхню думку, у службах АНБ, зайнятих у «Ешелоні», працюють до 30 тисяч співробітників по усьому світі – математики, програмісти, лінгвісти, криптологи. Іноді більшість із них і не підозрює, чим вони займаються. Так було, наприклад, з групою з 40 співробітників компанії «Брітіш Телеком» (*British Telecom*). Як з'ясувалося, ці люди не мали ніякого відношення до АНБ або британської радіоелектронної розвідки, але ними перехоплювалося все – від посольської пошти та ділових повідомлень до особистих привітань на день народження.

«Ешелон» сьогодні цікавить усе – від тероризму до новітніх промислових технологій. Однак як і раніше, незважаючи на умови, що змінилися (розпад СРСР і Організації Варшавського договору, закінчення «холодної війни» тощо), однією з основних завдань «Ешелону» залишається спостереження за країнами СНД.

До речі, у програми «Ешелон» існує також і європейський аналог «Енфопол» (англ. *Enfopol*). Якщо про першу написано досить багато, то друга залишається «в тіні». А тим часом її реалізація почалася ще у 1998 році, коли Рада міністрів внутрішніх справ і юстиції держав-членів Євросоюзу розробила проект положення про порядок доступу до даних, що циркулюють у сучасних засобах телекомунікацій. У першу чергу запропоновані заходи стосувалися супутникового зв'язку, зокрема:

проект «Ірідіум» (англ. *Iridium*), пейджерних систем, кабельних і мобільних телефонних систем, а також провайдерів «*Internet*».

Діяльність Міжнародного семінару правоохоронних органів з телекомунікацій «*ILETS*» має конспіративний характер. І це не тільки через те, що представники двадцяти спецслужб Західної Європи, Канади, США, Гонконгу, Австралії та Нової Зеландії звикли залишатися в «тіні». Організація була створена в 1993 році після того, як ФБР не вдалося «протягти» через американський парламент закон, що зобов'язує виробників телекомунікаційного устаткування встановлювати засоби перехоплення. Міжнародні вимоги з перехоплення «*IUR 1.0*», прийняті «*ILETS*», стали основою таємної політики Євросоюзу в сфері моніторингу систем зв'язку.

На початку 2000 року тимчасова комісія Європарламенту, яка була утворена для з'ясування факту існування таємної системи глобального шпигунства «Ешелон», остаточно з'ясувала факт її існування, що АНБ офіційно підтвердило. Висновки комісії ґрунтувалися на результатах дослідження, що підтвердили наявність такої програми, розробленої спільними зусиллями урядів США, Канади, Англії, Австралії та Нової Зеландії.

Крім того, АНБ ще з 40-х років минулого сторіччя розпочала «підривати» ефективність криптосистем інших країн. Найбільш важливою мішенню активності АНБ стала відома швейцарська компанія «Крипто АГ» (англ. *Crypto AG*), створена Борисом Хагеліном. «*Crypto AG*» мала сильні позиції як постачальник систем кодування після Другої світової війни. Багато урядів тоді не довіряли обладнанню, що пропонувалися до продажу основними світовими державами. Швейцарська компанія у цій сфері мала кращу репутацію завдяки іміджу нейтральності та чесності Швейцарії.

АНБ домоглася того, щоб системи шифрування, які використовувалися «*Crypto AG*», були скомпрометовані. Таємна операція АНБ була проведена через засновника й власника компанії Бориса Хагеліна та включала періодичні візити у Швейцарію «консультантів» зі США, що працювали на АНБ. Однією з них була Нора Мак-Кабі, співробітниця АНБ. В результаті, американська преса одержала копії конфіденційних документів «Crypto AG» із записами участі Мак-Кабі в обговоренні розробки нових машин у 1973 році. Було виявлено, що протягом тривалого часу АНБ перехоплювало та розшифровувало таємну інформацію майже 120 країн, що користувалися устаткуванням «*Crypto AG*».

З іншого боку, АНБ проводить «шпіонські» операції щодо зібрання розвідувальної інформації в інтересах американського уряду. Вона здійснює перехоплення даних з трафіка мережі «Internet». Для того, щоб усе проходило без проблем, була проведена «невелика» підготовча робота. Агенція витратила багато часу та зусиль на те, щоб змусити виробників програмного забезпечення, а також комутаторів і маршру-

тизаторів внести до своєї продукції необхідні зміни. Наприклад, програмісти можуть при написанні вихідного коду додатків включити туди модулі, що реалізують якісь недокументовані можливості. Причому такі «вставки» дуже важко знайти. Мета дуже проста – гарантувати уряду США вільний доступ до чужих шифрованих даних.

Метою АНБ було також забезпечення ілюзії надійності систем шифрування для інших шифрувальників, у той час як для них самих процес дешифрування був би простим. Щоразу при використанні шифросистеми користувачі могли вибрати довгий цифровий ключ, що змінювався періодично. Природньо, користувачі хотіли мати свої ключі, невідомі АНБ. Для підтримання довіри користувачів, система шифрування повинна була дійсно працювати та бути складною для дешифрування. Рішення АНБ складалося в розробці шифросистеми таким чином, щоб та передавала використовуваний ключ одержувачам. Для запобігання одержання ключа несанкціонованими одержувачами ключ також пересилався в засекреченому вигляді – іншим шифром, відомим тільки АНБ. Таким чином, щоразу, коли АНБ перехоплювала повідомлення, зашифроване даною системою, вона могла спочатку прочитати їхню зашифровану частину повідомлення, названу «hilfsinformationen» (поле інформаційної підказки) і виділити використаний ключ. Після цього вона вже могла прочитати повідомлення навіть швидше, ніж його санкціонований одержувач.

АНБ також всіляко прагне до того, щоб послабити експортні версії криптологічних програм американських компаній. Вищезазначена технологія була використана у 1995 році, коли з'явилися системи криптозахисту, вбудовані в програмні продукти, що вироблялися компаніями «*Microsoft*», «*Netscape*» і «*Lotus*» для використання в мережі «*Internet*». Під натиском АНБ компанії погодилися знизити ступінь захисту, наданий користувачам поза межами США. У програмі «Lotus Notes» була надійна система електронної пошти з 64-бітним ключем. Це дозволяло забезпечити середній рівень безпеки, що у даний час може бути розкритий АНБ тільки через місяці або роки роботи. За рекомендацією АНБ компанія «*Lotus*» вмонтувала у свою систему «приховану відмичку», в результаті чого Агенція отримала доступ до шифрованої електронної пошти користувачів програмного забезпечення «*Lotus Notes*».

На той час це програмне забезпечення було застосовано для конфіденційного листування в головних урядових закладах Швеції, використовувалось 15 тисячами співробітниками податкових служб і 400-500 тисячами шведськими громадянами. «*Lotus Notes*» включало «фактор скорочення навантаження» в усі повідомлення, що посилалися неамериканськими користувачами системи. «Фактор скорочення навантаження», закодований з використанням «публічного ключа», що міг бути прочитаний тільки в АНБ, передавав 24 з 64 біт ключа, який використовувався при шифруванні.

Це було виявлено шведським урядом у 1997 році та викликало в нього сильний шок. Це стало можливим тому, що в систему захисту електронної пошти

«Lotus Notes», призначену для експорту, був включений модуль, що давав АНБ доступ до шифрованих даних. Це перетворювало завдання з розкриття таємних повідомлень у справу декількох секунд. Компанія «*Lotus*», що входила до структури компанії «*IBM*», визнала це в інтерв'ю виданню «*SvenskaDDagbladet*».

Аналогічні можливості були вбудовані в усі експортні версії «веб-браузерів», вироблених для користувачів мережі «Internet» компаніями «*Microsoft*» і «*Netscape*». Кожна використовує стандартний 128-бітний ключ для шифрування. В експортній версії ключ не скорочений за довжиною. Замість цього, 88 бітів ключа передаються в кожному повідомленні, а 40 бітів залишаються таємними. Отже, майже кожен комп'ютер у більшості країн має вбудовану стандартну можливість, що дозволяє АНБ розкрити код користувача та прочитати зашифровану електронну пошту.

Деякі компанії, у тому числі «Microsoft», раніше вже обвинувачувалися пресою в співробітництві з АНБ, тому що дозволили включити у свої програми спеціальні «чорні» коди. Аналогічний випадок, можливо, мав місце також з криптопрограмою Пилипа Циммермана «*PGP*» (англ. *Pretty Good Privacy* - достатньо хороша приватність), коли в ній був виявлений дуже серйозний дефект. Ця програма зазвичай використовується користувачами мережі «*Internet*» для шифрування електронної пошти.

Відомий криптолог Брюс Шнайер ще в 1999 році розповів читачам щомісячного електронного бюлетеня про одного таємничого співробітника АНБ Ллю Джайлзе. Він займався винятково тим, що змушував виробників послабляти системи захисту розроблених ними програмних засобів. Зрештою, говорив він, завжди можна всі «діри» у захисті пояснити випадково допущеними помилками. Саме в той час у «*PGP*» і була введена функція «відновлення ключа», що мала прихований дефект, який став недавно широко відомий. Згодом у різних версіях цієї програми були виявлені також інші серйозні недоліки. Наприклад, виявилося, що у версії «*PGP*» для операційних систем «*Linux*» і «*OpenBSD*», які були створені у 1997 році, вироблялися слабкі ключі.

Звичайно, більшість виявлених дефектів у програмах з'являється, як правило, з недогляду розробників. Але дуже ймовірно й те, що деякі з них є спеціально впровадженими «чорними» кодами. У різних засобах масової інформації час від часу публікується інформація, отримана від співробітників компаній з виробництва комп'ютерної техніки та програмного забезпечення, про те, як їх «обробляло» АНБ. Агенції новин «*CNN*» і «*Network World*» розповіли про те, як АНБ змушувало фірми, які виробляють мережеве устаткування, вносити до своєї продукції зміни в інтересах АНБ. До компаній, що співробітничають з АНБ, хоча і не завжди з бажанням, відносяться, наприклад, «*Microsoft*», «*Netscape*», «*Sun*».

Ще наприкінці 1990-х років в мережі «Internet» з'явилася історія про те, як один прискіпливий програміст, вивчаючи код підпрограм в операційній системі «*Microsoft Windows NT*», знайшов змінну с виразним ім'ям «*_NSAKEY*», тобто «ключ

АНБ». Особливого скандалу з цієї історії не вийшло, оскільки для присутності такої змінної знайшли більш-менш безневинні пояснення, а назву заради загального спокою змінили на нейтральне «*_KEY2*». Крім того, добре відомо, що саме АНБ, коли цього вимагали американські закони, завжди контролювало зниження криптостійкості в програмних продуктах, призначених для експортних продажів.

На початку 2005 року в мережі «Internet» з'явилася стаття сингапурського криптолога Хонг-юн Ву, який досліджував конкретну реалізацію алгоритму шифрування документів «*Word*» і «*Excel*» у сучасних версіях «*Microsoft Office*». Він виявив, що й тут існує досить серйозна слабкість, яка дозволяє без особливих проблем «розкривати» та читати файли, захищені шифруванням з довжиною ключа до 128 біт. І причина тому – споконвічна проблема неправильного застосування потокового шифру, а саме, кількаразове використання однієї й тієї ж шифруючої послідовності.

Серед фундаментальних основ криптографії є дуже важливе правило: якщо для засекречування використовується потоковий шифр, то ніколи одну шифропослідовність не накладають на два різні документи. У даному контексті під «однаковими» документами розуміються файли, що збігаються байт у байт, тобто повні копії. Будь-яка вставка або видалення знака призводять до зрушень інших байтів на інші місця, тобто за підсумком – до «різних» файлів. І якщо у «зломщика» є хоча б два різні документи, зашифровані одним ключем, то все шифрування – хоч й дуже стійке – у принципі можна «розкрити» простим побітовим додаванням двох шифротекстів разом, навіть не знаючи криптоалгоритму. При такому додаванні біти шифропослідовності «випадають» (взаємно знищуються), і залишається сума двох відкритих текстів. Маючи базові криптоаналітичні навички, а ще краще спеціальні програми, «зломщик» може обидва ці документи відновити за допомогою відомих криптометодів.

Як встановив Хонг-юн Ву, при реалізації процеса шифрування в «*Microsoft Office*» була допущена саме ця криптографічна помилка. Коли документ «*Word*» або «*Excel*» захищають паролем, то скільки б текст файлу не модифікувався, «*RC4*» увесь час генерує ту ж саму шифропослідовність. Іншими словами, якщо зловмиснику вдасться роздобути більше однієї, хоча б дві, версії зашифрованого документа, то «розкриття» цього комплекту – вже справа техніки. У реальному житті, відзначимо, поява таких комплектів не рідкість, оскільки при архівному копіюванні звичайно зберігається один із проміжних варіантів файлу, що знаходиться в роботі, а в організаціях і офісах багато документів готують-редагують кілька людей, переносячи варіанти з одного комп'ютера на інший. Зрозуміло, що ця помилка фірми «*Microsoft*» невипадкова та зроблена в інтересах АНБ.

Крім того, як повідомила газета «*Washington Post*», АНБ підтвердила, що надала допомогу в розробці безпеки операційної системи «*Microsoft Windows Vista*», щоб захистити її від «хробаків», «троянських коней» та інших підступних комп'ютерних загроз. Як сказав Тоні Сейджер, керівник одного з підрозділів АНБ, які брали участь у

роботі, «нашим наміром було допомогти усім у забезпеченні безпеки». При цьому і «*Microsoft*», і АНБ відмовилися вдаватися в подробиці щодо того, який саме внесок зробила спецслужба в підсистему захисту «*Windows Vista*». Також в АНБ відмовилися давати коментарі щодо своєї роботи у сфері комп'ютерної безпеки з іншими комп'ютерними фірмами, але відзначили, що «*Microsoft*» – єдина компанія, з якою є «такого роду відносини, коли факт співробітництва визнається привселюдно». За свідченням представників спецслужби, допомога «*Microsoft*» була безоплатною, а ідея про публічне визнання участі АНБ у розробці «*Vista*» виходила від корпорації...»

З боку захисту інформації, найважливіша, мабуть, особливість «*Vista*» – це криптографічна підсистема «*BitLocker*» (для версій «*Vista Ultimate*» і «*Vista Business*»), що дає користувачам можливість шифрувати всі дані на твердому диску та вже одержала репутацію надзвичайно надійного засобу. За свідченням відомого експерта Росса Андерсона, що виступив перед членами британського парламенту, без таємного «чорного» коду системи у компетентних англійських органів практично немає шансів одержати доступ до даних у комп'ютерах злочинців, якщо там є «*BitLocker*».

Крім того, АНБ вже добралося й до систем захисту банківських мереж. Коли компанія «*MasterCard International*» виробляла стандарт шифрування «*SET*», який використовується сьогодні в електронних транзакціях, АНБ швидко «остудило» її ентузіазм. «Вони повідомили нам, що можна і що не можна робити», – сказав Джон Ванкмюллер, що відповідав в компанії за електронну комерцію. АНБ наполягло на тому, щоб велика частина інформації при кожній транзакції взагалі не шифрувалася, оскільки хоче знати, хто і куди переказує гроші.

2.12. Народження асиметричної криптології

Наукові основи криптології істотно розширили дві наукові роботи, написані у післявоєнні роки минулого століття, а саме: стаття американця Клода Елвуда Шеннона «Communication Theory of Secrecy Systems» (Теорія зв'язку в таємних системах) і стаття радянського вченого Володимира Котельникова «Основні положення автоматичного шифрування». Ці статті цілком знищили райдужні надії й упередження, розвіяли міфи та зруйнували вікові легенди, а також зняли з криптології покрив таємниці.

Талановитий інженер Шеннон у 1941 році почав працювати в математичному відділенні науково-дослідного центра «Бел Лебораторіз» (англ. *Bell Laboratories* - лабораторії Белла), зосередженого переважно на проблемах військових комунікаційних систем і криптографії. Напружена робота в цій сфері за роки війни дала найбагатші плоди в мирний час. У 1948 році він опублікував свою епохальну працю «Математична теорія зв'язку». Мета цієї роботи була практична – як покращити передачу інформації телеграфним або телефонним каналом, який знаходиться під впливом електричних шумів. При вирішенні цього завдання в Шеннона народилася воістину революційна праця, що поклала початок цілій науці за назвою

«теорія інформації».

Наступна епохальна робота Клода Шеннона «Теорія зв'язку в таємних системах», що з'явилася практично одночасно з «теорією інформації» та була оприлюднена в 1949 році, з деяких причин не одержала такого ж широкого резонансу, оскільки явно випереджала свій час відразу на кілька десятиліть. Насправді дана стаття являла собою трохи перероблений звіт, підготовлений Шенноном ще в 1945 році. Світове значення цієї праці полягає в тому, що тепер вся історія криптології від античності до сьогодення поділяється на два періоди: до 1949 року, коли «тайнопис» вважався шаманством, окультизмом і видом мистецтва, і після 1949 року, коли криптологія стала повноцінною прикладною наукою на базі фундаментальної математичної теорії.

Шеннон довів, що запропонований Вернамом у 1917 році метод шифрування з застосуванням випадкової комбінації знаків (гами), об'єднаний з одноразовим шифроблокнотом, – це єдина абсолютно стійка система шифрування за умови, що довжина ключа дорівнює довжині самого повідомлення. У своїй статті він виділив два основні принципи, що використовуються у шифрах: розсіювання та перемішування. Розсіювання – це поширення впливу одного знака відкритого тексту (або, що більш важливо, одного знака ключа) на багато знаків шифротексту, що дозволяє сховати статистичні особливості тексту і, у свою чергу, ускладнити відновлення ключа.

Перемішуванням Шеннон назвав використання таких шифруючих перетворень, що ускладнюють відновлення взаємозв'язку між відкритим текстом і шифротекстом. Основною ідеєю його була суперпозиція простих шифрів, що реалізують розсіювання та перемішування, кожний з яких давав малий приріст складності дешифрування, але в сукупності можна було одержати досить стійку систему. Подібна суперпозиція називається складеним шифром. У практичних складених шифрах найчастіше використовуються перестановки (перемішування символів відкритого тексту) і підстановки (заміна символу або групи символів іншим символом з того ж алфавіту), при цьому конкретний алгоритм перестановки та підстановки визначається тільки таємним ключем.

Основним результатом згаданої роботи було те, що Шеннон увів поняття стійкості шифру і показав, що існує шифр, який забезпечує абсолютну таємність. Іншими словами, знання шифротексту не дозволяє супротивнику покращити оцінку відповідного відкритого тексту. Ним, як уже сказано вище, може бути, наприклад, шифр Віженера за умови використання нескінченно довгого ключового слова і випадкового розподілу символів у цьому слові. Вочевидь, що практична реалізація такого шифру (нескінченна випадкова стрічка) неможлива (точніше, у більшості випадків – економічно невигідна), тому звичайно розглядають практичну стійкість шифру, що вимірюється числом елементарних операцій, необхідним на його розкриття. Ця оцінка останнім часом використовується більш часто, ніж оцінка часу, оскільки стрімкий розвиток обчислювальної техніки робить оцінку часу більш некоректною.

Переважна більшість систем шифрування є лише розумно стійкими, оскіль-

ки криптоаналітик, маючи у своєму розпорядженні великий обсяг шифрованого тексту і досить часу, може знайти шляхи розшифрування повідомлень. Одноразовий же шифроблокнот – абсолютно стійкий як у теорії, так і на практиці. Яким би довгим не був перехоплений текст, скільки б часу не приділялося на його дослідження, криптоаналітик ніколи не зможе розкрити одноразовий шифроблокнот, використаний для одержання цього шифротексту.

Адже у криптоаналітика немає відправної крапки для досліджень, тому що «гама» не містить повторень, не використовується двічі, не є зв'язним текстом і не має структурних закономірностей. Тому криптоаналіз неспроможний. Залишається тільки метод прямого перебору всіх можливих ключів, що у кінцевому рахунку повинно привести до відкритого тексту. Однак тотальне випробування, що дійсно дозволяє одержати вихідний текст, також дасть і ще безліч пов'язаних текстів тієї ж довжини.

До теперішнього часу для захисту таємної державної інформації, військових і дипломатичних таємниць, державними організаціями й, насамперед, спецслужбами застосовується тільки симетрична криптологія. Симетрична криптологія – це шифрування інформації, симетричним або таємним, ключем, коли той же самий ключ використовується як для зашифрування, так і для розшифрування даних.

Перевагами такої криптології є велика продуктивність криптоалгоритмів та висока криптостійкість, що робить практично неможливим процес дешифрування. Разом із тим, симетрична криптологія монополізована державними структурами та потребує значних фінансових витрат. Для її використання потрібні дуже надійні механізми для розподілу ключів та їх велика кількість. Особливо важливою умовою функціонування симетричної криптології є таємність ключа та система його надійного та гарантованого розповсюдження, щоб він не попав у «чужі руки».

Ця проблема передачі ключа шифрування була теоретично вирішена в 1976 році, коли американці Уітфілд Діффі і Мартін Хеллман опублікували статтю «Нові шляхи криптографії», що зробила в шифрувальному співтоваристві дійсний бум.

Відкритий текст	Зашифрування *таємним* ключем	Шифротекст	Канал передачі	Шифротекст	Розшифрування *таємним* ключем	Відкритий текст

Вони запропонували концепцію шифрування з *відкритим*, або *асиметричним*, ключем. Це була воістину революція, причому дуже своєчасна, оскільки жоден з відомих у той час алгоритмів єдиного виду – симетричного шифрування із секретним ключем – більше не міг відповідати новим потребам, викликаним зростанням нових методів обміну повідомленнями і, зокрема, появою глобальних мереж передачі ін-

формації.

Але, як стверджує світовий досвід, великі наукові відкриття завжди роблять декілька вчених у різних країнах світу. Так, у 1997 році стало відомо, що група криптологів ШКУЗ відкрила основні принципи криптології з відкритим ключем на кілька років раніше, ніж їхнього колеги з академічного й індустріального співтовариства.

Наприкінці 60-х років минулого століття британські збройні сили вже цілком реально відчували наступ ери високих технологій, що обіцяла забезпечити кожного бійця власним входом у тактичну радіомережу. Перспективи розгортання таких мереж обіцяли грандіозні зміни у спрощенні керівництва військовими операціями, однак ставили і дуже серйозні проблеми перед службою, що відповідала за безпеку та засекречування такого зв'язку. Дійсним головним болем ставала необхідність розподілу та керування гігантськими кількостями криптоключів, причому передавати кожний з ключів треба було в найсуворішій таємниці від ворога.

Тому в 1969 році одному з видатних творчих «розумів» ШКУЗ Джеймсу Еллісу було доручено поміркувати над можливим виходом з цієї безнадійної ситуації. Спочатку для Елліса, як і для всіх, було очевидно, що не може бути ніякого засекреченого зв'язку без таємного ключа, якойсь іншої таємної інформації, або принаймні якогось способу, за допомогою якого законний одержувач знаходився б у позиції, що відрізняла його від того, хто перехоплював передачі. Зрештою, якби вони були в однаковому положенні, то як один мав би можливість одержувати те, що інший не може?

Але, як це часто трапляється напередодні відкриття, Елліс натрапив на давню технічну статтю невідомого автора з компанії «Bell Telephone», у якій описувалася дотепна, але так і не реалізована ідея засекреченого телефонного зв'язку. Там пропонувалося, щоб одержувач маскував мову відправника шляхом додавання в лінію шуму. Сам одержувач згодом міг відфільтрувати шум, оскільки він же його і додавав і, отже, знав, що той собою уявляв.

Принципово ж важливим моментом було те, що одержувачу вже не було необхідності знаходитися в особливому положенні або мати таємну інформацію для того, щоб одержувати засекречені дані... Первинний ідейний поштовх виявився достатнім: розходження між описаним і загальноприйнятим методом шифрування полягало в тому, що одержувач сам брав участь у процесі засекречування.

Далі перед Еллісом постало досить очевидне питання: «А чи можна щось подібне проробити не з каналом електричного зв'язку, а зі звичайним шифруванням повідомлення?» Як відомо, для вирішення завдання головне – правильно сформулювати питання, тому як тільки одного разу питання отримало потрібну форму, то доказ теоретичної можливості цього зайняло усього кілька хвилин. Так народилася «теорема існування». Те, що було немислиме, насправді виявилося цілком можливим.

Таким чином Елліс прийшов до схеми, що пізніше одержала назву «криптографія з відкритим ключем», але сам він назвав свою концепцію «нетаємним шифруван-

ням». Суть концепції, сформульованої і формально підтвердженої до початку 1970 року, зводилася до схеми з відкритим і таємним ключами, керуючих односпрямованою математичною операцією. Правда, оскільки Елліс був насамперед експертом у системах комунікацій, а не в математиці, то його революційна концепція не була доведена до конкретних математичних формул. Доповідь Елліса зробила велике враження на його керівництво, однак ніхто не зміг вирішити, що з цими екзотичними ідеями робити... В результаті справа на декілька років була «захована у шухляду».

А ось що відбувалося в той же час по інший бік океану, у Стенфордському університеті США. Тут на початку 1970 року молодий професор Мартін Хеллман почав займатися питаннями проектування електронних комунікаційних систем, активно залучаючи математичний апарат криптографії і теорії кодування. Цими речами він захопився з тих пір, як прочитав статті Клода Шеннона з теорії інформації та криптографії, опубліковані в 1948 і 1949 роках. За словами Хеллмана, до цього він «і уявити собі не міг, наскільки тісно пов'язане шифрування та теорія інформації».

У статтях Шеннона питання кодування розглядалися у зв'язку з завданням зниження шумів електростатичних перешкод, що заважали передачі радіосигналів. Хеллману стало зрозуміло, що «шифрування вирішує діаметрально протилежну задачу. Ви вносите перекручування за допомогою ключа. Для того, хто чує сигнал і не знає ключа, він буде виглядати максимально перекрученим. Але легітимний одержувач, якому відомий таємний ключ, може видалити ці перешкоди»... Неважко помітити, що траєкторія виходу на винахід у Хеллмана була по суті справи та ж сама, що й у Елліса.

Але в ті часи ні інформативних книг, ні довідників з криптології в академічних учених практично не було, оскільки ця наука вважалася суворо засекреченою справою військових і спецслужб. Намагаючись об'єднати розрізнені ідеї з шифрування даних, Хеллман одночасно шукав однодумців. Але трапилося так, що головний однодумець вийшов на нього сам.

У вересні 1973 року Хеллмана знайшов Уітфілд Діффі, випускник Массачусетського технологічного інституту та співробітник Стенфордського університету, жагуче захоплений криптологією. Їхня півгодинна зустріч плавно перейшла в обід у Хеллмана, після чого розмови затяглися далеко за північ. З цього моменту Хеллман і Діффі почали спільно працювати над створенням криптосхеми для захисту транзакцій купівель і продажей, що робилися з домашніх комп'ютерів. Головна проблема, яку з подання Діффі поставили перед собою вчені, зводилася до наступного: «Як (не пересилаючи таємний ключ) одержати повідомлення та перетворити його таким чином, щоб його сприймали тільки ті, кому воно призначено, а стороннім інформація була б недоступна»...

Тим часом у Великобританії у вересні 1973 року співробітником ШКУЗ став молодий талановитий математик Кліффорд Кокс, який тільки що закінчив Кемб-

ридж і був досить освічений у теорії чисел (яку в ті часи звичайно розцінювали як один з найбільш красивих і марних розділів математики). Вже на початковому етапі хтось з наставників розповів Коксу про концепцію нетаємного шифрування. Ідея вкрай його зацікавила, і він почав вичати її у контексті простих чисел і проблем розкладання чисел на множники.

В результаті Кокс прийшов до тієї ж схеми, яка через кілька років стане знаменитою під назвою «*RSA*», або алгоритм Рівеста-Шаміра-Адлемана. Сам же Кокс у той момент сприймав своє відкриття просто як вирішення достатньо простої математичної головоломки. Він був досить здивований тим, у яке хвилювання і, навіть, зворушення прийшли його колеги. Але керівництво ШКУЗ знову не стало робити ніяких кроків для практичної реалізації цієї ідеї, оскільки для широкого впровадження цілочисельних операцій над числами величезної довжини були потрібні обчислювальні потужності, що були надто дорогими у той час.

Кілька місяців по тому на роботу до ШКУЗ прийшов інший обдарований математик Мелколм Уільямсон, приятель Кокса ще за шкільних років. Коли Кокс розповів другу про цікаву криптосхему, то недовірливий Уільямсон вирішив, що вона надто красива, щоб бути правдою, і тому ринувся відшукувати в ній приховані дефекти. Слабкостей йому знайти так і не вдалося, але в процесі пошуків він дійшов до ще одного алгоритму формування загального ключа шифрування. Іншими словами, у 1974 році Уільямсон відкрив те, що вже майже народилося в Америці та незабаром стало відоме як схема розподілу ключів Діффі-Хеллмана-Меркля.

Жодної з винайдених криптосхем у ШКУЗ патентувати не стали, оскільки патентна інформація ставала відома широкому загалу, а абсолютно всі роботи велися спецслужбою в умовах найсуворішої таємниці. Коли в 1976 році Діффі і Хеллман оприлюднили свої відкриття, Уільямсон спробував було схилити керівництво ШКУЗ до публікації отриманих англійськими криптологами результатів. Однак молодій людині не вдалося пробити «залізобетонний» консерватизм керівництва, що вирішило не порушувати традицій та не «висуватися» зі своїми пріоритетами.

Через кілька років, завдяки знайомствам в АНБ, Уітфілд Діффі все ж таки дізнався про роботи в ШКУЗ і, навіть, особисто з'їздив до Челтнему, щоб зустрітися та поспілкуватися з Джеймсом Еллісом. Зустріч була вкрай теплою та привітною, однак безрезультативною. Елліс, зобов'язаний зберігати державну таємницю, ввічливо ухилився від усіх спроб Діффі перевести розмову про криптологію з відкритим ключем.

ШКУЗ декілька разів мала намір розповісти правду. У 1987 році Еллісу у зв'язку з його виходом на пенсію навіть замовили статтю для можливого оприлюднення, однак на головний крок так і не зважилися, сховавши її у таємному архіві. До читачів стаття дійшла лише в грудні 1997 року, уже як меморіальна публікація в пам'ять про Джеймса Елліса, що помер за місяць до цього у віці 71 року. Одночасно Кліффорду Коксу вперше дозволили опублікувати кілька робіт щодо вирішення деяких про-

блем навколо схеми «*RSA*» і виступити на відкритих наукових конференціях.

Таким чином, якщо до 1976 року єдиним способом пересилання таємної інформації була симетрична криптологія, а організувати канал для передачі таємних ключів могли собі дозволити тільки уряди, великі банки та корпорації, то поява шифрування відкритим ключем стала технічною революцією, яка понесла стійку криптологію «в маси».

Асиметрична криптологія є безсумнівно вигідною, оскільки вона легко застосовується та вирішує проблеми авторизації. Точніше, вона вирішує декілька таких проблем:

1. Ідентифікація користувача. Дає змогу користуватися сучасними засобами зв'язку, що дозволяють відправнику залишатися невідомим та, разом з тим, бути упевненим у тому, що той, з ким ми спілкуємося, – дійсно той, за кого себе видає. Для цього використовується протокол ідентифікації.

2. Автентифікація документа. Автор засвідчує документ за допомогою цифрового підпису. Операція підпису додає до повідомлення кілька біт, що є результатом якоїсь операції над самим документом і відомостями про автора. Більш того, кожен, хто має доступ до документа, повинен мати і можливість перевірити, чи дійсно підпис під ним поставлений автором.

3. Конфіденційність інформації, що гарантується як шифруванням таємним ключем, так і шифруванням відкритим ключем.

Прикладами криптосистем з відкритим ключем є «*Elgamal*» (названа на честь автора, Тахира Ельгамаля), «*Diffie-Hellman*» (названа на честь її творців) і «*DSA*» (англ. *Digital Signature Algorithm* – алгоритм цифрового підпису, винайдений Девідом Кравіцем).

Найкращий приклад такої криптосистеми з'явився двома роками пізніше, у 1978 році, та був названий «*RSA*». Її назва походить від перших букв прізвищ авторів системи: Рівест (*Rivest*), Шамір (*Shamir*) і Адлеман (*Adleman*), які придумали її під час загальної роботи в Массачусетському технологічному інституті у 1977 році. Автори пообіцяли премію в 100 доларів тому, хто першим розшифрує «*RSA*»-шифровану фразу:

9686137546220614771409222543558829057599911245743198746951209308162982251457083569314766228839896280133919905518299451578151 54.

Це було зроблено тільки через 17 років. Для того щоб розшифрувати фразу «*The magic words are squeamish ossifrage*», команді з 600 осіб треба було 220 днів роботи і 1600 комп'ютерів, з'єднаних між собою через мережу «Internet». Мабуть, витрати трохи перевищили розмір премії.

У 1997 році Американський інститут стандартів і технології «*NIST*» (англ. *National Institute of Standards & Technology*) оголосив конкурс на стандарт симетричного криптоалгоритму, названий «*AES*» (Advanced Encryption Standard).

Вимоги, пред'явлені до кандидатів на «*AES*» у 1998 році, були простими:

- алгоритм повинен бути симетричним,

- алгоритм повинен бути блоковим шифром,

- алгоритм повинен мати довжину блоку 128 біт і підтримувати три довжини ключа: 128, 192 і 256 біт.

Додатково кандидатам рекомендувалося:

- використовувати операції, що легко реалізуються як апаратно (у мікрочіпах), так і програмно (на персональних комп'ютерах і серверах),

- орієнтуватися на 32-розрядні процесори,

- не ускладнювати без необхідності структуру шифру для того, щоб усі зацікавлені сторони могли самостійно провести незалежний криптоаналіз алгоритму та переконатися, що в ньому не закладено яких-небудь недокументованих можливостей.

Протягом 2 років фахівці конкурсного комітету, досліджуючи самостійно та вивчаючи публікації інших дослідників, обрали 4 кращих представників з 15 кандидатів.

Алгоритм	Виробник	Країна	Швидкодія
MARS	*IBM*	США	8 Мбайт/с
RC6	*R.Rivest & Co*	США	12 Мбайт/с
Rijndael	*V.Rijmen & J.Daemen*	Бельгія	7 Мбайт/с
TwoFish	*B.Schneier & Co*	США	11 Мбайт/с

Усі ці алгоритми були визнані досить стійкими й успішно протидіючими всім широко відомим методам криптоаналізу.

2 жовтня 2000 року «*NIST*» оголосив про свій вибір – переможцем конкурсу «*AES*» став бельгійський алгоритм «*Rijndael*». З цього моменту з алгоритму-переможця були зняті всі патентні обмеження – його можна використовувати в будь-якій криптопрограмі. За оцінками експертів, для розкриття нового шифру з довжиною ключа 256 біт буде потрібна безперервна робота найбільш могутнього комп'ютера протягом часу, що перевищує вік нашого Всесвіту (20 мільйонів років).

Таким чином, у сфері захисту інформації, що не є державною таємницею, був зроблений принципово важливий крок на шляху відмови від традиційних «шифрувальних» методів і розвитку криптології з відкритим ключем.

Практика показала: чим відоміший алгоритм, чим більше людей працювало з ним, тим більше перевіреним, а значить і більш надійним він стає. Так, привселюдно відомі алгоритми витримують перевірку часом, а ось у засекречених державних шифрах можуть виявитися помилки та недоліки.

Криптологія з *відкритим* ключем – це асиметрична схема, у якій застосовуються пара ключів: *відкритий*, що зашифровує дані, і відповідний йому *закри-*

тий, що їх розшифровує. Ви поширюєте свій відкритий ключ по всьому світі, у той час як закритий тримаєте в таємниці. Будь-яка людина з копією вашого відкритого ключа може зашифрувати інформацію, яку тільки ви зможете прочитати.

Хоча ключова пара математично пов'язана, «розкриття» закритого ключа за допомогою відкритого в практичному плані нездійсненне. Кожний, у кого є ваш відкритий ключ, зможе зашифрувати дані, але не зможе їх розшифрувати. Тільки людина, що володіє відповідним закритим ключем може розшифрувати інформацію.

Короткий опис сценарію електронного обміну конфіденційною інформацією включає наступні етапи:

- створюється файл, який містить конфіденційну інформацію;
- він зашифровується *відкритим* ключем, який відомий відправнику;
- зашифрований файл передається електронною поштою одержувачу;
- на прийомному боці одержувач, володіючи *закритим* ключем, «відкриває» зашифрований файл.

Головне досягнення асиметричного шифрування полягає в тому, що воно дозволяє людям, які не мають існуючої домовленості про безпеку, обмінюватися таємними повідомленнями. Необхідність погоджувати таємний ключ спеціальним захищеним каналом зв'язку відправнику й одержувачу повністю відпала. Всі комунікації зачіпають тільки відкриті ключі, тоді як закриті зберігаються в безпеці.

У ході єдності та боротьби двох напрямків криптології народилася нова гібридна комп'ютерна криптосистема Пилипа Циммермана з назвою «*PGP*», що об'єднала в собі достоїнства як традиційної криптології, так і шифрування відкритим ключем. В алгоритмі «*PGP*» зручність криптології з відкритим ключем доповнюється швидкістю симетричних алгоритмів, що працюють майже в тисячу разів швидше асиметричних. Шифрування відкритим ключем, у свою чергу, знімає проблеми прихованої передачі ключів.

Історія «PGP» починається в 1991 році, коли програміст Пилип Циммерман на основі привселюдно відомих алгоритмів шифрування написав програму для захисту файлів і повідомлень від несанкціонованого втручання. На той час навколо криптологічних продуктів для цивільних цілей у США складалася неоднозначна ситуація, з одного боку, вони стали надбанням громадськості, а з іншого боку, урядові організації прагнули внести ряд обмежень. Так, у 1991 році з'явився законопроект «*S.266*»

(«Білль про читання зашифрованої кореспонденції») та почали діяти обмеження на експорт криптологічних продуктів, які були зняті лише недавно. Потім у 1994 році з'явився законопроект «Про цифрову телефонію».

Але щирим апофеозом став проект «Кліпер» (англ. *Clipper* - ножиці), ініційований у 1993 році АНБ, відповідно до якого організації та приватні користувачі повинні були б здавати на депонування використовувані ключі. Це давало би можливість спецслужбам одержати доступ до будь-якої цікавлячої їх інформації. Правда, через технологічну складність, дорожнечу та суспільний осуд проект був «заморожений».

У таких умовах програма «*PGP*» як своєрідний вираз технологічного протесту не могла не з'явитися. За це Циммерман був підданий переслідуванням: конкретно йому намагалися інкримінувати експорт криптолгоритмів, оскільки програма швидко поширилася за межі США через мережу «*Internet*». У 2003 році Міністерство оборони США обмежило експорт криптографічних програм примітивним 40-бітним алгоритмом шифрування, а у 2004 році їх експорт був узагалі заборонений.

Пізніше обвинувачення з Циммермана було знято, а у 1996 році ним була утворена компанія «*Pretty Good Privacy, Inc*». Знаменитий продукт був експортований офіційним, хоча і курйозним способом: вихідний текст програми був опублікований у вигляді книги, потім вивезений зі США, відсканований та скомпільований у вигляді програми.

«*PGP*» виконувала такі базові функції:

- генерацію пари (закритого/відкритого) ключів;
- шифрування файлу за допомогою відкритого ключа будь-якого користувача «*PGP*» (у тому числі свого);
- розшифрування файлу за допомогою свого закритого ключа;
- накладення цифрового підпису за допомогою свого закритого ключа на файл (автентифікація файлу) або на відкритий ключ іншого користувача (сертифікація ключа);
- перевірку (верифікацію) свого підпису або підпису іншого користувача за допомогою його відкритого ключа.

У процесі «*PGP*»-шифрування інформація спочатку компресується, тобто стискується за відомим алгоритмом «*ZIP*». Стиск не тільки зменшує час передачі та заощаджує обсяг пам'яті, але й, що набагато важливіше, підвищує криптостійкість. Пов’язано це з тим, що багато методів криптоаналізу засновані на пошуку стійких сполучень (так званих патернів), що завжди зустрічаються в тексті. Стиск зменшує їхнє число, чим істотно поліпшує протидію криптоаналізу.

Потім «*PGP*» створює одноразовий ключ сеансу – симетричний (таємний) ключ, що застосовується тільки для однієї операції. Цей ключ являє собою псевдовипадкове число, згенероване комп'ютером з імпульсів, отриманих ним від випадкових рухів миші і натискань клавіш. За допомогою цього ключа та дуже

надійного, швидкого симетричного алгоритму «*PGP*» шифрує стиснуте повідомлення, одержуючи в підсумку зашифрований файл. Після цього вона шифрує і сам таємний ключ сеансу – за асиметричною схемою за допомогою відкритого ключа адресата. Дані про ключ сеансу передаються разом із зашифрованим файлом.

Дешифрування виконується у зворотньому порядку. Спочатку «*PGP*»-програма одержувача «виймає» з повідомлення дані про ключ сеансу, дешифрує його, використовуючи закритий ключ, і тільки потім дешифрує саме повідомлення.

Ось уже три десятиліття можна спостерігати за розвитком відносин між традиційною (симетричною) та асиметричною криптологією. Після появи асиметричної криптології здавалося, що тепер можна вирішувати масу нових задач, але поки будувалися теоретичні моделі. В ідеалі – все елементарно. Якщо ви збираєтеся написати комусь таємного листа, то завантажуєте відкритий ключ адресата з сервера ключів, шифруєте за його допомогою листа та відправляєте його електронною поштою.

Однак у грі може з'явитися третій учасник, що якийсь час назад створив свій відкритий ключ з ідентифікатором вашого потенційного адресата та підмінив на сервері дійсний ключ на свою фальшивку. Ви, ні про що не підозрюючи, використали підробку. Тепер зловмисник може перехопити і розшифрувати ваше повідомлення. Він навіть може перешифрувати лист правильним відкритим ключем і відправити за призначенням, так що і найменшої підозри ні в кого не виникне. Просто, як у «чорному кабінеті», – «відпарили» конверт, прочитали листа, заклеїли та повернули його на пошту.

Єдиний спосіб уникнути подібних ситуацій – одержувати відкриті ключі безпосередньо від їхніх власників, тобто ми повертаємося до проблеми захищеного каналу передачі ключа.

Інший варіант – одержати ключ від довіреної особи, про яку вам відомо, що вона має достовірну копію необхідного відкритого ключа. Цей посередник може навіть засвідчити цілісність ключа своїм підписом, зашифрованим за допомогою власного приватного ключа, тобто створити підписаний сертифікат вірогідності ключа. Він може також зберігати і передавати бажаючим достовірну копію вашого відкритого ключа, виступаючи між вами і вашими кореспондентами як довірений представник.

Уітфілд Діффі і Мартін Хеллман у своїй статті «Нові шляхи криптографії» запропонували також і протокол «відкритого розподілу ключів». Відкритий розподіл ключів має на увазі незалежне генерування кожним з пари користувачів свого випадкового числа, перетворення його за допомогою деякої процедури обміну перетвореними числами каналом зв'язку та обчислення загального таємного ключа на основі інформації, отриманої каналом зв'язку від партнера та

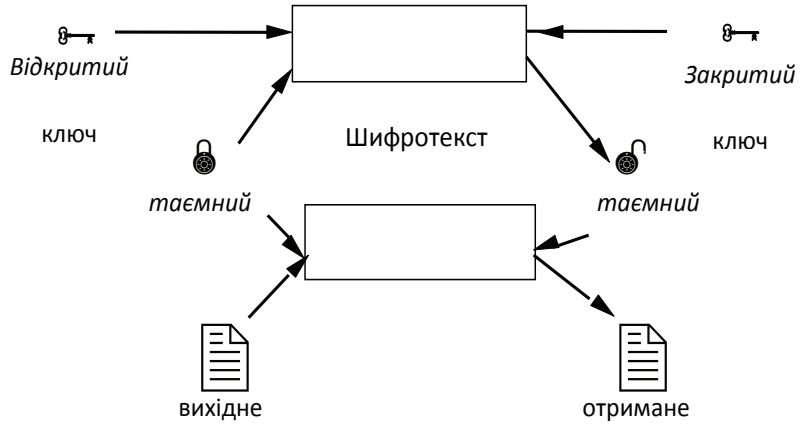
свого випадкового числа. Кожен такий ключ існує тільки протягом одного сеансу зв'язку (або навіть частини сеансу).

Таким чином, відкритий розподіл ключів дозволяє парі користувачів системи виробити загальний таємний ключ, не маючи заздалегідь розподілених таємних елементів. При цьому дві функції такого ключа, що доставляється традиційно з Центра, – захист інформації в каналі зв'язку від зловмисника та підтвердження дійсності кожного з абонентів його партнеру, – розділяються.

Дійсно, відсутність в абонентів перед сеансом зв'язку заздалегідь розподіленого загального таємного ключа в принципі не дає їм можливості упевнитися з абсолютною надійністю в легітимності один одного за допомогою тільки обміну повідомленнями відкритим каналом. Для достовірного підтвердження легітимності кожен із них повинен мати спеціальну ознаку (пароль), відому тільки йому та таку, що відрізняє його від усіх інших. Повинна бути забезпечена така процедура пред'явлення пароля, щоб його багаторазове використання не знижувало надійності доказу легітимності власника.

З практично діючих мереж зв'язку, що використовують систему відкритого розподілу ключів, найбільш серйозно захищеною є телефонна державна мережа США на основі апаратів «*STU-III*». Вона почала функціонувати в 1987 році і містить зараз більш 150 тисяч абонентів. У Росії аналогічна мережа, названа ще «АТС-1» або «вертушкою», теж надійно захищена, але абонентів там у сотні разів менше.

До початку вісімдесятих років криптологи прийшли до розуміння переваги так званих гібридних систем, у яких процедури шифрування з відкритим ключем використовуються лише для передачі ключів і цифрового підпису, а інформація, яку потрібно передати, захищається класичним алгоритмом типу «*DES*», ключ для якого передається за допомогою шифрування з відкритим ключем. Першим серійним при-



строєм даного типу був «*Datacryptor*» фірми «*RacalMilgo*», вироблений у 1979 році.

Апарат керування ключами шифрування «*Datacryptor*» був призначений, в основному, для урядових мереж зв'язку та атестований на відповідність англійському стандарту захисту нетаємної, але важливої інформації. У ньому передбачена сигналізація про порушення криптовимог і повідомлення про помилки. У цьому апараті використовується алгоритм установлення шифрованого зв'язку за допомогою вироблення та передачі загального таємного ключа за алгоритмом «*RSA*». У подальшому апаратів подібного типу для захисту інформації було випущено дуже багато.

2.13. Криптокартки «FORTEZZA»

Технологія «*Fortezza Cryptographic Card*», що була розроблена в АНБ, являє собою стандартний пристрій «PC-card» (раніше цей стандарт називався «*PCMCIA*») та призначена для реалізації автентифікації та шифрування згідно зі стандартами уряду США. Картки «*Fortezza*» застосовуються в системі електронного зв'язку «*DMS*» (англ. *Defence Message System* - система захисту повідомлення) МО США, у пошуковій системі «*Intelink*» розвідувального співтовариства уряду США, що використовує технології «*WWW*», а також в інших урядових системах.

«*Fortezza*» – ключовий компонент у забезпеченні секретного зв'язку для АНБ та інших урядових структур США. Даний криптографічний продукт є розробкою фірми «Rainbow» – провідного постачальника замовлених і високонадійних рішень для державних і комерційних організацій США. «Рейнбоу» (англ. *Rainbow* - веселка) підписала новий багаторічний контракт з Відділом захисту АНБ. Контракт передбачає постачання криптокарток «*Fortezza*» протягом 3-річного періоду в АНБ на загальну суму 33,6 мільйона доларів. Попередній контракт «*Rainbow*» і АНБ був укладений на 15,3 мільйона доларів.

Роботи зі створення «*Fortezza*» були розпочаті у 1991 році в рамках програми «*PMSP*» (англ. *Pre Message Security Protocol* - протокол безпеки попереднього повідомлення). Перед фахівцями АНБ було поставлене завдання розробити несекретну технологію захисту інформації. Первісною метою цього проекту було створення недорогого пристрою у стандарті «smart card», який забезпечує цілісність даних, шифрування даних, ідентифікацію й автентифікацію джерела даних.

Крім цього, необхідно було передбачити можливість сумісності з існуючими стандартами (наприклад, із протоколом поширення ключів «*X.509*»), забезпечити роботу мобільних користувачів, надати засоби розширюваності архітектури для підтримки потенційно великої кількості користувачів (до 4-х мільйонів). Першочерговими сферами застосування технології «*Fortezza*» передбачався захист електронної пошти й іншого електронного інформаційного обміну, що здійснюється по відкритих каналах зв'язку, а також контроль доступу до систем та їхніх компонентів.

За час розвитку технологія кілька разів міняла свою назву. Як уже говорилося, у

1991 році програма «*Fortezza*» називалася «*PMSP*», а сам криптографічний пристрій розроблявся згідно зі стандартом «*smart card*». У 1993 році назву програми було змінено на «*MOSAIC*», тип криптографічного пристрою був змінений на «*PC Card*», а сама PC-картка одержала назву «*Tessera Crypto Card*».

Потім, у 1994 році, програма була злита в об'єднаний проект АНБ і Агенції інформаційних систем МО США «*DISA*» - «*MISSI*» (англ. *Multi-Level Information Systems Security Initiative* - ініціатива безпеки багаторівневих інформаційних систем). Після цього назва технології була змінена на «*Fortezza*», а PC-картка перейменована у «*Fortezza Crypto Card*».

Технологія «*Fortezza*» володіє двома важливими властивостями, що роблять можливим її широке поширення (якщо тільки це поширення не виявляється в сфері дії експортних обмежень). Першою такою властивістю є «персоналізація» засобів забезпечення безпеки. Кожен користувач забезпечується індивідуальним криптографічним пристроєм (PC-карткою).

Ця PC-картка містить унікальну для кожної конкретної особи ключову інформацію та пов'язані з нею дані, а також виконує закладені в неї криптографічні алгоритми. Творці картки «*Fortezza*» виконали велику роботу з розробки складної системи генерації, розподілу й керування криптографічними ключами. Особлива увага була приділена контролю цілісності даних картки та поширенню необхідної криптографічної й системної інформації.

Другою властивістю є наявність відкритого прикладного програмного інтерфейсу (API). Апаратні й програмні специфікації картки розроблялися з урахуванням вимог до відкритої системи. Це дозволяє здійснювати просту інтеграцію технології «Fortezza» у більшість апаратних платформ, комунікаційних засобів, операційних систем, пакетів прикладних програм і мережних протоколів й архітектур. Крім цього, підхід «*Fortezza*» рятує розробників програмних засобів від необхідності вбудовувати в прикладні програми складні криптографічні підсистеми. Досить скористатися PC-карткою «*Fortezza*», якою можна керувати через «*API CI_Library*».

Алгоритм шифрування, застосовуваний у технології «*Fortezza*», відомий за назвою «*SKIPJACK*». Цей алгоритм був розроблений фахівцями АНБ і відповідає стандарту депонування ключів «*Escrowed Encryption Key Standard*». «*SKIPJACK*» є блоковим шифром з розміром блоку 8 байт, що використовує симетричні ключі (тобто для зашифрування й розшифрування застосовується той самий ключ).

Шифрування за алгоритмом «*SKIPJACK*» у картці «*Fortezza*» здійснюється за допомогою спеціалізованого криптографічного мікропроцесора «*CAPSTONE*», виконаного за «*RISC*»-технологією. Такі мікропроцесори виконують ті ж функції, що й мікропроцесори «*CLIPPER*», які застосовуються для реалізації алгоритму «*SKIPJACK*» у пристроях голосового (телефонного) зв'язку. Обговорення деталей реалізації «*SKIPJACK*» не представляється можливим, тому що цей алгоритм є засекреченим.

У технології «*Fortezza*» ключ шифрування даних називається «*MEK*» (англ. *Message Encryption Key*). У доповненні до цього ключа може використовуватися також вектор ініціалізації «*IV*» (англ. *Initialization Vector*), що фактично є додатковим вхідним параметром при шифруванні даних. Стандартний режим алгоритму «*Fortezza*» вимагає обов'язкового використання «*IV*» всіма учасниками інформаційного обміну. Це означає, що для розшифрування повідомлення одержувач повинен або мати можливість згенерувати точно такий же «*IV*», що використовувався відправником при зашифруванні повідомлення, або «*IV*» повинен бути переданий разом з повідомленням.

Алгоритм шифрування «*SKIPJACK*» має три режими роботи: «*ECB*» (англ. *Electronic Codebook* - електронна кодова книга), «*OFB*» (англ. *Output Feedback* - вихідний відгук) і «*CBC*» (англ. *Cipher Block Chaining* - шифроблоковий ланцюг). Як правило, алгоритм «*Fortezza*» використовує режим «CBC». У цьому режимі всі 8-байтові блоки відкритого тексту, крім першого, використовуються для виконання операції «*XOR*» із блоком зашифрованого тексту, отриманим на попередньому кроці роботи алгоритму з використанням «*MEK*». Вектор «*IV*» застосовується для зашифрування першого блоку відкритого тексту.

Для того, щоб зловмисник зміг розшифрувати повідомлення, йому необхідно знати не тільки «*MEK*», але й «*IV*». При цьому, компрометація «IV» не настільки істотна, якщо зловмисник не володіє «*MEK*».

Розподіл ключів шифрування «*MEK*» засновано на застосуванні розробленого в АНБ алгоритму обміну ключами «*KEA*» (англ. *Key Exchange Algorithm* - алгоритм обміну ключа), що посилає зашифрований «*MEK*» з кожним повідомленням. Оскільки обмін ключами «*KEA*» інтегрований у технологію «*Fortezza*», ключі шифрування можуть мінятися від повідомлення до повідомлення або від сеансу до сеансу.

Алгоритм «*KEA*» використовує для шифрування «*MEK*» спеціальний ключ, названий «*TEK*» (англ. *Token Encryption Key* - ключ полуторного шифрування). Необхідно мати на увазі, що в додатках, які використовують технологію «Fortezza», «*TEK*» може бути використаний при шифруванні даних як альтернатива ключа шифрування «*MEK*», однак «*MEK*» не може бути використаний для захисту «*TEK*» у процесі обміну ключами.

Шифрування з відкритим ключем у стандартному режимі алгоритму «*Fortezza*» використовується тільки для обміну ключами з використанням «*KEA*» і для цифрового

підпису повідомлень (включаючи тимчасові мітки). В описі алгоритму «*Fortezza*» зазвичай використовують такі позначення: 20-байтний закритий ключ називається «*X*», 128-байтний відкритий ключ називається «*Y*», «*P*» й «*Q*» – великі прості числа (секретні), «*G*» – просте число за модулем «*PxQ*» (загальнодоступне).

Загальний процес шифрування повідомлень із використанням відкритого ключа абонента виглядає таким чином. Відправник зашифровує повідомлення для одержувача, використовуючи відкритий ключ одержувача «*Y*» й алгоритм шифрування з відкритим ключем. Одержувач розшифровує послання відправника за допомогою свого відкритого ключа «*X*». Кожний, хто одержить доступ до місця зберігання відкритих ключів, зможе зашифрувати дані для одержувача, але тільки одержувач зможе розшифрувати ці дані, оскільки ніхто не знає його закритого ключа. Генерація й розподіл пар відкритого й закритого ключів для організації обміну ключами «*KEA*» і цифрового підпису виробляється для кожного користувача окремо згідно зі спеціальною процедурою.

Як відзначено вище, алгоритм обміну ключами «*KEA*» розроблений фахівцями АНБ і використовується для організації розподілу ключів шифрування «МЕК» при інформаційному обміні та для розсилання секретних ключів користувачам. Основною перевагою «*KEA*» є той факт, що обидві сторони можуть обчислити один і той же ТЕК самостійно, використовуючи два випадкові числа (*A* і *B*), власні параметри *P*, *Q*, *G* і відкритий ключ абонента. Коли «*KEA*» використовується при інформаційному обміні, приймаюча сторона може одержати всі значення, необхідні для розшифрування повідомлення, разом із прийнятим повідомленням.

Помітимо, що в даному алгоритмі значення *P*, *Q* й *G*, використані відправником для первісної генерації «*TEK*», а одержувачем для генерації «*TEK*» при одержанні повідомлення, не передаються по каналах зв'язку та однакові для всіх користувачів.

Алгоритм обміну ключами «*KEA*» застосовується як у додатках типу електронної пошти, так і при інформаційному обміні між абонентами, логічно та/або фізично з'єднаними між собою в режимі реального часу.

Необхідно відзначити, що те саме повідомлення, адресоване різним абонентам, зашифровується з використанням одного ключа «*MEK*», однак цей ключ повинен бути згорнутий за допомогою різних «*TEK*», що відповідають одержувачам даного повідомлення. Додаток – адресат повинен переглянути повідомлення та знайти «*TEK*», призначений для даного користувача, розгорнути «*MEK*» і розшифрувати отримане повідомлення.

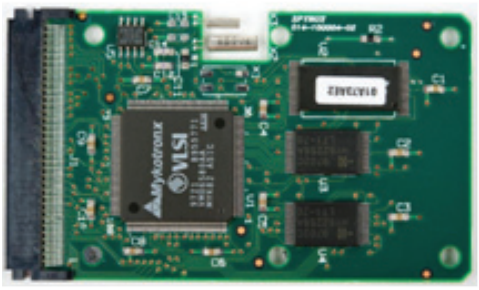
Для контролю цілісності переданих повідомлень, забезпечення автентичності та неможливості заперечення авторства технологія «*Fortezza*» використовує алгоритм цифрового підпису «*DSA*» і алгоритм безпечного хешування «*SHA-1*» (англ. *Secure Hash Algorithm*), що відповідають стандарту цифрового підпису «*DSS*» (англ. *Digital Signature Standard*).

Після обчислення хеш-функції повідомлення, 20-байтний хеш-блок перетвориться за допомогою алгоритму «*DSA*» у цифровий підпис повідомлення розміром 40 байт. Необхідно звернути увагу на розходження у використанні параметрів *P*, *Q* і *G* в алгоритмах розподілів ключів «*KEA*» і цифрового підпису «*DSA*». При перевірці цифрового підпису повідомлення відправника одержувач повинен мати доступ до значень *P*, *Q* і *G* відправника. Ці параметри повинні поширюватися або в заголовку повідомлення, або разом з відкритим ключем відправника.

З метою постачання кожного користувача набором власних значень *P*, *Q* і *G* прикладна бібліотека «*CI_Library*» має відповідні функції завантаження цих значень. Таке розходження у використанні цих параметрів пов'язане з можливістю «*DSA*», на відміну від «*KEA*», підтримувати інформаційний обмін між користувачами різних «доменів», які можуть розрізнятися процедурами поширення й сертифікації ключів.

На момент створення технології «*Fortezza*» не існувало урядових або промислових стандартів тимчасових міток цифрового підпису. Для «прив'язки» повідомлень до часу їхнього створення застосовується додаткова процедура обчислення хеш-функції від хеш-блока повідомлення й поточного часу, взятого з надійного джерела (наприклад, криптокартки «*Fortezza*»). Необхідно помітити, що значення *P*, *Q* і *G*, що використовуються алгоритмом «DSA» при обчисленні підпису із застосуванням тимчасових міток, є загальними для всіх карток «*Fortezza*» та записуються у пам'ять виробником криптокартки. Оскільки перевірка цифрового підпису у випадку застосування тимчасової мітки пов'язана з необхідністю синхронізації джерел часу, обчисленням часу доставки повідомлення та іншими складнощами, використання тимчасових міток у технології «Fortezza» не є обов'язковим.

Як випливає зі сказаного вище, у технології «*Fortezza*» повинен існувати протокол, що регламентує видачу й поширення відкритих ключів користувачів. Відкриті ключі асоціюються з їхніми власниками за допомогою так званих «сертифікатів». Сертифікат являє собою структуру даних, що пов'язує ідентифікатор користувача, відкриті ключі, призначені для алгоритмів «*KEA*» і «*DSA*», а також інформацію про особу, що видала сертифікат. З метою захисту від підробки сертифікат захищається цифровим підписом особи, що видала сертифікат. Сертифікати й пари секретних/відкритих ключів утворять основу системи керування ключами технології «*Fortezza*».



Як основу системи автентифікації «Fortezza» використовує схему автентифікації сертифікатів «*X.509*» та угоди про найменування об'єктів «*X.500*». Технологія «*Fortezza*» розрізняє дві структури

сертифікатів. Під сертифікатом «*Fortezza*» розуміється внутрішня структура даних технології «Fortezza», під сертифікатом «*X.509*» – блок даних стандарту «*X.509*», що утримується в сертифікаті «*Fortezza*».

Кожен сертифікат «*Fortezza*» складається із двох пар відкритих/секретних ключів (одна з них призначена для використання в «*KEA*», інша – в «*DSA*») і відповідних їм значень параметрів *P*, *Q* і *G*. Сертифікат «*X.509*» містить відкриті складові цих ключів. Відкриті ключі завжди доступні користувачеві картки. Ключі зберігаються в закодованому виді: секретні – за допомогою локальних ключів користувача «*Ks*» (він має розмір 80 біт, перебуває в спеціальному регістрі криптокартки та стає доступним після успішного уведення «*PIN*» користувача), відкриті – за допомогою «*ASN.1*». Поле даних розміром 2048 байт, зарезервоване для сертифіката «*X.509*», може використовуватися для зберігання будь-якої інформації (біометричних даних, фотозображень), якщо тільки такі «сертифікати» не використовуються у криптографічних функціях. Додатки можуть завантажувати ці дані в енергонезалежну пам'ять картки та зберігати їх там тривалий час.

Сертифікати «*X.509*» можуть бути розміщені в базі даних спеціалізованого «сертифікаційного сервера» (декількох серверів) або розподілені по мережі та збережені локально в картках всіх учасників інформаційного обміну. Єдиною умовою є доступність сертифіката для криптографічних функцій додатків «Fortezza». Деякі додатки дозволяють включати сертифікат відправника у заголовок повідомлення, надаючи одержувачу можливість динамічно створювати локальну базу сертифікатів абонентів. Така локальна база може служити свого роду «кешем» сертифікатів, що уможливлює посилку повідомлень без звертання до сервера сертифікатів. Однак довге використання локальної бази може привести до старіння сертифікатів, що утримуються в ній.

Таблиця всіх криптографічних функцій

Криптографічна функція	Назва	Розмір параметрів	Стандарт
Обмін відкритими ключами	*KEA*	секретний ключ 160 біт	модифікований *Diffie-Helman*
Шифрування повідомлень	*SKIPJACK*	ключ 80 біт	*NSA / FIPS 185*
Цифровий підпис	*DSA*	модуль 1024 біт	*NIST FIPS 186*
Хешування	*SHA-1*	160 біт	*NIST FIPS 180-1*
Тимчасові мітки	немає	160 біт	*Fortezza*
Пароль користувача	*PIN*	4-12 байт	*Fortezza*
Сертифікат	немає	2820 байт	використовується *CCITT X.509*

17 червня 1996 року компанія «*Netscape Communications Corporation*» анонсувала випуск бета-версії «*SSLRef 3.0*» – засобу розробки додатків, що забезпечують захист інформаційного обміну в середовищі «*Internet/Intranet*» з ви-

користанням відкритого протоколу «*SSL 3.0*». Компанія «*Netscape*» розпочала діяльність із стандартизації протоколу «*SSL*» (англ. *Secure Sockets Layer* - рівень захищених сокетів) ще в жовтні 1994 року. Групі інженерної підтримки мережі «*Internet*» (*IETF*) як основа вимог до безпеки інформаційного обміну, забезпечуваної на транспортному рівні, був запропонований протокол «*SSL 2.0*». При цьому, було виконано одне з основних умов, запропонованих до «кандидата на стандарт» – наявність комерційної реалізації протоколу. Першим поколінням продуктів, що підтримують протокол «*SSL*», стали «*Netscape Navigator 2.0*», «*Netscape Commerce Server 1.0*» і «*Netscape News Server 1.0*».

Основною відмінністю поточної, третьої, версії протоколу «*SSL*» є підтримка більшої кількості алгоритмів й апаратних засобів обміну ключовою інформацією й шифрування, у тому числі й технології «*Fortezza*». У жовтні 1995 року віце-президент «*Netscape*» Марко Андрісен заявив, що підтримка технології «*Fortezza*» дозволить зміцнити позиції компанії як провідного постачальника програмних продуктів, що використають «Web»-технології, як для федерального уряду США, так і для комерційних організацій.

Результати не змусили себе чекати: «*Netscape*» стала першою компанією, якій уряд США в липні 1996 року надав право поширювати по мережі «*Internet*» програмне забезпечення, що підлягає експортним обмеженням. «*Netscape Navigator*» і «*Netscape Fast Track Server*» стали першими програмними продуктами, що використовують алгоритм «*RC4*» з довжиною ключа 128 біт, які американські користувачі можуть одержати по мережі «*Internet*».

На даний час кількість компаній, що підтримують протокол «*SSL*», значно збільшилася. Серед них: *Apple Computer Inc., Digital Equipment Corporation, IBM, Master Card International Inc., Microsoft Corporation, Motorola, Novell Inc., Siemens Nixdorf, Silicon Graphics Inc., Sun Microsystems Inc., Visa International* та інші. Існують також і некомерційні реалізації, наприклад «*WWW*»-сервер «*Apache-SSL*». Широке поширення протоколу «*SSL*» робить можливим та необхідним більш детальне ознайомлення з одним із його засобів – криптокарткою «*Fortezza*».

Частина 3.

Історія російської криптології

3.1. Давньоросійський тайнопис

Найбільш ранньою з відомих за староруськими пам'ятниками писемності систем тайнопису була система *«иных письмен»*. У цьому виді тайнопису букви кирилиці замінювалися буквами інших алфавітів: глаголиці, грецької, латинської, пермської абетки.

Вживання грецького тайнопису пов'язують з певною модою, яка прийшла до кінця XVI ст. Поява ж цього способу тайнопису була обумовлена, з одного боку, другим південно-слов'янським впливом, що ніс деякі навики і грецького письма, ближчого півдню слов'янства, ніж Русі, а з іншого – пожвавленням стосунків Московської Русі з греками, що розпочалися з кінця XIV ст.

Вживання латинської азбуки як тайнопису відноситься до пізнішого часу та обумовлене західноєвропейським впливом, що посилився. У розповсюдженні цього виду тайнопису, що трапляється в рукописах XVI і XVII ст., ймовірно, відому роль грала школа з її латинською мовою викладання.

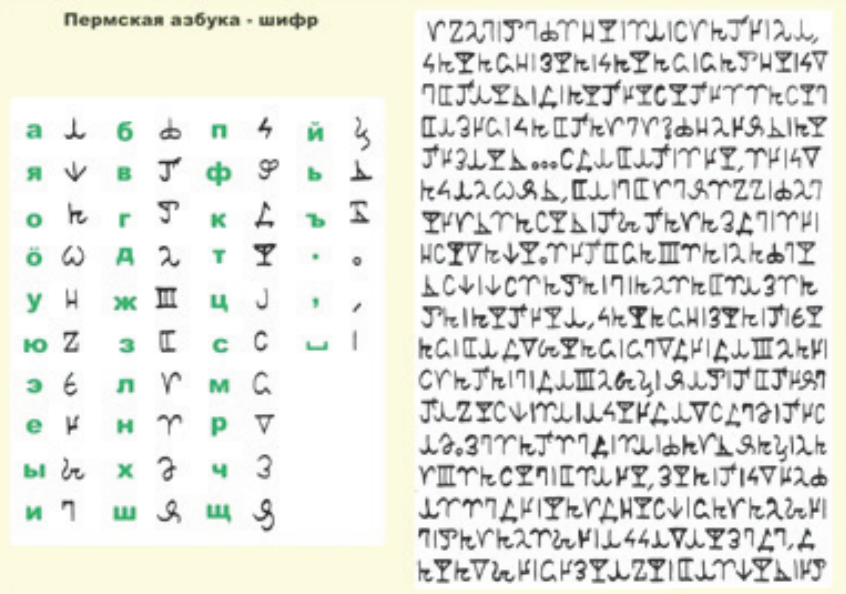
Дещо відособлене місце серед інших алфавітів у застосуванні до тайнопису займає пермська абетка. Ця абетка, що була створена пермським єпископом Стефаном на основах сучасного кириличного й грецького алфавітів, не набула практичного застосування та вже у XV ст., як маловідома, стала тайнописом. Але й в цій якості вона не була широко поширена.

Другою після системи *«иных письмен»* системою тайнопису, відомою з російських рукописів, є система «змінених знаків», зафіксована вже у XIV столітті. Виділяють два її різновиди: а) систему знаків, змінених «шляхом надбавок» до звичайних зображень, б) побудовану на принципі, схожому з грецькою «тахіграфією».

«Тахіграфія» – це зміна написання букв, коли писалася або частина букви, або навпаки, її написання доповнювалося новими елементами. Повідомлення нерідко записували праворуч-ліворуч або догори ногами. Часто «тахіграфія» сполучалася з використанням іноземних алфавітів.

Перший різновид такого тайнопису був відкритий вченим М.Сперанським у Смоленському Псалтирі 1395 року. За його свідченням цей Псалтир Онезького Хресного монастиря зберігався свого часу в Архангельському місцевому відділенні Церковно-археологічного комітету. Його писар, чернець Лука, що чудово володів мистецтвом письма, любив, мабуть, і тайнопис. У цьому рукописі він застосував три види тайнопису: один – змінених зображень, другий – цифра рахункова, третій – система в'язу.

Використовували писарі стародавніх рукописів і систему умовних алфавітів. Як



правило, в їх основі лежали вже відомі: грецький, глаголицький, кириличний, в яких привносилися якісь зміни або доповнення. Проте траплялися в рукописах і оригінальні умовні алфавіти, побудовані або за якимсь певним принципом, або абсолютно довільних зображень.

Зразком алфавіту, придуманого спеціально для тайнопису, притому за особливим принципом, може служити ключ до тайнопису, зображений на окремому листі другої половини XVII ст. (Збори Великої Патріаршої бібліотеки № 93).

Тут тайнопис полягає в заміні звичайних букв трикутниками і чотирикутниками, запозиченими з грат, складених з двох паралельних ліній, пересічених двома такими ж лініями під прямим кутом. У отриманих клітинках поміщено по чотири й по три букви в порядку азбуки: у тайнописі букви замінюються, при цьому перша – простим косинцем, а наступні – тим же косинцем з однією, двома або трьома крапками, зважаючи на місце букви в нім. Оскільки при такому розміщенні букв у клітинах вся азбука не могла вміститися, то в цьому тайнописі не виявляється знаків для таких букв кирилиці, як «ш», «ь» тощо.

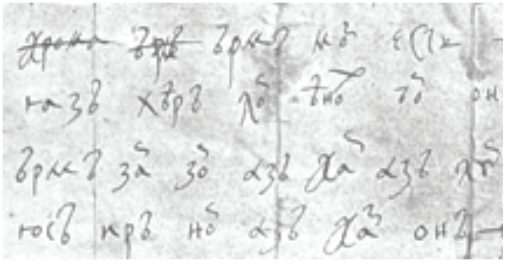
Наступний вид тайнопису, який використовувався писарями в російських рукописах, – це «система замін». Виділяють два види для такого тайнопису: «просту літорею» (від лат. *litera* – буква) і «мудру літорею», а також як варіант цієї останньої – тайнопис «в квадратах». «Проста літорея» полягала в тому, що кожен із десяти по порядку азбуки приголосних, поставлених в одному ряду, замінювався відповідною нею буквою в другому такому ж ряду, що складався з останніх десяти приголосних, що йдуть в зворотному (справа наліво) порядку.

Перший документ, який дійшов до нас та містив даний тип криптосистеми, датувався 1229 роком. Однак по-справжньому широке поширення вона здобула наприкінці XVII століття. Ключ до «простої літореї» такий:

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Слово «УКРАЇНА», записане «літореєю», виглядає так: «УТМАЇПА».

Більш складним різновидом «літореї» була так звана «мудра літорея», де всі букви кириличної абетки, включаючи голосні, замінялися на інші букви. До цього ж виду тайнопису, який використувався у XVI-XVII ст., відносився тайнопис «в квадратах», де таблиці заміни букв виписувалися у вигляді квадратів. Нерідко писарі вдавалися до написання фраз у



зворотному порядку, складаючи своєрідні криптограми, або не дописували букви – подібний шифр називався *«полусловицей»*.

Цифрова система тайнопису, яку тоді називали *«счётная»* або *«цифирная»*, заснована на вживанні букв як цифр і на різних практичних діях з ними, була дуже поширеною і, до того ж, із досить раннього часу. Слід сказати, що в староруських рукописах траплялися різні її види: проста та складна цифрова система, описова система, система особливого застосування арабських цифр, система значків, тобто з використанням різних значків для позначення цифр-букв. Цифровий тайнопис існував на Русі вже на самому початку XIV ст.

Простий цифровий тайнопис полягав у тому, що для кожної цифри-букви, яка відповідала бажаній в звичайному письмі букві, давалося декілька переважно однакових доданків. Так, щоб отримати потрібну букву, треба було провести складання, а отримана сума, зображена відповідною цифрою-буквою, і була шуканою буквою. Рідше сума складалася з різних цифр-букв, причому кожна група цифр-доданків відділялася яким-небудь знаком або пропуском від сусідніх. Букви, що не мали цифрового значення, залишалися незмінними.

Арабські числа почали використовуватися як тайнопис лише з того часу, як вони почали входити у вживання у російській писемності, тобто з другої половини XVI ст. на російському південному заході і з початку XVII ст. на північному сході.

До інших систем тайнопису, відомих за староруськими рукописами, належав *«мононкондил»*, різні прийоми образного й фігурного письма, а також *«акростих»* (вірш, в якому початкові букви рядків утворюють слово або фразу). *«Акростих»* – типовий для європейської середньовічної письмової культури прийом організації поетичного тексту – входив в арсенал художньо образотворчих засобів староруських авторів уже з кінця XI ст.

Довгий час державний тайнопис у працях вітчизняних учених, іменувався «дипломатичним тайнописом». Уперше такий термін був введений ученим Поповим, який у 1853 році опублікував працю «Дипломатичний тайнопис часів царя Олексія Михайловича з доповненням до нього». Слідом за ним і інші дослідники російського тайнопису почали називати листування при російському дворі «дипломатичним тайнописом», а шифри, якими воно велося, «дипломатичними».

Слід, проте, відзначити, що таємне дипломатичне листування складало лише частину (правда, велику) шифрованого листування при дворі, яке разом з дипломатичним, стосувалося військових питань, а також внутрішньодержавних справ. Але

саме в сфері дипломатії, з властивими їй специфічними рисами і особливостями, в Росії майже впродовж двох сторіч проходило основне становлення криптології як державно-значущої справи. Політична боротьба, політична гра – іншими словами, ведення «великої політики» немислиме без охорони державної таємниці.

Активна зовнішньополітична діяльність царя Івана IV Васильовича (Грозного) та пов'язані з нею війни вплинули на становлення й розвиток тайнописної справи. Роком народження російської криптологічної служби можна вважати 1549 рік, коли була утворена «*Посольская изба*», пізніше названа «Посольським наказом», при якому працювала «*цифирная*» палата таємних справ. З моменту його утворення в Росії почали активно використовувати криптологічні методи в дипломатичному та військовому листуванні.

Назву «цифирної» палата одержала, можливо, за старою алфавітною системою запису чисел. Виділення цифр та й власних імен у тексті раніше робилося за допомогою «титлу», спеціального знака, який проставлявся над рядком. Шифри доводилося виділяти в повідомленні так само, як і цифри, тобто «титлувати» їх. Тому цілком зрозуміла назва шифру «цифрою», тобто текстом, що вимагає спеціального прочитання. Втім, можливо, що слово «цифирна» у назві палати була буквальним запозиченням французького слова «chiffre», що означало як шифр, так і цифру.

З кінця XVI ст. російські посли за кордоном почали отримувати шифри у вигляді таблиць заміни, які потрібно було *«вытвердить гораздо памятно»*. У наказі царя Федора Іоановича, даному у 1589 році послу Миколі Воркачу, йому доручалося *«писать письма мудрою азбукою, чтоб оприч Царского величества никто не разумел»*. У тій азбуці кожна буква замінювалася своїм особливим знаком.

«Подъячие Посольского приказа», що підтримували зв'язки з царськими представниками закордоном, нерідко користувалися шифрованим листуванням, яке називали *«затейным письмом»*. Ключ до розшифрування цих послань не записувався, його заучували напам'ять. Існували різні варіанти таємного письма, але за правилами конспірації ніхто з піддaних не повинен був знати усіх варіантів тайнопису.

З початком правління династії Романових (1613)

KREMLENAGRAD,
CASTELLVM VRBIS MOSKVÆ
посольський наказ

зміцнюються основи феодального ладу. У 1619 році з польського полону повернувся батько царя Михайла Романова Федір, пострижений Борисом Годуновим у монахи під іменем Філарета. Він особисто займався справами «Посольського наказу» та навіть розробляв дипломатичні шифри. Шифри, що використовувались у той час, були шифрами простої заміни та перестановки.

Самі перестановки були достатньо простими. Наприклад, відкритий текст розбивався на склади, після чого в них здійснювалася перестановка букв. Так слово «УЖГОРОД» перетворювалося у слово «ЖУОГДОР».

У 1633 році патріарх Філарет написав *«для своих государевых и посольских тайных дел»* особливу абетку і *«склад затейным письмом»*. Зберігся наказ російському представнику у Швеції Д.Францбекову, з якого видно, що при складанні повідомлень царю посол повинен був використовувати тайнопис. Наказ закінчувався таким чином: *«Да что он, Дмитрий [Францбеков], будучи в Свее [Швеції], по сему тайному наказу о тех или иных о наших тайных делах и наших тайных вестей проведает и ему о всем писати ко государю царю и великому князе Михаилу Федоровичу всея Руси к Москве по сему государеву тайному наказу ~~затейным~~ закрытым письмом».*

До наших часів дійшла чернетка цього наказу, у якому слово *«затейным»* закреслене і замінене *«закрытым»*. Отже, можна дійти висновку, що в Росії тайнопис перетворився в один із засобів збереження державних таємниць.

Так, в інструкції російському агенту в Швеції Дмитру Андрєєву говорилося: *«Лета 7143 (1653) декабря 15 день... А про те тайные дела и про затейное письмо подъячий Иван Исаков и иной никто отнюдь не ведал, и чёрные о сих тайных делах тем же затейным письмом держать у себя бережно, чтоб о тех тайных делах и про то затейное письмо оприч его, Дмитрия, подъячий Иван Исаков и иной никто однолично не проведал».*

Приведемо також витяг з присяги перекладача-шифрувальника кінця XVII століття: *«...ему всякие государственные дела переводить в правду, и с неприятелями государскими тайно никакими письмами не ссылаться и мимо себя ни через кого не посылать, и в Московском государстве с иноземцами о государственных делах, которые ему будут даны для перевода, ни с кем не разговаривать».*

При посиленні центральної влади в роки правління царя Олексія Михайловича (1629-1676) застосування шифрів поширюється. У 1654 році цар утворив «*Приказ великого государя тайных дел*», яким керував особисто, а бояри до таємних справ не допускалися. Як писав Г.Котошихин, «*А устроен тот Приказ при нынешнем царе, для того чтоб его царская мысль и дела исполнилися все по его хотению, а бояре б и думные люди о том ни о чем не ведали*».

Головна посадова особа наказу - «*тайный дьяк*» - мав титул «*дьяка в государевом имени*», що означало право підписувати укази від імені царя. Головним завдан-

ням наказу був негласний контроль над вищими посадовими особами. *«Подъячие приказа*» наглядали за воєводами під час війни і посилалися з посольствами закордон: «*и те подьячие над послы и над воеводами подсматривают и царю приехав сказывают: и которые послы, или воеводы, ведая в делах неисправление свое и страшась царского гневу, и они тех подьячих дарят и почитают выше их меры, чтоб они будучи при царе их послов выславляли, а худым не поносили*».

Сам цар, дуже освічений для свого часу, особисто також використовував шифри і в своєму приватному листуванні. Посли і резиденти завжди забезпечувалися шифрами. Наприклад, у 1673 році резидентом у Річ Посполиту (Польща) був призначений полковник В.М.Тяпкин. По дорозі у Вільно його наздогнав царський гонець і вручив йому *«знаки тайнописи и повеление царское пользоваться ими для донесений».*

У державній криптології отримують розвиток і деякі інші способи тайнопису, відомі за стародавніми російськими рукописами, наприклад, такі як «мудра літорея». Цим способом, зокрема, був зашифрований текст, відлитий на великому дзвоні Саввіно-сторожевського монастиря під Звенигородом. Зашифрування тексту, за припущенням учених, здійснив сам цар Олексій Михайлович. Дешифрований він був філологами М.Ф.Калайдовічем, А.І.Єрмолаєвим, князем П.П.Лопухіним і ротмістром М.С.Сурідіним.

А.І.Єрмолаєв з приводу цієї обставини висловився так: *«Сия надпись во многих отношениях достойна особенного внимания. Представляя нам любопытный образец русской тайнописи (стеганографии) XVII века, она доказывает, что в России в старину шифры были пригодны не для одних дипломатических переписок или для внесения в книги разных обстоятельств, которые затейливые люди того времени ухитрялись сделать непонятными для многих из своих современников, долженствовавших быть видимыми народом...»*

3.2. Криптологія Петра Першого

Першим із російських царів, який чітко усвідомив важливість шифрування депеш і розвитку шифрувальної справи для забезпечення безпеки держави, був Петро І Великий (1672-1725). Епоха його правління характеризується посиленням Російської держави, всіх його управлінських структур, а також структур виконавчої влади. Петро І здійснив ряд найважливіших реорганізацій: організацію мануфактури, будівництво гірських і заводів зброї, розвиток торгівлі, включаючи міждержавну, створення Сенату – найвищого органу влади у справах законодавства і державного управління, створення колегій.

Активна зовнішньополітична діяльність Петра І вимагала створення постійної криптологічної служби, здатної забезпечити ефективний захист власних повідомлень і розкриття дипломатичного листування інших держав. Спочатку функції криптослуж-

би виконував *«Посольский приказ»*, пізніше паралельно з ним почала функціонувати *«Посольская канцелярия»* при Петрі.

Указом від 18 лютого 1700 року на чолі «Посольського наказу» і наказів, що належали до нього, був офіційно поставлений видатний діяч і дипломат раннього періоду петровского часу Федір Олексійович Головін (1650-1706). Він змінив там думного дяка Є.І.Українцева, який у 1699 році був відправлений послом до Константинополя на російському кораблі, що вперше з'явився у водах Босфору.

При своєму призначенні Головін отримав звання «початкового президента державної посольської канцелярії». Як генерал-адмірал Головін одночасно управляв флотом, очолював збройову палату, монетний двір, малоруський наказ. Окрім особистої участі в переговорах з іноземними державами і укладення договорів з ними, Головін керував діяльністю російських послів за кордоном, робив великий вплив на зовнішню політику Росії в період Північної війни. Під безпосереднім спостереженням Головіна працювало «цифирне» відділення.

Вже на самому початку XVIII ст. Петром I була створена *«Походная посольская канцелярия»*, що зосередила в своєму веденні найважливіше політичне листування. Створення її було викликане частими поїздками Петра. *«Походная канцелярия»* була переважно особистою канцелярією імператора, звідки виходили його найважливіші розпорядження по всіх галузях управління. Сюди стікалися на його вирішення справи зі всіх відомств. Але головною її функцією було ведення дипломатичних справ, чому до її назви додавалося слово *«посольская»*.

Перша згадка в документах про «Похідну канцелярію» відноситься до 1702 року. У цей час цар відправився «в похід» до Архангельська. У поїздці його супроводжував начальник *«Посольского приказа»*, перший міністр Ф.О.Головін. Незважаючи на те, що всі державні справи продовжували проходити через *«Посольский приказ»*, а *«печатанье государственной печатью грамот»* повинно було далі знаходитися під контролем бояр, найбільш важливі справи вже вирішувалися в Архангельську у Петра I.

У 1706 році *«Посольский приказ»* очолив Гаврило Іванович Головкін (1660-1734), який був родичем Петра I по материнській лінії. Після смерті Головіна, 23 вересня 1706 року помічником Головкіна був призначений Петро Павлович Шафіров (1669-1739), який з 1703 року працював «таємним секретарем» при «Похідній канцелярії».

До 1710 року *«Походная канцелярия»* остаточно обґрунтувалася в Петербурзі та з тимчасової установи стала постійною, причому з 1709 року її стали називати просто *«Посольской канцелярией»*. Саме там була зосереджена вся робота щодо зашифрування та розшифрування листування Петра I і його наближених з різними кореспондентами, а також утворення шифрів і рекомендацій щодо їх використання.

У період з 1710 по 1718 роки ця Канцелярія стала головним органом зовнішніх

стосунків Росії. Компетенція її розширилася у збиток *«Посольскому приказу»*, що залишився в Москві. Зросла чисельність особового складу Канцелярії. У 1709 році Головкін був призначений державним канцлером, а Шафіров – віце-канцлером. Саме ці перші особи держави керували діяльністю російської криптослужби.

Канцлер і віце-канцлер давали вказівки щодо створення нових шифрів, заміні застарілих, забезпечення шифрами кореспондентів – дипломатів, воєначальників, інших державних діячів. Безпосередньо їм докладалися звіти про створення нових шифрів і здобич іноземних шифрів.

Стосовно російських «*цифирных азбук*» і ключів 1700-1720-х років, то вони були шифрами заміни, де елементи, відкритого тексту, які надалі будемо називати шифровеличинами, замінюються умовними позначеннями – шифропозначеннями. Тексти, які шифрувались, писалися на російській, французькій, німецькій і навіть грецькій мовах. У різних шифрах шифровеличинами виступали окремі букви, слова і стандартні вирази.

Як шифропозначення використовувалися елементи, як правило, алфавітів, що спеціально складалися з цією метою, які могли бути буквами кирилиці, латиниці, інших абеток (наприклад, глаголиці), цифри, особливі значки. Частина з таких значків, що мали іноді химерні контури, були нейтральні за значенням, інші ж були символами, до нашого часу майже абсолютно забутими та відомими лише вузькому колу осіб, а в ту далеку епоху несли певне смислове навантаження. До цих останніх відносилися й астрологічні символи планет, що одночасно були й символами металів.

У шифрах петровської епохи уживалися тільки індо-арабські цифри, що з'явилося, ймовірно, наслідком того, що саме Петром I на початку XVIII ст. була виведена з уживання архаїчна буквена кирилична нумерація, що застосовувалася до цього. Реформував Петро і кириличне письмо, ввівши новий вигляд шрифтів, які визначають сучасну зовнішність російської писемності. Проте старі графеми продовжували використовуватися як тайнопис.

Вживалися як шифропозначення і буквені поєднання. Таким чином у той час в Росії використовувалися однобуквені, двобуквені, цифрові, буквено-складові шифрозаміни.

Перші державні шифри були шифрами простої або взаємно-однозначної заміни, в яких кожній шифровеличині відповідало тільки одне шифропозначення, і кожному шифропозначенню – одна шифровеличина.

У російські шифри даного періоду, як правило, вводяться «пустушки» – шифропозначення, яким не відповідає жодний знак відкритого тексту. Хоча зазвичай для цього використовувалося всього 5-8 шифровеличин як пустушки, зрозуміло, що введення їх у шифротекст, який виходив у результаті заміни елементів відкри-

того тексту шифропозначеннями, відображало прагнення творців шифрів осмислити дешифрування шифролистування.

Ці пустушки розбивали структурні лінгвістичні зв'язки відкритого тексту і, до певної міри, змінювали статистичні закономірності, тобто саме ті особливості тексту, які використовували, в першу чергу, при дешифруванні шифру простої заміни. Крім того, вони змінювали довжину відкритого повідомлення, що ускладнювало прив'язку тексту до шифроповідомлення. Тому, мабуть, не випадково, за даними Д.Кана, перший такий російський шифр був дешифрований англійцями лише у 1725 році.

Крім того, в деяких шифрах шифропозначення-пустушки могли використовуватися для зашифрування крапок і ком, що містилися у відкритому тексті. Як правило, це особливо обмовлялося в коротких правилах користування шифром, які поміщалися в цих випадках у шифри.

Зовні шифр Петровської епохи являв собою лист паперу, на якому від руки була написана таблиця заміни: під горизонтально розташованими в алфавітній послідовності буквами кириличної або іншої абетки, яка відповідала мові відкритого повідомлення, були підписані елементи відповідного шифроалфавіта. Нижче могли розміщатися пустушки, короткі правила користування, а також невеликий словник, що називався «суплемент» і містив деяку кількість слів (імен власних, географічних найменувань) або якихось стійких словосполучень, які могли активно використовуватися у текстах, призначених для зашифрування за допомогою даного шифру.

Найранішим шифром описаного типу була «*цифирная азбука*» 1700 року для листування Колегії закордонних справ (далі – КЗС) з російським послом в Константинополі Петром Толстим.

Вона була шифром простої заміни, в якому кирилічній абетці відповідав спеціально складений алфавіт. Тут же були два записи. Перший з них: «*Список с образцовой цифирной азбуки, какова написана и послана в Турскую землю с послом и стольником с Толстым сими литеры*». Другий особливо цікавий: «*Такову азбуку азволнил во 1700 г. написать своею рукою Великий государь по друго диво еси же*». З цього виходить, що автором даного шифру був сам Петро Великий.

У Державному архіві Татарстану знаходиться власноручний лист Петра I Толстому, в якому він пише, що посилає йому шифр для кореспонденцій. Цей шифр мав такі правила користування: «*Сии слова без разделения и без точек и запятых писать, а вместо точек и запятых и разделения речей вписывать из нижеписанных букв…*»:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л
ме	ли	ко	ин	зе	жу	ню	о	пы	ра	су
М	Н	О	П	Р	С	Т	У	Ф	Х	Ы
ти	у	хи	от	ца	чу	ше	ам	з	ъ	от

Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
ь	ъ	ю	я	ф	а	бе	ва	гу	ди	

Слово «УЖГОРОД» шифрувалося таким чином: «амнюинхицахизе».

Був тут і невеликий словник з іменами деяких державних діячів і найменуваннями декількох військових підрозділів і географічними найменуваннями. Ця обставина також знайшла віддзеркалення в правилах користування, де мовилося: *«Буде же когда случится писать нижеписанных персон имяна и прочее, то оныя писать такими знаки, какия против каждой отмечено, однакож писать все сплош, нигде не оставливая, а между ими ставить помянутыя буквы, которыя ничего не значат».*

Цікавим був і блокнот з шифрами, якими переписувався Петро І. Він був зошитом, листи якого були скріплені мотузком. Розмір зошита: 20х16 см. На кожній його сторінці було записано по одному шифру, всього їх шість:

1) шифр Петра І, який був йому присланий з Колегії закордонних справ до Франції у 1720 році для листування «*от двора ко двору*»;

2) шифр «*для писем к графу Г. и барону П.*»;

3) до князя Долгорукого;

4) до князя Репніна (1715);

5) «*азбука, которая была прислана от двора его царского величества при указе №..., а полученная 30 июля 1721 г.*»;

6) «*азбука цифирная, какову прислал Дмитрий Константинович Кантемир в 1721 г.*»

Останній шифр із російським алфавітом відрізнявся від попередніх тим, що як шифропозначення в ньому були використані не букви якого-небудь алфавіту, а числа. Розглянемо ще декілька шифрів раннього типу.

«*Азбука, данная из государственной коллегии иностранных дел 3 ноября 1721 г. камер-юнкеру Михаилу Бестужеву, отправленному в Швецию*», призначалася для шифрування листів Бестужева до Петра І і у КЗС. Алфавіт у цьому шифрі був російський із простою буквено-цифрово-значковою заміною без ускладнень. Ця і багато інших «*азбук*» зберігалися в конвертах, на яких були написи про те, для яких цілей призначався даний шифр.

Шифри для листування з царем або КЗС в обов'язковому порядку вручалися всім, хто прямував за кордон з державним дорученням. Це могли бути як дипломати, так і не дипломати. Наприклад, збереглася «*азбука для переписки с господином бригадиром и от гвардии майором Семеном Салтыковым, который отправлен к его светлости герцегу Мекленбургскому. Дана Салтыкову 1 декабря 1721 г.*».

Збереглися і шифри канцлера Р.І.Головкіна. Так, шифри, якими користувався канцлер у 1721, 1724 і 1726 роки для листування з різними державними діячами,

були підшиті в один зошит. У кореспондентів Головкіна були перші примірники цих шифрів, у канцлера – другі. У цей зошит було включено 17 шифрів. Серед них «Азбука Олексія Гавриловича Головкіна», «Азбука князя Бориса Івановича Куракіна», «Азбука Олексія Бестужева», «Азбука губернатора астраханського пана Волинського», «Азбука Флоріо Беневені» тощо.

Всі ці шифри побудовані однаково, хоча і мають деякі особливості. Так, в «Азбуці О.Р.Головкіна» російський алфавіт, де кожній приголосній букві відповідало по одному шифропозначенню, а голосній – по два, одне з яких – буква латиниці, а інше – двозначне число. Цікаво, що на відміну від багатьох інших шифрів, цей шифр написаний не в горизонтальних рядках, а по вертикалі у два стовпці. В ньому було 5 пустушок (букви кирилиці), як помічено: «*пустые между слов дабы растановок не знать*». Крім того, були особливі, також буквені позначення для ком і крапок. Таких позначень було також п'ять.

Як умовні позначення використовувалася ціла система цифр, ідеограм, особливих значків, спеціально складених алфавітів. Так, у шифровках Петро I зображував ім'я українського гетьмана Івана Мазепи у вигляді сокири й шибениці після того, як той перейшов до шведського короля Карла XII у жовтні 1708 року, а керівника повстання в 1707-1709 років К.Булавіна – у вигляді шибениці.

Петро I приділяв особливу увагу надійній розсилці шифрів і ключів до них. Він писав одному зі своїх послів: *«При этом посылаем к Вам ключ, и ежели посланный здорово с ним поедет, и о том к нам отпиши, дабы мы впредь нужные письма могли тем ключом писать и посылать»*. За указом Петра I кур'єр повинен був *«как можно менше знать, что он перевозит, и быть довольным оплатой своего труда»*. Самому ж кур'єру наказувалося: *«…отнюдь ничьей грамотки не распечатывать и не смотреть»*.

Отже, документи свідчать, що в петровську епоху центром, де створювалися шифри, де вони вручалися або звідки вони розсилалися кореспондентам, був спочатку Посольський наказ, потім Посольська похідна канцелярія, а з 1720 року – Перша експедиція КЗС.

Вся діяльність з виготовлення шифрів здійснювалася під безпосереднім керівництвом самого імператора, канцлера і віце-канцлера. Як у майбутньому в КЗС, вже в Посольському наказі існував спеціальний штат, якому доручалося зашифровувати і розшифровувати листування. Текст, який підлягав зашифруванню, переписували належним чином дяки Посольського наказу, а потім перекладачі і секретарі Колегії закордонних справ. Вони ж здійснювали й розшифрування листів.

У ділових паперах нерідко вживалося слово «переклад», коли мова йшла про розшифровані листи, і згадувалися «перекладачі» – особи, що займалися не тільки власне перекладом кореспонденції, але й її розшифруванням. У Посольському наказі, наприклад, перекладачем польських листів був Голембовський. Він же «перекладав», тобто розшифровував листи, написані тайнописом, які приходили з Польщі. П.П.Шафіров, посилаючи Р.І.Головкіну листа польських міністрів, писав: «*А цифирь такая, чаю, есть у Голембовского*».

Ключ до шифру вручали безпосередньо тій особі, з ким належало листуватися. Проте частини ключа могли пересилатися з нарочними. Для цього їх упаковували в конверт, який опечатувався декількома сургучними печатками. На конверті іноді писалося ім'я нарочного. Так, у 1709 році Я.У. Полонському було доручено стежити за рухом війська бобруйського старости та не допускати його до з'єднання з корпусом шведського генерала Крассау. Полонський був зобов'язаний застосовувати шифр. «*При этом посылаем к Вам ключ*, – писав Петро, – *и ежели сей посланный здорово с ним поедет, и о том к нам отпиши, дабы мы впредь нужные письма могли тем ключем писать и посылать*».

Повідомлення кореспондентів, отримані КЗС, читалися секретарями експедиції при отриманні їх з пошти, написані шифром розбиралися ними або підпорядкованими ним нотаріусом-реєстратором, канцеляристом і копіїстами. Після цього секретарі були зобов'язані, якщо президента і віце-президента в КЗС не було, посилати ці реляції до них додому, а під час засідань КЗС про них доповідати, записувати резолюції, що накладалися на них, і складати у відповідь рескрипти.

Ці рескрипти прочитувалися на наступному засіданні, причому, згідно з наказом від 5 квітня 1716 року, і чорнові їх списки, і переписані начисто підписувалися всіма членами КЗС та скріплялися секретарем. Потім текст рескрипту зашифровувався та направлявся у відповідну адресу з кур'єром. Вся робота КЗС була строго регламентована. Вхід в апартаменти КЗС дозволявся тільки особам, що там служили. Інструкція від 11 квітня 1720 року, в якій було встановлено побудову КЗС, закінчувалася приписом, як зберігати державні печатки і «*цифирные азбуки*».

Для збереження листа в таємниці застосовувалися відповідні охоронні заходи. Так, лист Петра I до Огильві від 17 лютого 1706 року супроводжувався таким записом: «*Февраля в 17 день цыфирью Реновою. А посланы в 22 день; замешкались за тем, что азбуку переписывали и в пуговицу вделывали. Посланы с маером Вейром*».

Посилалися в КЗС такі азбуки в конвертах, які опечатувалися червоними сургучними печатками, однак не державними, а особистими відправників. Пересилали шифри досить часто, адже термін їх дії був обмежений і документи, що вийшли з дії, направлялися в КЗС.

Постійно шифроване листування здійснювалося з дипломатичними представниками Росії за кордоном, зокрема: при віденському дворі – Голіциним, Урбіхом, Беклемішевим, Веселовським; при прусському дворі – з Льотом, а потім з Головкіним. Спеціальні шифри для листування з російським двором мали: Матвєєв – посол в Англії, Голландії, Австрії; Куракін – посол в Римі, Лондоні, Нідерландах, Ганновері, Парижі, і багато інших дипломатів, чиї шифри збереглися.

Часто зашифровувалися листи й коронованих кореспондентів – польського короля Августа II, прусського короля Фрідріха, хоча частіше це листування вели міністри і вельможі союзних держав: саксонську – Арнштедт, Флемінг, польську – Шембек, Синявський, Шанявський, Денгоф, данську – Юст Юль. Листування це стосувалося питань міжнародної політики, укладання союзних договорів і військових питань. Шифроване листування прусського короля знаходилося в руках його міністра Кайзерлінга. Існувало таємне листування Росії і Молдавії. Відомі шифровані листи господаря Михайла Раковіци, молдавського «посланця» Георгія Кастріота. Короткочасні дипломатичні місії також супроводжувалися врученням таємної «азбуки» особі, що прямувала з Росії за кордон.

Вищий командний склад армії і флоту також мав шифри для листування з царем. Відомі шифровані листи Петра I до адмірала Апраксіна, фельдмаршала Огильві, фельдмаршала Шереметєва, фельдмаршала-лейтенанта Гольца та їх шифровані відповіді. При цьому Петро I приділяв велике значення якості тайнопису. Так, цар з невдоволенням повідомляв фельдмаршалу Огильві: *«Цыфирь вашу я принял, но оная зело к разобранию легка»*.

У своєму листуванні кореспонденти використовували шифри, призначені для шифрування листування на різних мовах. В основному, у цей період застосовувалися так звані російські, німецькі і французькі шифри, в яких як шифровеличини використовувались букви, склади, слова, словосполучення відповідно російські, німецькі, французькі. Петро I особливо часто використовував французькі шифри.

У одному з листів Огильві скаржився Головкіну, що не зумів прочитати присланих розпоряджень Петра: «*Французские цифирные грамотки нихто читать не может, тако не знаю, что на них ответствовать. Прошу… до изволте мне на все мои письма ответ учинить немецкою цифирью, ибо той французжкой нихто не разумеет*». Такі ж скарги Огильві адресував і Петру: «*… никого здесь нет, который бы французское ваше мог разуметь, понеже Рен ключ от того потерял... Изволте ко мне через цифирь мою писать, чтоб я мог разуметь...*».

Петро пояснив, чому він перейшов у листуванні тайнописом з німецької мови на французьку: «*Французскою азбукою к вам писали для того, что иной не было. А которую вы перво прислали, и та не годна, понеже так, как простое письмо, честь можно. А когда другую прислал, то от тех пор ею, а не французскою к вам пишем. А и французской ключ послан*».

Вручалися шифри для таємного листування і особам, що отримували спеціальне військове завдання від царя. Найбільш близькою особою до Петра I, як відомо, був Меншиков, якому після Полтавської перемоги цар присвоїв чин генерал-фельдмаршала. Шифроване листування між Петром I і Меншиковим стосувалося надзвичайно важливих питань. Так, Петро I у січні 1708 року послав Меншикову шифроване «*Рассуждение*», яке розглядалося на військовій раді у місті Вільно 3 лютого, і просив його висловитися з даного питання. У іншому випадку Петро вимагав, щоб Меншиков зі свого боку прислав «*Рассуждение*» цифрою.

Меншиков, у свою чергу, листувався таємною азбукою і з дипломатами Долгорукими, і з підпорядкованими йому особами – генерал-майором Волконським, Боуром, Кропотовим і іншими. Комендант Полтави Келін отримав 19 червня 1709 року, тобто за тиждень до Полтавської битви, шифрований лист Петра I, відправлений до нього в шести примірниках. Цар писав: «*Когда сии письма получите, то дайте в наши шанцы сегодня знак, не мешкав, однем великим огнем и пятью пушечными выстрелами рядом… что вы те письма получили*».

Таким чином, військова шифрована кореспонденція супроводжувалася ще й умовною сигналізацією. Самі листи пересилалися в порожнистих бомбах, оскільки облога шведами Полтави не давала можливості листуватися іншим чином. Через 2 дні, 21 червня, Келін зумів повідомити Меншикова у шифрованому листі про тривогу, що спостерігалася у Полтаві, у шведському таборі та про перегрупування військ ворога у зв'язку з переходом російської армії на правий берег Ворскли.

Листування, що стосувалося важливих внутрішньополітичних питань, також шифрувалося. Так, спеціальний шифр був розроблений для листування про повстання на Дoні у 1707-1708 роках. Ключ до цього шифру мали: Петро I, що стежив за ходом повстання, Меншиков – командувач кавалерією, адмірал Апраксін, який вів будівництво гаваней і флоту на півдні Росії, де розвивалося повстання, підполковник Преображенського полку Долгорукий, призначений начальником всіх озброєних сил, виставлених проти повстанців, і азовський губернатор Толстой, якому була підпорядкована територія, де знаходився оплот від турецької небезпеки – Азовська фортеця.

Таємне листування, для якого були розроблені особливі шифри, велося з адміністраторами прикордонних районів і губерній – з київським губернатором Голіциним і обер-комендантом Нарви Наришкіним.

У 1711 році для внутрішнього управління державою був створений Сенат.

Дуже скоро після цього Петро I почав шифрувати свої листи Сенату. Зашифровані частини цих листів зазвичай стосувалися військових питань.

Таким чином, можна сказати, що урядове, загальнодержавне шифроване листування в петровську епоху активно велося у сфері зовнішньої політики та дипломатії, військової діяльності та вирішення внутрішньо-політичних питань.

Разом із тим, Петро чудово розумів, що Росія в значній мірі відстала від провідних європейських держав у сфері криптології, тому ліквідувати це відставання можливо було лише перейнявши європейські шифросистеми та запросивши провідних криптологів Європи для роботи в Росії. Спочатку вибір Петра зупинився на одному з кращих фахівців у цій сфері того часу – Лейбниці, однак через смерть останнього криптослужба Росії ще впродовж довгого часу не могла досягти європейського рівня.

3.3. «Чорний кабінет» XVIII ст.

У часи перебування на російському престолі Катерини I віце-канцлером Росії і, отже, керівником її криптослужби став Андрій Іванович Остерман (1686-1747). У 1708 році він був прийнятий в число перекладачів Посольського наказу та служив у Похідній канцелярії царя. У липні 1710 року він був посланий до прусського і данського королів. Після повернення до Росії він був призначений секретарем Посольської канцелярії.

В утвореній у 1720 році КЗС він зайняв місце таємного радника канцелярії. Посидючість, працьовитість, дипломатичне мистецтво і знання досконало 4-х європейських мов зробили його незамінним для імператриці. 24 листопада 1725 року вона нагородила Остермана званням віце-канцлера з чином дійсного таємного радника, а на початку наступного року він був призначений членом Верховної таємної ради. У листопаді 1726 року Остерман став головним начальником над поштою (пошт-директором), а 1 січня 1727 року отримав орден Андрія Первозванного.

У створеному 10 листопада 1731 року Кабінеті Міністрів барон Остерман набув першорядного впливу на справи.

Після смерті канцлера Головкіна Остерман отримав звання першого кабінет-міністру та, не зважаючи на відносини, що загострилися між ним і Бироном, зберіг міцне положення при дворі. Імператриця Анна Іоанівна в скрутних випадках радилась з ним, тому сучасники називали його «оракулом» цариці, «душею» кабінету.

При Остермані криптологи Колегії закордонних справ продовжували роботу відповідно до вже сталих традицій. Наукова думка не стояла на

місці, постійно велися пошуки нових шифрів. Такими новими шифрами були спочатку алфавітні, а потім неалфавітні коди. У цих кодах словникові величини вміщувалися у декілька розділів: алфавіт, склади, *«суплемент», «счёты», «месяцы».*

Алфавіт у цих шифрах міг бути російський або латинський, залежно від того, на якій мові писалося повідомлення. Склади постійні та характерні для кожної мови, тому ці розділи шифрів для кожної мови були однакові. Наприклад, для російських шифрів це були: ба, бе, би, бо, бу, би, бя, ва, ве, ви, в, ву, ви, вя тощо.

«Суплемент» був достатньо великий і включав не тільки необхідні імена царствених персон, державних діячів («персони») і географічні найменування, як це було раніше, але й іншу активну лексику. У цей розділ, наприклад, могли входити слова: домагання, схильність тощо.

Розділ *«счёты»*, або як його ще називали *«исчисления»*, як правило, у всіх кодах був однаковий. Він включав такі величини: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, 00, 000, 0000, 00000, мільйон. Іноді цей розділ якось доповнювався, наприклад, могли бути додані числа 50 000 і 100 000.

Місяці також перераховувалися в особливому розділі, і майже у всіх шифрах це пояснювалося так: *«Месяцы для того особливыми литерами изображены, чтоб оные употреблять, когда в контексте нужда востребует, а инако в обыкновенном месте датума писать не надлежит».*

За рідкісним винятком шифропозначення – це арабські цифри. Цифри-шифропозначення для різних частин словника завжди мали відмінності. Наприклад, якщо для алфавіту вони могли бути одно-, дво-, тризначні, то для *«суплемента»* тільки три- або чотиризначні, а для інших частин *(месяцы, счёты)* тільки чотиризначні. Крім того, могли бути й інші відмінності. Так, якщо для алфавіту і *«суплемента»* шифропозначеннями могли бути різні числа, то для інших розділів – лише числа, що закінчувалися нулями: 700, 750, 720, 4000 тощо. Взагалі для кожної подальшої частини словника характерна була все зростаюча значність шифропозначень.

Ці шифри мали велику кількість пустушок, що вводилися з метою ускладнення шифру. Могли вводитися помилкові додаткові цифри, що також не мали сенсу, але не входили до числа пустушок. У правилах користування шифрами, хоча вони були ще дуже короткі, явно проступала тенденція до використання при шифруванні навіть невеликих текстів значної частини або навіть більшості словарних величин. Як шифропозначення використовувалися майже виключно цифри на відміну від шифрів першої чверті століття, коли в цій ролі частіше виступали різні ідеограми. У новому типі шифрів вони застосовувалися вкрай рідко та лише для позначення «персон».

Проте разом із цими шифрами продовжували активно використовуватися і шифри старих зразків, в яких був лише алфавіт із шифропозначеннями, – цифрами, буквами або химерними старовинними ідеограмами, такими, наприклад, як у ранній *«цифирной азбуке»* для листування з Григорієм Волковим і князем Куракіним.

Розробники шифрів у цей період вже знали, що частота використання голосних букв у мові вища, ніж приголосних. Тому в 1730-1740-і роки в нових шифрах голосним обов'язково відповідало по декілька шифропозначень, приголосним – однодва. Спостерігалися спроби запису шифротексту без розділень шифропозначень крапками (що раніше було абсолютне виключено) або з розділенням їх фальшивими крапками. Спосіб розшифрування в правилах обмовлявся заздалегідь. Приклад такого зашифрування наведений у *«цифирной азбуке»* для листування з державним віце-канцлером графом Воронцовим.

Це був шифр простої заміни, де буквам кирилиці відповідали двозначні цифрові шифропозначення, причому голосним додано по шість шифропозначень, приголосним – по два. У правилах сказано: *«Сею цифирью писать двояким образом, без точек, и с фальшивыми точками, которые как бы расставлены не были, токмо для разбору всегда по два номера брать надлежит».*

Шифропозначення в цей період вибиралися завжди за певними порядковими алфавітними схемами, що, зазвичай, не сприяло надійності шифрів. Наприклад, цей шифр виглядав так:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	...
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	...
40	57	58	59	60	41	74	75	42	80	81	82	83	43					44	...
62	.....				63	.....		64	.....				65	.....				66	...
85	.....				86	.....		87	.....				88	.....				89	...
99	.....				98	.....		97	.....				96	.....				95	...
56	.....				55	.....		54	.....				53	.....				52	...

Слово «УЖГОРОД» можна зашифрувати таким чином: «441.7592.426.5.315», «8.974.1.488.266.560» тощо.

З початку 1730-х років у Росії спостерігався перехід від алфавітних кодів до неалфавітних. У алфавітних кодах відкритий текст і шифропозначення (власне код) нумерувалися паралельно один одному. Відхилення від цього порядку хоча і були, але практично дуже незначні і мало впливали на підвищення надійності або, як прийнято говорити, стійкості коду. Мабуть, розробники шифрів відзначили, що такий паралелізм істотно полегшував відновлення відкритого тексту і самого коду, оскільки правильне вгадування деякого числа шифропозначень дозволяло упорядкувати в алфавіті шифропозначення інших словарних величин.

Зрозуміло, що уникнути такої слабкості коду можна було шляхом перемішування шифропозначень. У цих випадках для полегшення процесів зашифрування та розшифрування необхідно було скласти *«шифрант»* і *«дешифрант»* – частини коду, призначені відповідно для зашифрування та для розшифрування. У шифранті в алфавітному порядку розташовувалися елементи відкритого тексту (шифровеличини), тобто букви, склади, слова, словосполучення, а у дешифранті – в порядку

зростання – шифропозначення, якщо вони були цифрові. Якщо ж вони були буквені, то у дешифранті шифропозначення також розташовувалися в алфавітному порядку. Проте в шифрах цього другого типу буквені шифропозначення були вкрай рідкісні, вони траплялися лише іноді в окремих частинах шифрів, наприклад, у суплементі.

У цей період у розробників шифрів з'явилося явне прагнення додати кожній букві алфавіту у шифрі якомога більше шифропозначень. Проте всі ці шифропозначення мали одну дуже велику ваду: вони писалися підряд, що давало змогу легко їх розкрити. Так, наприклад, *«цифирная азбука»* для листування з бароном Кейзерлінгом, відправленим до Польщі у грудні 1733 року, мала такий вигляд:

A 11 12 13 14 15
B 16 17 18 19 20
...
Z 131 132 133 134 135

У невеликому суплементі цього шифру кожній величині відповідали по два шифропозначення, вибрані підряд у числовому ряду тризначних цифр: 260, 261 тощо.

А у ще одному шифрі камергера графа Льовенвольда кожній букві латинського алфавіту відповідає навіть по 10 шифропозначень:

A 12 13 14 15 16 17 18 19 20 321
B 21 22 23 24 25 26 27 28 29 332
C 30 31 32 33 34 35 36 37 38 343 тощо.

У невеликому суплементі два тризначні цифрові шифропозначення, додані кожній словарній величині, також вибрані підряд. Крапкам і комам відповідали тризначні шифропозначення. Таким чином, традиція вибору різних шифропозначень для різних частин шифру, що склалася у петровську епоху, знайшла своє продовження у цьому другому типі шифрів XVIII ст.

Однотипні по суті, ці шифри другого типу зовні могли оформлятися порізному. Так, в одних випадках шифрант і дешифрант могли поміщатися на одному розвороті великого листа паперу. У інших випадках шифрант міг виділятися окремо і був листами, зшитими нитками в зошит, а дешифрант писався на окремому розгорненому листі. В обох випадках у шифранті шифровеличини могли поміщатися по-різному: або в порядку алфавіту з виділенням крапок і ком окремо в кінці, або по розділах (словник, складова таблиця, алфавіт, числа – *«счёты»*, календар – *«месяцы»*, пустушки). В цей же час почали поміщати у шифрант, а часто і у дешифрант, правила користування шифром. Ці правила пояснювали ті ускладнення, ті хитрощі, якими відрізнявся даний шифр.

Розглянемо деякі найбільш характерні зразки таких шифрів того часу.

У 1735 році резидент Олексій Вешняков прислав у КЗС *«цифры, которыми он корреспондует с генералитетом и министрами российскими, обретаю-*

щимися при чужестранных дворах».

Цифра оформлена у вигляді прошитого нитками зошита. На першій сторінці – заголовок: *«Цифирь секретная, посланная к ея императорского величества господам министрам в Лондон и Дрезден»*. Вся сторінка розбита на три вертикальні графи. Перша графа – *«Алфавит для сложения*». У цю графу поміщені букви російського алфавіту, яким відповідають двозначні цифрові шифропозначення (довільні). Сюди ж поміщені в алфавітному порядку найбільш вживані прийменники, займенники, частинки: въ, изъ, як тощо.

Друга графа – *«Разные знаменования»* – містила словник шифру. Цікаво, що разом з тим, що кожному шифропозначенню могли відповідати, як завжди, по одній словниковій величині (наприклад, 100 – *«Ея Императорское Величество»*, 199 – *«двор Ея Императорского Величества»*), деяким з шифропозначень відповідали цілі групи словникових величин, необхідні величини з яких вибиралися відповідно до контексту (наприклад: 198 – Англійський король, двір, Англія).

Третя графа – *«Для разбору»* – дешифрант. На другому листі тут приведені *«Изъяснения для употребления сей цифири»*.

В *«Изъяснениях*» розкриті хитрощі цього шифру. У шифропозначеннях відсутні цифри 3 і 7, тобто може бути 46, але не 47, 36 тощо. Самі по собі будь-які двозначні або тризначні цифри, що містять 3 і 7, служили для позначення ком і крапок. При цьому рекомендувалося: *«Мешать оныя между всеми как в десятичных, так и в сотенных, яко прибавкою оных число умножится. Следственно знаменательное скроется так, что никакая комбинация открыть не может. Например: А – 29 можно представить: 729, 279, 297 или 329, 239, 293. Сим образом на всяку литеру, по малой мере, шесть номеров, которы знаемы будут токмо тому, кто ведает, что 3 и 7 ничего тут не значатъ. Следственно, яко оне бы не были, но едино 29 будет видеть».*

Писати рекомендувалося всі цифри як без вставок, так і зі вставками підряд *«без роставок буква от буквы и речь от речи».* Особливо рекомендував автор шифру вводити *«смешения с 3 и 7»* при зашифруванні по буквах, де шифропозначення – двозначні («*от большей части десятеричных надлежит мешать с пустыми*»), бо «*когда в 10 строках один номер чаще найдется, то можно догадаться, что гласная буква или какое обыкновенное частое окончание, но расставливая всякой пятою на преди, в средине или на конце прибавлять. Как явствует в следующих двух примерах в цифири сей речи, сей образец есть неразборимый, ежели будет писана смешением пустых прилежно*».

І далі наводився приклад на зашифрування, з якого можна було зробити висновок про те, що голосні легко виділити, «*понеже оных токмо пять против двадцати нужно чаще употреблять. А когда будут смешаны с пустыми, то знающий оные иного опричь сих не увидит, ведая, что 3 и 7 ничего не знаменуют. А не-*

знающему все различными номерами покажется, смешанные с пустыми, ибо ни один на другого походить не будет, и не однем, но разными те образы особливо в одной строке и ближних перемешивать надлежит».

Зберігся також шифр, який Вешняков вручив у січні 1737 року для листування абату Косу, що був російським агентом. На шифрі був напис: *«Цифры с аббатом Косом, данная ему в Каменце от резидента Вешнякова при проезде его от Турской крепости в Россию».* Цей шифр був побудований за принципом шифрів 1720-х років: російський алфавіт, кожній букві відповідали одно-, дво- і тризначні цифри. Правда, було багато пустушок – 85. Такий же шифр був вручений Вешняковим абату Косу і з латинським алфавітом.

Політичними агентами Росії були не тільки державні іноземні діячі, але й інші особи. Наприклад, в Туреччині російськими агентами у цей період були єрусалимські патріархи Досифей, а пізніше Хрісанф. Через Досифея йшло листування Росії з молдавським правителем. Патріарх Хрісанф запропонував Головкіну таємну «азбуку» для листування, яка була прийнята російським двором з деякими поправками, з приводу чого Хрісанф писав Головкіну: *«Прийняли ми цифру, яка прислана в дополнку наший, і зело неабияка».*

Крім того Хрісанф запропонував ввести у таємне листування ще деякі умовності: *«А чтоб нам чащей писать к Великому Государю и к Вашему Высочеству и безопасно сделали мы сию цифирь. Посылаем и образ печати. И как придет к вам какое письмо, в котором есть та печать, ведомо буди, что есть наше писание. А с лица печать какая-нибудь, только бы что была сия внутри. К тому же, которое письмо имеет с лица круг, тое к Великому Государю; а которое имеет треугольный знак, есть к Высочеству Вашему. И сие всегда до будет за подлинное».*

Введення безлічі пустушок у старі типи шифрів свідчило про виразне розуміння розробниками *«цифирных азбук»* того впливу, який мала на розкриваність зашифрованого тексту частота вживання одних і тих же величин, особливо букв. По мірі ускладнення шифрів кількість пустушок в них все збільшувалася, деколи їх обсяг у словнику міг перевищувати обсяг його значущих величин.

Так, наприклад, німецький шифр від січня 1744 року, що був отриманий від генерала барона Любераса для листування з ним російських міністрів при іноземних дворах, мав 165 пустушок, а у шифрі від січня 1745 року для листування КЗС з дійсним камергером і надзвичайним посланником у Берліні Петром Чернишовим пустушок взагалі була велика кількість. У звичайній таблиці пустушок було 90 – від 1003 до 1093. Крім того, у примітці було написано: *«Все нумера свыше 3015 служат тако ж пустыми, како пустыми употребляются и те нумеры, которые по порядку до 3015 не доставаают»*. Значущих величин в даному шифрі було близько 400, таким чином пустушки значно перевищили цю кількість.

У тому ж 1745 році Чернишову був надісланий ще один шифр, у якому було пе-

рераховано 90 пустушок, а крім того, вказано: *«Прочие числа все от 500 до 1000 и выше можно писать пустыми же, но каждое число... разделять точками. При употреблении сего ключа цифирного надо особливо того наблюдать, чтобы каждое число точками разделяемо было с частым при том вмешиванием пустых».*

Ще одним прикладом того, що розробники шифрів прагнули в цей період помістити в них якомога більше пустушок, може служити шифр, надісланий у 1747 році до дійсного таємного радника у Берліні Кейзерлінгу. У цьому невеликому за обсягом шифрі для шифропозначень були обрані числа з різних, окрім першої, сотень, а також першою, шостою, сьомою, восьмою тисяч. А як пустушки були вказані такі числа: 1-100, 190-199, 243-299, 327-427, 442-549, 573-674, 682-789, 807-906, 921-1000, 5635-7009, 7043-10000. Конверт, у якому доставили цей шифр до Берліна, був опечатаний безліччю сургучних печаток і на ньому був напис про те, що доставлений він лейб-гвардії поручиком Ізмайловим.

У середині XVIII ст. під час царювання Єлізавети Петрівни була створена секретна служба перлюстрації. Результати роботи цієї служби декілька разів на місяць доповідалися цариці, однак це зажадало створення сильної криптоаналітичної служби для «злому» іноземних шифрів. Новий етап у розвитку російської криптослужби (іншими словами - ЧК) був пов'язаний з ім'ям Олексія Петровича Бестужева-Рюміна, призначеного в 1742 році головним директором пошт. Він уперше у вітчизняній практиці залучив до криптоаналітичної діяльності професійних вчених-математиків, причому кращих з них, що були тоді «світилами» європейської математичної науки.

Першим, кого Бестужев-Рюмін залучив до такої роботи, став відомий математик і фахівець з теорії чисел Християн Гольдбах. Іменний указ імператриці Єлізавети про його призначення на «особливу посаду» був датований 18 березня 1742 року, а справа про це названа *«Об определении в Коллегию иностранных дел бывшего при Академии наук профессора юстиц-рата Христиана Гольдбаха статским советником с жалованьем 1500 рублей, о выдаче недоданного ему в Академии наук жалованья и о выдаче ему вперед жалованья».*

Більше року Гольдбах витратив на придбання практичних навичок у новій справі, але перший успіх у дешифруванні цифрових текстів невідомого змісту прийшов до нього лише в липні 1743 року. З липня по грудень 1743 року ним був дешифрований 61 лист «міністрів прусського й французького дворів». Навесні 1744 року він уже міг «ламати» шифри підвищеної складності. На Гольдбаха посипалися всілякі милості імператриці, але необхідно відзначити головне – владні особи відчули, що математика для держави та для них особисто, це не щось престижно-декоративне, а «щит і меч», що охороняли їхні безпосередні інтереси.

Збереглися російські копії дешифрованих листів 1742 року: від *«голштинского в Швеции министра Пехлина к находящемуся в Санкт-Петербурге обер-маршалу голштинскому Бриммеру»*, *«голландского в Санкт-Петербурге резидента Шварца к Генеральным штатам, к графине Фагель В Гаагу, к пансионерному советнику фон*

дер Гейму и пр.», «австро-венгерского в Санкт-Петербурге резидента Гогенгольца к великому канцлеру графу Ульфельду и к графу Естергазию, а также секретаря его Босслера к маркизу Вотте», «английского в Санкт-Петербурге министра Вейча к милорду Картерсту в Ганновер и к герцогу Ньюкастльскому», а також копії деяких інших документів.

Найбільшого успіху Гольдбах домігся у перших числах червня 1744 року, коли ним була прочитана шифрована депеша французького посла Шетарді до Парижа. Цей випадок став хрестоматійним в історії криптології. Знаючи, що його листи на пошті розкривалися, Шетарді був упевнений, що прочитати його шифр було неможливо й тому легковажно писав про імператрицю, що вона цілком віддавалася своїм задоволенням, була несерйозна, дурна та розпусна.

Бестужев-Рюмін, який став канцлером, спритно використав саме цей текст у боротьбі проти «французької» придворної партії (раніше в нього вже були дешифровані тексти практично всіх листів цього посла). Він розіграв перед Єлізаветою сцену дешифрування депеші, «вимушено» вимовляючи *«поносные слова»*. В результаті 17 червня Шетарді був вигнаний із країни, а робота Гольдбаха на терені дешифрування не залишалася без уваги та високо була оцінена імператрицею.

У 1744 році вона дала вказівку про видачу йому надалі річної платні у 2000 рублів із статс-контори. У 1760 році Гольдбах отримав звання таємного радника з щорічною платнею у 4500 рублів. Це було одне з найвищих звань в російській державі, і нагороджувалися ним дворяни за особливі заслуги перед Вітчизною. Відзначимо, до речі, що Леонарду Ейлеру, незважаючи на його видатні наукові досягнення та постійне заступництво з боку російського двору, вказане звання так і не було подароване.

Саме з моменту появи Гольдбаха в штатах КЗС директору Санкт-Петербурзького поштамта Фрідріху Ашу почали поступати розпорядження Бестужева-Рюміна ретельно копіювати листи цілком, у жодному випадку не опускаючи в них шифротексту. Не довіряючи рядовим копіїстам, Бестужев-Рюмін наказав копіювати в ЧК *«цифрами писанные»* частини листів професору математику Тауберту.

З цього приводу Бестужев-Рюмін писав Ашу: *«Усмотренные в переписываемых унтер-библиотекарусом Таубертом в цифрах писем неисправность причиною, что я Вам особливо рекомендовал, за нужно признать впредь списываемые им копии не токмо в речах, но и в цифрах все нумеры противу оригиналов сходны, с ним сличать и исправность оных прилежно наблюдать, ибо то необходимо потребно... Еще рекомендуется отсюда отходящие за границу иностранных министров письма прилежно рассмотреть и оные все верно списать... и того для не худо когда б и закрепленные иногда пакеты отворить возможно было, к чему благоволите приложить особливое старание».*

За розпорядженням Бестужева-Рюміна поштові служби повинні були розкри-

вати й копіювати всі листи закордонних послів (навіть до дам), що пересилалися через кордон. Приватні листи, що перетинали кордон, так само, по можливості, розкривалися всі, але копіювалися найцікавіші. Основний масив інформації надходив безпосередньо до Бестужева від Аша.

Справа перлюстрації листів виявилася надзвичайно складною, такою, що вимагала терпіння, уваги і особливих навиків, які отримувалися зовсім не відразу. Конверти слід було розкривати акуратно, по можливості не порушуючи їх цілісності. Дипломатичний лист зазвичай поміщали в конверт, який прошивали ниткою та опечатували сургучними печатками. Таке упаковане послання могло вкладатися ще в один конверт, що також прошивався та опечатувався.

Технічні проблеми безулікового розкриття листів були дуже значними. Так, Аш скаржився Бестужеву-Рюміну: *«...куверты не токмо по углам, но и везде клеем заклеены, и тем клеем обвязанная под кувертом крестом на письмах нитка таким образом утверждена была, что оный клей от пара кипятка, над чем письма я несколько часов держал, никак распуститься и отстать не мог. Да и тот клей который под печатями находился (кои я искусно снял) однако ж не распустился. Следовательно же, я к превеликому моему соболезнованию никакой возможности не нашёл оных писем распечатывать без совершенного разодрания конвертов. И тако я оные паки запечатал и стафету в ея дорогу отправить принужден был...»*.

Якщо розкривав і запечатував листи особисто пошт-директор, то копіював їх особливий секретар, переводив же особливий перекладач. Оскільки листам необхідно було надати їх первинний вигляд, тобто заклеїти, прошити ниткою та опечатати такими же печатками, якими вони були опечатані до розтину, то велике значення мала майстерність людини, що виготовляла печатки. Цей майстер-різьбяр також містився у штаті відомства Аша. Робота його була тонка й відповідальна, адже вживалася велика кількість особистих і державних печаток, якими дипломати користувались при опечатуванні своїх листів.

У той час печатка відливалася зі свинцю за формою, знятою гіпсом з негативу печатки, зробленого з воску. Цей спосіб, крім того, що був складний через 4-кратне перезнімання відтиснення (негативу – воском, позитиву – гіпсом, знов негативу – свинцем і, нарешті, знову позитиву вже на самому листі – сургучем), давав не достатньо чіткі відбитки. В подальшому у середині XIX ст. один з чиновників МЗС винайшов спосіб виробництва підробленої печатки зі срібного порошку з амальгамою. Цей спосіб був дуже простий і швидкий, а печатка виходила чіткою. Проте вона мала істотний недолік – була дуже недовговічною та ламалася від щонайменшого необережного дотику.

Аш особисто перевіряв всі вироби різьбяря печаток, робив зауваження, а потім відправляв готові зразки для оцінки Бестужеву-Рюміну, який давав вже остаточний висновок. З цього приводу велося листування.

З листа Аша Бестужеву-Рюміну від 29 лютого 1744 року: *«Печатнорезчик Купи от своей болезни отчасти оправился и уже начало подделыванием некоторых штемпелей учинил, из которых он и сегодня два отдал, но один назад взять принужден был, дабы усмотренное мною в нем погрешение поправить, а другой, который барона Нейгауза есть, я за нарочитой нахожу и оной при чем посылаю...».*

Через декілька днів Бестужев-Рюмін написав Ашу відповідь:

«Из Государственной коллегии иностранных дел санкт-петербургскому почт-директору господину Ашу.

На рапорт Ваш от 29-го февраля здесь в 6-е марта полученный в резолюцию объявляется... присланная от Вас печать барона Нейгауза при сем возвратно к Вам отправляется, дабы Вы, оную имев, столь меньшим трудом в распечатывании без формы исправляться могли. Рекомендуя, впрочем, резчику Купи оные печати вырезывать с лучшим прилежанием, ибо нынешняя нейгаузова не весьма хорошего мастерства».

У протоколах доповідей імператриці Єлізаветі можна прочитати таке: *«В Санкт-Петербурге. 12 февраля 1745 г. пополудни при докладе происходило: ...20. При сих же докладах Ея Императорское Величество о потребности в сделании печатей для известного открывания писем рассуждать изволила: что для лучшего содержания сего в секрете весьма надежного человека и ежели возможно было, то лучше из российских такого мастера или резчика приискать, и оного такие печати делать заставить не здесь, в Санкт-Петербурге, дабы не разгласилось, но разве в Москве или около Петербурга, где в отдаленном месте, и к нему особливый караул приставить, а по окончании того дела все инструменты и образцы печатей у того мастера обыскать и отобрать, чтоб ничего у него не осталось, и сверх того присягою его утвердить надобно, дабы никому о том не разглашал».*

Петро III, вступивши на престол, одержав службу перлюстрації вже в стані повного розвалу. При відсутності перехоплених депеш таку ж оцінку варто дати й ефективності дешифрування. Потрібно сказати, що якщо Гольдбах у цей час не мав масштабних успіхів у дешифруванні, то створені ним шифри, що нараховували до 3500 цифрових груп, були одними з кращих у Європі.

20 листопада 1764 року помер Гольдбах, після чого керівник КЗС граф Микола Панін запросив на його місце математика і фізика, німця за національністю Франца Ульріха Теодора Епінуса. В обов'язки Епінуса та його підлеглих входило створення шифрів і підбір ключів до шифросистем перехопленої кореспонденції.

У 1769 році Епінус був «пожалован статским советником и определен при Коллегии иностранных дел при особливой должности». За успішну роботу на терені дешифрування у 1773 році він отримав чин дійсного статського радника. Епінус майже все своє життя провів у Росії, яка стала для вченого другою Вітчизною.

Користувачами шифрів, створених в КЗС, були: імператриця (індивідуальні шифри для листування з обраними особами), кабінет імператриці (загальні й індивідуальні шифри для листування з вищими чиновниками держави), КЗС (загальні й індивідуальні шифри для листування, приблизно з 70 дипломатичними представниками Росії за кордоном та їх між собою; для листування з іноземними дворами; спеціальні шифри для листування з таємними агентами російського уряду), армія та флот.

Перлюстрація була найважливішим поряд з повідомленнями платних закордонних агентів джерелом інформації для прийняття зовнішньополітичних рішень. Перлюструвалася вся закордонна кореспонденція незалежно від положення одержувача та відправника. У 1779 році імператриця наказала доставляти їй з Санкт-Петербурзького поштамту таємно розкриту кореспонденцію. Найчастіше Катерина II читала дешифровані депеши до послів у Санкт-Петербурзі навіть раніше, ніж вони самі.

Обсяг перлюстрації був фантастично великим. У 1771 році кількість перехоплених депеш тільки прусського посла становила 150 (125 відправлених та 25 отриманих), написаних різними шифрами. У 1780 році австрійський посол використовував 8 типів шифрів, обсяги цифрових текстів досягали 15 сторінок перехоплених близько 140 депеш. Поточне дешифрування здійснювали «канцелярські служителі» за допомогою ключів, знайдених, перекуплених або викрадених Епінусом.

У кінці XVIII ст. дешифрувальна служба Росії також читала французьке дипломатичне листування. Цей результат був отриманий в результаті поєднання аналітичних методів розкриття шифрів, якими користувалася криптослужба, і роботи агентів російської розвідки, що здобували французькі шифри. Російське посольство через секретаря посольства Мешкова завербувало до себе на службу як секретного агента одного з чиновників Міністерства закордонних справ Франції.

Таким чином, російський посол у Франції барон Смолін отримував і пересилав до Петербурга шифри та ключі до них, якими користувалися у своєму листуванні міністр закордонних справ Франції граф Монморсі і французький повірений в справах в Росії Дружині. В результаті Росія отримувала розвідувальну інформацію протягом тривалого періоду, навіть після того, як Смолін вимушений був покинути революційну столицю Франції після невдалої спроби допомогти відвезти Людовика XVI з Парижа.

Крім дешифрування Епінус займався також і розробкою шифросистем. Його підлеглі готували конкретні «цифири», які тиражувалися на бланках, що друкувалися в академічній друкарні (аркуші обліковувалися). «Цифирные азбуки и разныя другия бумаги тайн подлежащие» зберігалися в КЗС в окремому від користувачів сховищі в ідеальному порядку та видавалися для шифрування й дешифрування депеш на лічені години, що були вказані у відомостях. Ці операції проводилися навченими «розбирачами», які перебували на посадах актуаріусів.

Шифрування кореспонденції імператриці й Кабінету здійснював кабінет-

міністр та його штат, а у Канцлера – чотири секретарі, які працювали цілодобово. Одним з них багато років був російський письменник Денис Іванович Фонвізін. Перевезення шифрів і депеш до Канцлера або Кабінету здійснювалося кур'єрами з сержантів гвардійських полків із жорстко нормованим часом руху.

Завданням незрівнянно більш складним, ніж створення шифрів, було для Епінуса дешифрування текстів. Цією справою Епінус займався особисто зі своїм помічником, вихідцем з німців, Йоганом Георгом Кохом. Розпочавши свою кар'єру в 1762 році копіювальником в Академії Наук, він був витягнутий звідти Епінусом у КЗС.

Свою діяльність з дешифрування Епінус повинен був почати з проблеми воістину історичної – знайти ключ до «писаного в цифрах» у 1714 році і підписаних Петром I листах до Амстердама Осипу Соловйову. В указі Сенату від 4 січня 1765 року наказувалося *«...если возможно отыскать той азбучной прежней ключ или другим каким по искусству в том средством оные разобрать переписать литерным письмом и взнесть в сенат...».*

Результати протиборства Епінуса з петровським шифром невідомі, але є численні свідчення успішного дешифрування його службою перлюстрованої кореспонденції. За успішну діяльність він отримав звання дійсного статського радника.

Значний внесок у російську криптологію зробили Єрофей Каржавін і його племінник Федір Каржавін, які навчалися у Парижі, працювали на посадах перекладачів КЗС і займалися складанням шифрів та дешифруванням. Вони стали першими вітчизняними професійними криптологами в Росії.

З середини XVIII ст. в Росії стали використовувати нові шифри. Їхні основні відмінності від попередніх шифрів були такими. По-перше, на російській мові розпочали активно використовуватися коди («номенклатори») на велику кількість букв, складів, слів, фраз тощо; їх число досягало 1200 символів. Як правило, це були алфавітні коди з цифровими шифропозначеннями. Буквам, складам тощо, що найбільш часто використовувались, надавалося декілька шифропозначень. Таким чином, застосовувався шифр гомофонної заміни, але на рівні не тільки букв, а й словосполучень. Коди мінялися регулярно, оскільки ключем такого шифру був сам код-таблиця заміни.

По-друге, збільшилась кількість пустушок, що вставлялися у шифротекст. З цього приводу в одній з інструкцій з користування шифрами вказувалося: «Пустые числа писать где сколько хочется, только чтобы на каждой строке было сих чисел не меньше трёх или четырёх». Так визначався лише нижній рівень кількості пустушок, а верхній рівень не встановлювався. Крім того, «не начинать пиесы значащими числами, но пустыми...». Тим самим початок істинного шифротексту у повідомленні маскувався пустушками, що посилювало стійкість шифру.

Крім того, у шифри вставляли «особливі числа», шифропозначення яких визначало ті частини шифротексту, що при розшифруванні необхідно було вважати пустушкою. Так, зашифрований знак «+» означав, що наступне за ним шифропоз-

начення не мало ніякого значення. Два знаки «++» говорили дешифрувальнику, що не слід читати два наступні за ним шифропозначення тощо. Знак «=» означав, що не слід брати до уваги всі шифропозначення, що стояли за цим знаком в даному рядку шифротексту, а знак «==» знищував весь подальший шифротекст на даній сторінці. Знак «*» знищував попереднє шифропозначення, два знаки «**» знищували два попередні шифропозначення тощо.

Таким чином, текст, зашифрований в результаті застосування численних пустушок і написання нічого не значущих відрізків, виявлявся значно довшим за відкритий текст. Розрахунок розробників шифрів саме і полягав у тому, що шифротексти були величезними цифровими масивами, у яких, на їх думку, лише той, хто знав ключ, міг відокремити «зерно від полови».

Надзвичайно істотним для шифрів цього типу було продовження в них традиції використання при зашифруванні одного повідомлення різних мов: як правило, всі шифри були двомовними. Словник їх складався з двох частин: російською та французькою (рідше німецькою). Відкритий текст депеші складався на цих двох мовах, при переході у процесі зашифрування з однієї мови на іншу ставилися особливі, заздалегідь обумовлені в правилах числа, яких для кожного шифру було декілька.

Цей прийом, коли різні частини однієї і тієї ж депеші писалися на різних мовах, приводив до того, що при зашифруванні не тільки практично удвічі збільшувалася кількість використовуваних кодових позначень, але, що найістотніше, змішувалися і певною мірою вирівнювалися статистичні характеристики шифротексту. При цьому основні правила як для російської, так і для іншомовної частини були однаковими, тобто наявність безлічі пустушок, зашифрування великих шматків псевдотексту, які при розшифруванні знищувалися, тощо.

Як мовилося у правилах до цих шифрів: «*В случае нужды смешаемы быть имеют между русскими французские речи и сочинения, равно как и между французскими русские... Пустые числа употребляются в начале и в конце параграфов по строке, по полуторе, по две и более, а иногда по одному только, по два и по три числа. Иногда пиесы начинаются или оканчиваются самыми значущими. Но во всяком случае часто пишутся пустые в самой середине параграфа и вместо просодии, а иногда и вмешиваются и в середине фразисов и речений. Да сверх того ставятся между пустыми и самые значущие числа, кои не понадобятся и уничтожаются».*

Катерина II особисто приділяла значну увагу шифруванню повідомлень. Так, відправляючи Олексія Орлова до Європи з розвідувальним завданням, вона забезпечила його «нарочно сочинённым цифровым ключом», додавши, що «этот ключ используется для корреспонденции вашей с Нами, которая по важности предмета свого требует непроницаемой тайны». Орлову були надані також окремі шифри на російській, німецькій та французькій мовах для листування при необхідності з ро-

сійськими послами «при государственных дворах». Для забезпечення шифрованого листування Орлов мав надійних і підготовлених «служителей канцелярских».

У той період у Росії з'явилися «циркулярні» шифри, тобто загальні шифри у послів і КЗС, що дозволяло оперативно передавати послам єдині вказівки, накази тощо.

Таким чином, до середини XVIII ст. в Росії була створена мережа загального шифрованого зв'язку. Загальний шифр отримав назву «генеральная цифирь». Разом із ним збереглися й «індивідуальні» шифри для зв'язку «центру» з кореспондентами мережі. Кожний кореспондент, як правило, мав декілька «індивідуальних» шифрів.

З *«генеральных цифирь»* XVIII ст. відомі такі:

- 1762 року на російській мові, за допомогою якої обмінювалися кореспонденцією з КЗС і між собою: Бестужев-Рюмін (Париж), Кейзерлінг (Відень), Корф (Копенгаген), Панін (Стокгольм), Голіцин (Лондон), Пушкін (Гданьськ), А.Симолін (Мітава), Д.Симолін (Регенсбург), Салтиков («закордонна армія»), Обрізків (Константинополь);

- 1762 року, що об'єднувала тих же кореспондентів, але листування по ній можна було вести відразу на 3-х мовах: російській, французькій і німецькій. Додатково цей шифр у 1764 році був даний генерал-майору князю Репніну, що прямував як повноважний міністр до прусського двору, а також генерал-аншефу князю Волконському;

- 1764 року на російській і французькій мовах, яка була розіслана російським представникам у Відні, Варшаві, Копенгагені, Лондоні, Стокгольмі, Берліні, Гаазі, Парижі, Дрездені, Мітаві, Регенсбурзі, Гданьську, Мадриді, Гамбурзі, Константинополі;

- 1768 року на російській і французькій мовах була розіслана у ті же 15 адрес;

- 1771 року на французькій і російській мовах, яка була розіслана у Мітаву, Гданьськ, Берлін, Дрезден, Париж, Мадрид, Гаагу, Лондон, Гамбург, Копенгаген, Стокгольм, Відень, Регенсбург, Варшаву, командувачу 1-ою і 2-ою арміями генерал-фельдмаршалу графу Румянцеву, генерал-аншефу князю Долгорукову. У 1779 році цей же шифр був даний відправленому до Португалії надзвичайному послу і повноважному міністру графу Нессельроде;

- 1773 року на російській мові під знаком «165», яка була розіслана, у порівнянні з попередньою, у перші 14 адрес;

- під знаком «40, 68 і 77» – найбільша з відомих цифр XVIII ст. Вона включала 2000 словникових величин і об'єднувала КЗС з 15 кореспондентами за кордоном: Стакельбергом у Варшаві, міністром Голіциним у Відні, міністром Ассебургом у Регенсбурзі, міністром Барятінським у Парижі, міністром Зіновьєвим у Мадриді, послом Белосельським у Дрездені, послом Голіциним в Гаазі, міністром Симоліним у Стокгольмі, міністром Долгоруковим у Берліні, міністром Сакеном у Копенгагені, міністром Мусіним-Пушкіним у Лондоні, резидентом Гроссом у Лондоні, послом Стахієвим у Константинополі, резидентом Ребіндером у Гданьську, князем Репніним у Берліні.

У 1771 році була паралельно організована загальна мережа зв'язку, що охоплювала абсолютно інший регіон. Так, за допомогою «генеральной *цифири*» 1771 року

під знаком «1631» переписувалися між собою і з КЗС 10 кореспондентів: повноважний міністр Булгаков у Константинополі, граф Воронцов у Венеції, граф Разумовський у Неаполі, повноважний міністр Мордвінов у Генуї, повноважний міністр князь Юсупов у Турині, граф Мореніго у Флоренції, Псаро – повірений у справах на Мальті, колезький радник Хемніцер у Смірні, генеральний консул у Молдавії, Валахії і Бесарабії Северін, колезький асесор Юлініц у Сицилії.

У КЗС вівся ретельний облік всіх цифр. Перелік цифр, списки осіб, кому вони були розіслані, від кого отримані назад окремі примірники, на якій мові шифри складені, та інші необхідні відомості заносилися в особливі реєстри.

Якщо примірник шифру кимось з кореспондентів втрачався або виникала підозра, що шифр виявлявся відомий ворогу, то негайно видавався імператорський указ про виведення цього шифру з дії та заміну його іншим. Цей указ відразу ж розсилався всім кореспондентам, що входили в дану мережу зв'язку.

Дотриманню таємниці шифролистування в КЗС приділялася велика увага. Міркуючи *«о наилучшем содержании в секрете всех в секретной экспедиции дел»*, Колегія ще у 1744 році визначила наказати всім служителям цієї експедиції (і архіву) *«ни с кем из посторонних людей об этих делах не говорить, не ходить на дворы к чужестранным министрам и никакого с ними обхождения и компании не иметь»*.

Цей наказ був підтверджений повторно 28 березня 1758 року: «Для сохранения вящего секрета при нынешних военных и всяких важных обстоятельствах» секретарям таємної експедиції ставилося в обов'язок суворо наглядати за перекладачами, «чтобы дела, им порученные, по столам не лежали и чтобы товарищи их не читали этих дел». Наприкінці наказу підтверджувалася заборона кого-небудь стороннього пускати в апартаменти, зайняті таємною експедицією.

При імператриці Катерині II 15 березня 1781 року КЗС утретє отримала наказ не допускати знайомства *«чинов департамента иностранных дел»* з іноземними міністрами та їх свитою. При цьому імператриця вказала, щоб, окрім *«министров департамента иностранных дел, каковыми ее величество почитает канцлера (или без сего звания управляющего оным департаментом), вице-канцлера и членов секретной экспедиции»*, ніхто з інших чинів колегії не ходив у будинки іноземних міністрів, не мав з ними розмов про справи, нікого з них у своєму будинку не приймав і ні під яким виглядом не вів з ними листування. Та ж сама заборона була повторена указом від 3 серпня 1791 року.

КЗС також уважно стежила за збереженням шифрів. Особисто державний канцлер, а ним у той період був граф Іван Остерман (син Андрія Остермана), неухильно стежив за суворим дотриманням правил користування вітчизняними шифрами, вимагав їх своєчасної заміни. При щонайменшій підозрі про компрометацію шифрів він давав вказівки про їх дострокову заміну або про внесення в них істотних змін.

Коли стало відомо, що один із канцелярських службовців при послові Росії у

Гданську загубив шифр, Остерман зробив послу Волчкову суворе попередження: *«...признано здесь за нужно подтвердить Вам в то же время единожды навсегда, чтоб Вы сами впредь хранили у себя цифирнык ключи и заочно не выпускали их из рук, в чем и обязываетесь Вы Вашею присягою верности Ея Императорскому Величеству».*

Поступово встановилася ієрархія шифрів, коли складні системи використовували лише для найважливіших повідомлень, а зі зниженням їхнього рангу, спрощувався й шифр. Якщо складання власних шифросистем, насамперед для російського алфавіту, ще відставало від Європи, то криптоаналітика була на висоті. З цього часу російська криптологія остаточно зайняла одну з провідних позицій у криптології європейській та стала ефективним знаряддям у руках дипломатичних і військових відомств країни.

3.4. Криптологія першої половини XIX ст.

На початку XIX ст. в Росії була зроблена реорганізація органів керування країною. У 1802 році Маніфестом Олександра I замість колегій були засновані міністерства. Зокрема, було утворене міністерство закордонних справ (далі – МЗС), канцелярія якого містила чотири основні експедиції та три таємні. Перша таємна – шифрувальна, друга – дешифрувальна, третя – служба перлюстрації.

До 1808 року начальником першої експедиції, куди входила «*цифирная*» частина, був Жерве. Потім він був призначений керівником Канцелярії, а начальником цієї експедиції, перетвореної у відділення, став Міллер. Дешифрувальну частину у цей період очолював Християн Бек. Збереглися деякі документи, що дозволяють охарактеризувати діяльність таємної експедиції Канцелярії МЗС періоду початку XIX ст. та війни з Наполеоном.

Лист від 8 березня 1812 року Міллеру:

«Г. Канцлеру угодно, чтобы Вы, милостивый государь мой, Христиан Иванович, немедленно занялись составлением двух совершенно полных лексиконов как для шифрования, равно и для дешифрования на российском и французском языках, и чтобы Вы снеслись по сему предмету с Александром Федоровичем Крейдеманом, стараясь соединенными силами привести работу сию к скорейшему и успешнейшему окончанию. А. Жерве».

Міллер і Крейдеман були не тільки розробниками «лексиконів», тобто словників до шифрів, але й самих шифрів. Цю роботу виконували і деякі інші співробітники. Після складання шифру фахівцем-криптографом у XVIII ст. він начисто переписувався від руки спеціальним

секретарем в потрібній кількості примірників. Тепер шифри виготовлялися вже друкарським способом. Відносно кожного шифру завідувачам таємною експедицією при цьому складалася доповідна записка такого змісту:

«В Государственную коллегию иностранных дел.

От нижеподписавшегося покорнейшее доношение.

Составив по приказанию сей Коллегии новую генеральную цифирь на российском и французском языках, ею одобренную, и отобрав цены за изготовление передвижных машин, равно и за напечатание наборных и разборных таблиц и за бумагу, имею честь представить о том подробную записку, прося покорнейше помянутую Коллегию благоволить на сей расход определить сумму.

Коллежский советник Христиан Миллер.

Октябрь дня 3 1804 года.

За машины:

за 15 пар машин с двойными передвижными дощечками по 125 р.

за пару – 1875 рублей.

Типографщику:

за набор разборных таблиц для российской цифири с напечатанием, по 20 р. за таблицу – 40 р.

за набор двух разборных таблиц для французской цифири с напечатанием, по 20 р. за таблицу – 40 р.

за набор одного листа и напечатание чисел и букв, принадлежащих к разборным таблицам обеих сих цифирей – 10 р.

за набор 112 1/2 страниц российской наборной азбуки и напечатание по 30 р. за страницу, а за все 112 1/2 страниц – 3375 р.

за набор 122 1/2 страниц французской наборной азбуки и напечатание, по 30 р. за страницу, а за все 122 1/2 страницы – 3675 р.

Бумаги:

Александрийской 83 л. по 2 р. 50 к. каждая – 207,50

Итого 9222 р. 50 к.

Коллежск. сов. Хр. Миллер».

На початку XIX ст. у МЗС був організований так званий «*Цифирный комитет*», до складу якого увійшли найбільш досвідчені та кваліфіковані криптографи. У завдання комітету входив аналіз і введення нових систем шифрів, контроль за їх правильним використанням і зберіганням, вивід з дії застарілих або скомпрометованих шифрів, складання висновків, звітів і доповідей для керівників МЗС і імператора з питань діяльності шифрувальної та дешифрувальної служб. Цей комітет був підпорядкований міністру, а очолював його «*главный член цифирного комитета*».

Російська дешифрувальна служба ще з середини XVIII ст. вела успішну бо-

ротьбу з королівською Францією, практично без особливих труднощів «зламавши» її шифри. Подібний стан справ перекочував і у XIX ст. Російські дешифрувальники і тут попрацювали добре: цар Олександр I мав досить інформації про листування наполеонівських генералів.

Більш того, полковник Чернишов, співробітник Особливої канцелярії (спеціального органу російської зовнішньої розвідки), що використовував шифр Суворова, виконав у Парижі значну роботу з розшуку даних про стан великої армії Наполеона. У результаті своєї роботи Чернишову вдалося завербувати одного співробітника військового міністерства Франції, завдяки якому документи, що мали стратегічне значення для Франції, Наполеон одержував ледве не одночасно з Олександром I.

Як не дивно, але геній Наполеона залишився байдужим до таємниць криптології, хоча, зазвичай, імператор використовував тайнопис. Використовував його і наполеонівський генералітет, що застосовував, наприклад, «книжковий» шифр.

У 1812 році російські дешифрувальники зіграли значну роль у розгромі армії Наполеона, який розпочав війну проти Росії. У ході військових дій вони розкрили не тільки найпростіші шифри для зв'язку з невеликими підрозділами, але й «Великий» та «Малий» шифри Наполеона. Незважаючи на те, що ці шифри були недостатньо стійкими, французи їм цілком довіряли, розраховуючи на те, що росіяни не зможуть їх розшифрувати.

Російські шифри, що використовувалися на той час у військових мережах зв'язку, за складністю їхнього дешифрування були аналогічні французьким, однак російське керівництво приділяло набагато більшу увагу їх правильному використанню. Значні зусилля були спрямовані на розвиток служби перехоплення та дешифрування. Отримана з дешифрованих повідомлень інформація вчасно передавалася командуванню армії та вищому політичному керівництву.

Наполеон же знаходився на захопленій території та не мав можливості «партизанського» перехоплення повідомлень російських воєначальників. Він не надавав великого значення криптології та цілком покладався на міць своєї «непереможної» армії, тому не мав дешифрувальної служби у військах. Дані щодо ефективного дешифрування французами російських військових депеш в історії відсутні. Таким чином, можна стверджувати, що російська криптологія перемогла в боротьбі з французькою.

Американський історик Флетчер Пратт привів такий витяг з розмови, що відбулася після війни 1812 року між Олександром I і командувачем одного з корпусів армії Наполеона маршалом Макдональдом: «Звичайно, – сказав імператор Росії Олександр, намагаючись заспокоїти маршала щодо поразок Франції, – нам дуже сильно допомогло те, що ми завжди знали наміри вашого імператора з його ж власних депеш. Під час останніх операцій в країні була велика незадоволеність, і нам вдалося захопити багато депеш». «Я вважаю дуже дивним, що

Ви змогли їх прочитати, – відзначив дещо сумно Макдональд, – хто-небудь, напевно, видав Вам ключ?» Росіянин був здивований: «Ні в якому разі! Я даю Вам чесне слово, що нічого такого не було. Ми просто дешифрували їх».

Період царювання імператора Миколи I був відначений найбільш істотною зміною у побудові центрального управління МЗС Росії – утворенням у 1828 році Департаменту зовнішніх стосунків, до складу якого увійшли три секретні експедиції: шифрувальна, дешифрувальна та перлюстрація. Таємними експедиціями у той час завідували Х.Бек (дешифрування), П.Шилінг (шифри і літографія), М.Лаваль (перлюстрація).

У 1846 році найменування Департаменту зовнішніх стосунків було замінено новим – Особлива канцелярія міністерства. Керівники експедицій були безпосередньо підпорядковані канцлеру (міністру зовнішніх стосунків) К.Нессельроде нарівні з директорами департаментів МЗС. В Особливій канцелярії було зосереджено політичне листування.

У XIX ст. продовжувалася практика перехоплення та дешифрування іноземних послань і листування антидержавних організацій у самій Росії. Цим питанням надавалося величезне значення на вищому державному рівні. Так, наприклад, Микола I і Олександр II охоче читали витяги з перлюстрованих листів і, використовуючи цю інформацію, приймали важливі рішення.

Російський ЧК, який був зосереджений, в основному, у МЗС, постійно удосконалював методи, техніку перехоплення та перлюстрації повідомлень іноземних держав. На поштамтах Петербурга, Москви, Варшави, Одеси, Києва, Харкова, Риги, Вільно, Томська і Тифліса були також створені ЧК – професійні служби з перехоплення та перлюстрації дипломатичного листування, де розроблялися методи швидкого копіювання, перлюстрації без доказів (підробка печаток тощо), оперативного ознайомлення зі змістом повідомлень та їх передачі дешифрувальним органам.

Більшість співробітників ЧК були іноземцями, які отримали російське громадянство. В основному, це були німці, що говорили російською мовою з великим акцентом, оскільки з метою власної безпеки вони вели ізольований спосіб життя. Для розкриття листів, як правило, використовувалася пара або гарячий дріт, за допомогою яких знімалася воскова печатка. Начальник київського ЧК Карл Зіверт, згодом засуджений як австрійський шпигун, винайшов пристрій, який цілком виключав можливість випадкової поломки або обгорання печатки, що свідчило би про розкриття конверту. Цей пристрій являв собою тонку круглу відполіровану паличку розміром з в'язальну спицю, розщеплену приблизно до половини. Зіверт вводив паличку під клапан конверта, розрізом захоплював лист, намотував його на паличку та витягав з конверта, не залишаючи після себе яких-небудь видимих ушкоджень.

Як стверджував колишній співробітник ЧК В.Крівош, «іноземне дипломатич-

не листування попадало до рук російських «фахівців» практично цілком. У російському «чорному кабінеті» мався повний набір бездоганно скопійованих печаток для закордонного листування всіх посольств, що знаходилися в Петербурзі, і консульств... У російського «чорного кабінету» були копії багатьох шифрів іноземних держав».

Успіхи російського ЧК визнавали навіть досить високопоставлені діячі закордонних держав. Так, наприкінці XIX століття «залізний канцлер» Німеччини О.Бісмарк виявляв особливе занепокоєння щодо схоронності таємних послань, що відправлялися з Петербурга. Він писав: «...німецький шифр не залишається невідомим російському імператорському двору; адже я знав по досвіду, що навіть у будинку нашої місії в Петербурзі зберегти наші таємниці міг не мистецьки зроблений замок, а тільки часта зміна шифру. Я був упевнений, що не міг телеграфувати в Ливадію нічого, що не дійде до відома імператора».

Сам імператор Олександр II не соромився у використанні відомостей, отриманих у результаті дешифрування. Він скаржився Бісмарку, що його, імператора, різко критикують німецькі правителі у своїх шифрованих посланнях до Росії. Читання шифролистування він вважав природним правом самодержця. Тут треба відзначити, що при використанні відомостей, добутих шляхом дешифрування, варто було виявляти особливу обережність, оскільки супротивник, довідавшись, що його шифри розкриті, міг змінити ключ і навіть усю шифросистему.

Однією з яскравих особистостей, пов'язаних з російською криптологією початку XIX ст., був барон Павло Львович Шилінг фон Канштадт. Він народився в 1786 році в місті Ревель (нині – Таллінн). Різнобічна й обдарована особистість, полковник російської армії, вчений-сходознавець, член-кореспондент Російської Академії наук, винахідник електромагнітного телеграфу, керівник «цифирного» відділення МЗС – такі найбільш яскраві моменти його біографії.

У історію криптографії Шилінг увійшов перш за все як винахідник шифрів так званого біграмного типу. Такий шифр він винайшов, працюючи в «*цифирном*» відділенні МЗС, ще до свого призначення його начальником, і документальні відомості про цю подію є у справі першої експедиції за 1823 рік. Збереглося розпорядження Нессельроде «*цифирному*» комітету від 22 березня розглянути шифр, запропонований Шилінгом, а також рапорт членів «*цифирного*» комітету Нессельроде з цього приводу від 14 червня.

Словник біграмного шифру складав двозначні буквені поєднання (французька мова), кодовими позначеннями були дво-, три- або чотиризначні числа, «*взятые по два раза каждое для переменной передачи буквенных биграмм то одним, то другим числом*». Зовні біграмний шифр був набірно-розбірною таблицею, наклеєною на коленкор, при якій була обов'язкова настанова для користування шифром. Буквені поєднання словника такого шифру могли бути російськими або французь-

кими, могли бути і подвійні російсько-французькі словники.

Листування за допомогою біграмного шифру, винайденого Шилінгом, велася французькою мовою та шифрувалися при цьому біграмами (подвійні поєднання букв і розділових знаків) французького алфавіту. Тип шифру – проста заміна, в основному на 992 знаки (992 = 32 х 31) з пустушками. Важливо відзначити, що шифрувалися біграми відкритого тексту, які не йшли підряд, а букви та знаки, розташовані на довжині *T* періоду транспаранту, на якому розписувалося вихідне повідомлення. Біграми, таким чином, складалися по вертикалі з двох рядків транспаранту: перша буква – з першого рядка, друга – з другого. Якщо в кінці повідомлення не вистачало знаків другого рядка для утворення біграми, то бракуюча частина другого рядка заповнювалася довільним чином і шифрувалися вже окремі знаки.

Граничний термін дії кожного з таких шифрів був визначений «*Цифирным*» комітетом у 6 років, якщо за цей термін шифр не буде скомпрометований. Пізніше у 1858 році цей граничний термін був зменшений до 3 років. Однак це правило часто порушувалося, що не могло не позначитися на таємниці листування.

Відомі деякі біграмні ключі барона Шилінга. Про них є відомості в «*Описи цифирям*», складеною Трефуртом, де разом з даними про інші цифри, складені з часу утворення «*Цифирного*» комітету, указується, що «*13 августа 1823 г. от члена оного Комитета Г [осподина] Ст [атского] Сов [етника] Бар [она] Шиллинга фон Канш [тадта] получены его сочинения биграммный ключ № 1 и № 2, № 3 на франц [узском] языке, а также пакет с бумагами, относящимися к составлению этих цифирей*».

У лютому 1824 року примірник № 1 біграмного шифру Шилінга був направлений Цесаревичу Костянтину Павловичу; у січні 1826 року той же перший, а також другий примірники були надані князю Меншикову при відправленні його до Персії; у 1828 році граф Нессельроде отримав третій примірник цього шифру при відправленні до Америки.

У 1826 році Шилінг склав шифр для адмірала Синявіна. У 1827 році цей примірник шифру був переданий Нессельроде, у тому ж році ще три примірники цього шифру були направлені у місію до Вашингтона. У тому ж році Шилінг склав «*генеральную цифирь*» № 16, «*партикулярные цифири*» № 4, 5, 6, 8, 9 і 10, а також військовий шифр російською мовою № 28.

У літографії, яку Шилінг організував і якою завідував всі роки служби в міністерстві, проводилися роботи з розмноження та копіювання різних державних документів. З часів діяльності Шилінга до практики МЗС увійшов звичай щодня надавати на перегляд міністру літографовані копії з перлюстрованих документів і листів, більшість з яких, природно в дешифрованому вигляді, також прямувало для ознайомлення правителю. Матеріали перлюстрації та дешифрованого листування були звичайною темою обговорення на засіданнях «*Цифирного*» комітету.

Шилінг вельми дбайливо відносився до співробітників літографії, враховуючи важливість їх роботи. Текст однієї з його доповідей віце-канцлеру Нессельроде свідчить: «*Литографские ученики Ефимов, Пальцев и Григорьев при хорошем поведении усердным исправлением своей должности, а первый из них сверх того и оказанным искусством в печатании противу своих товарищей, заслуживают внимания начальства, почему долгом поставляю себе испрашивать у Вашего сиятельства в награждение им, первому звание унтерофицера и 75 рублей, а двум последним по 50 рублей, равно и переплетчику Пазову, занимавшемуся наклейкою цифирных таблиц 100 рублей*».

Після смерті Шилінга у липні 1837 року керівником першої таємної експедиції Канцелярії МЗС був призначений Артур Міллер. Однак вже через 3 роки його на цій посаді замінив дійсний статський радник барон Дрізен.

Біграмні шифри Шилінга в порушення існуючих правил використовувалися для дипломатичного шифролистування у незмінному вигляді аж до початку XX століття, що природно не могло не позначитися на їхній стійкості. Відомі такі французькі біграмні шифри Шилінга:

1. Телеграфний ключ № 302. Введений в дію у 1856 році, виведений з дії у 1867 році. Використовувався «уповноваженим при Паризькому конгресі» бароном Бруновим для стосунків з МЗС. Видано було 5 примірників цього ключа.

2. Ключ № 303. Аналогічний попередньому. Введений в дію у 1857 році для стосунків МЗС з місією в Дармштадті.

3. Ключ № 313. Аналогічний ключу № 302. Введений в дію у 1857 році. Призначався для консульств на Балканському півострові (Мостар, Рагуза, Сараєво, Бєлград, Віддін, Яніна), місій у Константинополі і Відні, а також використовувався для ведення таємного листування з Азіатським департаментом МЗС, Канцелярією і Похідною канцелярією. Виведений з дії у 1872 році.

4. Ключі № 314 і № 315. Аналогічні попереднім. Введені в дію у 1858 році. Ключ № 314 через три роки був замінений біграмним ключем № 328, ключ же № 315 залишився у використанні на тривалий термін. Використовувалися для стосунків МЗС з посольствами і місіями в Афінах, Берліні, Берні, Бухаресті, Брюсселі, Константинополі, Копенгагені, Дармштадті, Дрездені, Франкфурті, Гамбурзі, Ганновері, Гаазі, Лісабоні, Лондоні, Мадриді, Мюнхені, Неаполі, Парижі, Римі, Стокгольмі, Штутгарті, Турині, Варшаві, Відні, Вашингтоні, Веймарі.

5. Ключ № 316. Введений в дію в 1857 році виключно для стосунків МЗС з місією в Дармштадті. Знищений у 1867 році.

6. Ключ № 323. Введений в дію у 1860 році для консульств на Балканах і в Туреччині (Адріанополь, Бітолія, Варна, Бєлград, Віддіна, Відень, Константинополь, Мостар, Рагуза, Сараєво, Ськутара, Філліполь, Яніна), а також для листування з МЗС генерального консульства в Лондоні. Використовувався до

початку XX ст., коли було визнано *«Цифирным»* комітетом, що і надалі його можна використовувати, але «для спеціальної потреби».

7. Ключ № 324. Введений в дію у 1860 році та діяв до початку XX ст. на лініях зв'язку МЗС з Берліном, Константинополем, Лондоном, Парижем, Віднем, Бухарестом. Використовувався для листування з генерал-губернатором Одеси.

8. Ключ № 328 був створений як генеральний. Мав словник меншого обсягу, ніж вищеперелічені, – 992 двобуквені поєднання. Введений в дію у 1861 році для зносин між собою і з МЗС місій в Афінах, Берліні, Берні, Бухаресті, Брюсселі та інших європейських державах. Виведений в резерв у 1891 році.

9. Ключ № 329. Аналогічний попередньому. Ключі № 328 і № 329 були введені на заміну ключів № 314 і № 315.

У МЗС Росії й інших міністерствах та відомствах продовжували активно використовуватися коди. Коди одержали поширення в Росії з XVIII ст. і були основним способом шифрування досить тривалий час. Обсяг кодів у той час лежав у межах від 300 до 1000 словникових величин.

Коди були «прив'язані» до словникової мови листування (дипломатичного, військового, торговельного тощо). При цьому найбільш часто уживаним словам і фразам надавалося декілька кодопозначень: чим частіше зустрічалася кодовеличина, тим більша кількість кодопозначень їй привласнювалося. Стійкість такої системи значно зростала за рахунок «вирівнювання» частотної характеристики зустрічальності кодопозначень у шифротексті. Таким чином, тут мало місце застосування шифру багатозначної заміни по відношенню не до окремих букв, а до цілих кодовеличин (слів, фраз тощо). У кодах також передбачалися буквено-складові одиниці тексту. Характерна риса російських кодів – наявність значної кількості «пустишок».

Коди, в основному, були алфавітними, а кодовеличини (букви, склади, слова, словосполучення) в них розташовувалися за абеткою. Кодопозначення, в основному, були цифрові – від 3 до 5 десяткових цифр, які розташовувалися в порядку зростання чисел. Практична зручність такої системи шифрування полягала в тому, що при шифруванні та дешифруванні застосовувалася та сама кодова книга, у якій і кодовеличини, і кодопозначення розташовувалися в природному порядку. Однак одночасно це було й слабкістю кодування, оскільки дозволяло супротивнику, який довідався хоча б про одне кодопозначення, висувати правдоподібні гіпотези про наступні.

Рідше застосовувалися неалфавітні коди, а також коди багатозначного кодування. В останньому випадку одній кодовеличині могли відповідати декілька кодопозначень. Практична незручність цих набагато більш стійких систем полягало в тому, що для підвищення оперативності роботи шифрувальника були необхідні дві книги (кодування й декодування), причому в книзі декодування кодопозначення (числа) розташовувалися в порядку їхнього зростання, у книзі кодування кодовеличини роз-

ташовувалися в лексикографічному порядку, а кодопозначення були довільними.

Іноді застосовувалося й подвійне кодування різними кодами. При цьому перший код не був таємним і використовувався для «стиску» відкритого тексту (зменшення його довжини), тоді як другий – безпосередньо забезпечував його захист. Досить часто кодовані тексти додатково перешифровувалися. Поряд із простими шифрами (типу простої заміни) використовувалися й досить складні, наприклад, «Лямбда».

3.5. Криптологія другої половини XIX ст.

З 1870 року офіційноим «дахом» служби перлюстрації стала Цензура іноземних газет і журналів при крупних поштамтах. З 1881 року у зв'язку з переходом поштового відомства до складу міністерства внутрішніх справ (далі – МВС) російський ЧК остаточно вже до 1917 року був підпорядкований міністру внутрішніх справ. На протязі багатьох років ним керував безпосередньо пошт-директор Санкт-Петербурзького поштамту. У 1886 році керування перлюстрацією на території всієї імперії було вперше покладено на старшего цензора Цензури іноземних газет і журналів при Санкт-Петербурзькому поштамті Карла Карловича Вейсмана.

У другій половині XIX ст. криптослужба Росії перестала бути привілеєм МЗС, а була створена ще у двох відомствах: військовому міністерстві та МВС. Цей факт свідчив про зростання значення криптології в діяльності державних органів, про істотне розширення сфер її використання.

Розвиток зовнішніх і внутрішніх мереж зв'язку, зростання обсягу шифрованого листування спричинили збільшення кількості шифрів і кодів, що вводилися в дію. З'явилася досить велика різноманітність таких систем. Поступово викристалізовувалася класифікація шифрів за своїм призначенням і метою.

Шифри розділялися перш за все за мовним принципом. Залежно від мови шифрованої інформації з'явилися російські, французькі, німецькі, англійські та інші шифри. За галузевим призначенням вони ділилися на шифри МЗС, шифри військового відомства, включаючи й імператорські шифри, шифри жандармерії та утвореного у 1880 році в структурі МВС Департаменту поліції, а також шифри, які використовувались цивільними відомствами для зашифрування своєї таємної інформації (наприклад, міністерства фінансів). Окремо виділялись агентурні шифри, що були призначені для зв'язку з розвідниками та агентами.

Всі шифри розділялися на таємні і нетаємні. Крім них вводилися ще так звані шифри спеціального призначення. В одній з інструкцій до шифрів МЗС мовилося, що нетаємними ключами слід було користуватися у всіх тих випадках, коли зміст повідомлення само по собі не міг вважатися таємним, але коли передача його в незашифрованому вигляді не представлялася зручною, наприклад, коли бажано було уникати передчасного розголосу таких повідомлень у пресі тощо.

Цікаве додавання містилося в примітках до цієї інструкції: *«Следует полагать, что несекретные ключи известны иностранным правительствам, тем не менее они представляют безусловную тайну для публики и должны храниться, если не с секретными ключами, то, во всяком случае, с секретными делами установлений, которые ими снабжены».*

Ключі спеціального призначення використовувалися для відносин із *«различными правительственными установлениями, а также с частными учреждениями и лицами».*

У 1872 році було введене удосконалення в структуру біграмних шифрів Шилінга. Розробник шифрів співробітник шифрувального відділу МЗС Нелідов запропонував істотно зменшити число букв латинського алфавіту та розділових знаків у відкритому тексті з тим, щоб можна було використовувати як шифропозначення латинські біграми та букви.

Тому французький ключ № 359/360, винайдений у 1872 році Нелідовим, отримав назву біграмно-буквеного. Він містив біграмні поєднання букв латинського алфавіту (окрім *к, w, у*), розділові (. , -) знаки – 676 величин, а також 26 букв латинського алфавіту – всього 702 величини. Шифропозначення – двозначні поєднання з 26 букв латинського алфавіту і 26 окремих букв латинського алфавіту, призначених для передачі окремих букв тексту. Призначався він для телеграфу та був введений в дію у 1873 році.

Принцип системи цього шифру був біграмним з тією лише різницею, що: 1) дві букви тексту передавалися не трьома числами, як в біграмах, а двома буквами; 2) при шифруванні двобуквені поєднання не складалися з букв двох рядків переписаного для цієї мети по відомому транспаранту тексту, але з крайніх букв кожного рядка переписаного по транспаранту тексту, рухаючись з двох кінців до середини.

Останнє удосконалення несло і деяке криптографічне навантаження. Оскільки на той час стало зрозуміло, що супротивнику відомий принцип шифрування за цією системою, то доцільно було ввести деякі зміни в цей принцип, що, звичайно, ускладнювало роботу дешифрувальників. Потрібно було ще здогадатися, в чому полягали ці зміни.

Друга група біграмних шифрів – це російські біграмні шифри, за якими шифрувалися повідомлення, написані російською мовою. Призначалися вони як для внутрішнього, так і для зовнішнього листування. Оскільки в російській мові кількість біграм перевищувала кількість тризначних чисел (разом з розділовими знаками їх було 1296), то розробники шифрів поповнювали нестачу чисел шифропозначень – тризначних чисел – однозначними, двозначними та чотиризначними.

Відомі такі російські біграмні шифри:

1. Ключ № 304. Так називаний «генерал-губернаторський шифр» призначався для таємного спілкування з Петербургу з тими з генерал-губернаторів,

в місцеперебуванні яких знаходилися телеграфні станції. Це були такі пункти: Петербург, Москва, Київ, Одеса, Рига, Гельсингфорс, Варшава, Вільно. Примірники цього ключа були у військового міністра, міністра внутрішніх справ і шефа жандармів. Шифр був введений в дію у 1857 році. Саме цей ключ був першою спробою складання російського біграмного шифру.

Згодом, коли було введено правило про з'єднання цифр для передачі по телеграфу спочатку у 3-значні, а потім у 5-значні групи, користування цією системою було визнане неможливим, і вона була замінена спочатку поєднаннями з цифр і букв для передачі російських двобуквених поєднань (як, наприклад, у біграмному ключі № 334), а потім вже біграмними ключами, в яких кількість букв було скорочена до 28 (ключі № 347, 375, 380, 381 тощо). Ці ключі використовувалися і на початку XX ст. Ключ № 304 був виведений з дії (у своєму первинному вигляді) у 1892 році як унаслідок вказаних причин, так і внаслідок втрати під час використання великої кількості його примірників.

2. «Двозначний» ключ № 331. Був складений за системою біграмних шифрів Шилінга у 1861 році. Цей шифр відрізнявся тим, що не мав подвійних чисел як кодових позначень. До 1296 двобуквених поєднань було додано 1296 чисел: 7 однозначних, 75 двозначних, 591 тризначне і 633 чотиризначні. Використовувався цей ключ для шифролистування між Міністерством народної освіти з опікунами навчальних округів. Виведений з дії у 1883 році.

3. Ключ № 334. Був складений Р.Ф.Естом за системою Шилінга. Друкував цей шифр, як і інші шифри того часу, Ф.Годеніус. Ключ включав 1482 двобуквені поєднання. Кодовими позначеннями служили 1500 тризначних чисел, з яких 1000 – числа від 000 до 999, 500 – поєднання з двозначних чисел з однією з 10 латинських букв, узятих кожна по два рази «для переменной передачи валер» (словарних величин). Шифр цей призначався для листування поштою між консульствами в Туреччині: у Адріанополі, Бейруті, Біталії, Бухаресті, Варні, Віддіні, Бєлграді, Єрусалимі, Коржу, Мостарі, Прізряні, Рагузі тощо. Виведений з дії у 1872 році.

Це був перший російський біграмний ключ, в якому двобуквені поєднання (словарні величини) передавалися при наборі лише тризначними поєднаннями. Але зважаючи на перевищення кількості можливих буквених поєднань тодішнього російського алфавіту (1396) над кількістю тризначних чисел Р.Ф.Ест, якому була доручена робота над шифром, доповнив бракуючі числа поєднаннями з двох цифр і одної з десяти букв (французького) алфавіту. При складанні наступних біграмних шифрів для російських текстів вже обійшлися без таких поєднань цифр і букв, оскільки скоротили кількість двобуквених «валер» до 1000, виключивши деякі букви російського алфавіту. Таким чином були складені, наприклад, ключі № 347, 356, 375 тощо.

4. Ключ № 347. Введений в дію у 1865 році. Використовувався для листування МЗС з консульствами на Балканському півострові: у Бухаресті, Константино-

полі, Галаці, Яссах, Ізмаїлі, Тульчі, Бєлграді. У 1871 році був замінений ключом № 356 з причини використання більше чотирьох років. Проте у 1903 році цей шифр знов був введений в дію у консульствах Австро-Угорщині, а саме у Будапешті, Сараєві, Трієсті, Відні тощо.

5. Ключ № 356. Введений в дію у 1869 році у консульствах на Сході, де використовувався до 1888 року.

Відомо, що ключ № 356 був одним з тих шифрів, примірники яких були викрадені з Російської місії у Пекіні 19 серпня 1888 року. Внаслідок цього шифр був виведений з дії, але лише на деякий час. Не дивлячись на очевидність компрометації, на початку 1890-х років ключ № 356 знову ввели в дію, але вже в іншому регіоні. У 1894 році він був направлений у Амстердам, Гаагу, у 1896 році – у Берн, Женеву, у 1893 році – у Гаммерфест і Стокгольм. У 1898 році відбулася ще одна компрометація цього шифру: один його примірник був втрачений начальником Адріатичної ескадри. Ймовірно, саме ця подія, нарешті, змусила керівників шифрослужби остаточно вилучити ключ № 356 з вживання, як указувалося у відповідному висновку *«вследствие почти 1/4-векового всемирного использования»*. Відомо, що за весь період застосування його використовували у 124 пунктах.

6. Ключ № 361, подібний попередньому, був складений Нелідовим у 1876 році. Цей ключ містив біграмні поєднання з 28 букв спрощеного російського алфавіту, розділового і 31 окремого російського буквеного та знакового знаків. Всього, таким чином, його словник містив 992 величини, яким відповідали тризначні кодові позначення. Спочатку цей ключ був розісланий у консульства на Сході: до Александрії, Афін, Бухареста, Пекіна й інших, потім поширений на Австро-Угорщину, Персію, Балканський півострів, а, крім того, направлений у Тифліс і Одесу.

Під час турецької війни цей шифр відіслали в діючу армію (генерал Ігнатьєв, барон Фредерікс, великий князь Михайло Миколайович), військовому губернатору в Болгарії, адміралу Лесовському, контр-адміралу Крамеру. З 1882 року він використовувався у різних консульствах в Європі, а також на міжнародному конгресі. Не дивлячись на те, що примірник цього шифру був також вкрадений в Пекіні у 1888 році, його остаточно вивели з дії лише у 1903 році. Але й після цього тодішній начальник шифрувального відділу МЗС і член «Цифирного» комітету барон Таубе писав: «ключ № 361 може застосовуватися як тимчасовий у спеціальних випадках, окрім Далекого Сходу».

Цікаво, що російським криптологам того часу представлялося можливим використовувати шифри на лініях зв'язку в якомусь регіоні навіть у тих випадках, коли вони були скомпрометовані в іншому регіоні. Ймовірно, вирішальною обставиною тут була дальність відстані. Такий же ейфоричний настрій вселяв у криптографічні розуми і поняття часу: виведений з дії в якийсь час шифр, можливо навіть скомпрометований, міг знову вводитися в дію через значний проміжок часу.

Вочевидь, передбачалося, що за давністю часу він буде забутий супротивником.

Автором французьких двобуквених ключів № 362 і 363 також був Нелідов. Розроблені у 1876 році, вони були подібні до біграмних ключів № 359, 360 і 361. Про ці ключі барон Таубе також писав, що їх можна використовувати і на початку XX ст.

У той час були розроблені також шифри біклавної системи, автором яких був барон Дрізен. Ці шифри використовувалися дуже широко протягом XIX ст. в установах МЗС паралельно з біграмними шифрами Шилінга.

Біклавний шифр був шифром багатозначної заміни, що складалася з 26 різних простих замін з достатньо складним вибором заміни на кожен знак відкритого тексту, що визначався двома ключами. При цьому окремим знакам відкритого тексту (буквам і розділовим знакам) відповідали два знаки шифрованого тексту. Таким чином довжина шифрованого тексту не відповідала довжині відкритого тексту.

Основу шифру складали: портфель з 24 пересувними смужками – головна частина подвійного ключа, дві таблиці (шифрувальна і дешифрувальна) – друга частина подвійного ключа та календар набору і розбору.

Кожна смужка була випадковим набором з повтореннями 20 букв латинського (французького) алфавіту з 26 букв. Таким чином, кожна смужка могла містити 20 або менше латинських букв. Для зручності вони записувалися групами по чотири букви в кожній з пропусками. Кожна смужка мала свій номер, позначений цифрою або буквою.

Наприклад, смужка «*W*» мала вигляд:

q d u f до z i v d k i l s w до m p z l g

Шифруюча таблиця була квадратом 26х26, рядки якого були позначені 23-ма буквами латинського алфавіту (без букв *k, w, y*) і трьома знаками пунктуації, а стовпці якого були позначені всіма 26 буквами латинського алфавіту. Кожна колонка цієї таблиці заповнювалася випадковим чином 26 знаками, що складалися з 17 букв латинського алфавіту і 9 цифр: 1, 2, 3, 4, 5, 6, 7, 8, 9.

Процес шифрування здійснювався таким чином. Відкритий текст, призначенный для шифрування, записувався на транспарант, де кожний рядок містив 24 клітинки. Текст писався по 4 знаки з пропусками в одну клітку. Таким чином, в кожному рядку транспаранту записувалося по 20 знаків, форма запису відповідала формі шифрованої смужки. Якщо текст закінчився не в кінці рядка, то додавалося слово «кінець» і ще які-небудь довільні знаки. Кожен транспарант містив 8 горизонтальних рядків.

Таким чином довге повідомлення могло бути записане на декількох транспарантах. При записі шифрованого тексту на транспарант рекомендувалося спочатку виконати всі можливі скорочення тексту, що не міняли сенсу повідомлення. Далі проводилася заміна трьох букв і деяких розділових знаків на знаки, що входили

у проміжний текст, а саме: буква «k» замінювалася на «qq», буква «w» замінювалася на «vv», буква «y» замінювалася на «ii», знак «;» замінювався на «.,» тощо.

Після запису повідомлення на транспарант проводилося шифрування.

З 24 смужок у певному порядку вибиралися 8 смужок згідно з добовим ключем. Маркантом цього ключа була дата зашифрування, яка ставилася на початку повідомлення. Перша смужка підставлялася до першого рядка повідомлення, наприклад, отримуємо наступний текст і набір знаків на смужці:

zes- miss ions -se- serv

W

qduf kziv akil swkm pzeq

Знаки тексту з буквами смужки утворювали вертикальні біграми, які визначали входи шифрувальної таблиці (координати шифрованого тексту). Наприклад, перша вертикальна пара «zq» визначала знак шифротекста «j», що знаходився у «z» рядку і «q» стовпці шифрувальної таблиці, тобто знак «z» зашифровувався як знак «j». Так шифрувалися перші 20 знаків. Наступні 20 знаків шифрувалися за допомогою наступної смужки, яка визначалася добовим ключем тощо. Якщо шифрований текст перевищував 20 x 8 = 160 знаків, то процедура шифрування повторювалася, починаючи з першої смужки (у нашому прикладі «W»).

Розшифрування повідомлення проводилося у зворотному порядку, а відкрите повідомлення відновлювалося однозначно за наявності, зазвичай, у кореспондента відповідних ключів. Таким чином, криптостійкість даного шифру трималася на невідомому супротивнику заповненні смужок, що визначали вибір послідовності 26 замін, і добовому ключі.

Хоча це число і достатньо велике, проте криптостійкість даної системи шифру жодною мірою не могла триматися на цьому добовому ключі, оскільки вона допускала послідовне випробування смужок шифру одну за іншою. Спочатку при дешифруванні (при відомій шифрувальній таблиці і відомих смужках) випробувалися одна за одною смужки (24 варіанти). Критерієм правильності випробування першої смужки була поява відкритого (читаного) тексту. Далі випробувалася друга смужка з числа тих, що залишилися тощо. Всього виходило T = (24 + 23 + ... + 17) = 164 елементарні випробування (е.в.). За одне е.в. приймалося випробування одного варіанту смужки. Якщо текст шифрувався не з початку, а десь з середини, то число варіантів випробування збільшувалося не істотно: T = 164 + 10 = 174 (е.в.).

Зміст смужок, як мовилося вище, був основним ключем. Він діяв значно довше, ніж добовий ключ, але, проте, його теж досить часто міняли (смужки мінялися зазвичай двічі в рік).

Багато кореспондентів мали різні набори цих ключів, чим забезпечувалася конфіденційність листування та створювалася певна гарантія від компрометації шифру.

Перешифрувальні таблиці, що визначали 26 простих замін, були другою частиною ключа. Даний шифр для свого часу можна вважати достатньо стійким при збереженні в таємниці основного ключа (вмісту смужок) і добового ключа.

Головна слабкість цього шифру полягала в порівняно короткому періоді Т цього шифру (Т=160 букв) і відсутності разового ключа. Можливо в ті часи за добу шифрувалося не більш за одне повідомлення (у мирних умовах) від конкретного кореспондента, тому не було необхідності у введенні ще додаткових разових ключів. Самі повідомлення також не були достатньо довгими, тому глибинних перекриттів шифру тут не очікувалося. Не випадково тому шифри цього оригінального типу використовувалися разом з біграмними шифрами впродовж майже сорока років.

Відомі такі біклавні шифри:

1. Російсько-французький ключ № 305. Був винайдений у 1853 році Дрізеном і ним же надрукований. Календарі були введені в дію у 1858 році. Призначався виключно для листування місій в Константинополі з МЗС. У 1860 році Дрізеном було запропоновано включити в цей шифр таблиці для зашифрування російського тексту, а не тільки французького, як це було спочатку. Ця пропозиція була прийнята *«Цифирным»* комітетом на засіданні 24 березня 1860 року, протокол якого підписали тодішні члени цього комітету: таємний радник Толстой, таємний радник Гильфердінг, таємний радник Вестман і дійсний статський радник барон Дрізен. Тепер шифр складався з двох набірних і розбірних таблиць для французького та російського набору. Проте в тому ж році шифр був виведений з дії.

2. Французький ключ № 306. Був винайдений Дрізеном і введений в дію у 1856 році. Призначався цей шифр для стосунків з МЗС місії в Турині (Флоренції). У 1865 році був замінений біклавним ключем № 342, оскільки використовувався вже більше 6 років. У 1869 році *«ввиду устарелой системы»* був знищений.

3. У 1856 році були введені в дію аналогічні попередньому і також складені Дрізеном ключі: № 307 – для місії у Афінах, № 308 – для місії у Стокгольмі, № 309 – для місії у Римі, № 310 – для місії у Неаполі і № 311 – для місії у Мадриді.

4. У тому ж році був введений в дію французький ключ № 313 для циркулярного зв'язку місій у Афінах, Берліні, Брюсселі, Константинополі, Копенгагені, Дрездені, Франкфурті, Гамбурзі, Ганновері, Лісабоні, Лондоні, Мадриді, Мюнхені, Неаполі, Парижі, Римі, Стокгольмі, Турині, Відні і дипломатичній канцелярії у Варшаві. Був спалений у 1867 році «вследствие устарелости системы».

5. У 1859 році були введені в дію складені Дрізеном російсько-французькі ключі: № 317 – для листування МЗС з Лондоном, № 318 – з Парижем, № 319 – з Віднем, № 320 – з Парижем.

6. У тому ж році був складений французький ключ № 322 для листування князя Горчакова з імператором. Проте цей ключ не був своєчасно введений у дію і згодом, у 1877 році, отримав інший номер (364). Ним користувалися під час російсько-ту-

рецької війни для листування між головною квартирою Південної армії і МЗС.

7. Російський шифр № 322. Був складений за системою Дрізена і введений в дію у 1862 році для листування МЗС з Віднем і Константинополем. У 1876 році примірники цього шифру були відіслані до Тегерана і Токіо, а також великому князю – Головнокомандувачу діючою Армією в російсько-турецькій війні, і генералу Ігнатьеву.

8. Французький шифр № 339. Був складений Дрізеном і введений в дію у 1864 році для 28 місій у Європі і Америці. Використовувався в мережі загального зв'язку. Окрім кореспондентів МЗС примірники цього шифру мали в своєму розпорядженні Похідна канцелярія і Імператорська головна квартира. Був виведений з дії в кінці 1890-х років *«вследствие устарелости системы»*.

9. Французькі шифри №№ 340-345. Були складені для телеграфу у 1865 році також Дрізеном. Призначалися шифри для стосунків у мережі загального зв'язку, в яку входили МЗС Росії, а також посольства в Берліні, Відні, Константинополі, Лондоні, Парижі, Флоренції. Проте незабаром ці ключі були замінені на старіші ключі тієї ж системи № 305 і № 306.

10. Французький шифр № 348. Був складений за системою Дрізена і введений в дію у 1870 році для місій у Європі, а з 1871 по 1882 роки використовувався також на азіатських лініях зв'язку. Крім того, примірники цього ключа були у міністра закордонних справ князя Михайла Горчакова, в Імператорській головній квартирі, Похідній канцелярії, азіатському департаменті МЗС, у діючій армії у генерала Ігнатьева і барона Фредерікса. На європейських лініях зв'язку цей ключ був виведений з дії лише у 1891 році.

11. Французькі шифри №№ 350-355. Діяли паралельно з попереднім ключем на європейських лініях зв'язку. Введені ці ключі в дію були у 1869 році, а виведені з дії лише у 1891 році.

12. Французький ключ № 357. Був складений за системою Дрізена для телеграфу і введений в дію у 1871 році для листування МЗС з місією у Вашингтоні. Був спалений у Вашингтоні у 1884 році.

13. Французький шифр № 364. Був складений за системою Дрізена і введений в дію у 1877 році для листування з начальником канцелярії при діючій Південній Армії. У 1878 році був відправлений до посольства у Константинополі та діючу армію барону Фредеріксу. Не використовувався з 1888 року.

Як бачимо, біклавні шифри застосовувалися тривалий час дуже успішно та вважалися російськими криптологами достатньо надійними. Вони були виведені з дії не через криптографічні вади, а за іншими причинами. Так, у своєму огляді шифрів XIX ст. Таубе писав у 1901 році: *«Система биклавная не применима в настоящее время ввиду смешанной передачи буквами и цифрами, не допускаемой телеграфными конвенциями»*. Відомо, що деяка незначна кількість шифрів біклавного типу застосовувалася для зашифрування таємної поштової

кореспонденції і на початку XX ст.

Продовжували активно використовуватися у XIX ст. також коди і кодові таблиці. Коди були різних типів, вони поступово видозмінювалися і удосконалювалися як в експлуатаційному, так і в криптографічному відношенні. До кінця XIX – початку XX ст. з'явилися коди обсягом 10 тисяч словникових величин і більше. До 1917 року найбільше розповсюдження мали коди саме такого обсягу.

Більшість кодів Росії кінця XIX – початку XX ст. були алфавітними, тобто букви, склади, слова, словосполучення словника коду розташовувалися в порядку алфавіту, а відповідні ним кодові позначення являли собою природні числові послідовності. Ця обставина у величезному ступені полегшила дешифрування, оскільки місце кожного кодового позначення визначалося місцем слова у словнику відповідної мови еквівалентного обсягу. Всі ці міркування, природно, давали можливість досвідченим криптологам супротивника відновлювати код і дешифровувати повідомлення. Застосовувалися і неалфавітні коди, коди пропорційні і непропорційні. Залежно від виду кодових позначень розрізнялися цифрові, буквені і буквено-цифрові коди. Останні два види кодів перетворювалися у цифрові, коли повідомлення передавалися по телеграфу.

З кінця XIX ст. у Європі з'явилися теоретичні праці, в яких описувалися методи дешифрування алфавітних і неалфавітних кодів. З того часу повсюдно почали використовуватися коди з перешифруванням. Перешифрування були різними, від дуже наївних, за суттю своєю чисто маскувальних, до дуже складних. Останні застосовувалися на найбільш важливих каналах зв'язку.

Коди і кодові таблиці інтенсивно використовували: МЗС, військове відомство, МВС, Міністерство фінансів і деякі інші цивільні відомства. Коди і кодові таблиці обсягом до 1000-1200 словарних величин було прийнято називати *«словарными ключами»* і, залежно від словника конкретного коду, називати французькими, російськими, німецькими.

Відомі російські словарні ключі XIX ст., які розробули все той же барон Дрізен і інший співробітник «*цифирного*» відділення МЗС М.Сухотін:

1. Ключ № 299 на 600 словарних величин. Був введений в дію у квітні 1854 року, вилучений з дії у 1901 році. Винайшов цей шифр Дрізен. Призначався він для зв'язку командувачів частинами Дунайської Армії під час Кримської кампанії. У 1891 році цим шифром були забезпечені Бухара, Кашгар, Кульджа, Сеул, Пекін, Токіо, Іркутськ, Омськ, Ташкент, Хабаровськ, Ургa, Чугучак, Владивосток.

2. Ключ № 300 на 600 словарних величин. Склав також барон Дрізен. Був введений в дію у 1855 році, вилучений з дії відразу після закінчення Кримської війни у січні 1857 році. Призначався він для головнокомандувача Південною Армією та військових і морських сил у Криму князя Горчакова. У 1860 році цей ключ був надісланий до Вашингтона. Не використовувався з 1871 року.

3. Ключ № 317 на 1000 словарних величин. Був призначений для таємного листування по телеграфу та введений в дію у 1859 році. Цим кодом був забезпечений генерал Ігнатьев, направлений до Китаю, для його листування з МЗС і з місією у Вашингтоні з 25 лютого 1859 року по 11 лютого 1861 року, а також для стосунків місій у Пекіні з Вашингтоном і азіатським департаментом МЗС. Використовувався до 1871 року.

4. Ключ № 326 на 1000 словникових величин. Був введений в дію у 1861 році для листування МЗС з місіями у Пекіні, Урзі, Хакодаті. Не використовувався з 1880 року.

5. Ключ № 330 на 1000 словникових величин. Був введений в дію у 1861 році для листування Морського міністерства з начальником ескадри у Середземному морі. Не використовувався з 1888 року.

6. Ключ № 333 на 300 словарних величин. Був введений в дію у 1862 році «*для сношений Варшавского военного генерал-губернатора с шестью военными начальниками в Царстве Польском*». У 1863 році цей ключ був перероблений та надрукований у Варшаві під тим же номером і названий *«Шифр Царства Польского. Новый шифр»*. У свою чергу сам ключ № 333 був перероблений із старого ключа № 151.

7. Ключ № 336 на 920 словарних величин. Зовні він був паперовими таблицями, наклеєними на коленкор. Виготовлявся ключ на вимогу Морського міністерства «для сношений Министерства морского в случае открытых военных действий». Був введений в дію у 1863 році. У 1871 році був надісланий до Вашингтона, Токіо, Пекіна, Нагасакі; у 1886 році – до Афін, Фучжоу, Ханькоу, Сеула, Нью-Йорка. Цей ключ був також у військових губернаторів у Владивостоку і Хабаровську. У 1888 році перший примірник ключа був вкрадений у Пекіні, у 1891 році – у Вашингтоні. У зв'язку з компрометацією коду в тому же році він був виведений з дії.

8. Ключ № 337. Так само, як і попередній, був введений в дію у 1863 році. Спочатку служив для листування намісника на Кавказі з місіями в Константинополі і Тегерані, потім поширений на консульство в Персії. Був виведений з дії у 1895 році.

9. Ключ № 338 на 900 словникових величин. Був виданий у 1864 році. Використовувався для листування азіатського департаменту МЗС з генерал-губернаторами в Оренбургу, Східному і Західному Сибіру, Туркестані. Не використовувався з кінця XIX ст.

10. Ключ № 346 на 600 словникових величин. Був введений в дію у 1865 році для листування Міністерства фінансів з державними митницями, Міністерством шляхів сполучення, Державним контролем. Був виведений з дії у 1867 році унаслідок втрати одного примірника.

11. Ключ № 349. Був введений в дію у 1868 році на лініях зв'язку Міністерства фінансів для телеграфного шифролистування. Був вилучений із дії у 1879 році унаслідок втрати двох примірників. У 1901 році знов введений в дію для стосун-

ків Міністерства фінансів з митницями. Крім того, цей шифр був введений в дію у 1900 році в Міністерстві державного майна, у 1902 році – у Порт-Артурі, Харбіні, Мукдені. У 1904 році він був надісланий у Маньчжурську армію та діючу армію.

12. Ключ № 368 на 650 словникових величин. Був введений в дію у 1879 році для стосунків Міністерства фінансів з митницями. Цей ключ також належав до загального типу малих кодів (словникових ключів).

Як писав у той час начальник секретної експедиції МЗС Ф.Годеніус, у 1862 році було визнано необхідним забезпечити російські консульства у Туреччині російським біграмним шифром. Хоча застосування особливостей російського алфавіту являло собою значні труднощі, експедиція їх подолала та складений нею російський біграмний шифр № 334 (у кількості 12 примірників) був розісланий у консульства. В той же час до цих же консульств були відправлені нові пересувні смужки для російського біклавного шифру № 332 у кількості 90 примірників.

Услід за цим експедиції була доручена величезна праця, а саме виготовлення винайденого дісним статським радником Р.Гамбургером шифру. Після *«неусыпных семимесячных трудов»* зазначений шифр був виготовлений та за наказом керівництва розісланий у 1863 році у головні місії.

Відомо, що в цей же час Р.Гамбургером був складений шифр, який отримав назву «*Chiffre polilexique»*, на 900 словарних величин. В ньому кодовими позначеннями були тризначні числа, що повторювалися 26 разів кожне залежно від букв спеціальних смужок, які вибиралися в особливих календарях. Цей шифр був введений в дію у квітні 1862 року та використовувався до 1897 року у листуванні МЗС з посольствами в Європі.

У той же час експедиція виготовила винайдений дійсним статським радником Румом так званий «економічний» шифр. Хоча було видано 30 примірників, цей шифр не був визнаний зручним до застосування.

У 1864 році перша «цифирная» експедиція забезпечила всі місії новим біклавним шифром № 339 для загального зв'язку замість № 312, який знаходився у використанні вже тривалий час. Всього було виготовлено 12 його примірників. Азіатський департамент отримав для використання 4 примірники російського словникового шифру № 338 для кореспонденції з генерал-губернаторами в Оренбургу та Західній частині Східного Сибіру.

У 1865 році були виготовлені та розіслані нові партикулярні біклавні шифри з календарями №№ 340, 341, 342, 343, 344 і 345, новий російський біграмний шифр № 347. Крім того, на вимогу Міністерства фінансів туди було вислано 30 примірників знов виготовленого російського словникового шифру № 340.

Отже, можна зрозуміти, що «*цифирная*» експедиція працювала активно та напружено. Проте успіх справи залежав від організації діяльності служби в ціло-

му, зокрема від правильного ведення таємного діловодства, дотримання правил користування шифрами, умов їх зберігання. Щодо цих питань положення справ залишало бажати кращого.

Так, наприклад, у 1866 році «*цифирная*» експедиція МЗС займалася перевіркою всіх шифрів, що знаходилися в деяких країнах, та всіх книг, в яких велися записи про стан виготовлених і розісланих експедицією шифрів. При цьому було виявлено, що, з одного боку, деякі місії мали у себе шифри у величезній кількості, з яких багато вже не використовувалися. З іншого боку, деякі вже закриті місії не повернули шифрів, що знаходилися в них. Внаслідок цього були надані необхідні розпорядження та прийняті відповідні заходи щодо виправлення існуючого становища.

Наприкінці XIX ст. шифрувальна служба в МЗС була організована таким чином. При канцелярії міністра функціонував шифрувальний департамент з двома відділеннями. У одному відділенні шифрувалися свої російські повідомлення МЗС закордонним послам і консулам та розбиралися отримувані від них повідомлення. На чолі цього відділення довгі роки стояв барон Таубе.

У другому відділенні розбиралися копії з шифротелеграм, отриманих з ЧК Петербургу та інших міст Російської імперії (Москви, Варшави, Києва, Одеси тощо), де перебували іноземні консули. Штат цього відділення складався з 10-12 осіб на чолі з М.К.Долматовим.

Разом із тим, зростання революційного руху, постійно зростаючий обсяг перехопленого конспіративного листування революціонерів, важливість її дешифрування для прискорення їх розшуку та арешту – усе це змусило створити криптослужбу при самому Департаменті поліції (далі – ДП). 1 січня 1898 року в його структурі розпочав свою діяльність Особливий Відділ, де був зосереджений весь політичний розшук і переслідування революціонерів. Його спеціальне відділення цілеспрямовано стало займатися вивченням перехоплених шифрованих листів революційного підпілля.

Слід зазначити, що вже наприкінці XIX ст. у Росії були розпочаті спроби щодо створення апаратів для механічного шифрування телеграфних повідомлень. Так, у 1879 році головний механік Петербурзького телеграфного округу Іван Дерев'янкін запропонував оригінальний прилад із шифрування телеграм, який він назвав «Криптограф». Цей пристрій нагадував відомий шифратор епохи відродження – диск Альберті. Прилад являв собою два диски, один з яких був рухомим, однак ні прилад, ні будь-яка інформація про нього не збереглися.

Цікавою особистістю того часу, яка працювала у різних російських спецслужбах і займалася криптологією, був Володимир Іванович Крівош. Він народився у 1865 році в Словакії, яка входила до складу Австро-Угорській монархії. Після закінчення гімназії він володів французькою, німецькою, угорською, італійською, чеською, словацькою та хорватською мовами. Не будучи за походженням дворянином, йому вдалося вступити у Віденську Орієнтальну (Східну) Академію, однак через рік у 1886

році він був з неї виключений за неуспішність. Тем не менше завдяки своїм лінгвістичним здібностям у період навчання в академії Крівош вивчив додатково ще англійську, сербську, турецьку, арабську та новогрецьку мови. Того ж року він виїхав до Росії та став слухачем факультету східних мов Санкт-Петербурзького університету.

Одночасно Крівош вів активну громадянську, журналістську та літературну діяльність у різних слов'янських та словацьких суспільствах Санкт-Петербургу. У 1888 році він одержав російське громадянство. З причини свого захоплення вищезазначеною діяльністю та небажанням "протирати штани" в університеті Крівош у 1889 році його "кинув", в результаті чого вищої освіти не отримав.

У 1891 році він почав працювати на Петербурзькому поштамті, а у 1892 році був призначений перекладачем Санкт-Петербурзької поштової цензури, тобто почав займатися перлюстрацією. Однак спокійна праця на одному місці Крівоша не влаштовувала. З 1901 року він почав читати лекції зі стенографії у Санкт-Петербурзькому Технологічному інституті (до 1914 року). З 1904 року - за сумісництвом - цензор у Санкт-Петербурзькому комітеті іноземної цензури (до 1915 року) та перекладач при Секретному відділенні ДП (до 1906 року). З 1906 року - завідувач стенографічним бюро Державної Думи (до 1907 року) та Державної Ради. З 1907 року - керівник Секретного бюро Морського генерального штабу та Генерального штабу Військового міністерства (до 1911 року).

На початку 1900-х років Крівош проявив у сфері перлюстрації свої творчі здібності. Він зробив два винаходи, якими співробітники ЧК користувалися на протязі десятиліть. Перший полягав у новому способі розкриття листів за допомогою спеціального апарату на зразок електрочайника. Тепер цензор у лівій руці тримав конверт над струменем пари, а у правій - тонку голку, якою обережно відгортав клапани поштового конверту.

Другим винаходом Крівош раціоналізував техніку виготовлення складу для підроблених печаток, які наносилися на дипломатичну пошту: замість срібної амальгами використовувалась мідна, яка була зручніша та дешевша. За ці винаходи у 1908 році він отримав орден Святого Володимира IV ступеня та зайняв посаду молодшого цензора Санкт-Петербурзької цензури іноземних газет і журналів.

За спогадами самого Крівоша, завдяки знанню ним багатьох мов його залучали також до дешифрувальної роботи ЧК МЗС. У 1904 році під час Російсько-японської війни він був посланий до Парижа для вивчення іноземного досвіду з питань перлюстрації та розкриття дипломатичних кодів. Французи ввели його у «свята святих» своєї секретної служби – «Сюрте» (Surete generale). Там він проробив близько десяти днів, поки не був розкритий четвертий варіант японського коду.

Крім того, Крівошу вдалося докладно ознайомиться з роботою паризького ЧК, який, як виявилося, працював аналогічно петербурзькому. Він розташовувався в приватному будинку під вивіскою якогось землемірного інституту. Один із

службовців ЧК розбирався в питаннях лісівництва та землевпорядження і завжди давав кваліфіковану довідку приватним особам, що цікавилися цими питаннями.

Майже всі коди французи добували агентурним шляхом. Так, вони активно використовували для отримання криптоматеріалів (включаючи порвані чернетки таємних телеграм, що відправлялися в зашифрованому вигляді з цих посольств) підкуплених службовців іноземних посольств. Мали вони і деякі російські коди, що від Крівоша і не приховували.

За спогадами Крівоша, усі працівники криптослужби Франції (включаючи технічний персонал: секретарів, друкарок, посильних тощо) повинні були бути зацікавленими у своїй роботі та боятися її втратити. У таємній частині досить часто працювали дружини, сестри службовців. Таким чином, цілі родини споювалися одною ідеєю збереження довірених їм таємниць. Від цього істотно залежав їх сімейний матеріальний добробут.

Крівош став першим російським криптологом, що докладно познайомився з роботою дешифрувальної служби Франції того часу. Отримані ним відомості були використані російськими співробітниками ЧК у своїй практичній діяльності.

Разом з тим, з 1910 року російська контррозвідка стала підозрювати Крівоша у шпіонській діяльності. Крім того, у той же час його колеги по службі перлюстрації запідозрили Крівоша у фінінсовій неохайності та присвоєнні казенних грошей. В результаті у 1911 році він був звільнений із Санкт-Петербурзької цензури іноземних газет і журналів, а також Секретного бюро Морського генерального штабу та Генерального штабу Військового міністерства. Як далі склалася судьба Володимира Івановича Крівоша, буде описано у частині 4.

3.6. Криптологія початку XX ст.

Наприкінці XIX ст. у Росії вже добре розуміли слабкості застосування кодів у чистому вигляді, без ускладнень, особливо слабкості алфавітних кодів. Тому виникла насущна необхідність у введенні ускладнень для збільшення стійкості кодів.

В інструкціях до шифрів МЗС і Військового міністерства Росії неодноразово рекомендувалося застосовувати різні способи збільшення стійкості. До цих способів відносили: і своєчасну зміну ключів і кодів, і застосування одночасно декількох кодів у тих місцях, де була така можливість, і застосування різного роду прийомів типу використання різних варіантів кодових позначень, і, нарешті, застосування різних способів і систем перешифрувань.

Паралельне застосування декількох кодів вимагало великих витрат на складання і видання великої їх кількості і тому широкого розповсюдження не отримало. У Росії, як у багатьох інших країнах, застосовувалися різні види перешифрувань кодів: за допомогою колонної заміни, гамування та перестановок. Зупинимся на найбільш типових видах перешифрувань.

Всі перешифрувальні ключі (системи) мали свій порядковий номер і кожному привласнювалося найменування за буквами грецького алфавіту: Альфа, Бета, Гамма, Дельта, Лямбда тощо. Кожне поєднання кодів із перешифруванням перешифрувальним ключем також отримувало своє найменування. Наприклад, поєднання «Російського консульського ключа № 447» (коду) з перешифруванням перешифрувальним ключем № 448 «Лямбда» називалося «Ангарою».

Для одних кодів перешифрування було обов'язковим, для інших – у випадках передачі особливо таємного повідомлення. Розробники шифрів розуміли, що коди легко компрометуються (втрачається їх стійкість), якщо зміст зашифрованого за їх допомогою повідомлення стає дослівно відомим супротивнику. Тому у випадках, якщо з МЗС в яке-небудь посольство, консульство або назад передавався якийсь текст, що відомий або ставав відомим, то цей текст необхідно було передавати, в обов'язковому порядку, використовуючи поєднання спеціальних кодів і перешифрувань.

Так, наприклад, у 1916 році для цієї мети використовувалися «Французький загальний малий дипломатичний ключ № 431» і «Англійський малий дипломатичний ключ № 407» з обов'язковим перешифруванням.

Невід'ємною частиною шифрів стали гасла (у сучасній термінології – ключі, паролі), змінні в ті або інші моменти часу відповідно до наявних правил. Гаслом був більш менш короткий цифровий або буквений ряд. Ключі були декількох видів. Одні з них носили назву «загальних», ними забезпечувалися закордонні установи певного регіону. Решта всіх ключів називалася «спеціальними». Одні з них призначалися для зв'язку лише вузького кола кореспондентів або навіть для одного посольства з центром (індивідуальні ключі).

При зашифруванні стандартні словосполучення, включаючи цілі фрази, замінювалися умовними словами – «постійними», що робилося для скорочення довжини повідомлення, і «змінними» – для додаткового забезпечення таємності.

Розглянемо деякі типові варіанти таких шифрів:

1. Пересувний умовно-словарний ключ № 437.

Перша згадка про нього в документах відноситься до 1910 року. У «Керівництві» до цього шифру сказано, що він був призначений для шифрування приведених у таємних повідомленнях виразів загального характеру та посилань, незалежно від набору будь-яким

таємним ключем (або поєднанням ключів) відкритого тексту шифрованого повідомлення.

Шифр цей складався з 4-х частин. Перша частина була безпосередньо кодом (словниковим ключем), цифровим, тризначним, обсягом 1000 словникових величин. Друга частина – перешифрувальна – була набором «перешифрувальних груп». На кожну добу була своя перешифрувальна група, що містила тризначне число (додатковий до коду ключ). Під первинним шифрованим текстом, отриманим при зашифруванні за кодом, підписувалася ця тризначна перешифрувальна група, та з верхніх цифр віднімалися нижні за модулем 10. Таким чином, перешифрувальна група була не чим іншим, як короткою періодичною гамою з періодом 3.

Третю частину шифру складала таблиця з 1000 пересувних умовних виразів (слів), в якій кожен вираз відповідав тризначному числу. Таким чином, отриманий після перешифрування набір тризначних чисел замінювався на набір умовних виразів. Кожним умовним виразом було якесь латинське слово (або ім'я власне, таке, що траплялося в літературі). Умовні латинські вирази розташовувалися у таблиці в алфавітному порядку, тризначні числа – у зростаючому арифметичному порядку, тобто третю частину шифру можна було назвати зворотним алфавітним кодуванням. Слово «пересувний» означало, що ця частина повинна була з часом мінятися, і, таким чином, вона служила таємним ключем шифру.

Четверту частину шифру складали 25 таблиць цифрових замін, які мали назву *«Секунда»*. У кожній таблиці були 20 замін, тобто всього було 20 х 25 = 500 простих замін. Вони були призначені для зашифрування чисел у повідомленні (дат, посилань на номер попереднього або даного повідомлення тощо). Таким чином, ці числа шифрувалися не за кодом, а за допомогою замін «Секунда». Для цього вказані числа відкритого повідомлення представлялися у вигляді 5-значних груп із приписуванням зліва бракуючого до повної п'ятірки кількості нулів. Далі на початку шифроповідомлення вказувався умовний номер обраної таблиці заміни, наприклад, відповідний першій таблиці, і далі проводилося шифрування кожної цифри набору 5-значних груп за своєю порядковою заміною. Перша цифра – першою заміною (стовпцем), друга – другою тощо. Якщо кількість цифр перевищувала 20, то наступні цифри після 20 шифрувалися за другою таблицею тощо.

Таким чином, ключ № 437 був шифром, який можна назвати «код + гама + зворотний код + набір простих замін для шифрування чисел».

Методи дешифрування були засновані на використанні цифрової структури гами перешифрування, на її короткій періодичності та можливості проводити арифметичні операції (складання, віднімання) з цифровими знаками шифротексту.

Застосування у цьому ключі зворотної операції кодування практично зводило нанівець можливості застосування вказаних методів дешифрування, принаймні, до тих пір, поки не вдавалося накопичити достатньо великий обсяг шифромате-

ріалу, щоб з достатньо великою надійністю можна було б зняти зворотний (алфавітний) код.

Що стосується застосування четвертої частини шифру – особливого зашифрування дат і посилань, то її доцільність можна якоюсь мірою пояснити бажанням відійти від кодування стандартів у повідомленні, які, як відомо, служать необхідною допомогою для дешифрування коду, особливо в найбільш важкий момент початку цієї роботи. Це пояснення можна підтвердити і тією обставиною, що у «Керівництві» рекомендувалося стандартні вирази, що входили в повідомлення, не шифрувати кодом, а замінювати на постійні умовні вирази (на відміну від «пересувних», таких, що брали участь в третій частині шифрування) і ставити їх на початку шифроповідомлення, відокремлюючи від його тексту двома структурними 5-значними групами – групою дня.

При передачі повідомлення по радіотелеграфу, де потрібно, щоб весь текст був представлений у вигляді набору 5-значних цифрових груп, рекомендувалося не застосовувати третьої частини шифру – зворотного кодування цифрових груп пересувними умовними виразами. Мабуть, передбачалося, і небезпідставно, що і без цього ускладнення шифр виходив достатньо стійким.

2. Перешифрувальний ключ № 448 «Лямбда».

Він призначався для перешифрування первинного цифрового щифротексту, отриманого при шифруванні повідомлення за допомогою якого-небудь цифрового коду. Був шифром колонної заміни з періодом Т = 10 000 сумарних шифрів, при цьому всі підстановки шифру (розміру 10х10) набиралися випадково. Всі вони були надруковані та зброшуровані у дві книги по 667 сторінок кожна. На всіх сторінках було по 15 вертикальних стовпців, кожним стовпцем був зайвий ряд підстановки. Всі вони були пронумеровані цифрами від 1 до 10 000. Крім того, були пронумеровані всі стовпці на кожній сторінці від 1 до 30 (внутрішня нумерація).

Верхній рядок підстановки мінявся та служив одним з ключів. У якості цього рядка брався один із стовпців книги. Його порядковий номер указувався *«Цифирным»* відділенням на певний період і, як правило, мінявся двічі в місяць.

Шифрувальник, приступаючи до роботи, вибирав початковий стовпець, який називався *«исходным столбцом»*. Його номер він поміщав у криптограму, заздалегідь зашифрувавши за допомогою *«особых указательных групп»*, про які докладніше буде сказано нижче. Далі він шифрував первинний шифротекст, послідовно застосовуючи до кожного знаку тексту свою заміну. Після зашифрування заміною з номером 10 000, шифрувальник переходив до стовпця з номером 1 (за циклом).

Для більшої зручності користування такою складною системою шифру використовувався прилад «Скала». Цей дерев'яний прилад містив вертикальну целулоїдну ламу з 10-ма порожніми клітками, розмір яких збігався з довжиною шифрувальних стовпців у книзі. Шифрувальник вписував в клітки лами цифри, відповідні вказа-

ному ключу (номеру стовпця), і прикладав прилад послідовно до шифрувальних стовпців. Кожного разу виходила підстановка для шифрування.

Номер початкового стовпця шифрували особливо. Для цього шифрувальник 3 рази підряд виписував номер початкового стовпця (3 х 4 = 12 цифр) і додавав двічі записаний номер останнього використовуваного стовпця (з тією метою, щоб допомогти розшифрувати текст при яких-небудь збоях або помилках). В результаті виходив *«указательный ряд»* з 20 цифр. Наприклад: 2563 2563 2563 4812 4812. Далі брався стовпець, вказаний як ключ *«Цифирным»* відділенням (стовпець, виписаний на ламі), і стовпець, що стояв поряд з ним (10 + 10 = 20 цифрам). Ця послідовність, яка називалася *«календарным рядом»*, підписувалася під вказівним рядком і проводилося віднімання за модулем 10. Отриманий рядок вставлявся у криптограму в умовному місці.

Як бачимо, дана система перешифрування була значно складніше гаслового гамування короткою періодичною гамою і, вочевидь, криптографічно більш стійкою.

Шифром «Лямбда» були забезпечені *«Центральные и все штатные заграничные установления МИД, а равно чиновники МИД при наместнике Е [го] И [мператорского] В [еличества] на Кавказе и начальнике Закаспийской области и чиновники по дипломатической части при Приамурском, Туркестанском и Иркутском генерал-губернаторах»*. На час війни цим шифром забезпечувалася також дипломатична канцелярія при штабі Верховного Головнокомандувача.

Під час Першої світової війни організацією шифрозв'язку в МЗС займався «*Цифирный*» комітет. У 1915 році в нього входили Нератов, Арцимович, Базілі, Таубе, Феттерлайн, Колемін, Чекмарьов, Шилінг, фон дер Фліт. Члени цього комітету були в курсі всіх питань, пов'язаних з організацією шифрозв'язку в Росії. Зокрема, члени комітету мали інформацію про всі шифри, що використовувалися на лініях зв'язку, про діючі системи ключів тощо.

Війна показала, що Росія не змогла передбачати небезпеку затягування зі своєчасним введенням нових спеціальних шифрів і кодів на військовий період по лінії МЗС. Вже до кінця 1914 року стало зрозуміло, що діючі коди не забезпечували в достатній мірі таємницю шифрованої кореспонденції і разом з тим не дозволяли прискорити самий процес шифрування. Міністерством було запропоновано терміново виготовити для постачання своїх установ:

- особливі словники у 10 тисяч знаків, набірних і розбірних: дипломатичний російський, дипломатичний французький, два східні й консульський;
- словникові набірні і розбірні таблиці з особливими вертикальними шифрами;
- особливі ключі для перешифрування.

Проте через 2 роки, восени 1917 року, в доповіді, представленій керівництвом шифрувального відділу Тимчасовому уряду, констатувалося, що виконання цієї запланованої на початку 1915 року програми провалилося і довелося як тим-

часові заходи вводити слабші шифри – «тризначні словники».

5 жовтня 1917 року керівник шифрувального відділення МЗС Колемін подав підготовлену ним разом з його помічником Чекмарьовим доповідну записку на ім'я міністра закордонних справ Сазонова. У ній Колемін дав конкретні пропозиції щодо організації корпорації працівників криптослужби, діяльність якої була б обумовлена відповідними гарантіями як економічної, так і моральної властивості, і, що не менш важливо, корпорації, вільної від протекціонізму та інших вад.

Він писав: «Відділення [шифрувальне] тепер функціонує. Але я не бачу можливості, щоб воно виявилося згодом життєздатним без проведення в життя указаних мною принципів, які, на моє глибоке переконання, можуть бути змінені частково, але не по суті». Інакше справа йде «до неминучого банкрутства, наслідки якого можуть бути для нас незліченними».

Необхідність перебудови діяльності криптослужби загалом розуміли і керівники міністерства. Але питання намагалися вирішити лише формально, хоча і був підготовлений проект, створений поспішно, в якому була зроблена спроба скопіювати подібну німецьку спеціальну службу. У цих умовах і з'явився документ Колеміна.

Діяльність Колеміна мала активну підтримку серед службовців шифрувального відділення МЗС. 8 жовтня 1917 року відбулися чергові загальні збори службовців шифрувального відділення, порядок денний якого, записаний у протокол, свідчив: «1) вибори двох делегатів у міжвідомчу нараду для обговорення проекту Ю.О.Колеміна про організацію шифрувальної служби, 2) вибори п'яти осіб в комісію з організації шифрувальної служби, 3) обмін думками і поточні справи».

Збори ухвалили виразити подяку від імені всіх службовців шифрувального відділення Колеміну і Чекмарьову за їх працю з поліпшення діяльності відділення та умов служби. 19 жовтня 1917 року кожний з чиновників шифрувального відділення підписав текст присяги, що склав Колемін для криптологів. Приведемо її текст у перекладі на українську мову:

«Я, що нижче підписався, приступаючи до виконання моїх обов'язків, обіцяю, що буду завжди свято й непорушно дотримувати перед сторонніми особами мовчання про всі матеріали, за допомогою яких я буду виконувати покладене на мене ведення таємного листування Міністерства закордонних справ. Обіцяю, що буду свято й непорушно зберігати в таємниці від сторонніх осіб усі відомості, що будуть проходити через мої руки і перед очима моїми при веденні цього таємного листування. Обіцяю, що буду завжди обережно, обдумано й завбачливо обходитися з довіреними мені таємними матеріалами, обіцяю, що буду завжди обережно, обдумано й завбачливо відноситися до тих умов, при яких я можу з товаришами по службі у відділенні говорити про наявні у нас професійні відомості, щоб усіма силами моїми сприяти непорушності та непроникності цих таємниць, що склада-

ють власність не мою, а Міністерства, що довіряє їх мені, відаючого при допомозі їх, через мене, інтересами моєї Батьківщини. Обіцянки ці підкріплюю шляхетним і чесним моїм словом».

Однак повернемся до шифрувальної роботи, яка проводилася не тільки у МЗС. Шифри ДП, жандармерії та цивільних відомств істотно поступалися шифрам МЗС за своїми криптографічними якостями. Так, наприклад, «таємним телеграфним ключем шефа жандармів» 1907 року був набір із 30 простих замін, де буквам відкритого тексту відповідали 2 цифри шифротексту, номер ключа – простої заміни – проставлявся у відкритому вигляді на початку повідомлення.

При цьому адресат, підпис і всі числа не зашифровувалися та вставлялися в повідомлення у відкритому вигляді, відділяючись від шифропозначень з двох боків (або з одного боку – в кінці або на початку повідомлення) знаками «тире».

Збереглася навіть інструкція до цього жандармського шифру:

«22 28 37 53 32 65 34 49 39 14 66 18 41 24 67 13 61 26 20 35 30 17 46 36 19 38 42 15 27 31 33 40 21 57 68 50 56 29 64 48 63 47 62 16 54 11 45 23 44 25 52 43 58 10 55 60 59 51 12

↑ а б в г д е е ж з и к л м н о п р с т у ф х ц ч ш щ ъ ы ю я

[буква «е» фігурує двічі (вона ж відповідає за «э»), а весь числовий ряд виписувався в один рівномірний рядок – авт.]

1. Склавши депешу, необхідно насамперед у тексті підкреслити саме ті слова, що, укладаючи секрет депеші, повинні бути зашифровані. Потім після кожної 12-ої букви тексту, що шифрується, проводиться вертикальний штрих.

2. Шифруючий рухом абетки ставить стрілку проти бажаного нумера, під яким зашифровує депешу до передачі телеграфом. Нумер цей складається з двох цифр і пишеться на початку кожних 12 букв тексту, що шифрується.

3. Депеша набирається так. Для складання слів беруться букви, а до передачі телеграфом пишуться цифри, що знаходяться під ними, так, що кожні дві цифри виражають одну букву.

4. При шифруванні перших 12 букв стрілка пересувається проти іншого будь-якого нумера (тільки не сусіднього), що прописується та під яким продовжується шифрування наступної групи 12-ти букв. Потім знову пересувають стрілку довільно (уникаючи втім повернення в одній і тій же депеші до ужитого вже в ній №) і т.д. до кінця депеші.

5. Адреса депеші, підпис і цифри в тексті не зашифровуються, а пишуться просто, але при переході від шифру до цифр ставиться тире (–), потім кожне довільне число відокремлюється точкою або союзом, наприклад 6.15 і 350.

6. Розбір депеші. Одержавши таку з телеграфу, розділяють шифровані цифри комами на групи від лівої руки до правої попарно і за кожною 13-ою парою роблять вертикальний штрих. Потім рухом абетки ставлять стрілку проти першої

пари, тобто на №, під яким перші 12 букв депеші зашифровані, а з 2-ої пари підшукують цифри надалі до штриха, за цим ставлять стрілку на нумер, що випливає після штриха, підшукуючи під ним цифри до наступного штриха і т.д. Потім складають зміст депеші з букв, що під ними знаходяться.

7. Секрет цього ключа недоступний, тому що в ньому цифри складені в довільному порядку і до того ж мають ще 29 змін періодично обов'язкових.

8. У якому саме вигляді депеші пересилаються:

Саратов. Начальнику Губернського Жандармського Управління.

Прошу вислати 46382523471925 колишній 63275748273915465620611446241438174226271515563631361768206440534024671321153 3, замінений 61262021 новим – 8.57414213243162 – 1871.61152624. Граф Шувалов.

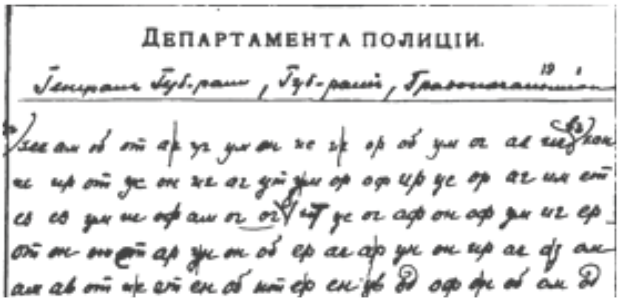
9. Розбір депеші: Саратов. Начальнику Губернського Жандармського Управління. Прошу вислати в штаб колишній секретний жандармський телеграфний ключ, замінений мною новим – 8 січня 1871 року. Граф Шувалов».

Інший жандармський шифр – це алфавітний цифровий код на 110 величин, одно- і двозначний, із зрушенням, тобто перші словникові величини (агітатор, адміністрація фабрики, заарештувати тощо) мають відповідно кодові позначення: 87, 88, 89 і далі за циклом.

Природно, дуже характерним було лексичне наповнення словників подібних шифрів: безлад, бити, буйство, поводитися зухвало, провина адміністрації фабрики, провина робочих, порушення справи про страйк, бійка, страйк, призвідник, козаки, спалити, соціалістичний тощо.

Серед безлічі шифрів Росії агентурні шифри завжди займали особливе положення. Відповідно до назви, вони призначалися для зв'язку розвідників і агентів з центром. На жаль, до теперішнього часу збереглися дуже мало відомостей про ці шифри. За інструкцією вони повинні були знищуватися, як тільки потреба в них пропадала, і ці правила неухильно дотримувалися. Проте нам вдалося знайти деякі матеріали, що дозволяють зупинитися докладніше на цьому питанні.

Однією з основних вимог, що пред'являються до агентурних шифрів, є забезпечення максимально можливої безпеки їх користувачеві. Тому вся документація до шифру (ключі, правила користування) повинна була володіти властивістю «приховуваної» або ж, в ідеалі,


ДЕПАРТАМЕНТА ПОЛИЦІИ.

властивістю *«безуликовости»*. Крім того, сам процес шифрування повинен був бути максимально простим і швидким, навіть якщо його доводилося здійснювати в найсприятливіших умовах. Ці вимоги часто входили в суперечність з вимогами високої криптографічної стійкості, і в цих умовах криптографи зазвичай вибирали якусь золоту середину. Розглянемо деякі види таких шифрів, що застосовувалися в Росії в епоху, що цікавить нас.

Простими агентурними шифрами в даний період були також шифри простої заміни, в яких використовувані прості заміни були достатньо структурними і тому легко запам'ятовувалися. Таким чином, це були найстаріші *«безуликовые»* шифри «на пам'ять», аналогічні системі «шифр Цезаря» з невеликими змінами: зсунення шифроалфавиту на 2, 3, 4 і більше знаків, заміна кожної букви алфавіту наступною за абеткою буквою, використання гасла. Зазвичай ключ визначався датою зашифрування повідомлення. Вочевидь, що ці шифри легко піддавалися дешифруванню вже у той час.

Складнішим шифром був шифр багатозначної заміни, що отримав назву «Стрибаючий шифр». Він з'явився наприкінці XIX ст. і криптографічний був декількома простими замінами, якими агент повинен був користуватися при шифруванні повідомлення, переходячи від однієї заміни до іншої через кожних 5-7 або 9 знаків тексту. Цей шифр був у дії нетривалий час, оскільки для агентів він був дуже складний, і вони віддавали перевагу «шифру Цезаря» з часто змінними ключами.

Як агентурні шифри використовувалися і книжкові шифри. Вибиралася певна книга, як шифропозначеня використовувалися номери сторінок, рядків, місць в рядках, де знаходилися шифровані букви. Цей тип шифру також можна віднести до безуликових шифрів, природно, при акуратному користуванні книгою. Книжкові шифри володіли незрівнянно більшою криптографічною стійкістю в порівнянні з шифрами заміни.

Проте в ЧК, де дешифровували такі шифри, було помічено, що шифрознаки, відповідні великим номерам рядків або місць в рядку, позначали, як правило, знаки відкритого тексту, що рідко зустрічаються. Це була зачіпка для розкриття повідомлення та пошуку відповідної книги. Річ у тому, що виявляється, як правило, кожен кореспондент вважає за краще знаходити в книзі букви, що стоять недалеко від початку рядка або початку сторінки. Інакше підрахунок займає багато часу, і при цьому збільшується вірогідність появи помилки. Букви, що рідко зустрічаються, з потреби можуть опинитися десь далеко від початку сторінки або рядка.

Проте, оскільки книга забезпечувала дешифрування всього повідомлення, завжди намагалися відшукати використовувану книгу. Не випадково при арешті та обшуку осіб, підозрюваних в шпигунстві, в першу чергу звертали увагу на їх бібліотеки. Відзначимо, що книжкові шифри широко застосовувалися в Росії в діяльності нелегальних партій і груп, про що докладніше ми розповімо

нижче.

На початку XX ст. набули великого поширення як агентурні шифри різні види шифрів перестановок – від старих шифрів – «Трафарету Кардано», винайденого математиком Жеромом Кардано в середині XVI ст., до нових шифрів – простих вертикальних перестановок, шахових і довільних лабіринтів, прямокутних і прямолінійних грат і подвійних перестановок.

До шифрів перестановок вносилися різні ускладнення, такі як спіральна виписка, виписка по діагоналях, виписка по гаслу і розподільникові, використання фігурних вертикальних перестановок (із стовпцями різної довжини).

Як агентурні в Росії часто використовувалися шифри вертикальної перестановки з ускладненнями. Текст повідомлення записувався в таблицю з колонками. Далі текст виписувався по колонках. Порядок вибору колонок визначався ключем, який користувачі знали на пам'ять. Цей ключ повинен був мінятися достатньо часто (наприклад, не рідше, ніж один раз в два місяці).

Головна перевага полягала в тому, що для їхнього використання не була потрібна наявність письмово оформлених ключів, які б могли скомпрометувати агента. Ключ (гасло) легко запам'ятовувався, а сам алгоритм шифрування був дуже простий та доступний для розуміння будь-якому агенту.

Приведемо невеликий спрощений приклад шифру вертикальної перестановки. Як таємний ключ використаємо слово «УКРАЇНА», букви якого нумеруються за абеткою (при цьому, якщо буква трапляється кілька разів, номери їй привласнюються послідовно):

У	К	Р	А	Ї	Н	А
6	4	7	1	3	5	2

Ця числова послідовність є так званим номерним рядком. Зашифруємо фразу: «Інформуйте про свій план». При шифруванні виписується номерний рядок, а під ним повідомлення по рядках:

6	4	7	1	3	5	2
І	Н	Ф	О	Р	М	У
Й	Т	Е	П	Р	О	С
В	І	Й	П	Л	А	Н

Шифрування робиться виписуванням тексту по стовпчиках за звичайним числовим порядком. У першому стовпчику стоять букви «ОПП», у другому – «УСН» тощо. В результаті одержимо такий шифротекст:

ОППУСНРРЛНТІМОАІЙВФЕЙ.

Розшифрування робилося в такий спосіб. У шифротексті утримується 21 буква,

а довжина гасла – 7, отже, при шифруванні використовувалася така конфігурація:

1	2	3	4	5	6	7

У цю конфігурацію вписувався номерний рядок ключа, після чого по стовпчиках вписувався шифротекст:

6	4	7	1	3	5	2
			О			У
			П			С
			П			Н

Таким чином отримувалося вихідне повідомлення.

Подальший розвиток цього способу шифрування полягав у використанні «подвійної вертикальної перестановки»: отриманий «первинний» шифротекст знову шифрувався за тим же правилом, але іншим ключем.

У 1916 році підпоручиком Ваві Попазовим був виготовлений шифрувальний пристрій, згодом названий «Прилад Ваві». Пристрій за своєю ідеєю був аналогічний «циліндру Джеферсона», але замість дисків на осі були 20 кілець, натягнутих на циліндр упритул один до одного, які могли обертатися на ньому. На ребрах (циліндричних поверхнях) кілець були нанесені змішані алфавіти (30 букв), а на першому та останньому кільцях були нанесені впорядковано цифри від 1 до 30. При заданому розташуванні кілець на циліндрі ключем шифру були: цифра, наприклад, 5 і буква, наприклад Б, а також «ключ кроку» – дві букви, наприклад, АГ. Повідомлення поділялося на частини по 17 букв.

Для зашифрування фрази «Інформуйте про план» на першому кільці відшукувалася ключова цифра 5. Напроти цієї цифри поворотом другого кільця ставилася ключова буква «Б». Потім напроти них поворотами інших кілець виставлялася фраза з 17 букв. Ця частина тексту замінялася на інші букви з рівнобіжних рядків ключа кроку «АГ». «А» – рядок, що відповідає букві «А» на другому кільці. Другий аналогічний рядок починався з букви Г другого кільця. Буква «І» замінялася буквою «Ж» 3-го кільця рядка «А», «Н» – буквою «Е» 4-го кільця рядка «Г» тощо. У такий спосіб шифровані букви бралися по черзі, то з рядка «А», то з рядка «Г».

5	Б	І	Н	Ф	О	Р	М	У	Й	Т	Е	П	Р	О	П	Л	А	Н	**5**
6	Я	И	А	Ж	С	Р	Е	П	У	У	Р	О	Б	А	З	У	Ф	Ш	**6**
7	Л	З	Б	Р	Л	О	Д	Ф	Ч	К	Б	Л	Т	Б	Х	Е	Д	Ч	**7**

8	А	Ж	Я	У	А	У	Л	О	Б	Г	Т	К	А	Ф	Н	Ч	Ш	И	**8**
9	Г	Т	Е	А	Ф	Ж	Ю	Д	Ш	Р	О	Ж	И	Т	Д	Х	Г	Ю	**9**

Шифротекст мав вигляд: ЖЕУФУЮОШГОКИФДЧГИ.

Помітимо, що принципова відмінність системи Попазова від шифру Джефферсона полягало в одиничності вибору шифротекста (за кроком ключа). Однак прилад не знайшов широкого застосування, тому що перевага у той час віддавалася ручним шифрам.

Дешифрувальники МЗС і ДП постійно обмінювалися розшифрованим дипломатичним листуванням. Під керівництвом Олександра Савинського, начальника ЧК МЗС з 1901 по 1910 рік, служба перехоплення та дешифрування одержала новий статус, тому її організація була значно покращена.

На початку XX ст. у країні працювало 8 перлюстраційних пунктів (далі - ПП): у Санкт-Петербурзі, Москві, Варшаві, Казані, Києві, Одесі, Харкові і Тифлісі. Пізніше такі пункти відкрилися у Вільно, Ризі, Томську і Нижньому Новгороді. Проте останні діяли короткий час. У Тифлісі ПП діяв з перервою з 1905 року по 1909 рік, оскільки був розгромлений під час революційних подій 1905 року.

Ці ПП створювалися на поштамтах при відділах цензури іноземних газет і журналів. Офіційно вони називалися «Секретними відділеннями». Загальне керівництво всією перлюстрацією в Росії покладалося на старшого цензора Санкт-Петербурзького поштамту, який був наділений правами помічника начальника Головного управління пошти й телеграфів і в той же час знаходився у підпорядкуванні міністра внутрішніх справ, від якого отримував розпорядження та санкції на проведення перлюстрації.

Більше 30 років, до звільнення у відставку в 1914 році, цю посаду виконував дійсний таємний радник Фомін, потім до жовтня 1917 року – таємний радник Мордарьєв. Перлюстровані матеріали з секретних відділень прямували до ДП для розшифрування, у разі потреби, а також подальшого використання. Старший цензор листувався з Департаментом поліції під псевдонімом. Листи, які надсилалися на ім'я *«его превосходительства С. В.Соколова»*, призначалися для відділу цензури.

Особливо ретельно підбиралися співробітники ЧК. Як правило, це були всебічно перевірені люди, які були *«безоговорочно преданные престолу»* і дали підписку про нерозголошування таємниці. Серед співробітників ПП у Санкт-Петербурзі окрім цензури були люди, що служили в інших установах: МЗС, банках, університеті тощо, тобто зберігалася традиція, заведена ще в середині XVIII ст.

Безпосередньо перлюстрацією по всій Росії до 1913 року займалося всього 45 осіб, яким допомагали працівники пошти, що відбирали листи. У місця, де ПП були відсутні, у разі потреби відряджалися чиновники з центрального пункту у Санкт-Петербурзі. Але частіше губернські жандармські управління привертали до цієї ро-

боти вузький круг місцевих поштових чиновників і проводили перлюстрацію самі.

Робота в ЧК була організована таким чином. Листи для розтину відбиралися за двома списками. Перший список Особливого відділу ДП містив прізвища осіб, листи яких підлягали перегляду, і адреси, послані по яких листи підлягали перлюстрації. Також повинні були перлюструватися листи, що висвітлювали діяльність з'їздів, партконференцій протиурядових організацій, що містили матеріали про їх підготовку, проведення, діяльність основного партійного складу та членів різних організацій. Другий список складався Міністерством внутрішніх справ і наказував перлюстрацію листів громадських і політичних діячів, редакторів газет і журналів, професорів, членів Державної ради і Державної думи, членів царської родини.

Не підлягали перлюстрації листи тільки самого міністра внутрішніх справ і царя. У матеріалах надзвичайної слідчої комісії Тимчасового уряду, що розбирала у 1917 році питання про перлюстрацію, є дані про те, що у 1910 році командир Окремого корпусу жандармів П.Курлов звернувся до старшого цензора з проханням, щоб адресовані йому листи не носили явних слідів розтину. Таке ж прохання висловлювалося поборником перлюстрації директором ДП С.П.Белецьким.

Найбільший потік листів йшов через Петербурзький поштамт. Щодня тут розкривалися від двох до трьох тисяч листів. Конверти розкривалися особливими кісточками або довгими голками, відпарювалися, відмочувалися у ваннах. Листи з «цікавими» відомостями відкладалися для зняття копій. Проглянуті листи запечатувалися, на зворотному боці в одному з куточків ставилася крапка (мушка) – умовний знак, що свідчив про те, що лист вже проглянутий і щоб він не був підданий перлюстрації повторно.

У ЧК листи затримували недовго – всього годину або дві. Лише у тих випадках, якщо їх текст був написаний симпатичним чорнилом або зашифрований, їх в оригіналі відправляли до ДП, де і піддавали відповідній обробці. Копії і виписки з листів робили у двох примірниках. Один примірник за списком ДП відправляли директору цього департаменту, а другий (і обидва примірники за списком Міністерства внутрішніх справ) йшов міністру внутрішніх справ. На місцях, в інших містах, перлюструвалася тільки та кореспонденція, яка йшла з цього міста або в місто, але не транзитна. Копії також робилися в двох примірниках, один з яких прямував до Петербургу на ім'я Соколова.

За даними ДП, щорічно по всій країні піддавалося перлюстрації приблизно 380 тисяч листів, з яких робилося від 8 до 10 тисяч виписок. За точнішими підрахунками, за 1907-1914 роки найбільша кількість виписок була у 1907 році (11 522), а потім зменшилася до 7935 у 1910 році. У 1911 році потік знову зріс до 8658, а у 1912 році – до 10 тисяч. Одночасно зросла кількість шифрованих листів і листів, написаних хімічним чорнилом.

Наскільки Микола II цікавився діяльністю ЧК видно з того, що він одного разу

власноручно відібрав три золоті і срібні з гербами і діамантами портсигари як царські подарунки та передав їх секретному чиновнику для вручення товаришам по службі у вигляді заохочення за корисну діяльність. В цьому відношенні імператор Микола II різко відрізнявся від свого отця імператора Олександра III, який, коли йому доповіли про «секретну експедицію» та пояснили її призначення, відповів: «Мені цього не потрібно» і протягом всього свого царювання відмовлявся читати виписки з перлюстрованих листів, хоча декілька міністрів робили спроби зацікавити його цим.

Крім того, шифрами у своєму листуванні користувалися і члени революційних організації. Тому в число завдань, які ставилися перед агентами ДП, входила здобич шифрів і ключів до них. Ось витяг з доповіді директору ДП, представленої начальником відділення «з охорони суспільної безпеки та порядку» в Петербурзі 12 листопада 1903 року:

«Все конспіративне листування партії есерів шифрується за допомогою відомого календаря Гатцука, що видається в Києві. Згаданий комітет користується адресою: Москва, Луб'янка, Варсоноф'євський пер., д. Рябушинських, Дмитру Ксенофонтовичу Тіхомірову.

Ключем до листування з Москвою і Харковом служить ім'я «Микола», з Єкатеринославом – «Огюст Кант», а закордонне листування шифрується по 8-ій книзі за серпень цього р. журналу «*Мир Божий*». 2-у відділенню при дешифруванні закордонного листування слід до проставленої на листі дати додати число 13, тобто різницю між старим і новим стилем, і отримане число вкаже ту сторінку у вказаній книзі, з якої почата шифровка».

Деякі відомості про шифри революціонерів, здобутих агентурним шляхом, дають журнали вхідних документів ДП за 1906-1908 роки і 1909-1915 роки. Так, наприклад, у 1906 році ДП було агентурним шляхом отримане та дешифроване шифролистування відомих меншовиків Степана Цосаря, Петра Кирноса, Леоніда Комендантова, М.Мандельштама. З Донського охоронного відділення сюди ж прислали ключ до шифролистування комітетів Російської соціал-демократичної революційної партії (більшовиків) (далі – РСДРП(б)) з Центральним комітетом (далі – ЦК), а також ключ до шифру більшовика М.Покровського.

У 1907 році ДП отримав і дешифрував листування більшовика Миколи Буреніна, отримав ключ до шифру ЦК РСДРП(б) для листування з Київською організацією, ключі до шифрів соціал-демократів Південного району.

У 1908 році за агентурним доносом був захоплений шифрований архів Московської військової організації РСДРП(б). Але в журналах є запис: «Розібрати неможливо». Проте відомо, що всього за 3 роки до цього при розгромі поліцією редакції газети «Нове життя» в числі інших документів був захоплений записник з шифрованими записами, які були дешифровані легко і швидко.

У тому ж 1908 році одеське охоронне відділення прислало в ДП ключ до шиф-

ру ЦК РСДРП(б), були також отримані шифри «Робоча азбука», «Бородіно», ключі до шифрів місцевих організацій РСДРП(б), наприклад, Полтавської тощо.

У 1909 році через агентуру ДП отримав ключ до шифру політичних заарештованих, що містилися в кутаїській в'язниці, отримав і дешифрував листування відомого більшовика-хіміка Олександра Чесського з Самари, з Харкова отримав ключ до шифру «Грунке», яким користувалися організації РСДРП. З Єкатеринославського охоронного відділення повідомили ключ до шифру РСДРП(б) (книжка «Смерть» № 70), з Іркутська поступив ключ до шифрів арештантів тюремного замку Іркутська. Начальник одеського охоронного відділення із зведенням агентурних відомостей по місту Керч повідомив ключ до шифру соціал-демократичного підпілля (збірка «Знання» № 17).

Московському охоронному відділенню вдалося отримати ключ до шифру ЦК РСДРП(б) для листування з Петербурзьким комітетом. Начальник губернського жандармського управління Самари повідомив ключ до шифру, що використовувався у листуванні саратовської та уральської соціал-демократичних організацій. У цьому ж році ДП отримав ключі до шифрів для листування кримської організації з ЦК РСДРП(б), ключі до шифрів пермської організації РСДРП, ключі до шифролистування Московського комітету з ЦК РСДРП(б).

У 1911 році ДП отримав і дешифрував листування Якова Свердлова та його дружини К.Новгородцевої, секретаря ЦК РСДРП(б) Н.Агаджанової, агента ЦК по центральному промисловому району В.Яковлевої і В.Куйбишева, Р.Пятакова. Були також отримані ключі до шифрів соціал-демократії Латиського краю, шифр для листування В.Леніна з В.Бажановим, Є.Розміровіч, копії шифрів Н.Крупської, Р.Петровського тощо.

У ДП, куди поступали матеріали з ЧК і іноді від міністра внутрішніх справ, йшла подальша «розробка» перлюстрації: реєстрація, розшифрування, прояв хімічних текстів, копіювання та розмноження копій. На підставі отриманих відомостей велося листування з губернськими жандармськими управліннями, з'ясовувалися особи тих, що писали, адреси, «приймалися заходи». Кожен перехоплений лист отримував свій номер. Прості і «хімічні» листи реєструвалися роздільно: перші просто отримували номер, до хімічних додавалася буква «Х».

Прізвища, що згадувалися в листах, заносилися до картотечного алфавіту. Іменні картки складалися на автора листа, одержувача, на всі імена і прізвища, що згадувалися в листі. Так детально розписувалися тільки листи революціонерів. Листи державних і суспільних діячів рідко проходили таку обробку. Вони, як правило, не реєструвалися, підшивалися в окремі справи у порядку хронології.

У ДП вся перлюстрація зосереджувалася в 5-му відділенні Особливого відділу ДП, де йшла розробка партійних матеріалів. Копії листів, що стосувалися діяльності партії есерів, анархістів, терористичних організацій, надходили у 2-е відділення Особливого відділу, яке займалося цими партіями. Матеріали щодо соціал-демократичних організацій надходили у 3-е відділення, а національних організацій – у 4-е. Тут же йшла подальша розробка цього листування, але вже розшукового характеру, на підставі відомостей, що отримувалися з листів. Це була кропітка і складна робота, що вимагала глибокого знання революційного підпілля.

Копії листів надсилалися у відповідні охоронні відділення та губернські жандармські управління для виявлення осіб, вживання заходів і встановлення спостереження. Ці, вже вторинні, копії разом з матеріалами з розробки та листування з відповідними губернськими жандармськими управліннями групувалися у справах по спостереженню за партіями, організаціями, окремими особами. Стосовно соціал-демократичного руху ці документи концентрувалися у справах по спостереженню за РСДРП.

Прочитанням тайнописного та шифрованого листування революційних партій і груп займалися спеціальні співробітники Особливого відділу ДП, зокрема, його 2-го і 5-го відділень. Серед них, в першу чергу, слід зазначити безумовно видатного криптографа Івана Олександровича Зибіна. Народився він у 1865 році та у серпні 1887 року як рядовий чиновник був прийнятий на службу в ДП. Маючи за плечима лише курс Санкт-Петербурзької класичної гімназії, завдяки своєму винятковому таланту та працьовитості, Зибін ще до моменту утворення Особливого Відділу став провідним криптологом ДП. У його документах (1902) він іменувався «старшим помічником діловода».

До кінця своєї служби в ДП (1916) Зибін офіційно почав іменуватися «діловодом». Працюючи в сфері дешифрування листування революційного підпілля, Зибін природно накопичив величезний теоретичний і практичний досвід. Крім того, буду-

чи від природи особою високообдарованою, маючи чудову пам'ять, Зибін був високоосвіченою людиною, що дозволяло йому отримувати відомості про шифри не чисто науково-аналітичним способом, але і за допомогою непрямих відомостей.

Перше літературне згадування про Зибіна ми знаходимо в записках про діяльність ЧК колишнього співробітника ДП Михайла Бакая: «Якщо траплялися листи з шифром, то вони розшифровувалися фахівцем цієї справи чиновником Департаменту поліції І.О.Зибіним, який у дешифруванні дійшов до віртуозності, і тільки в рідкісних випадках йому не вдавалося цього зробити. Зибін вважається єдиним свого роду фахівцем у цій сфері, і він навіть читає лекції про шифрування та дешифрування на курсах для офіцерів, що поступають в окремий корпус жандармів... Для Зибіна важливо вловити систему ключа, тоді для нього не важко підібрати відповідне значення для букв або цифр... Користуючись випадком, я звернувся до Зибіна з проханням ознайомити мене зі способом розбору шифрів і на це одержав вказівку, що лист із шифрами заздалегідь відомих ключів дешифрується дуже легко, при цьому він мені вказав на деякі ключі революційних організацій, отримані за допомогою провокаторів».

Інший великий жандарм, глава московського охоронного відділення генерал Заварзін у своїх закордонних мемуарах згадував про Зибіна ще більш красномовно: «Прості шифри він розбирав з першого погляду, зате більш складні приводили його в стан, подібний до афекту, що тривав, поки йому не вдавалося розшифрувати документ».

У 1903 році в ДП розробкою хімічних і шифрованих документів займалися 4 осіб. Один із працівників – Владіміров – займався розбором і перекладом хімічних листів, прокламацій тощо, написаних на єврейській мові. В.Зверєв, ротмістр Мец і Зибін вели журнали вхідних і вихідних документів, що доставлялися цензурою, поповнювали алфавіт осіб і адрес, які згадувалися у листуванні, проявляли та відтворювали документи, які підлягали відправленню за призначенням, вели листування з цензурою.

У ДП суворо охороняли криптологічні таємниці, прізвища співробітників відділення Зибіна не розголошувалися. Так, наприклад, у 1908 році з уфімського окружного суду тодішньому начальнику Особливого відділу ДП Є.К. Климовичу були направлені шифрована записка та ключ до шифру. У супровідному листі, підписаному судовим слідчим, висловлювалося прохання розшифрувати лист, повідомити, яка підпільна організація користується таким шифром, і дати можливість допитати як експерта співробітника ДП, який проводитиме цю роботу. Через тиждень до Уфи була направлена відповідь. У ній повідомлявся зміст записки, яку вдалося розшифрувати, давалася коротка характеристика шифру (достатньо поширеного), але ДП був категорично проти допиту фахівця-криптолога.

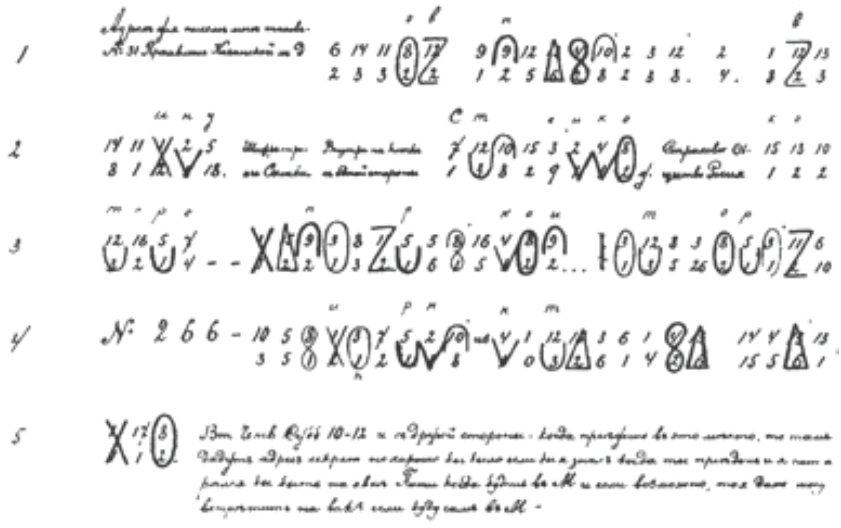
Аналогічний випадок був у 1915 році. Цього разу допитати криптолога побажав судовий слідчий з Вітебського повіту. За наказом директора ДП Брюн-де-Сент

Іполіта було направлено листа самому прокурору судової палати Петрограду з проханням *«одёрнуть»* провінційного слідчого. У листі вказувалося, що *«...разоблачение произведшего дешифровку лица является для Департамента полиции по особым соображениям весьма неудобным».*

Відділення Зибіна проводило і експертизу почерків. Так, наприклад, у вересні 1910 року *«старший помощник делопроизводителя, коллежский советник Зыбин и чиновник для письма ДП коллежский регистратор Жабчинский рассматривали фотоснимки воззвания под заголовком «РСДРП», начинавшееся словами: «Товарищи! Тяжелое и безотрадное время...» и подписанное: «Орловская группа РСДРП», а также протокол допроса ротмистром Шульцем крестьянина Ивана Федоровича Курбатова». Був проведений докладний аналіз почерку відозви та почерку Курбатова і даний дуже обережний висновок «про схожість букв».*

У своїй роботі Зибін і його помічники зовсім не були «сліпими» виконавцями керівних вказівок начальства. Вони постійно прагнули удосконалювати дешифрувальну службу ДП, неодноразово писали доповідні записки про стан її роботи, виходили з пропозиціями.

Вже у своїй доповідній записці від 22 травня 1903 року директору ДП Белецькому Зибін писав, що розробляти шифровані документи з кожним роком стає все важче і важче через ряд причин. По-перше, за останні два роки, тобто з 1901 по 1903 рік їх кількість стала «величезною», по-друге, порівняно легкі прийоми шифрування тексту, де ключем служило яке-небудь слово або вірш, поступово залишаються в минулому і «досвідченіші революційні діячі (група «Іскра» і ін.) користуються для



листування в даний час або подвійними ключами або сторінками маловідомих книг і брошур, обираючи для кожного окремого кореспондента окрему книгу і уникаючи повторення сторінок, що вкрай ускладнює роботу». Щоб зробити свої пошуки ключів успішнішими, криптологи ДП прагнули одержати декілька листів з одного пункту.

Умови роботи дешифрувальників також не сприяли успіху. Через тісноту приміщень і крайньої скупченості в них службовців хімічні тексти доводилося проявляти безпосередньо в кабінеті завідувача Особливим відділом ДП, а найбільш кропітку роботу з ними взагалі проводити вдома. Удома ж співробітники розбирали і всі шифровані листи.

Ще у 1901 році Зибін направив доповідь начальнику Особливого відділу ДП Л.Ратаєву, в якій указував на те, що різко почав зростати потік шифрованих листів, що отримувалися при обшуках і арештах. Разом з тим, всі ці листи, як правило, для дешифрування прямували в ДП, оскільки в середовищі чинів жандармського корпусу своїх фахівців з шифрів не було. Основи дешифрування викладалися тільки в Академії Генерального штабу. Стосовно жандармських офіцерів, для яких такі знання були також необхідні, то вони їх не отримували.

У зв'язку з цим Зибін пропонував свої послуги для занять з офіцерами штабу Окремого корпусу жандармів з метою ознайомити їх з технікою розбору найбільш споживаних у революційному підпіллі шифрів. Він вважав, що для отримання ними необхідних знань досить присвячувати цьому дві години в тиждень. Разом з ними могли б займатися офіцери найбільш важливих жандармських управлінь і охоронки. «І незабаром можна було б досягти того, щоб в кожному з найбільш важливих жандармських управлінь, а також в охоронних відділеннях були офіцери, «знайомі» з прийомами дешифрування», – писав Зибін.

Такі заняття Івану Олександровичу дозволено було проводити. Одночасно з цим він почав викладати основи дешифрування офіцерам Головного військового штабу.

Потребували фахівців із дешифрування й інші відомства. Так, у липні 1915 року проходив з'їзд керівників кабінетами науково-судової експертизи при прокурорах судових палат. На з'їзді увагу присутніх було звернено на те, що цим кабінетам нерідко доводиться мати справу з розшифруванням документів. Не маючи спеціальної літератури та відповідного керівництва, співробітникам кабінетів самим доводилося знаходити способи та прийоми розшифрування.

З'їзд ухвалив рішення про тимчасове відрядження чинів кабінетів до ДП, МЗС і Військового міністерства для ознайомлення з прийомами розшифрування, маючи на увазі, що в цих відомствах накопичений з даного питання вже великий досвід. Проте само Міністерство юстиції не поспішало виконувати рішення з'їзду. Лише через рік, у липні 1916 року, було направлено листа начальнику Особливого відділу ДП Є.К.Климовичу з проханням допустити співробітника московського кабінету Русецького на стажування в ДП і ознайомити його з найбільш поширеними

видами шифрів і прийомами їх розбору. Такий дозвіл був даний.

Звичайно, в боротьбі з революційним підпіллям без агентів було не обійтися, але володіючи технікою розкриття шифрів, можна одержати інформації набагато більше, ніж її давали кілька сотень агентів царської «охоронки». Саме Зибін ввів в практику чинів поліції, які проводили арешт або обшук революціонерів, звичай ретельно шукати серед книг, що були у них, саме ті, що могли бути цікавими для Зибіна-дешифрувальника.

Документальних підтверджень тому безліч, наприклад: *«3.01.1910. Начальнику Санкт-Петербургского губернского жандармского управления. Департамент полиции… препровождает при сём Вашему Превосходительству ключ к шифру и разбор шифрованной записки, отобранной по обыску у Якова Свердлова…»*

Ось уривок з його листа від 7 лютого 1910 року начальнику саратовського губернського жандармського управління: *«…отобранные по обыску у мещанина Николая Сергеевича Кузнецова записи зашифрованы 4, 15, 25, 29 и 35-й страницами какой-то неизвестной книги и разбору не поддаются по недостаточности материала. Прошу Ваше Высокоблагородие уведомить в самое непродолжительное время, не было ли обнаружено по обыску у названного Кузнецова, кроме означенных записей, какого-либо издания или легальной книги с пометками на отдельных страницах или загрязненной более других какой-либо страницей от частого, сравнительно с другими, употребления и, кроме того, не встретилось ли одно и то же издание у прочих лиц, принадлежащих к одной с Кузнецовым организации, т. к. подобное явление в большинстве случаев указывает, что таковое издание служит ключом для шифрованных сношений»*.

Улітку 1911 року Зибін прибув з Петербурга в Москву для роботи з одним з перехоплених революційних шифрованих листів. Встигнувши тільки привітатися з Заварзіним, він відразу попросив показати йому лист. Заварзін поступився столичному гостю своїм кабінетом, і Зибін із головою поринув у розбір депеші, зашифрованої дробовими числами. Коли Заварзін повернувся, щоб запросити гостя на обід, йому довелося двічі звертатися до Зибіна – той його просто не чув. За обіднім столом він продовжував дивувати присутніх. Доївши суп, Зибін відразу перевернув тарілку і спробував писати на ній. Але олівець на порцеляновій тарілці не було видно, тому він почав писати на манжетах, не звертаючи ні на кого уваги і забувши, де знаходиться. Раптом Зибін підхопився зі стільця і закричав: «*Тише едешь – дальше будешь!*» Після цього він знову сів, закінчив обід і пояснив Заварзіну, що чотириразове повторення в листі букви «Ш» дало йому ключ до квадратного шифру терористів. Вимовлена ним фраза й була потрібним ключем.

Зибіну надсилалися на експертизу і нові системи шифрів, які планували використовувати на внутрішніх лініях зв'язку. Ось один із зроблених ним висновків, датований 20 липня 1910 року:

«Предлагаемая система шифрования с помощью двух вращающихся концентрических кругов является мало удобной, во-первых, потому, что по ней подлежащий зашифрованию текст предварительно пишется длинными 40-буквенными группами в две строки каждая; последнее возможно лишь в тех случаях, когда весь текст депеши шифруется сплошь, без всяких пропусков; во-вторых, обязательное отделение каждого слова от следующего за ним знаком препинания, причем последний всякий раз обозначается парою цифр, излишне удорожает шифр и др.; в-третьих, сама система концентрических кругов излишне громоздка и не достигает цели в смысле сохранения секрета депеши, так как при любом наложении кругов и при всяких комбинациях для обозначения каждой буквы и каждого знака препинания имеется лишь два числа — четное и нечетное. Например, буква А всегда будет обозначаться числом 37 или 28; буква Б – 39 или 20 и т. п., вследствие чего круги эти являются совершенно излишними; значения букв удобнее можно расположить в виде таблицы как в Департаментском полицейском ключе, в котором, между прочим, для каждой буквы имеется от двух до четырех значений».

Незважаючи на численні сигнали «знизу», що виходили не тільки від рядових співробітників, але й від керівників середнього рівня, криптослужба ДП не піддавалася конструктивним змінам протягом багатьох років. Адже час був зовсім не простий, насувалися політичні зміни, і це добре розуміли і Зибін, і його колеги.

Головна проблема російської криптослужби того часу полягала не в поганій теоретичній та практичній підготовці кадрів і не у використанні застарілих прийомів шифрування, а з практичним застосуванням шифросистем, через що вся пророблена криптологами робота ставала марною. І якщо криптологія в Росії як наука перебувала на світовому рівні, то застосування її досягнень на практиці залишало бажати кращого.

3.7. Революційна криптологія

Починаючи з XIX століття, в Росії крім державних відомств шифрування активно використовували різні революційні підпільні організації, що протидіяли владі, такі як «Земля і воля», «Народна воля», «РСДРП», «БУНД» (єврейський робочий союз), есери, анархісти, нігілісти тощо. За характером свого використання шифри підпільників були подібні агентурним шифрам, тому до них застосовувалися ті ж вимоги: простота, бездоказовість, легка зміна ключів у кореспондентів мережі зв'язку тощо.

Необхідність застосування шифрів підпільними організаціями була викликана вимогами конспірації, тому що правоохоронні органи Російської імперії вели з підпільниками «запеклу» боротьбу. Видатний російський «дисидент» XIX століття Олександр Герцен у своєму листуванні використовував досить простий прийом. Букви переданого тексту замінялися на їхні числові позначення в старослов'янській абетці.

У той же час широко використовувалася жаргонна мова, заснована на підміні понять. Так, наприклад, слово «вірмени» означало «євреї», «греки» – «татари»,

«турки» – «шевці», «Грузія» – «Тула» тощо.

У 1860 році у Росії з'явилася революційна організація нігілістів (лат. *nihil* – ніщо), які не визнавали та заперечували традиції дворянського суспільства й кріпосництва та призивали до їхнього руйнування в ім'я радикальної перебудови суспільства. У 1880 році вони винайшли особистий шифр перестановки букв.

Їхній шифр був описаний у 78-му томі «Енциклопедії Брокгауза й Ефрона», який вийшов у Росії в 1903 році. Його суть була такою: букви, що входили до складу листа, залишалися ті ж, але записувалися в іншому порядку. Їх спочатку поміщали у клітини квадрата, а потім виписували з нього одну за одною, що визначало ключ до шифру. Далі процитуємо саму енциклопедію:

«Нігілісти для нумерації кліток квадрата (по Флейснеру) користувалися визначеним словом-секретом; букви секрету нумерувалися згідно з місцем, займаним ними в порядку алфавіту. Нумера ж наносилися як на лінію мови, так і на секретну лінію; числа секретної лінії в такому випадку позначали порядок рядків, а числа лінії мови порядок букв кожного рядка».

Це був шифр, що іменувався «подвійною перестановкою». Робилася квадратна таблиця за кількістю букв ключового слова. Слово-ключ записувалося зверху і збоку таблиці. Букви ключа й відповідні їм стовпчики та рядки нумерувалися за алфавітним порядком. З однакових букв та, що знаходилася праворуч, одержувала більш високий номер. Текст, що шифрувався, розміщався в таблиці відповідно до отриманої нумерації стовпчиків і рядків, а далі виписувався з неї горизонтальними рядками. У випадку, коли клітини залишалися незаповненими, у них вписувалися будь-які нейтральні букви.

Візьмемо такий таємний ключ (шкалу перестановки): 456321. Його можна було відобразити словом «МОСКВА», кожна буква якого мала порядковий номер згідно з місцем розташування у алфавіті. Відкритий текст, наприклад: «ІНФОРМУЙТЕ ПРО ПЛАНИ ТЕРОРИСТИЧНИХ АКТІВ» вписувався в квадрат розміром 6х6:

	1	**2**	**3**	**4**	**5**	**6**
1	І	Н	Ф	О	Р	М
2	У	Й	Т	Е	П	Р
3	О	П	Л	А	Н	И
4	Т	Е	Р	О	Р	И
5	С	Т	И	Ч	Н	И
6	Х	А	К	Т	І	В

Відповідно до ключа здійснювалася перестановка стовпців: перший стовпець ставився на 6-е місце, другий – на 5-е тощо. Одержимо:

	4	**5**	**6**	**3**	**2**	**1**

1	О	Р	М	Ф	Н	І
2	Е	П	Р	Т	Й	У
3	А	Н	И	Л	П	О
4	О	Р	И	Р	Е	Т
5	Ч	Н	И	И	Т	С
6	Т	І	В	К	А	Х

Потім за цим же правилом переставлялися рядки: перший – на 6-е місце, другий – на 5-е тощо.

	4	**5**	**6**	**3**	**2**	**1**
4	О	Р	И	Р	Е	Т
5	Ч	Н	И	И	Т	С
6	Т	І	В	К	А	Х
3	А	Н	И	Л	П	О
2	Е	П	Р	Т	Й	У
1	О	Р	М	Ф	Н	І

Шифротекст виписувався по рядках:

ОРИРЕТЧНИИТСТІВКАХАНИЛПОЕПРТЙУОРМФНІ.

У 1861 році з'явилася революційна організація «Земля і воля», яка спочатку використовувала квадратні шифри Полібія та числові ключі Гронсфельда. Деякі революціонери користувалися так званим «пі-шифром»: число π = 3,14 повинні були знати всі учасники мережі зв'язку. З цих трьох цифр утворювалася періодична послідовність з періодом «3» (гама шифру), що складалася з буквами таємного послання. Для цього букви переводилися в числа за алфавітом:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

В результаті слово «*УКРАИНА»* шифрується як «23122104101804»:

Текст	У	К	Р	А	И	Н	А
	20	11	17	01	09	14	01
Ключ	03	01	04	03	01	04	03
Шифротекст	23	12	21	04	10	18	04

Однак поступово з’явилася зовсім нова шифросистема, що одержала назву «гамбетівської» за іменем прем'єр-міністра Франції Леона Гамбети. Його внесок у криптологію полягав у відмові від застосування приладів шифрування та заміні їх простими алгебраїчними операціями. Букви тексту й гасла замінялися на чис-

ла (відповідно до порядку їхнього розташування в алфавіті), а потім складалися між собою, породжуючи шифротекст (додавання здійснювалося за модулем, рівним потужності алфавіту). Іменем Гамбети був також названий основний сучасний елемент шифрування – «гама» шифру.

Зручність нового способу криптології здавалася незаперечною. Зникала необхідність в складанні обширних буквених таблиць. Але конкретна реалізація ідеї Гамбети у революціонерів була своя, в чому ще належить не раз переконатися. Та і користувалися вони одночасно відразу двома варіантами шифрування.

В «гамбетівській» шифросистемі ключове слово, наприклад, «УЖГОРОД» містилося вертикально в лівий крайній стовпець таблички, а з боку виписувалися букви алфавіту, що випливали за кожною буквою ключа відповідно. Причому, при шифруванні використовувалася 30-буквена російська абетка, де буква «Й» стояла наприкінці алфавіту.

Після побудови таблиці зверху неї виписувався правильний алфавіт. Зашифрування тексту здійснювалася таким чином: букви його бралися з верхнього алфавіту, а букви шифротекста – з рядків таблиці по черзі.

А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ы**	**Э**	**Ю**	**Я**	**Й**
У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т
Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В	Г	Д	Е
Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н
Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й	А	Б	В	Г

В результаті слово «УКРАИНА» перетворюється у шифротекст «ЖРУОШЬД».

Ця система шифру стала основною протягом наступного десятиліття історії російського революційного підпілля. Але по суті цей шифр був шифром Віженера, винайдений ще в XVI столітті. Різниця полягала в тому, що з великої квадратної таблиці Віженера виписувалися один за одним тільки ті рядки, що відповідали буквам ключової фрази.

Але підпільники швидко зрозуміли, що користуватися громіздкою таблицею при шифруванні не дуже зручно. З метою конспірації її було потрібно складати тільки в момент роботи над криптограмами, а потім доводилося знищувати. Усе це привело до швидкої появи цифрового варіанта тієї ж системи, яка використовувала особистий цифровий варіант шифру Віженера. Шифрування здійснювалось таким чином: букви тексту і ключа замінялися відповідно номерами їхнього місця розташування в алфавіті та складалися між собою.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Э	Ю	Я	Й
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

При використанні ключового слова «УЖГОРОД» текст «УКРАИНА» перетворюється у шифротекст «38172015252706»:

Текст	У	К	Р	А	И	Н	А
	19	10	16	01	09	13	01
Ключ	У	Ж	Г	О	Р	О	Д
	19	07	04	14	16	14	05
Шифротекст	38	17	20	15	25	27	06

Саме за таким шифром у революційних колах остаточно закріпиться назва «гамбетівського» шифра.

Наприкінці літа 1879 року з'явилася революційна організація «Народна воля», яка також використовувала «гамбетівський» шифр. Але народники при шифруванні з усіх сум, більше 30, стали віднімати це ж саме число (30). Таким чином, замість 31 писали 1, замість 45 – 15, а замість 60 – 30 або 0.

При подібному шифруванні зовсім порушувалося правило – відповідність маленьких сум початковим буквам, а великих – кінцевим. При цьому зовсім відпадала необхідність складання громіздкої таблиці, і всі операції можна було проводити «у розумі». На десятиліття вперед «скорочений гамбетівський» шифр стане основним у практиці революціонерів Росії.

«Народна воля» застосовувала також і квадрат Полібія, що нерідко називали шифром «в'язнів». Цей шифр був зручний тим, що їм можна було легко перестукуватися через стінки тюремних камер. У ньому букви російського алфавіту по рядках вписувалися в прямокутник розміру 6х6, і буква замінялася на її координати в таблиці.

	1	**2**	**3**	**4**	**5**	**6**
1	А	Б	В	Г	Д	Е
2	Ж	З	И	І	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Ъ	Э	Ю	Я		

Наприклад, буква Б стояла в першому рядку на другому місці, тому вона передавалася при перестукуванні в такий спосіб: удар – довга пауза – два короткі удари. Ще до народовольців таким шифром активно користувався декабрист М.Бестужев, що знаходився в 1826 році в Алексеєвському равеліні Петропавловської фортеці. Народовольці використовували цей досвід.

Ще один із способів шифрування народників полягав у тому, що складалася табличка, розділена подовжніми і поперечними лініями на 9 або 10 клітин. У цих клітинах записувалася фраза (в кожній клітині по одній букві), що складала шифр. Кожний, як подовжній, так і поперечний рядок клітин позначався цифрою, так що кожна клітина, а, отже, і кожна буква, що знаходилася в ній, відповідала двом цифрам: подовжнього та поперечного рядка клітин. Однак ця система не одержала в майбутньому ніякого розвитку та залишилася «пам'ятником» шифрувальної думки революціонерів.

За короткий термін від періоду «ходіння в народ» до замаху на Олександра II народниками були реалізовані всі найважливіші системи шифрів революційного підпілля. Зокрема, вони творчо розвили ідею шифру Віженера, створивши його кілька оригінальних варіантів. А скорочений «гамбетівський» шифр став візитною карткою російського підпільника. Спочатку буквений запис криптограм поступово трансформувався в цифрову. Головною заслугою народовольців було удосконалення багатоалфавітного шифру Віженера та різних квадратних систем.

Наприкінці XIX століття в Росії з'явилися різні революційні соціал-демократичні кружки, зокрема, марксистська група «Звільнення праці», що продовжували широко використовувати квадратні та гамбетівські шифросистеми епохи народництва. Їхні шифри будувалися на коротких ключових гаслах, на яких було зручно будувати саме квадратні таблиці. Хоча до цього часу вони були вже порядком дискредитовані в очах старих народовольців.

За повідомленням 1895 року сумно відомого поліцейського агента, а в майбутньому – одного з керівників партії соціалістів-революціонерів (есерів) Евно Азефа можна довідатися про криптологію тодішніх марксистів: «Слово шифру «Великобританія». Абетка складена з перших чисел: 1 – А, 2 – Б, 3 – В і т.д. До кожної букви додається буква слова «Великобританія» і усі цифри, наприклад, слово «вода» пишеться так: В –3 (в) + 3 (в) = 6 (в одному рядку), О = цифра, що відповідає «О» + цифра для «Е» і т.д.». Наприкінці XIX століття цей шифр одержав назву «роздільного гамбетівського ключа».

Наприкінці 1901 року з'явилася партія соціалістів-революціонерів (есерів), що ввела у свою практику подвійний шифр з використанням цифрового ключа. Есери назвали його «вторинним злитим шифром», який фактично був ускладненим варіантом відомого вже «пі-шифра». З цифр ключа утворювалася гама шифру, що складалася з числовими позначеннями букв повідомлення. Для цього букви переводилися в числа таким чином:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ю	Я	-
27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	31	30	29	28	0

Роль «0» зводилася до поділу двозначних і однозначних цифр. При використанні ключа «3162» текст «УКРАИНА» перетворюється у шифротекст «11181729211533»:

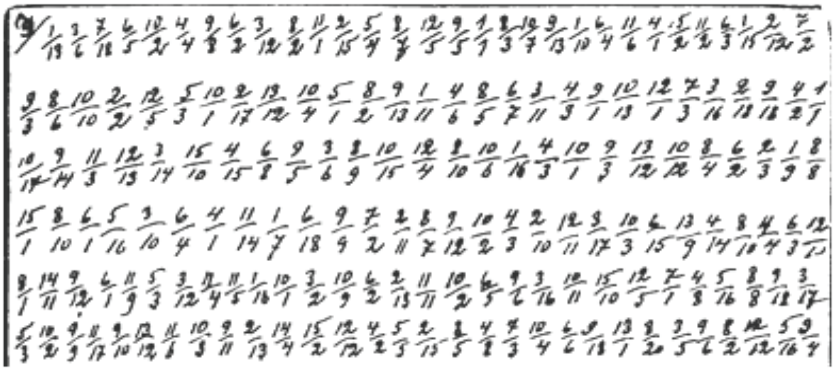
Текст	У	К	Р	А	И	Н	А
	8	17	11	27	19	14	27
Ключ	3	1	6	2	3	1	6
Шифротекст	11	18	17	29	21	15	33

Це був один із найбільш стійких видів серед усіх діючих криптосистем, що використовувалися революціонерами. Правда в даному випадку представлений його найпростіший варіант. У такий спосіб подвійні шифри міцно ввійшли в практику партії есерів.

Крім шифрів есери широко застосовували усілякі види кодів. Так, наприкінці 1906 року групою терористів був розроблений такий код. У телеграфній депеші завжди повинно було стояти слово «Приїжджайте». Слово «Занедужав» – означало ранкові години від 10 до 12; «Захворів» – вечірні від 5 до 10; «Степан», «Дядько» – Великий князь Микола Миколайович; «Іван», «Батько» – прем'єр-міністр Столипін. Таким чином, телеграма: «Приїжджайте, занедужав Іван» означала, що прем'єр-міністр приїжджає до царя на доповідь між 5 і 10 годинами вечора.

Одночасно в революційну практику розпочали входити також і інші шифросистеми. Починаючи з 1890-х років, з'явилися книжкові та віршовані шифри, що було викликано, у першу чергу, незадоволеністю підпільників стійкістю колишніх шифросистем.

Книжкові та віршовані шифри забезпечували достатню стійкість, але мали істотний недолік: кореспондентам мережі необхідно було завжди мати при собі книгу-ключ. Це нерідко було незручним, і, крім того, у разі «провалу» мережі зв'язку супротивник міг знайти ключову книгу, яка була у всіх кореспондентів.



Тому часто замість книги використовувалися слова, що легко запам'ятовувалися, або фрази, за якими відтворювалася гіпотетична сторінка книги.

У віршованому шифрі ключем був заздалегідь обумовлений вірш, наприклад: *«Птичка божия не знает*

Ни заботы, ни труда,
Хлопотливо не свивает
Долговечного гнезда».

Про процес шифрування соціал-демократ Катін-Ярцев писав так:

«Треба зашифрувати фразу: «Петро арештований». Перша буква першого рядка – «П», позначаємо 1/1, де чисельником буде рядок, знаменником – порядок букв у цьому рядку. Для «Е» ми можемо взяти, наприклад, тринадцяту букву першого рядка або дванадцяту третьої і т.д. Рекомендувалося вносити якомога більше розмаїтості, запозичаючи букву з різних місць ключа, щоб ускладнити для сторонніх фахівців розшифрування написаного. При шифровці в книгах ліворуч відраховувалася і відзначалася ледве помітною олівцевою крапкою буква, що вказує номер рядка в ключі, а праворуч – порядок букв у рядку. У конспіративному відношенні потрібен був менш загальновідомий вірш...».

Про використання книжкового шифру писав і учасник пітерського марксистського підпілля І.Михайлов:

«Розповсюджений між революціонерами шифр полягав у тому, що намічалася сторінка якої-небудь книги, по ній та або інша буква для потрібного слова записувалася двома цифрами, відділеними комою: перша цифра показувала рядок зверху або знизу, а друга – букву в рядку ліворуч праворуч або праворуч ліворуч, дивлячись по тому, як умовилися ті, що листуються. Іншого разу у книзі записувалися адреси розміткою букв у визначеному порядку».

Приведемо реальний історичний приклад віршованого шифру, що застосовувався революціонерами на початку XX століття. Ключем шифру був вірш Некрасова «Школьник»: *«Ну, пошёл же ради бога...»*. Вірш вписувався в квадрат розміром 10х10, а зайві букви рядка (що містить більше 10 букв) викидалися:

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	Н	У	П	О	Ш	Е	Л	Ж	Е	Р
2	Н	Е	Б	О	Е	Л	Ь	Н	И	К
3	Н	Е	В	Е	С	Е	Л	А	Я	Л
4	Э	Й	С	А	Д	И	С	Ь	К	О
5	Н	О	Г	И	Б	О	С	Ы	Г	Р
6	И	Е	Д	У	А	П	Р	И	К	Р

7	Н	Е	С	Т	Ы	Д	И	С	Ь	Ч
8	Э	Т	О	М	Н	О	Г	И	Х	Ъ
9	В	И	Ж	У	Я	У	К	О	Г	О
10	Т	А	К	У	Ч	И	Т	Ь	С	Я

Початок зашифрованого тексту «Сообщите…» могло мати різні варіанти написання: «3/5 1/4 5/6 2/3 1/5 7/7 7/4 7/2...», «5/7 5/6 8/6 5/5 1/5 5/4 9/9 6/2 ...» тощо. Чисельник давав номер рядка, а знаменник – номер стовпця. Через відсутність у таблиці букви «Щ» вона замінялася на «Ш» (що не заважало правильному розшифруванню).

Одна з помилок революціонерів полягала в частому використанні творів поетів-демократів, що були знайомі поліції. Це полегшувало дешифрування таємних посланнь, оскільки сама ідея шифрування була відома поліції. Захист забезпечував лише ключ – «таємний» вірш. Інша помилка, що полегшувала дешифрування, полягала в частому вживанні стандартних слів і виразів: «Повідомте...», «Направляю вам...», «явка», «адреса» тощо. Часте використання того самого ключа-вірша також полегшувало читання повідомлень поліцією, що ефективно використовувала ці помилки.

Іноді заздалегідь обумовлена фраза або початок деякого вірша використовувалися як вихідна гама шифру періодичного гамування (згаданий раніше гамбетівський шифр). Приведемо приклад:

«Небо голубое в море купалось, солнышко ласковое морю смеялось...»

Відповідно до заздалегідь обговореного правила підкреслювалися букви, що стояли на непарних місцях: 1, 3, 5, ..., 17.

Ці букви виписувалися: Н, Б, Л, С, Р, О, У, О, Е.

Потім ці букви переводилися в числа відповідно до їх положення в російському алфавіті. Виходило 17 чисел, що і були вихідною гамою шифру. Відкритий текст перекладався в числа аналогічно (за місцем букв в алфавіті). Вихідна гама періодично записувалася під перетвореним відкритим текстом, і шифрований текст виходив у результаті додавання букви (числа) відкритого тексту до відповідного знаку гами шифру. Неважко помітити, що даний шифр відтворював давно відомий шифр Віженера, описаний раніше. Цей шифр одержав широке поширення і виявився досить стійким при його грамотному використанні.

А ось один із шифрів анархістів, описаний ідеологом цього руху в Росії Петром Кропоткіним. Він спирався на 10 слів, що треба було запам'ятати, не записуючи:

«Пустынной Волги берег

Чернеют серых юрт рядами

Железный Финогеша Щебальский».

Кожна буква позначалася двома числами: номером за порядком слідування слова та букви в слові. Наприклад, буква «П» – 11, «У» – 12, «С» – 13 або 51, або 07

(10 слово, 7 буква). Букви, що часто траплялися (Е або А), позначалися по-різному: «Е» – 32, 34, 42, 72, 86, 02, «А» – 36, 74, 88, 04. Розшифрувати такий шифр було неможливо, тим більше, що писали суцільно, іноді ставлячи непарне число букв на початку листа і наприкінці і, ще заплутуючи розшифрування вставленими «пустими» парами: 26, 27, 28, 29, 20. Цей шифр був різновидом книжкового шифру, у якому замість ключа-книги використовувалися фрази (вірша), що легко запам'ятовувалися.

Кропоткін підкреслював, що «у нас є спеціальні шифри для кожного з провінційних гуртків». Таким чином, шифри були індивідуальними для кожного адресата. Однак одночасно він відзначав і надмірну трудомісткість шифрування: «Ми часто працювали ніч безперервно, списуючи аркуші кабалістичними знаками та дробовими числами».

Одним з варіантів шифру багатозначної заміни була побудова таблиця заміни за заздалегідь обумовленим словом, словосполученням або фразою. У разі використання ключового слова «*ПРЕКРАСНАЯ*» будувалася таблиця такого виду (стосовно до сучасного скороченого російського алфавіту): слово-гасло вписувалося у таблицю по вертикалі. Ці вертикалі позначаються числами від 1 до 0 (у слові 10 букв). Кожна буква порядково розверталася в послідовність букв російського алфавіту (циклічно). У результаті виходив прямокутник 10х10, що і був гіпотетичною сторінкою книги-ключа:

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**
1	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
2	Р	С	Т	У	Ф	Х	Ц	Ш	Ь	Э
3	Е	Ж	З	И	К	Л	М	Н	О	П
4	К	Л	М	Н	О	П	Р	С	Т	У
5	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Ь
6	А	Б	В	Г	Д	Е	Ж	З	И	К
7	С	Т	У	Ф	Х	Ц	Ш	Ь	Э	Ю
8	Н	О	П	Р	С	Т	У	Ф	Х	Ц
9	А	Б	В	Г	Д	Е	Ж	З	И	К
0	Я	А	Б	В	Г	Д	Е	Ж	З	И

Відповідно до цього квадрата робилася заміна букв відкритого тексту на їхні координати (перша цифра – номер рядка, друга – номер стовпця). Наприклад, буква П одержувала позначення: 11, 30, або 46 і т.д. Таким чином, слово «УКРАИНА» могло мати різні шифропозначення : «15, 35, 12, 61, 34, 38, 02» або «87, 90, 84, 91, 99, 44, 61» тощо. Цей шифр мав вже непогану криптостійкість.

Подальше ускладнення шифру багатозначної заміни було пов'язане із введенням пустушок. Наведемо приклад згідно з вищезазначеною таблицею. Заздалегідь домовлялися, що стовпці і рядки з номерами 2 і 9 були «порожніми», тобто викрес-

лювалися. Таким чином, з'явилася можливість вставляти в шифрований текст «порожні» комбінації, що містили зазначені цифри. 27, 95, 92, 29 тощо.

Наступне ускладнення полягало в одночасному використанні декількох квадратів, отриманих за різними ключами-гаслами. При шифруванні квадрати таблиці використовувалися циклічно один за іншим. Іноді перехід до наступного квадрата відзначався визначеними комбінаціями знаків, наприклад, триразовим повторенням однієї і тієї ж букви у відкритому тексті. Шифр став більш стійким, але менш зручним у застосуванні.

Можна відзначити «раціональний шифр» запропонований одним з лідерів організації «БУНД» Павлом Розенталем у його книзі «Шифрований лист», надрукованої в Женеві в 1904 році. Він вважав його досить стійким, але по суті цей шифр був шифром пропорційної заміни. Такі шифри вживалися раніше, і були відомі методи їхнього дешифрування.

Книга П.Розенталя була по суті теоретичним дослідженням у сфурі криптології. На конкретних прикладах автор найдокладніше продемонстрував, як можна розкрити ті або інші шифри, які вони мають вади і як їх можна уникнути. Усе це було дуже важливо на момент швидкого росту революційного руху, коли в його ряди вливалися все нові новобранці. Однак ця книга так і не змогла переломити негативні тенденції в шифролистуванні революціонерів більш пізнього часу.

Також у 1900 році в Женеві в друкарні «Союзу російських соціал-демократів» була опублікована брошура Володимира Акімова «Про шифри». Своєю книгою він також зробив вагомий внесок у розвиток шифрувальної справи російських революціонерів.

Наприкінці XIX століття з'явилася нова революційна партія – РСДРП, членом якої став майбутній «вождь пролетаріату» Володимир Ілліч Ульянов (Ленін). Його революційна група у період з 1895 по 1900 роки у своєму шифролистуванні використовувала тільки сторінкові книжкові ключі.

З кінця 1900 року вона розпочала впроваджувати віршовані шифри. Спосіб шифрування був завжди однаковий – чисельник шифродробу позначав потрібний рядок, а знаменник – номер потрібної букви цього рядка, рахуючи, звичайно, зліва направо.

Як приклад наведемо особистий шифр «ленінця» Миколи Баумана. Він вписував у 100-клітковий квадрат вірш невідомого поета таким чином:

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**-**	**12**
1	З	в	е	з	д	ы	у	с	ы	п		
2	В	ъ	с	у	м	р	а	к	е	н	е	ж
3	К	а	к	ъ	б	е	з	м	я	т	е	ж
4	Б	л	е	щ	е	т	ъ	и	х	ъ		

5	Т	у	ч	к	и	п	и					
6	Ф	л	о	т	о	м						
7	Д	а	н	а	д	о	с	ч				
8	Н	е	т	ъ	р	а	в	н	о	д	у	ш
9	Б	о	г	ъ	д	а	р	о	в			
10	В	ъ	м	е	с	я	ц	е	и			

Кожна літера при шифруванні замінялася дробом у загальноприйнятій системі. При цьому замість першого десятка цифр можна було брати другий або третій. Такі букви, як «Ж» і «Ш» не були присутні в основному ключовому квадраті, і був додатково введений ще 12-й стовпець, де вони за текстом вірша розміщалися.

Так, слово «УЖГОРОД» перетворюється у шифротекст:

5/2 2/12 9/3 6/3 8/5 9/2 1/5.

Важливий крок у розвитку віршованих ключів зробив Олександр Маліновський. Головна особливість його шифру полягала у великій кількості фіктивних дробів (пустишок) у самій криптограмі. Всі дроби зі знаменником більше 30 і чисельником більше 5 були пустишками. Це визначалося розмірами вірша «Думка людства», що послужив ключем до шифру.

При відсутності заздалегідь домовленого шифру революціонери використовували натяки, іносказання тощо. Так, у 1900 році соратник Леніна В.Ногін знаходився в Англії. Леніну було необхідно повідомити Ногіну прізвище петербурзького видавця книги (революційного змісту) К.Каутського.

Ленін так написав Ногіну: «Боюся довірити прізвище пошті – утім, передам Вам її в такий спосіб. Напишіть ім'я, по батькові (на російський лад) і прізвище Олексія і позначте всі 23 букви цифрами по їхньому порядку. Тоді прізвище… складеться з букв: 6-ої, 22-ої, 11-ої, 22-ої (разом же читайте наступну за алфавітом букву), 5-ої, 10-ої і 13-ої». Справжнє ім'я «Олексія», відоме обом кореспондентам, було «Юлий Осиповичъ Цедербаумъ». Пронумеруємо його по буквах:

Ю	л	и	й	О	с	и	п	о	в	и	ч
1	2	3	4	5	6	7	8	9	10	11	12
ъ	Ц	е	д	е	р	б	а	у	м	ъ	
13	14	15	16	17	18	19	20	21	22	23	

Тоді читання «шифрованого» повідомлення дає прізвище «Смирновъ». При шифруванні Ленін припустився помилки (пропустив букву Р = 18), однак вона була легко виявлена та усунута Ногіним.

Однак варто підкреслити, що підпільники допускали при використанні шифрів серйозні помилки, що приводили до дешифрування їхнього листування Департаментом поліції. Прикладами таких помилок були рідка зміна ключів, шиф-

рування тексту не цілком, а тільки найбільш «таємної» його частини тощо. Використовувалися і відверто слабкі шифри (типу простої заміни).

Редакція революційної газети «Іскра», стурбована провалами своїх агентів, у 13-му номері газети від 20 грудня 1901 року помістила статтю «Увазі революціонерів»:

«Додамо зі свого боку, що шифр – зброя, яка загострена з двох боків, тому що жандарми легко зуміють розкрити всякий шифр, якщо не бути при шифруванні особливо обережним. Безумовно, необхідно:

1) не відокремлювати слова від слова;

2) не повторювати часто однакових знаків, особливо знаків для найбільш уживаних букв;

3) писати шифр так, щоб не можна було довідатися системи шифру;

4) не вживати занадто відомих віршів і книг.

Без дотримання цих правил шифр просто неприпустимий».

Однак 4-ий пункт «інструкції» суперечив діючій тоді революційній практиці, тому що для шифрування використовувались твори відомих класиків російської поезії Пушкіна, Лермонтова, Крилова й Некрасова. Так, за весь період підпільної діяльності Надії Крупської на посаді секретаря різних партійних структур (1901-1905) для віршованих шифрів було використано понад 20 творів Пушкіна і стільки ж Лермонтова, 15 байок Крилова та 16 віршів Некрасова.

Особливого значення революціонерами надавалось правильному (без помилок) використанню шифрів. Так, у листі (грудень 1902 року) Ленін писав своєму брату: «Ваш лист отримано. Написаний він невідомим нам ключем, утім, ми розшифрували все, за винятком адреси. Не шифруйте інакше, як цілими фразами, інакше дуже легко розкрити ключ...». Тут мова йшла про те, що в таємних листах часто залишалися незашиф-

рованими «нетаємні» слова і фрази («клер»), які істотно полегшували дешифрування.

Аналогічне послання своєму кореспонденту в тому ж році направила Надія Крупська. Одержавши погано зашифрований лист, вона у відповідь обурювалася: «Насамперед дозвольте Вас насварити за недбалу шифровку. Не знаючи, що Ви умовилися про ключ з Євгенієм, я дивувалася, яким ключем Ви пишите, і, нарешті, розшифрувала Ваш лист без ключа в які-небудь 2 години. Це просто скандал. Не повторюйте тих самих знаків для однієї тієї ж букви, інакше шифровка нікуди не годиться».

Таким чином, помилки, що допускалися при шифруванні, часто зводили нанівець усі зусилля щодо захисту інформації. Тому ключі шифрів і правила їхнього користування часто змінювалися. Були введені так звані «одноразові ключі», що змінювалися з кожним новим шифруванням. Так, наприклад, ключовий вірш залишався тим же, але за простим правилом мінялася нумерація його рядків (починати з другого рядка, вважаючи його першим, тощо).

Іноді застосовувалася практика зміни ключа в процесі шифрування одного послання (за заздалегідь обговореною умовою). Зміна шифру практикувалася й у тих випадках, коли виникала підозра про поліцейське дешифрування раніше перехоплених листів. Так, у 1902 році Цедербаум писав до редакції газети «Іскра»: «Чи не вважає Текля потрібним змінити шифр, тому що, мабуть, кілька наших листів до неї потрапили».

Але обмежитися винятково книжковими ключами революціонери, зрозуміло, не могли. Занадто непередбачене було їхнє життя, щоб у будь-який момент під руками виявилася необхідна книга.

Так, у серпні 1903 року «ленінці» розпочали використовувати вже відомий гамбетівський ключ. А пов'язано це було з драматичними подіями, що почалися відразу після закінчення II з'їзду РСДРП, на якому партія «розкололася» на більшовиків («ленінців») і меншовиків. Єдине ускладнення, що внесли більшовики у гамбетівський ключ, полягало у введенні для цифр першого десятка додаткових чисел «8» і «9»: 6 = 86, 2 = 92, 8 = 98 тощо.

Відомо, що Фелікс Дзержинський, один із лідерів «Соціал-демократії королівства Польського й Литви» та майбутній організатор НЧК і ОДПУ СРСР, у 1910-х роках використовував у своєму листуванні гамбетівський ключ і ключові фрази «Матка боска ченстоховська», «Коли буде сонце і гарна погода», «Душі людські вічно самотні».

Разом із тим, ідея квадратного (координатного) шифру була настільки привабливо, що підпільники знову і знову зверталися до неї. Одним із таких нових варіантів був «круглий ключ» (або, як його називав В.Акимов у своїй книзі, шифр «за таблицею Піфагора»). Він являв собою пряме удосконалення квадратного шифру, відомого ще з часів народництва.

Складалася квадратна таблиця розміром 6х6, а букви в ній розміщалися згідно з положенням в алфавіті за схемою графічного лабіринту.

	7	**8**	**9**	**10**	**11**	**12**
6	-	ч	ц	л	к	а
5	Ѳ	ш	х	м	й	б
4	я	щ	ф	н	і	в
3	ю	ъ	у	о	и	г
2	э	ы	т	п	з	д
1	Ѣ	ь	с	р	ж	е

Буква повідомлення записувалася як координатний дріб. При чому число можна було збільшувати на цифру 7 або множити на 7 і 10. Тому максимальні числа, що траплялися в дробах – 84 і 120. Усі ці нововведення повинні були спантеличувати дешифрувальників і маскувати систему шифру. Існував і фіктивний дріб (пустишка): 6/7 = 7/6 тощо, що відповідав порожній клітинці таблиці. Він також використовувався як знак розділення між словами.

Будь-яку букву можна було зашифрувати багатьма способами, наприклад: А = 6/12=12/6=12/13=19/13=60/120=13/12=13/19=12/42=42/12=19/42=42/19.

Це була «вершина криптологічної думки» більшовиків до весни 1905 року. Однак цей шифр був дуже непрактичний і вимагав граничної уваги при роботі з ним. Досить було припуститися помилки в одному лише знаку, пропустити цифру або, навпаки, приписати зайву, як уся криптограма перетворювалася в абсолютну «абракадабру». А це, при «хімічному» копіюванні шифру або його неякісному прояві, відбувалося завжди і всюди.

У 1905 році на хвилі зростання революційного руху в Росії було засновано багато нових видавництв, що почали масовими тиражами випускати раніше заборонену літературу. І всі ці видання відразу розпочали використовуватися як книжкові шифри підпілля. Крім того, книжкові шифри постійно удосконалювалися, а фіксовані сторінки поступово відходили в минуле. У практику ввійшло правило постійної зміни ключових сторінок. При цьому вони позначалися визначеними дробами, що ставилися в заздалегідь обговорених місцях криптограм.

Номери сторінок визначалися різними прийомами – найчастіше добутком чисельника і знаменника або їхньою сумою. Іноді їх потрібно було просто поставити поруч. Так, 2/5 = 25. Або ж сторінка книги виписувалася як дата листа тошо. Дуже широко розпочали застосовуватися зміннозначні книжкові системи, де за визначеними правилами автоматично змінювалися сторінки ключа.

Серед соціал-демократів також були винахідники шифрів. Зупинимося на двох із них, які належали до ядра соціал-демократичної більшовицької партії і грали керівну роль у революційному русі, а також у ранній післяреволюційний період. Це Гліб Іванович Бокій і Варвара Миколаївна Яковлєва.

При арешті Бокія поліція знайшла у нього звичайнісінькі учнівські зошити, списані математичними формулами, а насправді – записами про підпільні справи, за-

шифрованими математичним шифром. Шифр цей був винаходом Гліба Івановича, і ключ до нього був відомий тільки йому одному. Кращі шифрувальники, які тільки мала в своєму розпорядженні царська охоронка, ламали голови над цими «формулами», підозрюючи в них шифр. Проте розкусити цей горішок вони так і не змогли.

Була автором власних систем шифрів і керівник більшовицької організації центрального промислового району – секретар московського обласного ЦК РСДРП(б) В.М.Яковлєва. Дочка московського купця другої гільдії, вона закінчила математичний факультет Вищих жіночих курсів у Москві. Активна учасниця революції 1905-1907 років Яковлєва була впливовим партійним організатором, кандидатом в члени ЦК, автором Статуту партії, прийнятого VI з'їздом РСДРП(б).

Так само як і Бокій, Яковлєва створювала шифри, якими користувалися і інші революціонери. На жаль, ні зошити Бокія, ні шифри Яковлевої не збереглися. У архівах ДП є лише деякі їх шифровані листи, зашифровані іншими, вже відомими нам шифрами.

Як відомо, здобич шифрів і ключів до шифрів революціонерів складала одне з головних завдань агентів поліції, що діяли в революційному середовищі. Отримавши відомості про шифри, агенти негайно передавали їх в поліцію або писали про них в своїх донесеннях. Так, в одному з таких донесень від 21 квітня 1915 року агент за кличкою «Пелагея» доповідав ротмістру ДП Ганько:

«...На днях до Москви з Петрограда приїхала за дорученням ЦК РСДРП(б) якась «Тетяна Сергіївна»... «Тетяна Сергіївна» має широкі повноваження з відтворення на місцях соціал-демократичних більшовицьких організацій та підготовки ґрунту до майбутнього літом поточного року скликанню партійного з'їзду або конференції, і з цією метою їй доручено об'їхати область центрального промислового району і південь, де вона повинна після виконання першого завдання заручитися адресами для транспортування партійної літератури...

«Тетяна Сергіївна» майже щодня спілкується з П [етербурзьким] К [омітетом], якому повідомляє про досягнуті нею результати та отримані зв'язки, причому користується цифровим шифром:

Ми.....1
Азбуку.....2
Весь.....3
День.....4
Писали.....5
Папери.....6
Книжку.....7
Винищили.....8
Ми.....9

Що фиркають.....10
Відкидали.....11
Ех.....12
Ящірку.....13
Вважали за краще...14
Плъшь.....15

Вказані цифри позначають тільки слова ключа, наприклад, 12 – ех. Потрібна ж для зашифрування буква позначається порядковою цифрою, займаною буквою в слові ключа, так, наприклад, зашифрована буква «а» буде позначена: 2-1, або 5-4, або 6-4, або 10-5, або 11-7.

Проте крім цих цифр при шифруванні між ними вставляються ще довільні цифри з таким розрахунком, щоб кожна буква була позначена чотирма цифрами; так, та ж буква «а» в остаточно зашифрованому вигляді буде позначена: 7251, або 3544, або 2634, або 1025, або 1147.

При цьому потрібно мати на увазі, що між цифрами ключа вставляється тільки однозначна цифра, тому, якщо зашифрована буква складається з двох однозначних цифр, то довільні цифри вставляються одна перед цифрою ключа, причому не можна ставити тільки 1, а інша — між цифрами ключа; якщо ж зашифрована буква складається з двозначної і однозначної цифр, як, наприклад, «а» – 11-7, то вставляється тільки одна однозначна цифра між ними. Таким чином, зашифроване слово «Москва» позначатиметься так: 392211171534327613873109 5.

Для розшифрування, оскільки всі вказані цифри пишуться підряд, потрібно весь зашифрований текст розбити на групи по чотири цифри, з яких викинути довільно вставлені цифри, маючи на увазі, що якщо перша цифра буде «1», то довільно вставлена – тільки одна цифра між цифрами ключа, тобто по рахунку третя, інакше – вставлено дві цифри – перша і третя...»

Разом із тим, шифри були основним, але не єдиним засобом приховування партійних таємниць. І найчастіше більшовики використовували для написання конспіративних листів так звану «езопівську мову» та словниковий жаргон. Дуже широко практикувалася мова кодів або умовних термінів. Ними позначалися міста, партійні підприємства, проведені заходи тощо. Наприклад: «килина» – підпільна друкарня, «журнал» – валіза з подвійним дном, «магазини» – комітети партії, «рахунок» – транспорт літератури тощо.

Дуже популярним був код при листуванні телеграфом. Однак цей спосіб зв'язку був пов'язаний зі значним ризиком. Але набагато частіше в телеграмах обмежувалися декількома умовними термінами або цифрами. Так, пропонуючи провести збір ЦК РСДРП у Стокгольмі, Ленін писав у жовтні 1905 року своїм колегам у Росію: «Дайте мені телеграму... За підписом Болеслав з одним числом, що означає дату, коли я повинен бути в Стокгольмі (30 = я повинен бути до 30

вересня, 2 або 3 = я повинен бути до 2 або 3 жовтня і т.д.)».

Таким чином, буквально усі види поштового та телеграфного зв'язку в Російській імперії використовувалися революціонерами для оперативних контактів між собою.

3.8. Народження телеграфного зв'язку

Враховуючи явища науково-технічної революції XIX століття, не можливо не сказати про такі важливі події, як винахід телеграфу та радіо, що підштовхнули розвиток криптології та секретних видів зв'язку. Значну роль у народженні та розвитку телеграфного та радіозв'язку відіграли російські вчені та інженери, які постійно працювали над створенням принципово нових засобів передачі інформації на далекі відстані.

Ще в 1794 році геніальний російський винахідник Іван Кулібін сконструював семафорний (оптичний) телеграф і розробив код до нього. Записаний у вигляді однієї таблиці код спрощував роботу з передачі повідомлень. Це дозволяло швидше передавати потрібну інформацію.

У 1808 році офіцер російського військово-морського флоту А.Бутаков розробив свою систему семафорного телеграфу. Вона успішно була застосована в 1810 році на російській ескадрі, що діяла на Середземному морі під прапором віцеадмірала Д.Сенявіна.

У 1824 році між Петербургом і Шліссельбургом була прокладена дослідна лінія семафорного зв'язку за проектом генерал-майора П.Козена, що проробила до 1836 року.

Перша урядова лінія оптичного телеграфу між Петербургом і Кронштадтом довжиною 30 км була обладнана французьким інженером Ж.Шато в 1833 році.

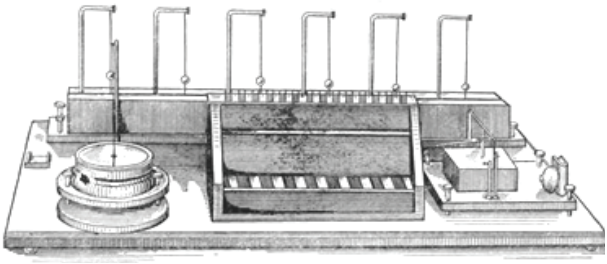
Зимовий палац у 1835 році одержав прямий оптичний телеграфний зв'язок з Царським Селом і Гатчиною. Тоді ж міжнародні події спонукали російський уряд виділити кошти для будівництва лінії оптичного телеграфу від Петербурга до Варшави. Лінія довжиною 1200 км, побудована наприкінці 1838 року, мала 149 проміжних станцій, через які сигнал проходив за 15 хвилин. Урядова шифрована депеша, що складалася з 45 сигналів, передавалася з Петербурга у Варшаву за 22 хвилини.

Оптичний телеграф проіснував у Росії близько півстоліття, приблизно до середини 1850-х років. Він зіграв значну роль у розвитку внутрішніх комунікацій як засіб оперативного керування виконавчими органами держави в мирний і воєнний час.

Цікаво, що в Росії винахідником електромагнітного телеграфу був завідувач криптологічною частиною МЗС барон Шилінг фон Кандштадт. Використовуючи астатичні магнітні стрілки, які були винайдені в 1821 році знаменитим французьким фізиком Ампером та про які він довідався при зустрічі з ним у Парижі, Шилінг розробив першу у світі конструкцію електромагнітного телеграфу, що принципово від-

різнялася від системи Земеринга.

Восени 21 жовтня 1832 року на його квартирі відбулася перша публічна демонстрація «телеграфної системи Шилінга». Передавач був встановлений в одному кінці будинку, де зібралися запрошені, а приймач – в іншому, у кабінеті Шилінга. Відстань між апаратами складала понад 100 м. Серед відвідувачів були академік Борис Семенович Якобі, граф Бенкендорф, Імператор Микола I, Великий князь Михайло Павлович. На демонстрації по лінії була передана перша телеграма, що складалася з 10 слів. Інтерес до винаходу виявився настільки великий, що демонстрація тривала до різдвяних свят.



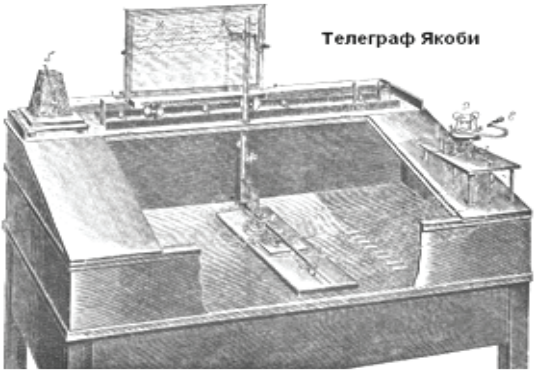
У 1836 році під керівництвом Шилінга була прокладена експериментальна підземна кабельна телеграфна лінія між крайніми приміщеннями будинку Адміралтейства в Петербурзі, що діяла більше року. У тому ж році він запропонував підвішувати лінійні проводи між телеграфними станціями на дерев'яні опори. У наступному році Шилінг почав роботу над проектом першої підводної телеграфної лінії зв'язку між Петергофом і Кронштадтом. Вона не була зупинена через смерть російського винахідника 25 липня 1837 року. Дослідження Шилінга як один з етапів робіт зі створення і поширення дротового телеграфу дуже вплинули на розвиток цієї галузі науки і техніки в інших країнах.

Спадкоємцем і продовжувачем робіт барона Шилінга з розвитку та впровадження телеграфу в Росії став академік Петербурзької академії наук Борис Якобі. У 1841 році він побудував телеграфну лінію між Зимовим палацом і Головним штабом у Петербурзі, обладнану оригінальними пишучими апаратами його конструкції. У 1842 році подібна лінія була прокладена від Зимового палацу до Головного управління шляхів сполучення і публічних будинків у Петербурзі. У наступному році була прокладена нова лінія до палацу в Царському Селі. Побудовані Якобі телеграфні лінії являли собою зариті в землю ізольовані мідні дроти.

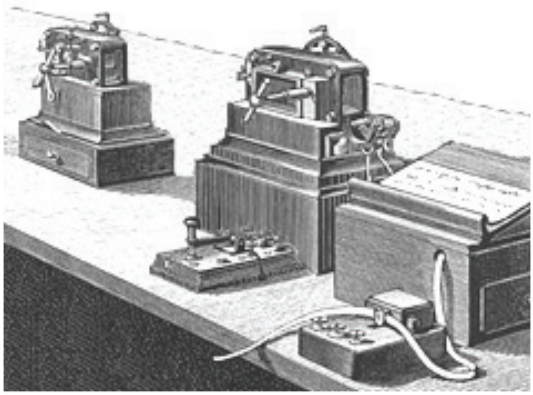
Перший пишучий телеграфний апарат Якобі сконструював у 1839 році. Його особливістю було те, що замість мультиплікатора використовувався електромагніт, що приводив за допомогою системи важелів у дію олівець. Запис сигналів відбувався на порцеляновій

дошці, що рухалася на каретці під дією годинного механізму. Телеграфний апарат Якобі протягом декількох років успішно працював на «царських» лініях: Зимовий палац – Головний штаб – Царське Село. Однак учений не був задоволений його роботою. Зигзагоподібні записи прийнятих депеш важко піддавалися розшифровці, не зручним був також пристрій каретки з екраном.

Протягом багатьох літ Якобі продовжував удосконалювання свого винаходу. У 1845 році він створив абсолютно нову конструкцію стрілочного синхронного апарата з горизонтальним циферблатом, електромагнітним приводом і прямою клавіатурою. Цей апарат набув практичного застосування в Росії, Європі і став основою для багатьох інших синхронних телеграфних апаратів. А в 1850 році Якобі винайшов перший у світі літеродрукувальний телеграфний апарат, що працював за принципом синхронного руху. Цей винахід був одним із найбільших досягнень електротехніки середини XIX століття.


Телеграф Якоби

У 1858 році англієць Чарльз Уітстон винайшов автоматичний телеграфний апарат з використанням перфострічки, на якій дірочки, розташовані відповідним чином, позначали крапки та тире абетки Морзе. На такому апараті можна було передавати до 500 букв у хвилину, тобто в п'ять-шість разів більше, ніж при ручній роботі за допомогою телеграфного ключа. Ці передавачі використовувалися й у першій половині XX століття. За спогадами маршала військ зв'язку І.Пересипкіна, цими апаратами поряд з апаратами Бодо і старт-стопними апаратами «СТ-35» була оснащена Червона Армія у період Великої Вітчизняної війни.



Інтенсивна робота зі створення телеграфу в Росії та пов'язані з цим теоретичні й експериментальні дослідження надають право вва-

жати Шилінга та Якобі основоположниками телеграфного зв'язку в Росії.

Однак уряд, зневажаючи вітчизняними винаходами та не організувавши в Росії електротехнічного виробництва, підписав угоду з прусським контрагентом Вернером фон Сіменсом, який запропонував поставити для російських телеграфних ліній «Стрілочні синхронні апарати Сіменса», що майже нічим не відрізнялися від стрілочних апаратів Якобі. У 1854 році стрілочні апарати були замінені апаратами Морзе, продуктивність яких у 10 разів перевищувала продуктивність стрілочних апаратів. Апарат був розроблений американцем Самюелем Морзе у 1837-1844 роках і вдосконалений іншими винахідниками.

У Москві перший телеграф почав діяти 13 жовтня 1852 року. Тоді на телеграфній станції у будинку вокзалу Петербурзько-Московської залізниці на Каланчевській площі було встановлено два телеграфні апарати стрілочного типу: один – для служби залізниці, другий – для урядової кореспонденції. З 1854 року на станції стали застосовуватися апарати Морзе.

Після того, як електричний телеграф почав використовуватися в системі керування державою, великий вплив на його подальший розвиток стали робити вимоги воєнно-стратегічного характеру. Кримська війна 1853-1856 років прискорила будівлю телеграфних ліній, тому що потрібний був оперативний зв'язок між великими містами. Тоді німецька фірма «Сіменс» одержала свій перший контракт на прокладення лінії телеграфного зв'язку Севастополь – Херсон – Одеса – Київ – Москва – Петербург.

У 1854 році була введена в експлуатацію телеграфна лінія Петербург – Варшава довжиною більше 1000 кілометрів. У травні 1855 року закінчилося будівництво лінії Київ – Кременьчуг – Миколаїв – Одеса, а у вересні того ж року була введена в експлуатацію телеграфна лінія Миколаїв – Перекоп – Сімферополь. З того часу Петербург одержав телеграфний зв'язок із Сімферополем, використовуючи для даної мети раніше побудовані лінії Петербург – Москва та Москва – Київ.

Розширення системи телеграфного зв'язку обумовлювалося й економічним розвитком Росії. У державну телеграфну мережу включалася усе більша кількість міст. Телеграфні повідомлення були встановлені між Москвою, Орлом і Харковом; Житомиром і Варшавою; Новочеркаськом і Херсоном; Тифлісом і Владикавказом і багатьма іншими містами. Споруджені телеграфні станції підрозділялися на урядові й приватні залізничні.

У 1857 році був побудований міський теле-

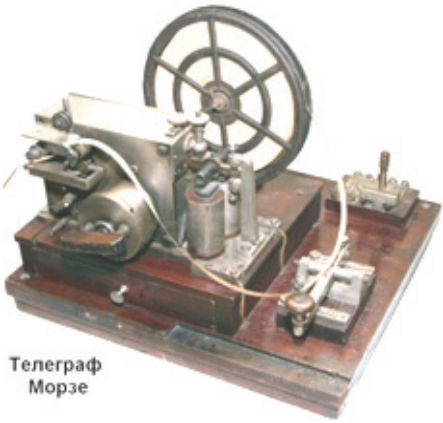
граф у Петербурзі, що об'єднав у єдину урядову мережу найважливіші пункти державного та військового керування. Міські телеграфи були введені в Москві у 1861 році й у Києві у 1881 році. У 1871 році було закінчено будівництво найдовшої за тих часів лінії урядового телеграфу Москва – Владивосток.

У вересні 1864 року був укладений договір на придбання російським урядом права використання літеродрукувального синхронного апарата американця Юза. Закуплені апарати в 1865 році були встановлені на магістралі Москва – Петербург. Принцип роботи цих апаратів ґрунтувався на синхронному та синфазному обертанні типових коліс передавального і прийомного апаратів.

Значний крок уперед у сфері розвитку ідеї частотного телеграфування був зроблений професором Харківського університету Юрієм Івановичем Морозовим. У 1869 році він розробив передавач, що представляв собою ємність, наповнену струмопровідною рідиною з двома опущеними в неї електродами. Один із них був виготовлений у вигляді металевої пластинки з жорстко укріпленим кінцем. При її коливанні між нею та нерухомим електродом за синусоїдальним законом змінювався електричний опір. Відповідно змінювався і струм у електричному колі. Передавач Морозова являв собою прообраз мікрофона.

У 1860-1870 роки військовим міністром Росії графом Д.А Мілютіним була проведена військова реформа. Поява нового засобу керування військами – телеграфу – порушила питання перед Генеральним штабом російської армії про необхідність регламентування його застосування та створення органів, які б повсякденно вирішували питання бойового застосування цього могутнього засобу керування військами.

Наказом військового міністра у 1870 році було затверджене «Положення про військово-телеграфні команди», що у воєнний час призначалися для посилення особовим складом існуючих ліній урядових і приватних залізничних телеграфів. У їхні функції входила будівля й експлуатація нових військових телеграфних ліній, ремонт ліній, зруйнованих супротивником при його відступі, а також ушкодження і знищення ліній, що переходять до ворога.



Телеграф Морзе

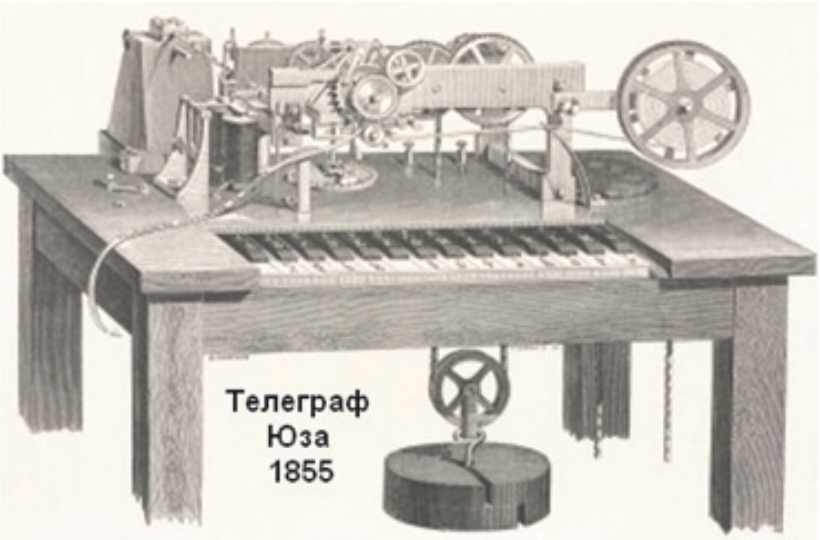
У 1876 році було затверджене «Положення про польове управління військ у воєнний час». Відповідно до Положення на чолі армії стояв головнокомандувач, що мав при собі польове управління армії, у складі якого було польове управління військових повідомлень із підпорядкованим йому відділом пошт і телеграфів. В обов'язках

завідувача відділом указувалося, що він відповідав за організацію й діяльність пошти і телеграфу на військових дорогах, що означало відповідальність за поштовий і телеграфний зв'язок усередині армії та зв'язок Головної квартири армії з центром.

Положенням передбачалася наявність при польовому штабі армії станції урядового телеграфу, що мали 4-6 телеграфних апаратів Морзе. Лінійне забезпечення телеграфного урядового зв'язку було покладено на військово-похідні телеграфні парки. Вони призначалися для організації зв'язку між штабами діючої армії і для зв'язку окремих частин армії як між собою, так і з державними телеграфними лініями. У 1867 році був сформований перший зразковий військово-похідний телеграфний парк, а восени 1870 року почате формування шести таких парків. Кожен парк мав 8 телеграфних апаратів Морзе, 35 верст телеграфного дроту та необхідну кількість тичин і ізоляторів для підвішування.

Військово-похідні телеграфні парки і військово-телеграфні команди, на відміну від підрозділів урядового телеграфу, перебували в підпорядкуванні польового інженерного управління, що значно утрудняло координацію дій по використанню системи телеграфного зв'язку для керування збройними силами у воєнний час.

У 1880 році на магістралі Москва – Петербург були застосовані швидкодіючі телеграфні апарати Уітстона з автоматичною передачею кореспонденції за допомогою перфострічки. У 1904-1906 роках телеграфна техніка в Росії поповнилася багаторазовими синхронними літеродрукувальними апаратами, сконструйованими французьким інженером Бодо. У 1913 році з загального числа телеграфних апаратів на телеграфній мережі Росії основну масу складали апарати Морзе (9014 штук), кіль-



кість апаратів Уітстона складало 121 штуку, Юза – 790 штук і Бодо – 115 комплектів.

За час Першої світової війни, революції і громадянської війни розвиток і удосконалення російської телеграфної техніки призупинилося, тому що заводи, що робили телеграфні апарати, в основному, виготовляли потрібні для армії прилади та військову апаратуру. У той час для низового зв'язку застосовувалися апарати Морзе, для міського та обласного зв'язку – апарати Юза, а для магістрального зв'язку – апарати Бодо, Уітстона та Сіменса, що мали велику продуктивність.

Настала ера нових оперативних засобів зв'язку, що вплинуло на криптологію. Багато «старих» шифрів стали непридатними для використання в телеграфних лініях зв'язку. Так, наприклад, екзотичні заміни букв на мудрі знаки виявилися принципово неприйнятними.

Оскільки телеграфні передачі коштували недешево, і ця вартість визначалася кількістю букв переданого повідомлення, то відразу ж були запропоновані ефективні методи «стиску» інформації – нетаємні телеграфні коди, у яких букви, слова, фрази «стискувалися» до коротких буквено-цифрових одиниць переданого тексту. Однак при передачі таємних повідомлень, крім такого нетаємного кодування, за необхідністю повинні були використовуватися шифри (шифрування кодованого повідомлення). Особливо гостро питання вартості телеграфного послання постало в 1866 році після прокладання трансатлантичного кабелю США – Європа.

Телеграфна передача була пов'язана з неминучими перекручуваннями повідомлення в лінії зв'язку. Тому з'явився новий напрямок у кодуванні – завадостійке кодування. За рахунок надмірності, що вводилася в передане повідомлення, на прийомному кінці з'являлася можливість усунути ці перекручування. Одночасно збільшилася увага до такої властивості шифрів, як завадостійкість: сприйняття приймаючою стороною змісту тексту, відмінного від переданого, було однією із найнеприємних ситуацій, пов'язаних із перекручуваннями.

Такого роду перекручування приводили до необхідності вживати заходів захисту. Найбільш важливі місця повідомлень дублювалися, що приводило до збільшення витрат на зв'язок. Використовували так званий «двобуквений диференціал»: ключові слова повинні були відрізнятися один від одного не менш ніж двома буквами. Це приводило до появи великого числа неологізмів – слів, що не були загальноприйнятими в даній мові (тобто вироблялася телеграфно-кодова мова, що мала вигляд жаргонних кодів). Нарешті, почали застосовуватися завадостійкі коди, що дозволяли виявляти й усувати перекручування. Але це знову призвело до подорожчання зв'язку.

З огляду на підвищені вимоги до точності передачі шифрованих телеграм, телеграфні компанії підвищили ціну за їхню передачу. Телеграфісти стверджували, що вони були змушені ретельно та по буквах передавати нечитабельні тексти, що істотно знижувало ефективність їхньої роботи порівняно до передачі звичайних «осмислених» повідомлень. У відповідь користувачі шифрів спробували додати

шифрованому (кодованому) повідомленню «осмислений» вигляд (хоча б на рівні наявних у шифротексті «слів»). Тому в 1889 році в Лондоні була проведена спеціальна конференція, присвячена тлумаченню поняття «шифрована телеграма». Нарешті, у 1890 році конференція в Парижі ввела в обіг офіційний словник кодової мови, що містив лише «слова, що читаються».

Цей словник викликав «хвилю» протестів, оскільки, власне кажучи, забороняв передачу таємних (кодованих) повідомлень. Конференція в Лондоні в 1903 році відмовилася від єдиного словника. Було дозволено застосовувати штучні слова, але за умови, що вони будуть складатися з «вимовних слів і тих, що читаються» та їхня довжина не буде перевищувати 10 букв. І все-таки в 1932 році на конференції в Мадриді всі обмеження з кодування та шифрування були зняті.

У 1904 році в Англії з'явився словник Уайтло для кодопозначень, що містив, за ствердженням автора, 400 мільйонів вимовних слів. Слова мали вигляд «*FREAN*», «*LUFFA*», «*LOZOI*», «*FORAB*» тощо, тобто були 5-буквеними. Уайтло допускав з'єднання слів для позначення нового словотвору. Ідею Уайтло вже в 1905 році підтримав і розвив Е.Бентлі, що створив універсальний 5-буквений код для телеграфних повідомлень. Розбивка шифротекстів на 5-буквені сполучення дійшла до наших днів. Також «нормовані» за довжиною коди витиснули коди, цілком засновані на використанні словникових величин.

Майже кожна промислова або комерційна компанія розробляла таємні коди для власних потреб. З'явилися коди торговців автомобілями, банкірів, біржових маклерів тощо, що викликало створення спеціальних професійних «криптографічних груп», що «за замовленням» складали таємні коди для користувачів з урахуванням їхньої професійної мови. Такі коди коштували досить дорого та стали звичайним ринковим товаром. Кодові книги, що складалися ними, за обсягом були порівняні зі словником англійської мови.

З'явився ринок торгівлі кодами. При цьому виникли й різномовні коди, призначені для кореспондентів, що говорили на різних мовах. Були створені й багатомовні кодові книги. Ці коди дійшли до наших днів. Сигнал «*SOS*» (англ. *Save Our Souls* - врятуйте наші душі) у всіх країнах сьогодні сприймається як прохання про допомогу. Сучасні коди «стискають» інформацію більш ніж у 10 разів (цей ефект залежить від багатства лексики відкритої мови). Стиск переданої по технічних каналах зв'язку інформації й у наші дні є актуальним завданням.

Тепер стосовно вітчизняного телеграфного зв'язку. У 1906 році Київський телеграф розташовувався на другому поверсі приватного будинку № 22 на вул. Володимирській. Персонал телеграфу становив 312 осіб, обслуговуючи за роки 4 мільйони 800 тисяч телеграм. У 1921 році телеграф перемістили в будівлю Земельного банку на вул.Володимирській, буд.10, де він розташовується й досі. У довоєнні роки постійний телеграфний зв`язок сполучав Київ не тільки з містами і селами

України та СРСР, а й з Берліном, Бухарестом, Будапештом, Лондоном.

У роки перших п'ятирічок у СРСР почалося відродження промисловості, що робила телеграфні апарати. У 1935 році інженерами М.Волковим, М.Гагаріним і С.Часовіковим був розроблений стартстопний стрічковий телеграфний апарат «СТ-35», який був великим досягненням радянської техніки. Цей апарат у видозміненому і поліпшеному вигляді з трансмітерною та реперфораторною приставками широко застосовувався для телеграфного зв'язку аж до 70-х років минулого століття. Швидкість «СТ-35» складала 380 знаків у хвилину. На його основі промисловість випустила рулонний стартстопний телеграфний апарат «РОТА-37», що друкував знаки рядками на широкій стрічці. Наприкінці другої п'ятирічки (1933-38) на магістральних лініях зв'язку використовувалися, в основному, багаторазові апарати «Бодо-дуплекс», а на внутріобласних і міських – старт-стопні апарати Шорина, Тремля, Юза, Морзе, СТ-35 тощо.

У післявоєнні роки (1946-47) були сконструйовані для радіотелеграфного зв'язку дві нові системи триразових стартстопно-синхронних апаратів: В.Кербі («ТРТ-1») і Л.Коробкова («МТП-3»), а в 1954 році для дротового зв'язку – дворазова стартстопно-синхронна установка В.Новікова і О.Шараєва («2ТУ»). Апарат «СТ-35» з доданими до нього реперфораторною та трансмітерною приставками автоматизації був переведений на роботу міжнародним кодом № 2 і одержав назву «СТА-2М», а з 1967 року – «СТА-М67»; а з 1978 року після модернізації став називатися «ЛТА-8».

СТ-35

Т-63

Київський центральний телеграф у післявоєнні роки використовував трофейну німецьку апаратуру тонального телеграфування «ВТ-34» і «ВТ-ЧМ». Згодом з'явилася вітчизняна апаратура «ТТ-14П». Перша вітчизняна (ризька) станція абонентського телеграфування «АТ-57» була запроваджена на Київському центральному телеграфі в

1960 році.

У 1960 році Київським відділенням науково-дослідного інституту зв'язку разом із Тбіліським конструкторсько-технологічним бюро телеграфної техніки був створений зразок рулонного старт-стопного апарату «РОТА-6», що працював зі швидкістю 400 і 600 знаків у хвилину. Однак його серійне виробництво організовано не було, а на телеграфних лініях зв'язку країни одержали широке поширення рулонні стартстопні апарати «Т-63», що випускалися німецькою промисловістю, та апарати «Т-100», що випускалися чехословацькою промисловістю.

3.9. Народження радіозв'язку

Винаходу радіо, традиційно пов'язаному в СРСР з ім'ям Олександра Степановича Попова, викладача Мінних офіцерських класів, передували фундаментальні й інженерні дослідження найвідоміших у світі фізиків, математиків і експериментаторів. Так, наприклад, піонером самої ідеї радіозв'язку по праву можна вважати і болгарського вченого Петра Атанасова (Хаджиберовича) Берона, який у додатку до 3-го тому семитомної «Панепистемії» (панепистемія – всенаука, тобто єдина наука існуючого світу) описав свій проект бездротової передачі повідомлень, який містив багато технічних креслень майбутнього бездротового телеграфу.

У 1888 році в «Лондонському науковому щорічнику» німецький фізик Генріх Герц повідомив про створення ним двох приладів. Один із них – вібратор, що випускав електричні хвилі. Інший – резонатор, що їх уловлював. Таким чином, Генріх Герц став першим ученим, що свідомо управляв електромагнітними хвилями. Але він так і не вийшов зі своїми дослідами за межі лабораторії, не усвідомлюючи значення практичного застосування свого відкриття.

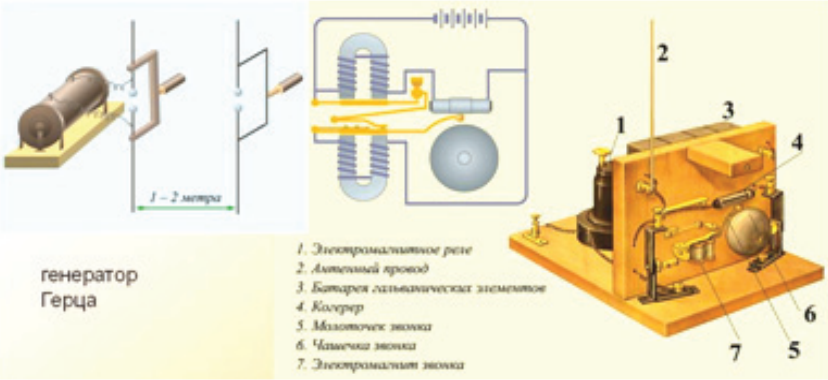
Англійський фізик Олівер Лодж на основі винаходу француза Едуарда Бранлі створив індикатор радіохвиль, який назвав «когерером» (від лат. cogerentia – «зчеплення»). Когерер являв собою скляну трубку, у якій знаходилися магнітні обпилювання. Під впливом електричного заряду обпилювання злипалися. Для того, щоб вони знову розсипалися, по трубці вдаряв молоточок, що приводився в дію годинним механізмом. Однак і Лоджу ввійти в історію як винахіднику радіо не вдалося.

У 1891 році американський винахідник Томас Едісон одержав патент на прилад, за допомогою якого без дротів на відстань 200 метрів були передані електричні сигнали з корабля, що рухався, на берег. Але геніальний фізик не став розробляти цей напрямок, захоплений іншими ідеями.

7 травня 1895 року викладач Мінного офіцерського класу Олександр Степанович Попов на засіданні Російського фізико-хімічного товариства (РФХТ) продемонстрував прилади, що створювали та сприймали електромагнітні хвилі. Статті про них були надруковані в журналах «Електрика» і «Метеорологічний вісник». У той час Мінний офіцерський клас у Кронштадті був кращим у Росії електротехнічним навчальним закладом, що мав у розпорядженні новітні устаткування. Усе це дало можливість Попову займатися важливою для нього проблемою – електромагнітними хвилями, що цікавили фізиків усього світу. Але вприту учений зайнявся цим після відвідування Всесвітньої виставки в Чикаго, що проходила під час третього Міжнародного електротехнічного конгресу.

На той час Попов уже був розробником приладу, який він назвав «грозовідмітчик». Прилад був встановлений у Лісовому інституті в Петербурзі. Дія апарата зводилося до успішного виявлення та реєстрування грозових розрядів на відстані до 30 кілометрів. Однак основні наукові дослідження вчений проводив у галузі бездротової телеграфії, що почав ще в 1888 році, відразу ж після повідомлень про досліди Герца. Проте результати досліджень Попова не розповсюджувалися. Професор В.Лебединський так написав у своїх спогадах: «Роботи Попова велися під контролем Морського міністерства і не могли бути розповсюджені...». Саме це стало причиною того, що Попов не запатентував свій винахід.

12 березня 1896 року в Санкт-Петербурзі на засіданні РФХС Попов, використовуючи вібраторні антени з рефлекторами, передав перше радіоповідомлення, що складалося з двох слів «Генріх Герц» на відстань 250 м. Продовжуючи удосконалювати апаратуру, Попов досяг дальності зв'язку в сотні кілометрів. У 1900 році на Між-



народному електротехнічному конгресі в Парижі Попову була присуджена Золота медаль і диплом Всесвітньої виставки за апаратуру бездротового телеграфу.

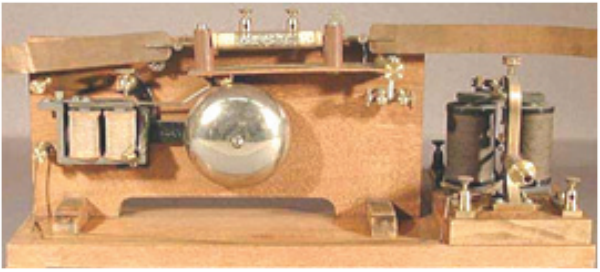
До весни 1897 року вчений зробив кілька приладів, що були встановлені на військових кораблях Балтійського флоту. Ця робота вимагала від нього величезного напруження і змусила пережити чимало гірких хвилин. В архівах Мінного класу зберігся документ такого змісту: «Видати викладачу Попову під звіт триста карбованців на витрати для дослідів бездротового зв'язку між судами ескадри». Але на створення тільки однієї радіоустановки було потрібно близько 5 тисяч карбованців. Однак царське морське відомство, не маючи сучасного зв'язку, не занадто щедро фінансувало дослідження.

Тільки завдяки підтримці адмірала Степана Макарова та голови Морського технічного комітету віце-адмірала Івана Дікова вдалося домогтися від уряду гідного забезпечення найважливіших для російського флоту досліджень в області зв'язку. Чимало сприяло визнанню винаходу Попова на батьківщині й та обставина, що за допомогою його приладу не раз успішно проводилися роботи з порятунку судів і екіпажів. Уперше це трапилося у 1899 році, коли в результаті навігаційної помилки у ніч з 24 на 25 листопада сів на мілину поблизу шведського острова Гогланд у Фінській затоці броненосець *«Генерал-адмирал Апраксин»*.

На борті криголама *«Ермак»* П.М.Рибкін доставив на острів Гогланд радіоапаратуру й щоглу для антени. Інша радіостанція була привезена й установлена під керівництвом О.С.Попова на острові Кутсала, неподалік від Котки. 24 січня 1900 року радіозв'язок між островами Гогланд і Кутсала був встановлений. Перша ж радіограма, відправлена Поповим і прийнята Рибкіним, допомогла врятувати рибалок, віднесених на крижині, що відірвалася, у відкрите море.

Система іскрового радіозв'язку О.С.Попова безперебійно працювала протягом усієї рятувальної операції броненосця *«Генерал-адмирал Апраксин»*. У квітні 1900 року броненосець був знятий з каменів і своїм ходом відправлений у ремонт.

Після успішного практичного використання радіотелеграфії без дротів почалося оснащення кораблів російського флоту іскровими радіостанціями. У вересні 1900 року в Кронштадті при участі Попова була відкрита радіомайстерня, перше вітчизняне підприємство з виготовлення й ремонту радіостанцій. З 1901 по 1904 рік тут були виготовлені 54 нові корабельні радіостанції системи Попова. Учений організував курси для підготовки радіотелеграфістів і розробив для них програми лекцій-



них і практичних занять.

Акціонерне товариство російських електротехнічних заводів (далі – АТ) *«Сименс и Гальске»* ініціювало підписання 21 травня 1904 року спільного 5-річного договору по впровадженню бездротових технологій у Росії з фірмою «Телефункен» і винахідником радіозв'язку Поповим. Після цього завод АТ *«Сименс и Гальске»* приступило до серійного виготовлення радіостанцій системи Попова.

Заслуги Попова були високо оцінені царським урядом. Винахідник на підставі «найвищого бажання» одержав 33 тисячі карбованців «у винагороду за... безперервні праці по застосуванню телеграфування без проводів на судах флоту». Йому були присуджені премії і почесні звання багатьох організацій у Росії.

Майже одночасно з О.Поповим свою радіотелеграфну установку створив італієць Г.Марконі, який вперше офіційно продемонстрував її у Великобританії у вересні 1896 року. 2 липня 1897 року Марконі став щасливим власником патенту на право «удосконалити апаратуру для передачі електричних сигналів». При цьому в британському патентному законодавстві був пункт: патент надійно захищав права винахідника на території Британської імперії, але не означав світового пріоритету в цій сфері. У Великобританії патент видавався на підставі висновку, зробленого англійськими вченими, – Королівська академія не проводила експертизи досліджень, зроблених вченими інших країн. Таким чином, отриманий Марконі патент означав

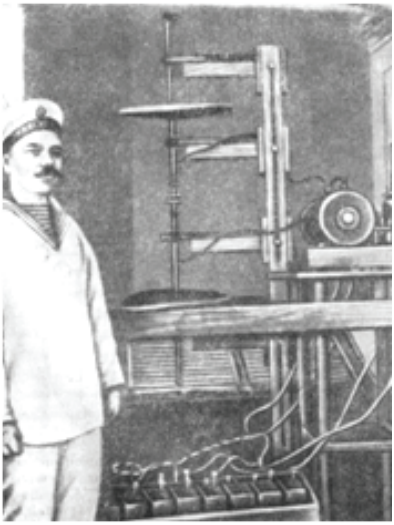
тільки те, що у Великобританії подібної заявки ніхто не подавав.

Марконі зумів поставити винахід на міцну комерційну основу. Вже в 1897 році він заснував «Компанію бездротового телеграфу Марконі» зі статутним капіталом 100 тисяч фунтів стерлінгів (близько 1 мільйона золотих карбованців). А в 1900 році з'явилася «Компанія міжнародного морського зв'язку Марконі».

Це дало йому можливість удосконалювати свій радіотелеграф, підвищити його чутливість, вибірковість і дальність зв'язку. Так, для здійснення вибірковості радіозв'язку Марконі використовував явище електричного резонансу та став налаштовувати коливальні контури передавальної й приймальної станцій на однакову частоту. Проводячи досліди з передачі радіосигналів на великі відстані, Марконі зробив відкриття. Він установив, що опуклість земної кулі не перешкоджає поширенню електромагнітних хвиль.

12 грудня 1901 року в готелі селища Сент-Джонс канадської провінції Ньюфаундленд Марконі прийняв за допомогою найпростішого приймача з когерером коротке радіопослання – дві букви «S». Воно було передано іскровим передавачем з диполем Герца, розташованим на мисі Полду в графстві Корнуол південно-західної Англії. Як антену приймача Марконі використовував дріт довжиною 150 метрів, який він підняв над землею за допомогою коробчатого змія власної конструкції. З того часу радисти усього світу відзначають дату початку ери далекого радіозв'язку, що почалася більше 100 років тому.

З того часу радіотехніка почала бурхливо розвиватися. У 1902 році Марконі здійснив прийом радіосигналів на відстані 2000 км, а в грудні того ж року був встановлений регулярний радіотелеграфний зв'язок між США та Англією. З цього приводу Президент Т.Рузвельт і король Едуард VIII послали один одному привітальні радіограми.



Цікаво, що 12 липня 1902 року Марконі на італійському військовому кораблі відвідав Кронштадт і показав свій приймач Попову, з яким був знайомий з листування. Два великі винахідники добре розуміли один одного. Відоме висловлення Попова: «Не підлягає, звичайно, сумніву, що перші практичні результати з телеграфування на значні відстані були досягнуті Марконі».

Крапку в питанні першості винаходу радіо поставила спеціальна експертна комісія, створена американцями. Під час Першої світової війни Марконі пред'явив американ-

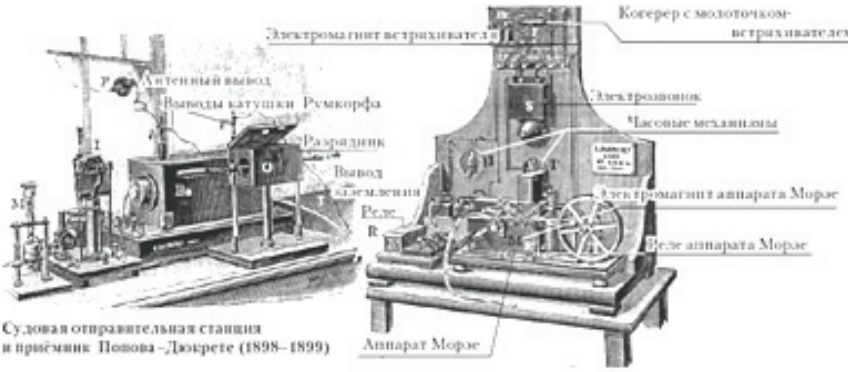
ським промисловцям багатомільйонний позов за використання його винаходів. І тоді американці «закотили рукави». Результати експертизи були викладені на 346 сторінках. Судовий розгляд тривав 19 років. Марконі особисто був присутній майже на всіх засіданнях і запекло відстоював свої інтереси. Але його претензії були відхилені.

Рішення суду було таким: «Марконі не був першим, хто відкрив, що електричні зв'язки можуть здійснюватися без проводів. Його прилад не міг бути практично використаний, поки Попов, росіянин, не винайшов спеціального пристрою, що...» А у заключній частині технічної експертизи було сказано: «У 1900 році на четвертому Всесвітньому електротехнічному конгресі в Парижі, що проводився в рамках Всесвітньої виставки, Попов за роботу в сфері бездротової телеграфії був нагороджений золотою медаллю. Отже, першість у винаході радіо належить йому».

Взагалі, термін «радіо» поступово затвердився в науці, техніці й у побуті лише в 1903 році після Міжнародної конференції з бездротового телеграфування, що рекомендувала для вживання термін «радіотелеграфія» замість термінів, що тоді існували: «бездротовий зв'язок» і «сигналізація без дротів».

Чимало сприяла розвитку радіозв'язку в Росії російсько-японська війна 1904-1905 років. Особливо допомогло цьому призначення віце-адмірала С.О.Макарова командуючим 1-ою Тихоокеанською ескадрою: після його вступу на посаду (24 лютого1904 року) були розпочаті енергійні кроки з впровадження радіозв'язку в керування флотом – уже до березня майже всі кораблі оснастили радіостанціями. Тоді ж розпочалося спорудження запропоноване Макаровим декількох радіостанцій на узбережжі Тихого океану.

У квітні 1905 року в Петербурзі були сформовані 1-а і 2-а Східно-Сибірські іскрові (радіотелеграфні) роти, що стали першими польовими радіочастинами російської армії. Рота мала на озброєнні 8 іскрових радіостанцій системи Марконі. Перша така рота під час бойових дій забезпечила радіозв'язок штабу головнокомандуючого зі штабами всіх 3-х маньчжурських армій. Однак під час російсько-

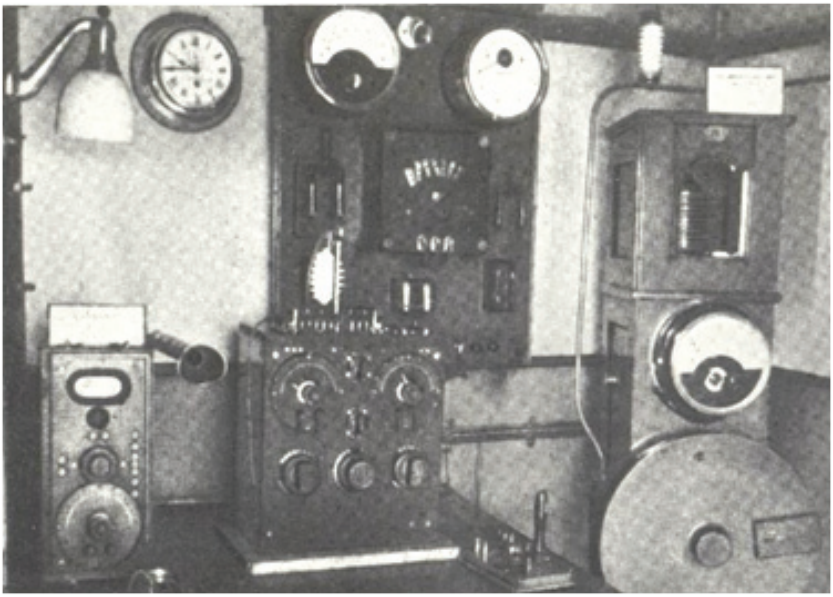


Судовая отправительная станция и приёмник Попова–Дюкрете (1898–1899)

японської війни, незважаючи на початі кроки по оснащенню флоту вітчизняними радіостанціями, кораблі 2-ої Тихоокеанської ескадри під командуванням віце-адмірала З.П.Рожественського прийшли до Цусимського бою (27-28 травня 1905 року) з німецькими радіотелеграфними станціями системи «Слаби-Арко» фірми «Телефункен» і декількома французькими радіостанціями фірми «Дюкрете».

Під час бойових дій на Далекому Сході радіозв'язок при керуванні військами показав свої переваги в порівнянні з дротовими засобами: головне з них полягало у швидкості встановлення зв'язку (тоді для цього було потрібно до 40 хвилин), а також можливості встановлення зв'язку через територію, зайняту супротивником.

До 1906 року наукові розробки іскрових радіостанцій в основному велися в Кронштадті в Мінному офіцерському класі під керівництвом Попова, а їх виготовлення здійснювалося в радіомайстерні Кронштадтського морського порту. Після 1905 року в Росії були створені й інші науково-виробничі центри, які займалися розробкою іскрових радіостанцій. Одним із помітних вітчизняних пристроїв бездротової телеграфії стала іскрова радіостанція, розроблена в 1911 році викладачем Учбово-мінного загону Балтійського флоту лейтенантом І.І.Ренгартеном. Радіостанція одержала назву «Звучна радіостанція типу Учбово-мінного загону» (скорочено російською – «*УМО*»), тому що мала у своєму складі іскровий передавач із розрядником Віна. Завод, що випускав радіостанцію, згодом майже щорічно модернізував цю апаратуру, привласнюючи їй нові індекси.



У довідці від 26 травня 1911 року, підготовленої начальником мінного відділу Головного управління кораблебудування Ремметом, про роботу радіотелеграфування в російському флоті за 1904-1911р. говорилося, що радіостанції типу «*УМО*» мали дальність телеграфування до 40 миль, а на Чорному морі при чистій воді прийом на телефонний приймач становив до 300 миль. Що цікаво, ці радіостанції дозволяли здійснювати нічний зв'язок кораблів у Севастополі з судами Балтійського флоту у Фінській затоці. Коштували радіостанції 35000 рублів.

У 1912 році на кораблях російського флоту почали встановлювати нові модифікації радіостанції типу «*УМО*», особливістю яких була наявність телефонного радіоприймача з підсилювачем звуку системи Нікіфорова (начальник радіомайстерні Радіотелеграфного депо Петербурзького порту). Звуковий підсилювач, побудований на реле, утроював силу звуку в порівнянні з телефонними навушниками, безпосередньо підключеними до радіоприймача. Прослуховування радіотелеграфного сигналу здійснювалося через спеціальний гучномовець.

З огляду на помилки російсько-японської війни, Військове відомство в 1905 році починає на Далекому Сході будівництво стаціонарних радіостанцій військового зразка: першою вводиться в експлуатацію військова радіостанція в м.Імані, а у 1906 році заробили станції у Владивостоці й Харбіні. У 1907 році радіостанції починають функціонувати в Хабаровську, Миколаївську та у селі Нижньо-Тамбовському. Радіостанція у Миколаївську офіційно підпорядковувалася штабу фортеці та називалася «Станція іскрового телеграфу Миколаївської-на-Амурі фортец».

Російсько-японська війна виявила всю вразливість російських далекосхідних володінь. Якщо Верхній, Середній, Нижній Амур, Примор'я і навіть Сахалін були зв'язані між собою «Амурським телеграфом» і військовими радіостанціями, то Охотомор'я, Камчатка, Крайній Північний схід не мали ніякого сучасного зв'язку та у разі військового нападу або природного катаклізму були зовсім беззахисні. Ситуація ставала настільки тривожною, що у 1908 році цим питанням змушений був зацікавитися не тільки сам цар, але й Рада Міністрів.

Ознайомившись із положенням справ на Охотському узбережжі та Камчатці, докладно описаному у записці Голови Ради Міністрів Столипіна, Микола II накладає резолюцію: «На Східний Сибір, і на Охотсько-Камчатський край особливо, варто звернути найбільш серйозну увагу й приступити до діяльності там негайно». Маючи царську підтримку, Рада Міністрів видає розпорядження: «Негайне встановлення зв'язку з містом Петропавловськ-Камчатський є справа першочергової важливості. Необхідно вдатися до допомоги бездротового телеграфу й спорудити телеграфні станції в містах Миколаївськ-на-Амурі й Петропавловськ-на-Камчатці».

Розробка проекту радіотелефонного зв'язку між устям ріки Амур і півднем півострова Камчатка, між якими лежить одне з найнеспокійніших морів на земній кулі – Охотське, а потім і здійснення цього проекту на практиці стали першим велико-

масштабним досвідом Головного управління пошт і телеграфів у радіотелеграфному будівництві. Одним із головних організаторів створення станцій та їхніх розробників був талановитий інженер Микола Олександрович Скрицький, що багато зробив для пропаганди нового виду зв'язку в Росії.

11 травня 1909 року спеціальна комісія Головного управління пошт і телеграфів під головуванням полковника Ейлера підписує контракт з АТ *«Сименс и Гальске»* на забезпечення радіотелеграфного зв'язку за системою *«Телефункен»* між Миколаївським-на-Амурі й Камчаткою.

3 лютого наступного року Скрицький відправляється у відрядження в Берлін для оформлення контракту на поставку радіоапаратури для Петропавловська-Камчатського й Миколаївська-на-Амурі. Відповідно до контракту товариство зобов'язувалося «виготовити, випробувати, доставити в Миколаївськ і Петропавлівський порт і з відкриттям навігації 1910 року всі необхідні прилади двох радіотелеграфних станцій, улаштувати потім їх та встановити радіотелеграфне між ними сполучення».

У жовтні 1910 року монтаж обох радіостанцій був завершений. Їхні випробування розпочалися 23 жовтня й закінчилися 9 листопада підписанням документу щодо остаточного приймання, після якого уряд Росії виплатив АТ «Сіменс и Гальське» 107254 рублі. Радіопередавачі, встановлені фірмою «Телефункен», працювали за принципом «звучної іскри» і мали потужність по 5 квт. Джерелом живлення служили гасові двоциліндрові двигуни Гарднера потужністю в 20 кінських сил. Обидві станції працювали в діапазоні довгих хвиль на хвилі 2000 метрів; дальність дії становила вдень 1200 км, а вночі – 2400 км. Кожна станція мала апаратуру по прийому радіограм на слух (при швидкості 15 слів у хвилину) і на стрічку телеграфного апарата Морзе (5 слів у хвилину), а також апарати для автоматичного прийому сигналу виклику.

10 листопада 1910 року між Миколаївським-на-Амурі й Петропавловським-Камчатським відкрилося радіотелеграфне сполучення загального користування. До осені 1918 року Миколаївська радіостанція стабільно постачала інформацією й представників усіх існуючих у той період урядів і місцеве населення: 1910 – березень 1917 року – царський уряд, березень 1917 – січень 1918 року – представників Тимчасового уряду, січень – початок вересня 1918 року – обласна Рада робочих, селянських і солдатських депутатів.

До 1910 року, крім мережі далекосхідних радіостанцій, була створена мережа стратегічного радіозв'язку в західно-європейській частині Російської імперії, що зв'язала Бобруйськ з узбережжям Балтики, Чорного моря й групою радіостанцій уздовж західного кордону. Радіостанція в Бобруйську була модернізована французькою компанією «*T.S.F.*», що дозволило їй підтримувати радіотелеграфний зв'язок із радіостанцією «Ейфелева вежа» в Парижі. Компанія *«T.S.F.»* побудувала

також потужну іскрову радіостанцію в Севастополі – вона забезпечувала зв'язок російського флоту з французькою військово-морською базою в Бізерті (Туніс). До речі, наприкінці 1920 року при евакуації білогвардійських військ під командуванням генерал-лейтенанта барона Врангеля збережені кораблі й судна Чорноморського флоту (загальним числом 150) були виведені до Бізерту.

Будівництво групи іскрових радіостанцій велося й уздовж північного узбережжя Росії. Передбачалося також створення радіостанцій у Москві для зв'язку з Баку, Ташкентом і Бобруйськом. У свою чергу через Ташкент Москва зв'язувалася з Кушкою на кордоні Афганістану, а через Баку – з Ашгабадом і Карсом (колишнє російське місто на північному сході Туреччини, що за Сан-Стефанським мирним договором 1878 року увійшло до складу Росії, однак за Брестським договором 1918 року відійшло до Туреччини разом з округами Батумі й Ардаган). Потрібно відзначити, що активне будівництво потужних іскрових радіостанцій, розпочате ще до 1914 року, мало своєю метою створення єдиної стратегічної системи зв'язку, що з'єднує європейську й азіатську частини Росії.

Передбачалося, що ця система буде готова до майбутньої війни. У планах її будівництва була транссибірська лінія радіозв'язку Москва-Хабаровськ з установкою ретрансляційних станцій в Уржумці, Красноярську й Читі. Так, радіостанція в районі залізничної станції Уржумка почала будуватися в 1908 році за вказівкою Військового міністерства, а працювати в 1912 році. Розташовувалася вона за вісім кілометрів від Златоуста (найбільш високогірне місто Уралу), на південному схилі Олександрівської сопки (названої на честь Олександра II, який відвідав ці місця за велінням свого батька Миколи I). За планом радіостанція повинна була розміститися в районі Златоуста, на горі Косотурі або хребті Уреньга, але місцева влада затялася: дощу, мовляв,тоді не буде, всі хмари радіо притягне до себе. Будівля обійшлася в мільйон рублів золотом.

Від Уржумської станції до радіостанції була прокладена дорога, вимощена кругляком. Навколо будинку радіостанції на кам'яно-цементних підставах установили 3 щогли для розміщення антенного устаткування висотою 80 м. Робота радіостанції *«Уржумка»* для військових потреб велася з квітня 1912 по грудень 1914 року, потім передача військової інформації припинилася, оскільки сигнали стали перехоплюватися японською розвідкою. У 1915-1916 роках радіостанція вже нерегулярно використалася для прийому-передачі цивільної інформації: виявилося, що прийому сигналів заважає гора. А наприкінці 1916 року станція припинила роботу й у 1922 році була повністю ліквідована.

Радіостанція в Читі – її потужність становила 35 квт – почала будуватися ще на початку 1913 року під керівництвом інженера Р.Л.Каулена та була введена в дію в лютому 1917 року. Ташкентська радіостанція такої ж потужності й радіостанція в Кушці потужністю 15 квт були закладені в 1913 році, а в дію введені у квітні 1916 року та вересні 1915 року відповідно. Закінчувало будівництво цих радіостанцій петербурзьке

відділення АТ «Сіменс и Гальське». В результаті була створена важлива стратегічна лінія радіозв'язку Владивосток – Чита – Ташкент – Москва – Санкт-Петербург.

За 10 років (1903-1913) АТ «Сіменс и Гальське» виготовило та встановило в Росії 325 радіостанцій, з них 178 – суднових, 59 – берегових для флоту й цивільного відомства та 88 – для армії. Компанія увійшла до числа провідних радіотехнічних фірм світу, а петербурзький завод на 6-й лінії з 1911 року став спеціалізуватися на виготовленні електричних апаратів слабкого струму. З 1905 по 1917 роки Військовим відомством було споруджено та введено в дію 26 стаціонарних радіостанцій різної потужності й призначення. Однак повністю втілити в життя план по будівництву серії радіостанцій так і не вдалося, частина їх спішно добудовувалися вже під час війни 1914-1918 років.

Разом із тим, для оснащення радіоапаратурою армії й відновлюваного корабельного складу флоту Росії потужностей вітчизняних радіотехнічних виробництв не вистачало, у зв'язку з чим уряд був змушений залучити іноземні компанії. Так, у 1906 році петербурзький завод «Сіменс і Гальске» виготовив 30 радіотелеграфних станцій для міноносців, а також установив апаратуру на ряді споруджуваних кораблів, у тому числі *«Таймыр»* і *«Вайгач»* – криголамах Головного гідрографічного управління. Після 1910 року завод освоїв випуск передавачів із розрядниками Віна та у 1910-1912 роках установив їх у ряді населених пунктів Далекого Сходу. Радіоапаратура заводу була також змонтована на бойових кораблях російського флоту, що будувалися в ті роки: лінкорах *«Андрей Первозванный»*, *«Император Павел I»* і крейсерах *«Адмирал Макаров»*, *«Баян»*, *«Паллада»*.

Для потреб армійського радіозв'язку в російської армії компанією «Сіменс і Гальске» була випущена типова воєнно-польова радіостанція зразка 1910 року з дальністю зв'язку до 250 км. Детекторний приймач «К-II», що входив до складу радіостанції, пізніше послужив основою для першої в Росії цивільної мережі приймних станцій серії «Всім-всім-всім». Напередодні Першої світової війни компанія налагодила випуск легких переносних ранцевих радіостанцій. У 1915 році розпочалося виробництво автомобільних польових іскрових радіостанцій. Тоді ж був організований випуск аеропланних радіостанцій і здійснені поставки прийомної апаратури для Царськосельської та Тверської радіостанцій.

Починаючи з 1910 року помітну конкуренцію іноземним радіотехнічним компаніям становить Російське товариство бездротових телеграфів і телефонів (скорочено російською – *«РОБТиТ»*). Ця вітчизняна компанія була утворена після реорганізації «Товариства бездротових телеграфів і телефонів системи Айзенштейна» (Санкт-Петербург). Семен Мойсейович Айзенштейн (1884-1962) з 1910 року був членом правління *«РОБТиТ»* і беззмінним директором свого заводу. У 1910 році тут була створена польова іскрова радіостанція, що містилася на 4 двоколках і забезпечувала зв'язок

на відстані 160,5 км. Діапазон хвиль передавача становив 400-2300 м, приймача – 320-2500 м. Антена – зонтичного типу. Висота телескопічної вежі – 25 м. Час розгортання станції – 30 хвилин. Аналогічна апаратура компанії Марконі вміщалася на 14 двоколках.

У 1912 році *«РОБТиТ»* була розроблена та випробувана легка портативна іскрова радіостанція для російської кавалерії «КСТ». Вона існувала у двох варіантах: в'ючному та двоколочному. Її характеристики: дальність дії – 60 км (в'ючна) і до 80 км (двоколочна), діапазон хвиль приймача – 200-1500 м, антена зонтичного типу, чотирипромінна з протидією, висота телескопічної щогли – 12 м (в'ючна) і 15 м (двоколочна). У наступному році компанія розпочала розробку автомобільних станцій *«АВ-1»* і *«АВ-3»*.

Перед початком Першої світової війни в російської армії було вже 7 окремих іскрових (радіотелеграфних) рот, оснащених станціями *«РОБТиТ»*. Аж до 1914 року завод діяв в умовах постійної конкуренції з фірмою «Сіменс і Гальске», що теж поставляла радіотелеграфні апарати для сухопутних військ російської армії.

У період 1910-1914 років Головному інженерному відомству Росії вдалося належним чином оснастити армію засобами радіозв'язку. До початку Першої світової війни російська армія відрізнялася досить високим ступенем насиченості радіоустановками: 17 стаціонарних, близько 100 польових і понад 30 легких кавалерійських радіостанцій. Однак у період воєнних дій армія зіштовхнулася з гострим недоліком у засобах радіозв'язку, і у 1917 році в Москві створюється «Електротехнічний завод Військового відомства». Але потужностей останнього вистачало тільки для часткового вирішення проблеми, і починаючи з 1915 року недолік зв'язної радіотехніки заповнювався поставками з Англії й Франції.

До речі, всі телеграфні сигнали, що передавалися іскровими радіостанціями під час Першої світової війни, легко перехоплювалися супротивником, тому що займали широкий частотний спектр. Та одного дня відбулося незрозуміле – усі німецькі радіостанції нібито раптово замовчали. Серед союзників Антанти вибухнула справжня паніка: «Мабуть, готується якийсь наступ і німці бояться витоку інформації!»

Таємницю такого «мовчання» розгадав російський вчений Михайло Васильович Шулейкін, який встановив, що німецькі радіостанції замість застосування іскрового розряду перейшли на передачу незатухаючих коливань на визначеній частоті, використовуючи ефект співаючої дуги (відкритий ірландським інженером Дуделєм, що, власне кажучи, першим у світі застосував у радіозв'язку коливальний контур).

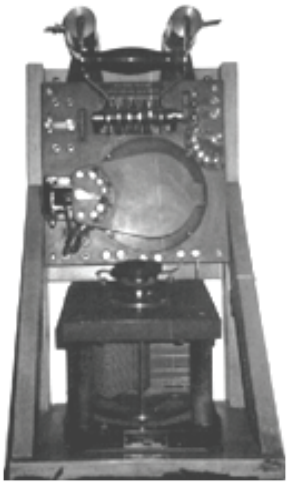
Крім того, до 1914 року система внутрішнього

радіозв'язку Росії не мала виходу в Західну Європу. Міжнародний зв'язок країни обслуговувався Північно-Датською та Індо-Європейською концесійними компаніями дротового телеграфу, які входили в мережу англійського світового кабельного зв'язку. Відмовитися від послуг іноземних компаній Росія не могла, тому що мала слабку науково-дослідну базу.

Тим часом підготовка до світової війни вимагала організації власного прямого міжнародного радіозв'язку з майбутніми союзниками. Однак фірма «Телефункен», власник контрольного пакета акцій АТ «Сіменс і Гальске», усіляко гальмувала будівництво передавальних радіостанцій, прагнучи до того, щоб до початку війни з Німеччиною Росія не мала потужних радіостанцій. Коли в перші місяці війни німці перерізали в Балтійському морі підводні телеграфні кабелі, що з'єднували Росію з країнами Заходу, було вирішено побудувати потужні іскрові радіостанції для зв'язку з «Антантою».

Поданням у Раду Міністрів від 14 серпня 1914 року військовий міністр Сухомлінов клопотав про спорудження 300-кіловатних радіостанцій у Москві на Ходинському полі та у Царському Селі під Санкт-Петербургом, а також окремої великої приймальної та малопотужної передавальних радіостанцій у Твері. Установку станцій передбачалося передати *«РОБТиТ»*. Для реалізації проекту Військового відомства «РОБТиТ» одержало від російського уряду 5 мільйонів рублів.

Вибір *«РОБТиТ»* обумовило те, що компанія мала досвід будівництва потужних іскрових радіостанцій: ще у 1913 році вона розробила, а у 1914 році побудувала на території свого заводу дослідний передавач іскрового типу потужністю 100 квт, що працював на хвилі 9300 м. У тому ж році був укладений контракт із Російським військовим відомством на виготовлення та встановлення 100-кіловатної іскрової радіостанції в м. Миколаєві Херсонської губернії. Згідно з відомостями міжвідомчого радіотехнічного комітету, до 1913 року одне тільки Військове відомство мало у своєму розпорядженні близько 20 стаціонарних радіостанцій, серед них близько половини були виготовлені заводом *«РОБТиТ»*.



Зацікавленість уряду в створенні потужних радіостанцій міжнародного радіозв'язку була настільки велика, що він погодився забезпечити перший платіж *«РОБТиТ»* у розмірі 1 мільйон 113 тисяч рублів. Крім власних радіотехнічних апаратів, пристроїв і приладів, *«РОБТиТ»* зобов'язаний був побудувати ціле містечко для розміщення в теплих будинках прийомної станції, машинного відділення, кочегарні, ремонтні майстерні, а також будинок для передавальної станції, агрегатне

відділення та 2 акумуляторні флігелі.

Вступ Росії у війну прискорив юридичне оформлення робіт. Уже в грудні 1914 року Московська радіостанція почала діяти. Радіостанції на Ходинському полі та Царському Селі були побудовані всього за 100 днів: Ходинська була введена в дію 7 грудня 1914 року, Царськосельська – 28 січня 1915 року, а Тверська – 11 листопада 1914 року.

Ходинська іскрова радіостанція мала потужність близько 100 квт і передавала інформацію на радіохвилях 7000, 9000 і 11000 метрів. Передавач Царськосельської радіостанції працював на хвилях 5000, 7000 і 900 метрів. Передавачі були пристосовані для роботи як ключем, так і машинним автоматом (трансмітер Уінстона). Автомати й інші прилади допускали швидкість передачі 70 слів у хвилину. У радіостанціях використалися системи зв'язку із розрядниками, що обертаються. По своїй конструкції вони були однотипними та на той період найпотужнішими в Європі.

Радіостанції цього типу дозволяли російському Генеральному штабу підтримувати зв'язок із союзниками зі складу Антанти, що перебували в Парижі, Корнарвоне (Уельс, Великобританія), а також Римом і Науеном (Nauen, місто в Німеччині). Відзначимо, що крім цих радіостанцій з липня 1914 року почала регулярну роботу з підтримки зв'язку із союзниками й заводська радіостанція *«РОБТиТ»*. Сюди для несення служби були направлені фахівці офіцерської електротехнічної школи. Спеціальна радіостанція у Твері, в основному, здійснювала прийом повідомлень закордонних радіоцентрів, у зв'язку з чим одержала назву «Тверська радіостанція міжнародних сполучень». Прийом радіоповідомлень здійснювався цілодобово протягом усього року в діапазоні хвиль від 400 до 10000 метрів.

Рознесення пунктів передачі й прийому радіограм один від одного мало на меті знизити вплив перешкод від роботи потужних іскрових передавачів при прийомі радіограм. Прийом далеких радіосигналів здійснювався за допомогою електронних підсилювачів на французьких радіолампах типу «Р» (лампа Пері) із прослуховуванням через телефонні навушники. При необхідності радіосигнали могли бути зафіксовані на телеграфну стрічку або записані на фонограф. Прийняті радіограми потім за допомогою апаратів Морзе передавалися в Москву й Царське Село.

Помічником начальника Тверської приймальної радіостанції був призначений М.А.Бонч-Бруєвич, який щойно закінчив Офіцерську електротехнічну школу в Санкт-Петербурзі.

На новому поприщі він одержав популярність завдяки тому, що організував невелику лабораторію з виготовлення радіоелектронних ламп для заміни дорогих французьких радіоламп із малим терміном служби.

Ходинська та Царськосельська радіостанції втілили в собі передові радіотехнічні ідеї іскрового способу передачі інформації. Для свого часу вони мали відмінні технічні характеристики, були надійні в роботі та мали чималий запас міцності. Ходинська радіостанція (як іскрова) проіснувала до 1922 року, після чого на ній установили інші типи передавачів.

25 листопада 1915 року Головне управління кораблебудування підписує контракт із *«РОБТиТ»* в особі С.М.Айзенштейна контракт на будівлю 25-кіловатної радіостанції Морського штабу в Петрограді, що одержала назву «Нова Голландія». У тому же році на озброєння флоту приймається двоконтурний приймач для корабельних і берегових радіостанцій, розроблений І.Г.Фрейманом і М.В.Шулейкіним у Радіотелеграфному депо Морського відомства.

Наближалася Лютнева революція 1917 року. Радіоефір імперії був заповнений екстреними повідомленнями, в основному від іскрових радіостанцій. Увечері 3 березня 1917 року по бездротовому іскровому телеграфу був переданий Маніфест імператора Миколи II про зречення від престолу, що відбулося 2 березня о 15 годині у Пскові. До цього всі головнокомандуючі арміями фронтів телеграфували імператору про необхідність відмовитися від престолу.

Цікаво, що командир кавалерійського корпуса генерал Федір Артурович (Августович) Келлер після оголошення маніфесту Миколи II про зречення, використовуючи іскрову радіостанцію Румунського фронту, послав цареві телеграму: «Третій кінний корпус не вірить, що Ти, Государ, добровільно відрікся від престолу. Накажи, ми прийдемо й захистимо Тебе». Через кілька годин прийшла відповідь. Щоправда, не від Миколи II. Командуючий Румунським фронтом наказував Келлеру здати кавалерійський корпус, інакше його оголосять бунтівником.

Через 6 місяців після «скинення» імператора Микола II, коли при владі вже перебував Тимчасовий уряд, 21 вересня закінчилося будівництво іскрової радіостанції «Нова Голландія». Тимчасовий уряд розумів важливу роль радіостанції. Під час Жовтневого перевороту 1917 року «Нова Голландія» була захоплена більшовиками. У той же день радіостанція передала повідомлення про «падіння» Тимчасового уряду та прихід до влади «більшовиків». Через декілька днів були захоплені й інші потужні іскрові радіостанції, у тому числі Царськосельська та Ходинська в Москві.

«Нова Голландія» стала радіостанцією не тільки революційного флоту, але й Радянського уряду. У ніч на 9 листопада 1917 року сюди приїхав вождь «більшовиків» В.І.Ленін із членами уряду, і звідси була передана написана ним відозва «Радіо всім» із закликом до армійських й інших комітетів, солдатам і матросам

взяти у свої руки справу укладення миру з Німеччиною.

Радянський уряд проявляв більшу турботу про забезпечення засобами зв'язку Робітничо-Селянської Червоної Армії й флоту (далі – РСЧА). Вже у 1918 році у складі стрілецьких дивізій формуються батальйони зв'язку, у кавалерійських, артилерійських й інших частинах створюються підрозділи та команди зв'язку. У 1919 році було створене Управління зв'язку РСЧА. Для підготовки кадрів і формування нових підрозділів радіозв'язку влітку того ж року були створені 3 бази радіотелеграфних формувань РСЧА у Володимирі, Твері й Казані.

Начальником 2-ої Казанської бази радіотелеграфних формувань (далі – база) був призначений Олександр Тихонович Углов. Добре технічно оснащений радіокабінет дозволив йому проводити численні досвіди із створеним радіотелефоном. Радіотелефон був виготовлений на радіотелеграфному заводі морського відомства й на початку жовтня 1917 року випробовувався на кораблях Балтійського флоту. При цьому була досягнута дальність зв'язку 25 верст.

Базі був переданий особовий склад і майно колишнього запасного електротехнічного батальйону навчально-запасної військової частини, що постачала в Першу світову війну російську армію радіотелеграфними приладами й фахівцями. Надалі база зіграла значну роль у розвитку вітчизняної радіотехніки. Там була лабораторія з навчально-дослідною радіостанцією, радіошкола, що випускала слухачів-радіотелеграфістів, майстерні для ремонту й зборки радіостанцій.

Крім того, база проводила велику дослідну й конструкторську роботу та незабаром одержала популярність як один із творчих центрів СРСР у сфері радіотехніки. Тут були проведені досліди, що поклали в країні початок передаванню звуків по проводах. Вони розпочалися з 1918 року, і за системою Углова було виготовлено декілька передавачів. У 1920 році розгорнулися великі роботи щодо збільшення дальності розмови по провідному телефону. Хоча розвиток техніки та виробництво радіопередавачів надалі пішов іншим шляхом – шляхом створення спеціальних генераторних ламп (Нижегородська радіолабораторія наркома пошт і телеграфів М.А.Бонч-Брує вича), роботи Казанської бази мали велике значення, тому що там були зроблені перші кроки в сфері радіотелефонії.

Радіотелефон системи Углова, встановлений на літак, дозволяв досягти радіуса дії 65 км. У 1920 році були надруковані праці співробітників бази. Радіоінженер Олександр Тихонович Углов в одній зі статей писав: «...досліди на радіотелефонії, проведені мною у 2-ій радіобазі, є продовженням дослідів по телефонуванню за допомогою підсилювальних ламп, що вироблялися в 1916-1917 роках у офіцерській електротехнічній школі в Петрограді та в 1919 році у Військовій радіотехнічній лабораторії в Москві. Також проводилося випробування іскрових радіостанцій конструкції Углова, що працювали на ходу потяга. Дальність дії цих радіостанцій досягала до 400 км».

Для РСЧА базою було розроблено та виготовлено 10 радіопеленгаторних станцій. Ці станції давали можливість виявити радіостанції супротивника на відстані 600 км. У 1920 році там же були розроблені та виготовлені й підсилювачі низької частоти. До виходу такого підсилювача підключили форпостний телефон, в результаті чого була отримана велика гучність звуку. Співробітники бази зробили розтруб (рупор), виставили цей телефон на балкон лабораторії та стали читати газетні повідомлення: вся площа наповнилася звуками. Вільно можна було розуміти мову на відстані до півкілометра від рупора. З цього моменту з балкона бази регулярно передавали політінформацію та музику. На честь першотравневих свят 1921 року рупори були встановлені на декількох площах Казані.

Уряд високо оцінив працю військових фахівців – 7 травня 1921 року про це повідомляли радянські газети «Правда» й «Вісті». 1 листопада того ж року була затверджена постанова про преміювання першої російської схеми бездротового телефону на далекі відстані та виплату Углову і його співробітникам значної премії – 31 мільйон рублів.

Крім того, треба відзначити, що 5 травня 1908 року був одержаний патент на систему передачі двоколірного зображення по дротах російським вченим Ованесом Абгаровичем Адамяном. Він вирішив застосувати до фотографії також і винахід радіо. У жовтні 1921 року Адамян виступив на VIII Всеросійському електротехнічному з'їзді з доповіддю про передачу фотографічних зображень на відстань. За свої винаходи в цій сфері він був визнаний гідним нагороди Вищої Ради Народного Господарства СРСР. А 30 червня 1930 року він здійснив прийом першої фоторадіограми за своєю схемою між Москвою і Ленінградом.

3.10. Військова криптологія

Впродовж всього XVIII ст. і першої половини XIX ст. криптослужба МЗС окрім дипломатичних і інших шифрів розробляла шифри і для військового відомства. У другій половині XIX ст. «цифирная» експедиція МЗС, також певною мірою забезпечувала це відомство шифрами, проте вже з кінця 1840-х років у Головному штабі військового міністерства була організована та почала працювати власна *«цифирная»* експедиція.

Шифри, що створювалися тут, затверджувалися військовим міністром. Екземплярами військових шифрів забезпечувалися старші начальники військ і військових управлінь, поіменовані в особливому списку. У цей список входили імператор і члени імператорської родини, котрі займали важливі військові пости, військовий міністр, начальники головних управлінь військового міністерства, командувачі військами в округах, начальники штабів округів, командири корпусів, коменданти фортець, отамани й ін.

Природно, що шифроване листування по лінії військового міністерства ве-

лося не тільки у військовий період, але і в мирний час. Зашифровувалися повідомлення, що стосуються мобілізаційної і військової підготовки, а також готовності армій і фортець до військових дій і деякі інші відомості.

У військовий час із *«цифирной»* експедиції МЗС у Військове міністерство поступали примірники тих шифрів, які діяли в мережах загального зв'язку, куди через політичні, військові або інші причини могли входити дипломатичні представники Росії за кордоном, командувачі арміями, військово-морськими силами й інші особи.

У другій половині XIX ст. більшістю шифрів військового міністерства були коди малого (до 1000 словарних величин) обсягу. Кодовими позначеннями тут були три- і чотиризначні числа. Військові шифри цього типу зазвичай використовувалися протягом тривалого часу, перероблявся лише відносно швидко старіючий словник, що пояснюється, наприклад, зміною географії військових дій тощо. Коди з перешифруванням, створені у 1860-х роках, використовувалися ще на початку XX ст.

Прикладом шифру, який використовувався під час Кримської війни, був російський словниковий ключ № 299 на 600 величин, який був введений в дію у квітні 1854 року. Призначався він для зв'язку командирів частин Дунайської армії. Після війни цей шифр продовжував використовуватися. У 1891 році ним були забезпечені Бухара, Кашгар, Кульджа, Сеул, Пекін, Токіо, Іркутськ, Омськ, Ташкент, Хабаровськ, Урга, Чугучак і Владивосток. З дії його вивели тільки у 1901 році.

Побудована система телеграфного зв'язку була небезуспішно застосована вже в ході російсько-турецької війни (1877-1878). Під час цієї війни в російській армії застосовувався французький біклавний ключ № 348, введений у дію в 1870 році, російський біграмний ключ № 361, складений у 1876 році, та деякі інші шифри.

Ключ № 361 мав 992 шифровеличин – 28 букв спрощеного російського алфавіту, 3 розділові знаки, а також деякі їхні біграмні сполучення. Їм відповідали 3-значні кодові позначення. Цей шифр був спочатку надісланий у консульства на Сході, а також у Тифліс і Одесу. Французький ключ № 348 використовувався на європейських лініях.

Під час російсько-турецької війни обидва шифри знаходилися в діючій армії. Їхні примірники були в генерала Ігнатьєва і генерала Фредерікса. Використовувалися ці шифри й після війни: французький ключ – до 1891 року, а російський – до 1903 року.

Під час російсько-японської війни (1904-1905) застосовувався російський словниковий ключ № 349, який був введений у дію в 1868 році на лініях зв'язку Міністерства фінансів для телеграфного шифролистування. У 1879 році він був

виведений з дії внаслідок утрати двох примірників. Але у 1901 році він знову був введений в дію для шифрозв'язку Міністерства фінансів із митницями. Крім того, цей шифр був введений в дію у 1900 році в Міністерстві державного майна, а у 1902 році – у Порт-Артурі, Харбіні, Мукдені і, нарешті, у 1904 році – в діючій армії.

«Словникові ключі» були найбільш поширеним типом шифрів, використовуваних наприкінці XIX ст. у військовому відомстві. Їх так і називали «військовими ключами». Маючи універсальні принципи побудови, шифри військового міністерства кінця XIX – початку XX ст. відрізнялися один від одного деякими особливостями. Розглянемо деякі з них:

1. Ключ військового міністерства № 6 1906 року. Був тризначним багатоваріантним цифровим кодом з маскуванням і прихованим початком повідомлення. Обсяг складав 1000 словарних величин. Останніми були слова, склади, букви російського алфавіту. Всім буквам і найбільшим словам, що часто зустрічалися, були додані по два і більше кодових позначень, решта словникових величин мала по одному кодовому позначенню. У правила, крім того, була введена одна обов'язкова вимога: якщо в тексті телеграми траплялися одні й ті ж слова, то їх слід було набирати різними способами, уникаючи повторень кодових позначень. Окремо були дані перешифувальні цифрові таблиці.

У правила була також введена обов'язкова вимога ховати початок повідомлення. З цією метою цифровий шифрований текст розбивався справа наліво (з кінця криптограми) на групи по 5 цифр кожна. У першій з кінця групі залишалися 4 цифри. 5-значні групи на листі відділялися одна від одної за допомогою тире. Якщо в останній групі, відповідній початку відкритого повідомлення, виявлялося менше 5 цифр, то шифрувальник додавав необхідне число довільних цифр. Кількість довільно доданих цифр вказувалася числом, яке ставилося в самому кінці цифрового набору, перетворюючи групу, раніше 4-значну, у 5-значну. Якщо на початку телеграми довільних цифр ставити було не потрібно, то в кінці останньої групи ставився 0.

У шифрі було передбачене маскування: у кожній 5-значній групі криптограми необхідно було перемістити 2-у і 4-у цифри одну на місце іншої, залишивши без змін 1-у, 3-у і 5-у цифри. В результаті цього маскування переміщалися цифри, що належали одній і тій же або різним 3-значним кодовим групам. Тим самим порушувалися порядкові (алфавітні) зв'язки, якщо код був алфавітним або містив якісь частини «з погано перемішаними», невипадковими кодовими позначеннями.

Вказані ускладнення не можна трактувати як перешифрування кодів, але як маскувальні заходи вони, природно, могли істотно ускладнити дії супротивника з дешифрування цих систем.

Звичайно, коли дешифрувальнику ставали відомими всі ці ускладнення, він легко від них позбавлявся, здійснюючи зворотні процедури перестановки знаків і визначаючи початок повідомлення по останній цифрі криптограми.

Отриманий номер проставлявся в кінці телеграми, причому він набирався буквами. Якщо телеграма була відповіддю на раніше отриману, то номер останньої проставлявся цифрами на початку даної.

З огляду на те, що іноді зашифровувався не весь текст телеграми, а окремі його частини, то в криптограмі цифровий текст міг перемежатися з текстом відкритим. При цьому кожна шифрована його частина оформлялася в групи з 5-значних цифр всякий раз як самостійна телеграма. Вказані правила користування шифром були підписані начальником відділу Генерального штабу генерал-майором Марковим і начальником «цифирного» відділення полковником Лео.

2. Ключ військового міністерства № 7 1905 року. Був алфавітним 3-значним цифровим кодом на 900 словникових величин, розміщених на 18 таблицях 5х10. При цьому перша цифра цього коду мінялася за ключем відповідно до показника (марканта) так званої малої таблиці.

При наборі повідомлень цим шифром вважалося за необхідне міняти показники і відповідні їм табличні цифри через довільну кількість букв, складів і слів. Проте визнавалося бажаним, щоб ця зміна проводилася не рідше, ніж через 13 набраних кодових позначень.

Якщо в тексті телеграми повторювалися одні й ті ж слова, то вони обов'язково набиралися кожного разу різним способом, уникаючи повторень одних і тих же кодових позначень. Решта всіх правил шифрування цим шифром були стандартними.

Після закінчення набору весь цифровий текст ділився зліва направо на 5-значні групи. При цьому перша група була 4-значною, а в кінці додавалася при необхідності потрібна кількість довільних цифр, щоб остання група шифротексту була обов'язково 5-значною. Число це ставилося на початку першої групи, перетворюючи її на 5-значну.

Перед відправленням шифротелеграми обов'язково перевірялася правильність її зашифрування шляхом розшифрування.

Особливістю побудови словникових величин у цьому шифрі було те, що різні частини мови могли поміщатися за одним і тим же кодовим позначенням, наприклад: возбу, д, жд; возвра, т, щ.

Ось список осіб, які користувалися в своєму листуванні цим ключем і мали його примірники: імператор, його імператорське превосходительство генерал-фельдцехмейстер, його імператорське превосходительство головнокомандувач військами гвардії і Петербурзького військового округу, військовий міністр, командувач Імператорською головною квартирою, начальник Генерального штабу, начальник Головного штабу, начальник канцелярії Військового міністерства,

товариш генерал-фельдцехмейстера, товариш генерал-інспектора з інженерної частини, головний інтендант, начальник Головного управління козачих військ, головний військово-медичний інспектор, командувачі військами в округах, начальник Варшавського укріпрайону, начальники штабів округів, командири корпусів, командири фортець, начальники кавалерійських і піхотних дивізій і стрілецьких бригад, військові отамани козацьких військ, морський міністр, начальник Головного морського штабу, начальники ескадр, військово-морські агенти.

3. Буквений ключ військового міністерства литер «В». У 1910 році був таблицею 30х30, в кожному рядку якої в довільному порядку були розписані всі букви алфавіту. У верхньому рядку і крайньому лівому стовпці був записаний алфавіт. Таким чином, кожна координата таблиці (кожен знак) визначався двома знаками алфавіту.

Шифрування здійснювалося таким чином: вибиралася показова група (показник) – слово або набір слів з кількістю знаків не менше 10 (наприклад, «Закарпаття»). Цей показник писався перед шифрованим повідомленням. Далі розписувався текст повідомлення, а над кожним знаком цього повідомлення – знак показової групи; показова група повторювалася стільки разів, скільки була довжина повідомлення:

показова група – ЗАКАРПАТТЯЗАКАРПАТТЯЗАКАР…

текст повідомлення – ЛИСТУВАННЯАБОЗНЯТТЯКОПІЙЗ…

Шифрознак знаходився на перетині стовпця з номером «З» і рядка з номером «Л». Таким чином, даний шифр – табличний шифр заміни, що складався з 30 простих замін, причому інформація про те, якій заміні належить той або інший шифрознак, відома. Очевидно, що стійкість такого шифру мінімальна.

Як показову групу можна було використовувати і нешифровану частину повідомлення, якщо така була в тексті.

4. Шифр військ гвардії і Петербурзького військового округу 1911 року. Складався зі 100 словникових величин – букв, цифр, складів і словосполучень. Кодовими позначеннями були двозначні числа. Був оформлений у вигляді таблиці, на якій було розташовано 10 таких кодів з однією і тією ж словниковою основою.

Користувалися цим ключем таким чином. Перед шифруванням кореспондент вибирав номер коду (ключа), ставив його на початку повідомлення і шифрував за цим кодом 10-13 словникових величин. Далі він переходив до іншого ключа і шифрував наступні 10-13 словникових величин. У цьому достатньо простому коді звертає на себе увагу знайдена зручна форма шифру, що дозволяла порівняно просто і швидко здійснювати процес шифрування.

5. Шифри імператора Миколи II.

Перший із них, шифр 1911 року, був невеликою витягнутою завширшки

книжкою розміром 14,5х21 см у дуже красивій смарагдово-зеленій муаровій палітурці. На обкладинці золотом був витиснений герб Росії – двоголовий орел і напис золотими літерами: *«Ключ Военного министерства. Лит. М».* Зберігався цей шифр у спеціальному шкіряному футлярі-гаманці.

Ключ складався з 10 кодових таблиць набору і стількох же таблиць розбору за № 0-9. У таблиці набору були поміщені всі букви алфавіту (крім Ъ і О) і цифри від 0 до 9. Крім того, в таблиці були включені найбільш вживані склади. Кодовими позначеннями були двозначні числа від 00 до 99, додані словниковим величинам у кожній із десяти таблиць в довільному порядку (тобто код був неалфавітним). Таким чином, код складався з 10 самостійних кодових таблиць, обсягом у 99 величин кожна.

При шифруванні користувалися одночасно всіма 10 таблицями. Для визначення номера використовуваної таблиці служив особливий показник (шифрувальний ключ), що складався з 5 цифр, який встановлювався особливим розпорядженням начальника Головного штабу на певний термін. Номери таблиць були винесені на клапани.

При наборі під всіма належними зашифруванню буквами, цифрами або наявними в таблицях складами шифрованого тексту послідовно писалися цифри показника. Цифра показника над буквою, складом або цифрою тексту позначала номер таблиці набору, з якої слід було брати відповідні кодові позначення. Оскільки показник мав довжину 5, то через кожних 5 знаків для шифрування використовувалася одна і та ж таблиця.

Знайдені в таблицях кодові позначення підписувалися під цими буквами, цифрами або складами в такому порядку, щоб цифра, яка позначала одиниці в кожному двозначному кодовому позначенні, доводилася під цифрою десятків (наприклад, кодові позначення 31 або 05 писалися: 3/5 або 0/5).

При закінченні набору всі ці позначення (стовпці) розбивалися на групи по 5 стовпців і писалися в наступному порядку, розділяючись група від групи межею: спочатку по порядку, рахуючи зліва направо, всі групи з верхніх цифр (що позначали десятки), а потім у такому ж порядку і відділяючись такою ж межею, групи з нижніх цифр (одиниці).

Якщо в останній групі опинялося менше 5 стовпців, але більше 2-х (наприклад, 460 391), то останнє позначення повторювалося для поповнення групи до 5 стовпців (46000/39111). Якщо ж таких позначень залишалося 1 або 2 (наприклад, 5/2 або 68/93), то їх слід було писати в один рядок і групу доповнити до 5 цифр повторенням останньої (наприклад, 5/2 писати 52222, в другому випадку 68/93 – 68933).

Крім Миколи II, примірники цього шифру були у трьох великих князів, військового міністра, начальника Генерального штабу, начальника Головного штабу,

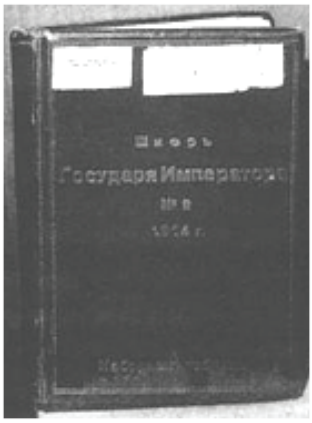
начальників канцелярії і законодавчого відділу військового міністерства, у начальників головних військових управлінь, командувачів військами в округах, начальників окружних штабів, корпусів, фортець, дивізій, бригад, у Голови Ради міністрів, міністра внутрішніх справ, міністра закордонних справ і деяких інших осіб. Всього у списку осіб, що володіли примірниками цього шифру, значилося 76 осіб.

Описаний вище показник повідомлявся особливим листом, у тому числі і до імператора, начальником Головного штабу.

Другий шифр Миколи II – «Особливий шифр № 1-й Государя Імператора». Був кодом з перешифруванням. Перешифрування являло собою двозначну гаму, яка періодично мінялася після кожних 19 знаків за лінійним законом. Це перешифрування також можна класифікувати як маскування, оскільки воно легко знімалося, як тільки дешифрувальник отримував інформацію про процес її отримання (з дати посилки телеграми). Як і попередній, цей код складався з самостійних кодових таблиць (їх було вже 13), що містили по 99 словарних величин (букв, складів, цифр) кожна.

Користуватися цим шифром так. Слова тексту, які підлягали набору, розбивалися зліва направо на групи по 19 букв кожна, в останній групі букв могло бути менше. На початку кожної групи ставилася межа. Для набору довільно вибиралася одна з 13 набірних таблиць і її номер ставився на початку першої 19-буквеної групи над межею. При наборі кожної букви першої 19-буквеної групи до кожного числа, що мало відповідне кодове позначення, додавалося одне і те ж число, що називалося «ключ телеграми». Цей ключ визначався з числа і місяця, які писалися на початку тексту телеграми. Щоб визначити ключ даної телеграми, слід було скласти число дня з числом, якому відповідав місяць.

Так, наприклад, якщо телеграма починалася словами: «дванадцятого серпня...», то число дня буде «12», а місяця – «8» і, отже, ключ телеграми: 12 + 8, тобто 20. Якщо при складанні виходило однозначне число (наприклад, 5 лютого), то до нього слід було приписати 0.



Дійшовши до наступної, другої 19-буквеної групи, шифрувальник міняв набірну таблицю, не дотримуючи при цьому ніякої послідовності. Номер нової таблиці ставився над межею. За цією таблицею набиралися 19 букв другої групи. Перед кожною наступною 19-буквеною групою також мінялася таблиця. При цьому до чисел, що відповідали по таблиці буквам, що набиралися, додавався ключ телеграми, зменшений для другої групи на одиницю, для третьої – на два, для

четвертої – на три тощо.

Такий зменшений ключ телеграми називався «Ключем групи». Коли ключ групи такими послідовними відніманнями доходив до наступної за шифрованою з ключем групи, рівної 1, 19-буквена група шифрувалася з ключем, збільшеним на 1, тобто 1, рівним 2, потім – 3 і так далі до числа, що відповідало первинному ключу телеграми. Від нього ключ групи знову послідовно зменшувався до одиниці тощо.

Для відправлення по телеграфу перешифрований таким чином текст шифротелеграми розбивався на 5-значні цифрові групи. Оскільки в кожній 19-буквеній групі двозначних чисел попереду ставилося двозначне число, що позначало номер таблиці, то кожна з цих груп складалася з 40 цифр. При розбитті їх на 5-значні групи виходило 8 таких груп, що дуже полегшувало перевірку тексту криптограми.

Зберігся і ще один шифр, яким користувався Микола II. Це різнозначний код обсягом 10 000 словникових величин. Складався він з двох книг, перша з яких включала «Набірні таблиці», а друга – «Розбірні таблиці». Зовні кожна книга була оформлена як досить об'ємний том розміром 16,5х22 см у вишневій муаровій палітурці з золотим тисненням.

У словнику коду було декілька типів словникових величин, кожному з яких були додані кодові позначення різної значності. Так, на задній кришці палітурки був наклеєний спеціальний аркуш, на якому були надруковані відмінкові та дієслівні закінчення. Ця категорія словникових величин мала однозначні кодові позначення.

Таблиці чисел, дні місяців, імена членів імператорської родини, найважливіші міста світу мали кодові позначення від 000 до 999. Основна маса словникових величин, що була буквами, складами, словами, словосполученнями, мала 4-значні кодові позначення від 0000 до 9999. Остання по порядку тисяча таких кодових позначень (від 9000 до 9999) позначала губернські та повітові міста Росії.

Всі словникові величини були розташовані на аркушах коду у 2 стовпці по 50 величин на сторінці. Цифри, що позначали тисячі і сотні були розміщені у верхніх кутах сторінок (00-99). Важливо відзначити, що використання в кодових величинах одного коду кодових позначень неоднакової довжини, як це мало місце в даному випадку, істотно ускладнювало дешифрування.

Миколі II доповідали щодо всіх питань, що стосувалися використання імператорських шифрів. Ось доповідь військового міністра, представлена Миколі II 15 липня 1906 року: *«В[есьма] секретно. Всеподданейше представляю при сем Вашему Императорскому Величеству экземпляр № 1 изменений порядка набора и разбора телеграмм по шестому ключу Военного министерства,*

вводимых в действие с 25-го сего июля, причем начальству военных округов указано, что при сношениях с центральными управлениями министерств эти изменения должны быть применяемы немедленно по получении их на местах...».

Тут же рукою військового міністра написана резолюція царя: *«Высочайше повелеваю экземпляр № 1 изменений порядка набора и разбора телеграмм по шестому ключу Военного министерства передать в Военно-Походную Его Императорского Величества канцелярию».*

Наскільки детально інформувався Микола II з питань використання шифрів, можна побачити і з доповіді царя, складеної військовим міністром 9 серпня 1906 року, в якій, зокрема, мовиться: *«Седьмой ключ Военного министерства военного времени входит повсеместно в действие с 10-го сентября сего года... но до 10-го сентября следует в начале телеграммы ставить пятизначную группу «31475»...».*

Примірники шифрів, що належали царю, знаходилися завжди в місці його перебування та містилися в канцелярії Міністерства імператорського двору, в Імператорській головній квартирі, а у військовий час у військово-похідній Його Імператорської Величності канцелярії.

У військовому відомстві суворо дотримувалися правил користування шифрами та їх зберігання. Правила наказували при втраті хоча б одного примірника шифру негайно виводити його з використання та замінювати новим. Така ж заміна повинна була проводитися при підозрі, що таємниця шифру супротивником відкрита.

Зняття копій з шифрів категорично заборонялося, а тому у військовий час польові штаби армій, окремих корпусів і окремо діючих загонів забезпечувалися запасними примірниками шифрів для видачі їх в необхідних випадках тим особам, яких не було у списку, згаданому вище, але яким, на думку командувачів арміями або інших головних військових начальників, слід було мати той або інший шифр.

Примірники ключів військового часу, видані командувачам військами в округах, командирам корпусів, комендантам фортець і наказним отаманам, хоча і знаходилися в безпосередньому розпорядженні цих осіб, повинні були зберігатися в приміщенні відповідних штабів у замкнутих секретних сховищах і обов'язково в особливо секретних пакетах, запечатаних особистою печаткою тих осіб, кому вони були видані. Так само суворо зберігали примірники шифрів (ключів) і начальники головних управлінь військового міністерства і начальники штабів округів. Заміну старих примірників шифрів, передачу шифрів від осіб, що звільнялися, тощо проводив Головний штаб. Там же визначався термін дії шифрів.

З метою збереження шифрів у таємниці інструкціями було наказано у жодному випадку не залишати у справах документи, зашифровані шифром. Особи,

що користувалися шифром, зобов'язані були поміщати в справи копії відправлених шифроповідомлень, але викладені *«простым письмом»*. Чернетки знищувалися. Особа, яка отримала шифроповідомлення, також була зобов'язана знищити оригінал, помістивши в справу вхідних документів відповідну копію, викладену *«простым письмом»*. Перевірка шифрів військового часу, що знаходилися в окрузі, в армії тощо, проводилася не рідше одного разу на рік.

Для воєнного часу військове відомство мало спеціальні шифри для військових з'єднань. Але в них були численні недоліки. Це були досить складні шифригасла подвійної вертикальної перестановки за двома номерними рядами – розподільниками з частою зміною ключів.

На жаль, в організації шифрозв'язку в діючій армії були серйозні недоліки. Якщо повідомлення в оточений японцями Порт-Артур, що посилалися з фельд'єгерями, шифрували, то по телеграфу інформація досить часто передавалася у відкритому вигляді. При цьому вже у 1904 році японські спецслужби вперше в історії радіотехнічної розвідки реалізували на практиці схему дистанційного «знімання» інформації з телеграфного кабелю.

У російській пресі лише у 1915 року була оприлюднена інформація про те, що під час бойових дій у період російсько-японської війни були випадки перехоплення телеграфних повідомлень, якими обмінювалася Ставка Головнокомандувача та війська. Під час війни дротовий телеграф, особливо апарати Юза, російське командування помилково вважало абсолютно надійними для передачі таємних телеграм у незашифрованому вигляді.

Досвід російсько-японської війни показав, що в умовах бойової обстановки неможливо забезпечити стійке керування військами без покращення роботи штабів за рахунок застосування всього комплексу засобів зв'язку. Найважливішим засобом зв'язку в стратегічній і оперативній ланках у цій війні став телеграф. Традиційно використовувався для організації документального шифрованого зв'язку Фельд'єгерський корпус. Цілком виправдали себе телефон і радіозв'язок як засоби керування збройними силами.

На жаль, російське військове керівництво виявилося неспроможним використати цей досвід у Першій світові війні та забезпечити усіма видами зв'язку російські армії під час ведення бойових дій на Західному фронті. Після початку війни російські плани ведення військової кампанії проти Німеччини передбачали вторгнення двох армій на територію Східної Пруссії.

Армія під командуванням генерала Ренненкампфа повинна була вести наступ у західному напрямку та своїми бойовими діями скувати німців. Перед арміею генерала Самсонова, що розташовувалася південніше, було поставлене завдання обійти Мазурські болота, вийти в тил німцям і, блокувавши шляхи відходу, знищити їх. Зрозуміло, що успішне вирішення цього завдання залежало від

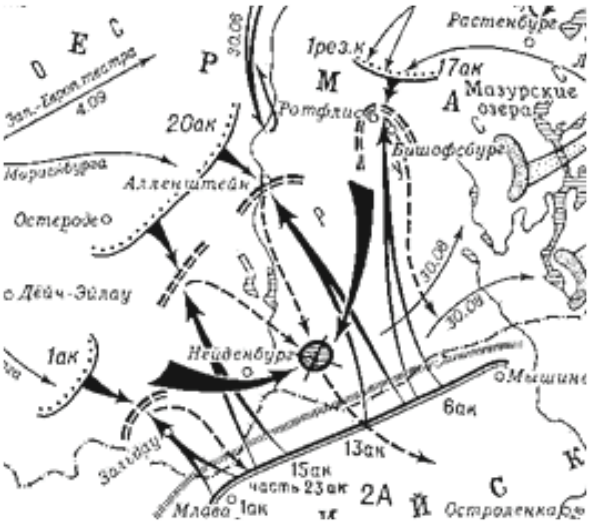
погодженої ретельної взаємодії двох російських армій.

На жаль, начальник армійського шифрувального бюро полковник Андреєв аж до початку бойових дій утримувався від розсилання копій нового шифру, призначеного для використання в період війни. Цей запобіжний захід призвів до сумних наслідків.

Коли армії Ренненкампфа та Самсонова виявилися розділеними Мазурськими болотами і стали здійснювати зв'язок один з одним в основному по радіо, з'ясувалося, що в армії Ренненкампфа новий шифр одержали, а старий знищили, у той час, як у Самсонова залишався старий шифр, оскільки нового не було. У результаті переговори між ними якийсь час велися по радіо у відкритому режимі.

До цього треба додати, що і матеріальне забезпечення російських армій було налагоджено погано. У розпорядженні армії Самсонова знаходилося не набагато більше 600 кілометрів проводу, що був незабаром витрачений. Таке незадовільне забезпечення дуже відрізнялося від постачання Збройних сил, наприклад, Англії і Франції, що на Західному фронті щодня витрачали дроту майже в 10 разів більше.

У той же час засоби радіозв'язку використовувалися тільки в штабах обох російських армій і в штабах підлеглих їм корпусів. Штаби дивізій і штаби більш низької ланки радіозв'язку не мали зовсім. Тому штаби корпусів для зв'язку з дивізіями були змушені використовувати проводові засоби. А штаби армій у свою чергу витратили мізерні запаси дроту для зв'язку з тиловим командуванням. У результаті радіо залишилося єдиним засобом зв'язку між штабами корпусів і армій.



Тому зміст їх радіоповідомлень не був таємницею для супротивника. Загальна неефективність проведеної Росією мобілізації негативно вплинула й на доведення до військ нових шифрів і ключів до них. Наприклад, 13-ий корпус армії Самсонова не мав ключів для читання криптограм, що надходили від його сусіда,

6-го корпуса. Тому через два тижні після початку війни російські зв'язківці, навіть, не намагалися шифрувати свої повідомлення, а передавали їх по радіо відкритим текстом.

Східна Пруссія вже в той час у буквальному значенні слова була обплутана телефонними дротами. З будь-якої ферми німці могли доповідати про просування російських армій прямо у свої штаби. Російська військова розвідка виявляла заховані телефони супротивника в льохах і, навіть, у бджолиних вуликах. Під час відсутності достатніх запасів телефонного дроту командування російських військ намагалося вести переговори по телефону з квартир місцевих жителів, що аж ніяк не сприяло збереженню таємниці змісту цих переговорів.

У відповідності зі стратегічними планами командування армія Ренненкампфа 17 серпня 1914 року почала просування вглиб Східної Пруссії. Для її оборони німці залишили тільки одну армію, тому що в їхні стратегічні плани входив у першу чергу швидкий розгром Франції. Ця німецька армія не поступалася жодній із двох армій росіян, але була слабшою, ніж їхні об'єднані сили, і тому німецьким Генеральним штабом передбачалося почергово завдавати ударів по російських арміях.

Після бою з Ренненкампфом при Гумбінені німці залишили свої позиції і почали поспішний відхід. Їм удалося зупинитися тільки тоді, коли вони уже відійшли на 30 кілометрів. Усе-таки німецькі війська до деякої міри «пошарпали» армію Ренненкампфа, і той, замість розвинути успіх, на певний час зупинив наступ.

Переляканий німецький командувач уже був готовий залишити межі Східної Пруссії. Про свої наміри він доповів Верховному головнокомандуванню, яке в результаті почало підшукувати йому заміну. Але його талановитий начальник штабу М.Гофман повідомив, що армія Самсонова дуже далеко вклинилася на територію Пруссії, і переконав свого шефа в необхідності завдати удару саме по цьому флангу російських військ. Він запропонував зняти з фронту два німецькі корпуси, що діяли проти Ренненкампфа, перекинути їх по відмінних залізницях Німеччини на південний напрямок і завдати раптового удару по південному угрупованню під командуванням Самсонова.

Перевезення вже почалися, коли прибув новий командуючий німецькими військами Гінденбург і його начальник штабу Людендорф. Вони залишили план операції без змін. У північній частині лінії фронту Людендорф поставив кавалерійський заслін для прикриття відходу військ із займаних позицій та спостереження за військами Ренненкампфа. Розпилення сил було порушенням стратегічної військової доктрини Німеччини, в основу якої був покладений принцип їхньої концентрації. Коли 24 серпня в німецькому штабі йшло обговорення всіх плюсів і мінусів варіанта Гофмана, мотоцикліст привіз дві перехоплені російські радіограми. Вони були надіслані начальником радіостанції фортеці Кенігсберг.

Підпорядковані йому оператори, у яких було мало документів для передачі, щоб якось розважитися, стали прослухувати роботу російських радіостанцій.

Обидві радіограми надійшли від штабу 13-го корпуса армії генерала Самсонова та були передані відкритим текстом, тому що штаб цього корпуса усе ще не одержав відповідні ключі до шифрів. У них точно вказувалися пункти призначення частин корпуса, очікуваний час їхнього прибуття та плани дій. Ці дані цілком збіглися зі змістом директиви, виявленої напередодні в сумці убитого російського офіцера. Однак перехоплені повідомлення не дали головного – інформації про наміри Ренненкампфа. Але, незважаючи на це, Людендорф вирішив, що при наявності таких даних, заради досягнення повної перемоги над Самсоновим, необхідно піти на ризик. Був відданий наказ про передислокацію інших німецьких військ.

Наступного ранку після наради в німців з'явився документ, що поклав кінець сумнівам Гінденбурга і Людендорфа. Це була перехоплена радіограма, яку Ренненкампф передав відкритим текстом своєму 4-му корпусу. У ній, зокрема, було сказано, що його армія буде продовжувати наступ, і позначався рубіж, на який вона збиралася вийти. Німцям стало зрозуміло, що Ренненкампф мав намір і далі просуватися вперед «черепашачим» кроком.

Поспішний відхід німців, сліди якого знайшов генерал Ренненкампф, коли неквапливо проїжджав через залишені ними позиції, зайвий раз утвердив його в помилковій думці про загальний відступ німецьких військ після Гумбінена. Він не мав наміру робити на німців сильний тиск, тому що боявся відкинути їх зі Східної Пруссії раніше, ніж Самсонов зможе їх розбити.

Німці, у свою чергу, відразу ж зробили висновок про те, що Ренненкампф вчасно не вийде ні на один з рубежів, щоб завдати удару по тилах німецьких військ раніше передбачуваного розгрому Самсонова. Одержавши перепочинок, вони вирішили кинути усі свої сили проти армії Самсонова.

Того ж ранку зв'язківець вручив Гофману ще одну перехоплену радіограму, також передану відкритим текстом. Самсонов відправив її о шостій ранку нещасливому 13-му корпусу, у якого не було шифру. У ній давалася повна характеристика становища з докладним описом наступних дій військ армії Самсонова. Рівного цьому прецеденту не було у всій військовій історії.

При розробці своїх планів німці врахували слабкості в розташуванні російських військ. Генеральний бій почався 26 серпня 1914 року, а до 30 серпня німецькі війська взяли росіян у залізне кільце, з якого змогли вийти тільки дві тисячі осіб. Армія Самсонова перестала існувати. Загинув і її командуючий, у розпачі вчинивши самогубство. Після здобутої перемоги Гінденбург став настільки популярним у Німеччині, що був призначений верховним головнокомандуючим, а після війни – президентом.

Гофман, що подав ідею цієї блискучої операції, вказав причину її нищівного

успіху у своїй книзі «Війна втрачених можливостей»: «Російська радіостанція передала наказ у нешифрованому вигляді, і ми перехопили його. Це був перший з ряду незліченних інших наказів, що передавалися росіянами на початку з неймовірною легковажністю... Така легковажність дуже полегшувала нам ведення війни на Сході, іноді лише завдяки їй взагалі можливо було вести операції». Перехоплення незашифрованих повідомлень російських військ дозволило німцям здобути перемогу в першій битві у світовій історії.

Хоча на початку війни Росія мала великі труднощі у забезпеченні своїх військ усім необхідним, у тому числі і засобами зв'язку, але вже в першій половині вересня 1914 року їй удалося цілком забезпечити їх шифрувальними засобами. 14 вересня російська ставка верховного головнокомандування віддала розпорядження про те, що усі військові накази підлягають зашифруванню.

Прийнята шифросистема ґрунтувалася на багатоалфавітному шифрі цифрової заміни, у якому допускалося зашифрування декількох букв підряд за одним алфавітом. Цей шифр являв собою таблицю, у верхній частині якої в рядок були виписані букви російського алфавіту. Сама таблиця складалася з восьми рядків двозначних цифрових груп, виписаних у довільному порядку. Рядки відрізнялися один від одного порядком розташування в них цих груп. Ліворуч вони були безсистемно пронумеровані. При зашифруванні ці рядки використовувалися по черзі: спочатку під номером 1, потім 2 і так далі. Кожен із рядків застосовувався для зашифрування декількох знаків відкритого тексту. Кількість знаків, що підлягали шифруванню даним рядком, визначалася самим шифрувальником.

Для того, щоб адресат міг розшифрувати отримане повідомлення, у його заголовку п'ять разів проставлялася цифра, що відповідала кількості знаків, що були зашифровані кожним з рядків. Коли в процесі шифрування оператор хотів змінити це число, він вставляв у текст шифровки п'ятизначну групу, елементами якої була та сама цифра, яка відповідала новому числу знаків, що шифрувалися одним і тим же рядком. Таким чином, шифротелеграми російської армії складалися з груп букв, зашифрованих тим же самим алфавітом. Довжина кожної групи букв визначалася однозначно п'ятизначною цифровою групою, що складалася з однієї і тієї ж цифри.

Однак уже до 19 вересня молодий і обдарований начальник російського відділення дешифрувальної служби Австро-Угорщини капітан Герман Покірний розкрив цю систему та цілком відновив усі рядки. Справа в тому, що такі шифросистеми не становили нездоланних перешкод для криптоаналітиків, оскільки в шифротексті найчастіше зберігалася структура слів, що найбільш часто траплялися у відкритому тексті, таких як «атака» і «дивізія», які цілком шифрувалися одним рядком таблиці. До того ж спочатку російські зв'язківці нерідко вставляли

відкритий текст у шифрований. Незабаром одночасне використання відкритих і шифрованих текстів у повідомленнях було заборонено, але було вже занадто пізно, тому це встигло зіграти свою негативну роль.

Першу важливу шифротелеграму капітан Покірний прочитав 25 вересня. Це було довге повідомлення генерала Новікова про результати розвідки з приміткою наприкінці: «Я прийняв рішення не форсувати Віслу». Шифротелеграма була відправлена о 9-ій годині, а о 16-ій офіцер зв'язку австрійських військ довів до відома німецького штабу її зміст. Знання рішення, прийнятого генералом Новіковим, забезпечило успіх дій австро-німецьких військ у початковій стадії битви на річці Вісла.

Читання іншого шифролистування теж дуже вплинуло на хід бойових дій. З телеграми полковника російської кавалерійської дивізії князя Інгаліщева німці довідалися про підготовку наступу на фортецю Перемишль. Попереджений про це комендант фортеці успішно відбивав атаки, поки наступ австрійських військ не змусив росіян зняти облогу фортеці. Під час цього наступу група Покірного читала щодня до тридцяти шифротелеграм супротивника.

Приблизно в цей же час росіяни вперше змінили шифр. Самі рядки залишилися без змін, але змінився порядок вибору рядків для шифрування. Новий шифр був розкритий Покірним протягом декількох хвилин: усі труднощі відпали, коли одна з російських радіостанцій двічі передала одну й ту ж телеграму, спочатку зашифровану старим шифром, а після закінчення його дії – новим.

Продовжували розвивати свою дешифрувальну службу й німці. Професор філології Кенігсберзького університету Людвіг Дойбнер був зарахований у народне ополчення Німеччини як перекладач із російської мови. Він почав свою службу в сфері криптоаналізу з перекладу перехоплених повідомлень, переданих у відкритому режимі. В міру появи в цих текстах зашифрованих слів він намагався їх прочитати. Поступово в професора накопичився такий досвід роботи в цій сфері, що він зміг читати й цілком зашифровані тексти супротивника.

У середині вересня 1914 року Дойбнер був викликаний у штаб і призначений керувати перекладачами, відібраними для навчання криптоаналізу. Після підготовки з них була утворена дешифрувальна група при штабі. Щовечора до 23 години вона направляла Людендорфу вже прочитані криптограми. Той очікував їх з великим нетерпінням і часто запитував у своїх підлеглих, чи є дешифровані криптограми супротивника. Накази, що Людендорф віддавав наступного дня, значною мірою ґрунтувалися на інформації, отриманої від дешифрувальників.

Незабаром був установлений прямий телефонний зв'язок між групами Покірного і Дойбнера. Вони спільно читали майже всі російські шифроповідомлення, отримані на постах перехоплення. З радіообміну стало відомо про план російського наступу на Сілезію, що була промисловим центром Центральної Європи. До кінця вересня перед Гінденбургом і Людендорфом лежала інформація про

склад, дислокацію, чисельність і плани російських військ. Невідома була тільки дата початку наступу, але німці вирішили взяти ініціативу у свої руки та завдати випереджаючого удару.

11 жовтня 1914 року армія під командуванням Макензена вклинилася в російську оборону. У 14.10 наступного дня начальник штабу однієї з російських армій, по яких було завдано удару, передав по радіо довгу шифровку. Крім дати запланованого наступу в шифровці вказувалася найбільш уразлива зона в бойовому порядку цієї армії – стик між її військами та армією сусіда. Наступного дня дешифрована й перекладена радіограма вже знаходилася в штабі німецьких військ Східного фронту, а її зміст був негайно переданий Макензену. У 19.30, маючи перед собою карту зі схемою розташування росіян, він віддав наказ про перехід підпорядкованих йому військ у наступ по усьому фронту з нанесенням головного удару в стик двох армій.

До цього часу росіяни вже щодня змінювали порядок використання шифроалфавітів, але як і раніше залишали без змін самі шифроалфавіти. У результаті дешифрувальники супротивника не переставали читати їхнє шифролистування. Потік інформації, що добувався за допомогою криптоаналізу, не скорочувався. Німці вже настільки звикли до цього, що 19 жовтня Макензен не віддавав наказів доти, поки не були отримані дані від дешифрувальників.

20 жовтня стало «чорним» днем для німецької дешифрувальної групи. У перехопленій шифротелеграмі 4-ої російської армії говорилося про те, що німці мають ключі до російського шифру. Оскільки росіяни зуміли захопити ключі до німецького шифру, то припустили, що аналогічно міг зробити й супротивник. У дію був уведений новий шифр, причому цього разу – з заміною всіх елементів шифросистеми. В результаті позбавлені інформації війська генерала Макензена до 21 жовтня виявилися в «мішку». Росіяни смакували перемогу та вже замовили потяг для вивозу військовополонених. Але наступного дня група Покірного розкрила новий шифр, і до німецького штабу знову пішов потік цінної інформації. З нього німцям стало відоме слабке місце в кільці російських військ, тому до 25 жовтня кільце оточення було успішно прорване.

До весни 1915 року в російських військах цілком відмовилися від старої системи шифрів і стали застосовувати простий шифр Цезаря. Велика кількість таблиць, що використовувалися в умовах ведення активних бойових дій, і щоденна зміна ключів ставили непосильну задачу перед зв'язківцями. У цих умовах розкриття чергового російського шифру для дешифрувальних служб Австро-Угорщини і Німеччини не потребувало майже ніяких зусиль.

Читання російських криптограм дозволило країнам німецького блоку здійснювати такі заходи, що були єдино правильними тактичними рішеннями у даній ситуації. Російський Генеральний штаб був здивований прозорливістю супротив-

ника. Одного разу німці залишили займані ними позиції за два дні до початку великого наступу російських військ. Одним із пояснень точної відповідності рішень німецького командування обставинам, що склалися, росіяни вважали використання супротивником аерофотозйомки.

Але поступово міцніло переконання, що супротивник читав російське шифролистування. Коли на другий рік війни німецький весняний наступ досяг апогею, росіяни знову змінили шифр. 17 червн 1916 року був введений новий дуже складний шифр із 300 шифрувальними групами. Але ця зміна завдала їм же більше турбот, тому що майже всі шифровки, передані по радіо в перші два дні після зміни шифрів, через допущені помилки так і не були прочитані адресатами. Тому деякі штаби продовжували працювати старим шифром, а це значно полегшувало розгадку нового шифру, тим більше, що розташований у районі 8-ої армії гвардійський загін дозволив собі навіть схованою радіограмою повідомити цифровий ключ до цього шифру.

Крім того, в російській спеціальній службі навіть не була поставлена на належний рівень інформація про скомпрометовані шифри, через що вони продовжували вживатися і після компрометації. Так, 6 лютого 1915 року помічник начальника канцелярії МЗС І.Базілі повідомляв в політичний відділ: *«Ввиду обнаружившейся несомненной скомпрометированности наших ламных словарных ключей (номера 335, 371, 374, 379, 382 и 391), из коих некоторые, как ключ 379 (Шпейера), прямо захвачены неприятелем, оказывается совершенно необходимым изъять все эти ключи из употребления...».*

Дезорганізація російської армії, що наростала разом з революційними настроями населення, негативно впливала й на її службу зв'язку. Пропорційно зниженню дисципліни у військах росла балакучість радистів. На початку 1917 року тільки протягом одного дня австрійська дешифрувальна служба прочитала більше 300 російських шифротелеграм, з чого випливало, що служба забезпечення безпеки військового шифрованого зв'язку росіян взагалі не відповідала ніяким вимогам.

Разом з тим, дешифрувальна служба МЗС Росії безпосередньо перед війною і під час війни досить успішно працювала над розкриттям шифрів і кодів та читала листування багатьох іноземних держав і, в першу чергу, країн, що знаходилися у стані війни з Росією. За 1914-1916 роки було дешифровано 588 австрійських, 60 німецьких, 606 болгарських, 225 турецьких, 457 італійських телеграм тощо.

Дешифрування вказаних повідомлень проводилося не тільки за допомогою здобутих розвідкою шифрів і кодів, але й за рахунок аналітичної дешифрувальної роботи. У звіті за 1915-1916 роки, підготовленому старшим чиновником при Канцелярії МЗС Долматовим і направленому товаришу міністра закордонних справ указувалося на труднощі, що траплялися при дешифруванні за рахунок появи в листуванні великого числа нових слів (у італійських і англійських кодах) та частої зміни кодів. Так, Англія до війни щорічно випускала два нові коди, а у звітному ж військовому

році вона випустила їх п'ять, що вкрай ускладнило їх дешифрування.

У вказаному звіті, як і вимагали традиції того часу, висловлювалося клопотання про нагородження криптологів, які досягли найбільших успіхів у дешифруванні, а саме: нагородити грошима Наньєрського (італійські шифри) – 1000 рублів, Циглера (англійські і грецькі шифри) – 2300 рублів, фон Берга (австрійські і німецькі шифри) – 1100 рублів, Раммінга (японські шифри) – 1150 рублів, Феттерлейна (персидські і французькі шифри) – 2400 рублів і Струве (англійські шифри) – 900 рублів.

Масштабно розгорнути дешифрувальну роботу багато в чому не вдавалося через слабкість підрозділів радіоперехоплення та великого браку фахівців із криптології. Історичні матеріали показують, що багато невдач російської криптології цього періоду обумовлено в першу чергу і головним чином не її низьким теоретичним і практичним рівнем, а розладом всієї державної машини в цілому і, як наслідок, розладом у самій організації криптослужби, в її координації, фінансуванні, постачанні тощо. Ініціатива та пропозиції рядових співробітників і керівників середньої ланки управління розбивалися об бездіяльність «вищого ешелону».

Журнали вхідних документів Особливого відділу ДП того часу, дозволили встановити, що і сюди з фронту присилали шифровані документи для дешифрування. Матеріали почали поступати вже у 1914 році. 25 серпня 1914 року з Архангельська від військового губернатора поступило в ДП повідомлення, що на рейді біля села Ковда Александрівського повіту був затриманий німецький пароплав «Удгарт», що мав радіотелеграфну станцію, причому в каюті радиста була виявлена шифротелеграма. Ця телеграма і була надіслана для дешифрування в ДП. Лише через півроку, у січні 1915 року, Архангельськ дочекався відповіді: «Експерт прийшов до висновку, що зазначена телеграма складена на умовній мові (зашифрована) і без ключа не може бути прочитана-перекладена. Перекладав колезький асесор Ярілов».

Тим часом Зибін залишався вірний собі. 13 березня і 14 квітня 1915 року генерал-квартирмейстером при Верховному головнокомандувачі були доставлені в ДП «шифровані документи з театру війни». Вперше було привезено 5 коротких радіограм, з яких 4 виявилися спотвореними при передачі, а п'ята складалася з виправленого тексту двох попередніх. При розробці виявилось, що вони зашифровані за допомогою особливого коду. ДП звернувся з листом до генерал-квартирмейстера, але відповіді не отримав. 14 квітня ДП отримав копію телеграми австрійського військового міністра з Відня, обсягом всього в 10 знаків, зашифровану словниковим ключем, розібрати яку, природно, також було неможливо.

У своїй доповіді з цього приводу Зибін з гіркотою писав, що немає ніякої можливості отримати які-небудь додаткові відомості про прислані документи. Надсилання їх у ДП займає 3-5 днів, тому, якщо вони і будуть дешифровані, то відомості вже застаріють і представлятимуть лише історичний інтерес. І знов Іван Олександрович

сам пропонує свої послуги, для того, щоб попрацювати якийсь час безпосередньо в Головному штабі, своїми знаннями «послужити Батьківщині в годину випробувань». На жаль, невідомо, чи було задоволено прохання статського радника.

Проте в дешифрувальній роботі були і деякі успіхи. Ще у січні 1915 року з Генеральної квартири Генерального штабу поступили фотографічні знімки німецького шифру з перекладом і правилами користування. Незабаром – ще 1 німецький і 5 австрійських ключів до шифрів. У квітні було прислано 8 копій шифрованих телеграм австрійських і німецьких військових агентів до Відня, Берліна і Брашова. Відомо, що тексти цих телеграм були дешифровані. У серпні 1915 року були також прочитані австрійські шифроповідомлення. В цей же час дешифрували телеграму Берковіча до Маннергейма, прислану зі штабу командувача 6-ою армією.

У квітні 1916 року були отримані та дешифровані 3 німецькі шифроповідомлення, надіслані начальником контррозвідки штабу 3-ї армії, та 2 шифроповідомлення – зі штабу Південно-західного фронту. 31 березня було отримано 4 книги німецьких дипломатичних шифрів, а через деякий час – 2 книги турецьких шифрів, відібраних у Ахмета Джеміль Бея, і незабаром шифр, який використовувався «німецькими шпигунами в Данії і Швеції».

За допомогою здобутих шифрів або іншим способом навесні і влітку 1916 року було прочитано понад 30 шифрованих німецьких повідомлень. У серпні 1916 року чинам 5-го відділення Особливого відділу ДП, яким керував Зибін, в нагороду за дешифрувальну роботу було видано 540 рублів. У той же час і в 1915, і в 1916 роках в ДП поступали у великій кількості німецькі і австрійські шифровані радіограми. Але жодна з них дешифрована не була.

«Велика жовтнева соціалістична революція», яка відбулася 7 листопада (за старим стилем – 25 жовтня) 1917 року, та громадянська війна привела до майже повної ліквідації криптологічних служб Росії. Більшість кваліфікованих криптографів й криптоаналітиків виявилася на боці «Білого руху» («білих»), що небезрезультатно використав їхній досвід і знання в ході громадянської війни. Завдяки цьому шифрувальна справа «білих» була поставлена на більш високому рівні, ніж у своїх супротивників – «червоних».

Багато найцінніших матеріалів Тимчасового Уряду Росії, архівів командуючих збройними силами білих армій, що включали й документи таємного листування та шифрів, були вивезені з Росії. Те ж саме варто сказати про архів, що включав документи царської охоронки з 1895 по 1917 рік. Вони були передані колишнім російським послом у Парижі відомому американському розвіднику та промисловцю Герберту Гуверу. В даний час усі ці документи та архіви знаходяться в Гуверівському інституті війни, революції та світу при Стенфордському університеті в Каліфорнії.

Шифрувальна справа в білій армії була поставлена достатньо солідно: збе-

рігалися традиції, технічна база царської шифрувальної служби, частково кадри шифрувальників, криптографів і перекладачів. «Цифирное» відділення, як воно продовжувало іменуватися, знаходилося у МЗС уряду адмірала Колчака та підпорядковувалося безпосередньо начальнику 1-го департаменту цього міністерства. Широко використовувалися старі шифри і коди, що залишилися з колишніх часів. Разом з тим, створювалися і нові шифри.

Так, 2 лютого 1919 року керівник *«цифирного»* відділення писав, звертаючись до начальства: *«...ввиду скомпрометированности старых ключей Министерства иностранных дел, цифирное отделение приступило к составлению новых секретных ключей для телеграфных сношений заграничных представителей с центральными установлениями министерства и между собой».*

У тому ж місяці *«цифирным»* відділенням були виготовлені два перешифрувальні ключі № 560 і № 570, введення яких у дію, на думку виготівників, «цілком забезпечувало б збереження таємниці таємної кореспонденції міністерства». Видавалися виготовлені ключі друкарнею військової газети «Російська армія», де дотримувалися відповідні умови для збереження таємниці видання. Перед виготовленням шифрів або ключів друкарня визначала кошторисну їх вартість. Ці дані повідомлялися друкарнею в *«цифирное»* відділення, і його керівник складав прохання про грошове забезпечення.

В архіві Колчака збереглися лише одиничні зразки шифрів, що використовувалися. В основному, це були буквено-складові різнозначні таблиці заміни. Термін дії таких шифрів був піврічним. Це були типові шифри, що широко застосовувалися в білих арміях. Як відомо, криптографічна стійкість їх була невелика. Такі шифри розкривалися на матеріалі в декілька десятків знаків. Окрім таких шифрів у білій армії використовувалися і коди обсягом у декілька тисяч словникових величин.

Коди були в основному алфавітні, рідко використовувалися неалфавітні невеликого обсягу, в яких була певна кількість пустушок. Такі коди, навіть при дотриманні всіх правил користування, не були шифрами високої стійкості і могли розкриватися на матеріалі достатнього обсягу. Оскільки шифрувалися телеграми порівняно великої довжини та масив цих телеграм, зашифрованих одним і тим же кодом, був достатньо великий, при організації регулярного перехоплення таких шифротелеграм дешифрування їх було доволі простим завданням. Воно полегшувалася ще тим, що шифрувалася не вся телеграма цілком, а тільки окремі її частини. Хоча відомо, що ще в період Першої світової війни це було категорично заборонено.

Розробка і видання шифрів велися постійно. Так, 17 липня 1919 року *«цифирным»* відділенням була завершена робота над виданням нового таємного ключа (коду) МЗС обсягом 8000 словникових величин, а через тиждень ще одного – нової буквено-складової таблиці. Як агентурні шифри біла гвардія використовувала і шифри перестановки, а саме: шифри гасел вертикальної перестановки.

У своєму зовнішньому і внутрішньому листуванні, в радіограмах всі важливі відомості зашифровувалися в обов'язковому порядку. Короткі повідомлення, що містили важливі відомості, шифрувалися повністю, а у довгих повідомленнях шифрувалися лише вибіркові, найбільш важливі місця.

Передачі повідомлення, як завжди, передувала деяка підготовча робота з текстом: підкреслювалися частини тексту, які слід було зашифрувати, далі текст телеграми або перекладався французькою мовою, або просто писався латинськими буквами (свого роду попереднє шифрування), необхідна частина його зашифровувалася і записувалася 5-значними цифровими групами.

Так, телеграма, направлена генералом Міллером 16 жовтня 1919 року лондонському представнику Сабліну готувалася для передачі таким чином:

1. Складався відкритий текст телеграми і в ньому підкреслювалися слова, що підлягали зашифруванню:

«Зимние рейсы между Норвегией и г. Мурманском будут установлены с наступлением зимы не менее раза в неделю, согласовывая со срочными норвежскими пароходами, но пока замерзания нет, это не установлено точно. В настоящее время три парохода находятся на пути в Берген и четвертый выходит из Бергена и Мальмо, все для вывоза продовольствия. Генерал Миллер».

2. Текст, що підлягав зашифруванню, писався латинськими буквами:

«Zimnie reisy mejdu Norwegiei gorodom Murmanskom budut ustanovleny s nastupleniem zimy ne menee raza v nedeliu soglasovyvaia so srocnymi norvejskimi parohodami...»

3. Текст телеграми, який підлягав зашифруванню та був написаний чорнилом від руки або надрукований на машинці, розбивався олівцем на словникові величини, а потім шифрувався. Шифротекст був таким: «18566 24307 54945 38536 20043 45496 63241 81137 82174 15070 64444 17004 57526 85551 88317...».

Далекі відстані, на які передавалися повідомлення, мала потужність і слабке технічне устаткування радіостанцій, невисока кваліфікація шифрувальників, – все це не могло не позначитися на якості отримуваних адресатами телеграм, що приводило до необхідності їх повторювати. Типовими для 1919-1920 років були телеграми про те, що якісь слова або цілі телеграми не піддавалися розшифруванню.

З часом «білий рух» завдяки зусиллям радянських спецслужб поступово зійшов нанівець, а царські фахівці-криптологи перейшли на службу до інших держав, одним із яскравих прикладів цього був Ернест Фетерлейн. Тим самим історія царської російської криптології у 1917 році практично була завершена, після чого розпочалася історія радянської криптології.

Частина 4.

Історія радянської криптології

4.1. Народження радянських криптослужб

1917 рік став переломним не тільки в історії Росії, але й усього світу. Країна була розколота на два конфронтуючі табори. Як й інші верстви населення, фахівці-криптологи виявилися «по різні боки барикад». Однак основна їхня частина після революції перейшла на бік супротивників радянської влади.

Тому, незважаючи на те, що у розпорядження радянської влади потрапили майже всі шифродокументи «цифирных» підрозділів царської Росії, вони були добре відомі криптологам царської Росії, що працювали на «білих». А фахівці-криптологи, що перейшли на бік радянської влади, під час громадянської війни були розкидані по всій країні.

В результаті використання «царських» і «підпільних» шифрів не могло служити діючим засобом захисту таємної інформації Радянської республіки. Керівники республіки розуміли, що необхідно вкрай «архіважливо й досить терміново» створювати свої власні шифрувально-секретні служби.

Вже у грудні 1917 року в структурі наркомату закордонних справ (далі – НКЗС) Радянської республіки з'явився «Відділ шифрувальний і друкарський». А 29 квітня 1918 року він був реорганізований у самостійний Шифрувальний відділ. Після реорганізації наркомату в серпні 1918 року, коли Канцелярія НКЗС у справах Заходу була перейменована у Відділ Заходу, в нього було включено також і «шифрувальне відділення».

В структурі Робітничо-Селянської Червоної Армії (далі - РСЧА) на початку травня 1918 року обов'язки з шифрування та розшифрування телеграм покладені на Загальне відділення Військово-статистичного відділу Оперативного управління Всеросійського головного штабу (далі - ВГШ) РСЧА.

Разом із цими структурами активно використовуати засоби криптології розпочали й органи Всеросійської надзвичайної комісії з боротьби з контрреволюцією, саботажем і злочинами (далі – ВНК). Так, у прийнятому 11 червня 1918 року «Положенні про надзвичайні комісії на місцях» був 36-ий пункт, у якому говорилося про те, що «для таємних стосунків губернських комісій, надзвичайних комісій з ВНК, виробляється певний шифр, шляхом якого й відбуваються стосунки».

При цьому, структури місцевих органів ВНК на той час ще не передбачали ні окремого шифрувального підрозділу, ні посади шифрувальника. Шифри повинні були зберігатися у керівника місцевого органа ВНК або його заступника. Саме він персонально відповідав за таємність шифрів.

Крім того, у функції ВНК входило проведення контролю за іноземним листуванням. Органи ВНК організували, за прикладом відповідних служб царській Росії, службу перлюстрації шифрованої кореспонденції акредитованих у Москві представників деяких іноземних держав. Відомо, що вже на початку 1920-х років у Москві знаходилися дипломатичні і торгові посольства і місії Німеччини, Англії, Туреччини, Італії, Фінляндії, Польщі, Ірану, Афганістану і прибалтійських держав.

Окрім телеграм, що поступали з телеграфу, частина шифрованого іноземного листування і листування білої гвардії за завданнями ВНК і військових органів перехоплювалася на Серпуховській приймальній радіостанції Революційної військової ради республіки (далі - РВРР) та Шаболовської радіостанції Наркомата пошт і телеграфів. Ці повідомлення разом з перехопленням відкритих повідомлень іноземної преси прямували в так званий «відділ обробки матеріалів» Особливого відділу ВНК.

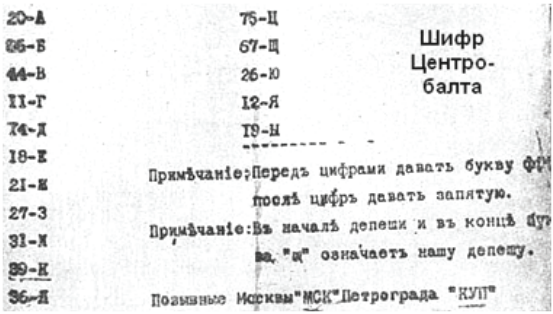
У відділі обробки матеріалів робилися спроби розшифрувати перехоплені радіограми, отримані при обшуках і арештах членів контрреволюційних організацій шифровані документи. В окремих випадках це вдавалося зробити. Однак більшість шифродокументів, що надходили у відділ, залишалася не розшифрованою. Стосовно дипломатичного шифрованого листування, то воно зовсім не читалося.

Потребувала своїх шифрувально-дешифрувальних підрозділів також і військова розвідка. Тому 8 листопада 1918 року наказом по ПШ РВРР № 46 відповідно до наказу РВРР № 197/27 від 5 листопада у складі утвореного Реєстраційного (розвідувального) Управління (скорочено російською *«Региструпр»*) були введені посади «завідувача шифром» і його помічника (В.Панін і П.Озолін відповідно). А 13 листопада того ж року Наказом РВРР № 217 було створено шифрувальне відділення звітно-організаційного відділу Організаційного управління ВГШ РСЧА із штатом 14 осіб.

19 червня 1919 року у затвердженому новому штаті *«Региструпра»* ПШ РВРР з'явилася «шифрувальна частина» (начальник – В.Панін, його заступник – П.Озолін). А у вересні 1920 року у затвердженому новому штаті *«Региструпра»* з'явилися шифрувальне відділення (начальник – П.Озолін) і відділення зв'язку (начальник – Вольдемар Янович Закіс).

Будучи зацікавленою у використанні даних шифролистування, ВНК направляла матеріали для дешифрування у військові органи. Ось один з таких документів: «У Польовий штаб Реввійськради Республіки. 14.IV.1920. Згідно з резолюцією начальника відділу обробки матеріалів Особливого відділу ВНК при цьому супроводжуються три копії перехоплення ворожих радіограм від 3 і 4 квітня з проханням розшифрувати в терміновому порядку і повернути у відділ обробки матеріалів ОВ ВНК».

Через 20 днів, 4 травня 1920 року, у Польовий штаб (далі – ПШ) РВРР був надісланий вторинний запит з цього питання. І лише в червні була отримана типова для подібної ситуації того часу відповідь: «Зважаючи на неможливість


20-А
86-Б
44-В
11-Г
74-Д
18-Е
21-Ж
27-З
31-И
89-К
36-Л
75-Ц
67-Ш
26-Ю
12-Я
19-Ы
Шифр Центро-балта
Примѣчаніе: Передъ цифрами давать букву ФФ
послѣ цифръ давать запятую.
Примѣчаніе: Въ началѣ депеши и въ концѣ ду
ва "ц" означаетъ нашу депешу.
Позывные Москвы "МСК" Петрограда "КУП"

встановити ключ до цих телеграм останні повертаються в нерозшифрованому вигляді...».

У той же час були створені аналогічні шифрувальні структури в Головному артилерійському управлінні, Управліннях зв'язку, постачання, військових повідомлень й інших. У більш низових ланках управління шифрувальних органів, як такого, не було та вся робота з даного питання велася, як правило, за сумісництвом, без належних норм таємності та конспірації, найчастіше неосвіченими та непідготовленими належним чином людьми.

На лініях зв'язку Радянської республіки, в основному, застосовувалися шифри простої та пропорційної заміни. У період боротьби з адміралом Врангелем радянською стороною застосовувався шифр «Республіка», що являв собою шифр Віженера з чередуванням букв алфавіту усередині квадрата відповідно до ключа-гасла. Не менш широко застосовувалися шифри «Москва» і «Секунда».

Шифр «Москва» також являв собою шифр Віженера, де як гасло використовувався той же відкритий текст, але зрушений на один крок вправо, інакше процес дешифрування був би неможливий. При цьому перша буква гасла була заздалегідь обговореною та мінялася відповідно до розкладу.

Шифр «Секунда» був звичайним шифром заміни на 9, 2, 13 колонок. У 1919-1920 роках були розроблені та застосовувалися більш стійкі шифри «Кулемет», «Агітатор» та інші, що лише незначно поліпшили несприятливу в цілому ситуацію з забезпеченням таємниці шифролистування в Радянській республіці.

Але й ці швидкі розробки будувалися за старими принципами та не забезпечували захист таємниці. Перехоплені радіоповідомлення РСЧА легко дешифровувались. Так, наприклад, генерал-майор Дентервиль, що командував експедиційними військами Антанти в Персії та Баку в 1918 році, у своїх спогадах писав, що завдяки використанню «червоними» на Каспійському морі старого царського коду, копія якого малася в його штабі, англійським військам удалося одержати важливу інформацію про дії РСЧА. Ця інформація істотно вплинула на хід бойових дій та дозволила англійцям зайняти Баку та інші райони Кавказу.

Відомо, що у період з 1918 по 1920 рік майже всі шифровані радянські військові та дипломатичні повідомлення успішно читалися білогвардійцями, поляками, англійцями, шведами. Так, у серпні – вересні 1919 року шифрувальники Генерального штабу польської армії розкрили шифри РСЧА. У серпні 1920 року вони дешифрували 410 таємних телеграм, підписаних Троцьким, Тухачевським, Гаєм і Якіром. З серпня 1919 і до кінця 1920 року польські шифрувальники розшифрували декілька тисяч радіограм РСЧА, в основному, накази керівництва армії з управління військами.

Крім того, польські шифрувальники нав'язували помилкові накази командирам військових з'єднань РСЧА за допомогою телеграм, зашифрованих військовим шифром РСЧА. Їм вдалося перехопити та розшифрувати спеціальну директиву Головнокомандувача Каменєва про те, що 1-а і 2-а Кінні армії повинні бути підпорядковані командувачу Західним фронтом Тухачевському та наступати на Люблінському напрямі. Змінивши її зміст, вони склали фальшиву шифровку від Каменєва зі вказівкою 1-ій Кінній армії йти в наступ на Львів.

В результаті управління військами РСЧА було абсолютно порушене, що привело до їх повного розгрому. Коли б не ця помилкова команда, РСЧА могла б звитяжно завершити свій наступ. Те, що польські розвідслужби змогли порушити управління РСЧА за допомогою помилкових наказів, підтверджується наявністю величезного числа полонених червоноармійців - близько 100 тисяч осіб, що склало, приблизно половину чисельності військ РСЧА, що брали участь у цій битві. Ця битва, названа «Дивом над Віслою», увійшла до списку 18 найбільш видатних переломних битв у світовій історії.

Також перехоплювалося та дешифровувалося листування радянського уряду з делегацією на переговорах у Брест-Литовську. Ретельно відбиралася та аналізувалася інформація про діяльність ВНК. Завдяки радіоперехопленню та дешифруванню керівники «білого руху» контролювали операції РСЧА на Східному та Туркестанському фронтах, стежили за зв'язком командування цих фронтів з Москвою. Навесні 1919 року адмірал Колчак писав російському послу в Греції: «Єдиним джерелом інформації нам служать перехоплені більшовицькі радіо».

Системи шифрування, що застосовувалися військами Будьонного та Куйбишева в Середній Азії, іноді «розколювалися», навіть, «басмацтвом». Слабка професійна підготовка кадрових працівників шифрослужби РСЧА не могла забезпечити належного рівня захисту переданої інформації. Допускалося безліч порушень та послаблень при шифруванні. Так, для економії часу найчастіше шифрувалися тільки окремі ділянки повідомлення тексту, а інша його частина передавалася відкрито.

Вкрай погані були справи в Радянській країні з дешифруванням іноземного та військового листування. У РСЧА не було організованої дешифрувальної служби, тому що створені при штабах шифрогрупи мали головною задачею створення шифрів і захист ними таємного листування. Можна сказати, що дешифрувальна служба практично була відсутня. У той період Радянська держава не мала в розпорядженні сили та засоби для успішного проведення такої роботи.

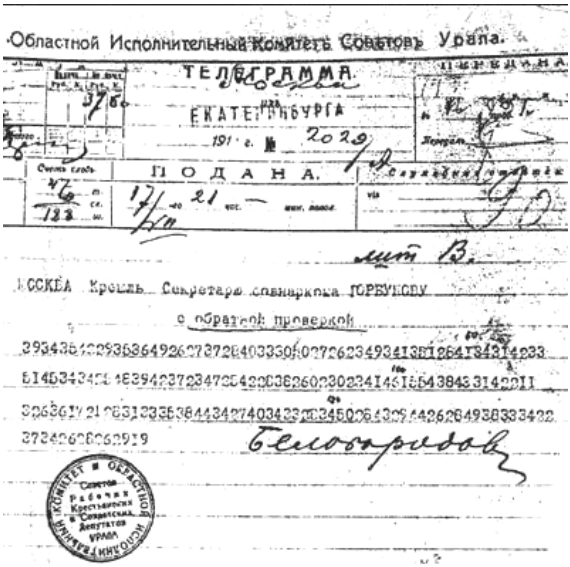
Разом з тим, наприкінці 1917 року був виявлений архів посольства Англії, в якому були діючі англійські шифри. У результаті радянськими криптоаналітиками був дешифрований ряд телеграм англійського посла в Росії Б'юкенена, а по-

тім і дипломатичного агента Англії Локарта, що його замінив. Це допомогло ВНК розкрити змову останнього, спрямовану проти більшовиків. У цій змові, метою якого була організація повстання в Москві та фізичне усунення керівництва Радянської республіки, брали участь посли ряду західних країн. Цікаво відзначити, що всі подробиці розкриття змови Локкарта стали відомі білогвардійцям з перехоплених та дешифрованих радянських радіопередач.

Аналогічним чином був виявлений шифр румунського військового аташе. У результаті був розкритий план генерала Корнілова щодо здачі Риги німцям і отримані інші важливі матеріали.

У 1920 році при розгромі армії Врангеля в Криму був захоплений начальник станції радіоперехоплення Ямченко. Він дав згоду співробітничати з новою владою та розповів про практично повне дешифрування «білими» перехоплених повідомлень. З цими даними був ознайомлений Михайло Фрунзе, головнокомандувач Південною групою РСЧА. Ось яку оцінку стану справ у сфері криптографічного захисту інформації в Радянській республіці він дав:

«...З наданого мені колишнім начальником врангельської радіостанції Ямченком доповіді встановлюється, що всі наші шифри внаслідок їхньої нескладності читаються нашими ворогами. Весь наш радіозв'язок є чудовим засобом орієнтування супротивника. Завдяки тісному зв'язку з шифрувальним відділенням морфлота Врангеля, Ямченко мав можливість особисто читати цілий ряд наших шифровок найбільш секретного військово-оперативного та дипломатичного характеру; зокрема, секретне листування Наркомінсправа з його представництвом у Європі та у Ташкенті слово в слово відоме англійцям, що спеціально організували для підслуховування наших радіо цілу мережу станцій особливого призначення. До шифрів, що не піддавалися негайному злому, надсилалися ключі з Лондона, де на чолі шифрувального відділу поставлений англійцями російськопід-


Областной Исполнительный Комитет Советов Урала.

ТЕЛЕГРАММА

ЕКАТЕРИНБУРГА

191 г. № 2029

ПОДАНА.

МОСКВА Кремль Секретарю совнаркома ГОРБУНОВУ

с обратной проверкой

Белобородов

Совет Рабочих Крестьянских и Солдатских Депутатов Урала

даний Фетерлейн, що відав колись цією справою в Росії. Загальний висновок такий, що всі наші вороги, зокрема, Англія, були постійно в курсі всієї нашої військово-оперативної та дипломатичної роботи...».

Ось як охарактеризував таку ситуацію нарком закордонних справ Григорій Чичерін у своєму листі Голові Ради Народних Комісарів (далі – РНК) Володимиру Леніну від 21 серпня 1920 року:

«Я завжди скептично відносився до наших шифрів, найбільш таємні речі зовсім не повідомляв і кілька разів застерігав інших від повідомлення таких. Не вірна думка тов. Каменєва, що важко дешифрувати. Від нашого співробітника Сабаніна, сина старого дешифрувальника Міністерства закордонних справ, ми знаємо, що всі іноземні шифри розшифровувалися російськими розшифровувачами. В останній період існування царату не було іноземної депеші, яка б не розшифровувалася, при цьому не внаслідок зрадництва, а внаслідок мистецтва російських розшифровувачів. При цьому іноземні уряди мають більш складні шифри, ніж уживані нами. Якщо ключ ми постійно змінюємо, то сама система відома царським чиновникам і військовим, що знаходяться в стані білогвардійців за кордоном. Розшифрування наших шифровок я вважаю цілком припустимим».

У той же день, 21 серпня, В.Ленін склав термінову відповідь:

«Пропоную:

1) змінити систему негайно;

2) змінювати ключ щодня, наприклад, відповідно до дати депеші або відповідно до дня року (1-ий ... 365-ий день і т.д. і т.п.);

3) змінювати систему або подробиці її щодня (наприклад, для букви 5 цифр; одна система: перша цифра фіктивна; друга система: остання цифра фіктивна і т.д.).

Якщо змінювати хоча б щотижня (а) ключ і (б) такі подробиці, то не можна розшифрувати».

Слабка стійкість радянських шифрів була обумовлена ще тим, що в урядовій криптологічній школі Британії, створеній при Адміралтействі у 1919 році, головою секції, що працювала проти Росії, служив Ернест Фетерлейн, літня людина на прізвисько Фетті. У Росії перед революцією Фетерлейн займав пост провідного криптолога, мав ранг адмірала та був царем нагороджений перснем з величезним рубіном за виконання делікатних доручень. Після революції Фетті втік до Англії та успішно «розкривав» слабкі радянські шифрувальні системи.

Завдяки Фетерлейну та його англійським колегам британський уряд читав значну частину найважливішого дипломатичного листування росіян під час англо-радянських торгівельних переговорів. Перехоплена інформація мала надзвичайно важливе значення. Так, на самому початку переговорів у червні 1920

року Ленін писав Красіну: «Ця свиня Лойд Джордж піде на обман без тіні сумніву або сорому. Не вірте жодному його слову та у три рази більше дуріть його». Лойд Джордж філософськи ставився до подібних образ. Однак деякі з його міністрів відносилися до цього інакше. Керзон і Черчилль, використовуючи розшифровану інформацію про фінансову допомогу газеті «Дейлі геральд» і англійським «більшовикам», а також про інші форми радянської підривної діяльності у Великобританії та Індії, вимагали вислати радянську делегацію та припинити торгівельні переговори.

Не бажаючи підривати перспективи досягнення торгівельної угоди, Лойд Джордж, проте, вважав необхідним відреагувати на праведний гнів своїх міністрів, причина якого крилася в розшифрованих документах, що свідчили про підривну діяльність більшовиків. 10 вересня прем'єр-міністр звинуватив Лева Каменєва, що прибув у Лондон у серпні як керівник радянської торгівельної делегації (у той час Красін був його заступником), у «грубому порушенні даних обіцянок» та у використанні різних методів підривної діяльності. Красіну дозволили залишитися.

Каменєву ж, який наступного дня повинен був повернутися в Росію для одержання нових інструкцій, було оголошено, що йому не буде дозволено в'їхати назад у Великобританію. Лойд Джордж заявив йому, що він має незаперечні докази, які підтверджують висунуті проти нього обвинувачення, однак відмовився повідомити, які саме.

Вочевидь, радянська делегація все-таки зрозуміла, що її телеграми були перехоплені та розшифровані. А вже в серпні Кабінет Міністрів Великобританії дав згоду на публікацію частини перехопленої інформації. 8 розшифрованих телеграм, які доводили, що радянський уряд надавав фінансову допомогу газеті «Дейлі геральд», були передані до редакцій всіх загальнонаціональних газет, за винятком самої «Дейлі геральд». Для того, щоб ввести в оману росіян щодо джерела інформації та спробувати переконати їх у тому, що витік відбувся в Копенгагені в оточенні Максима Литвинова, цей матеріал був переданий у газети з умовою посилання на «нейтральну» країну. Однак газета «Таймс» не прийняла умов гри. До крайнього невдоволення Лойда Джорджа, вона почала свою статтю з наступних слів: «Ці радіограми були перехоплені британським урядом».

10 вересня 1920 року Леонід Красін написав з Лондона листа Леніну:

«Ще в травні при перебуванні в Копенгагені за деякими ознаками я почав підозрювати, що з шифрованим листуванням через Наркомінсправ не все йде благополучно. У Англії ці підозри зміцнилися, і в подальший мій приїзд до Москви я звертав увагу тов. Чичеріна на необхідність корінного чищення у відповідному відділі... Нарешті, сьогодні ми майже офіційно сповіщені, що таємні наші депеші зовсім не є таємницями для Велпра [уряд Великобританії]. Справа не в

провалі шифру або ключа, а в тому, що в Наркомінсправ неблагополуччя, так би мовити, абсолютне і змінювати це треба радикально... Здається, виправити справу можна тільки створенням при Наркомінсправ шифрувального відділення незалежно від самого Комісаріату і персонально підібраного з людей або по партії, або особисто відомих протягом десятка - півтора років... Крім того, треба завести особливий ключ з Оргбюро або Політбюро і особливо важливі депеші посилати цими ключами, абсолютно епатуючи К[омісаріа]т у справі їх розшифрування. Не думайте, що все це зайва недовіра, ні, справа дуже серйозна...».

Однак сам Ленін зовсім не розділяв підозри Красіна щодо зрадництва в НКЗС. 25 листопада 1920 року він знову звернувся до Чичеріна: «Питанню про більш суворий контроль за шифрами (і зовнішньому, і внутрішньому) не можна давати заснути. Обов'язково черкніть мені, коли всі заходи будуть прийняті. Необхідне ще одне: з кожним важливим послом (Красін, Літвінов, Шейнман, Йоффе і т.п.) встановити особливо суворий шифр тільки для особистої розшифровки, тобто тут шифруватиме особливо надійний товариш, комуніст (можливо, краще при ЦК), а там повинен шифрувати або розшифровувати особисто посол (або «агент»), не маючи права давати секретарям або шифрувальникам. Це обов'язково (для особливо важливих повідомлень, 1-2 рази на місяць по 2-3 рядки, не більше)».

Відповідь була дана наступного дня: «Узагалі питанням про кращу постановку шифрувальної справи в Республіці займається комісія тов.Троцького... Єдиний особливо суворий шифр є книжковий. Користуватися книжковими шифрами можна лише в окремих випадках унаслідок крайньої громіздкості цієї системи. Потрібно занадто багато часу. Для окремих найбільш таємних випадків це можна робити. На початку всі наші кореспонденти мали книги, але внаслідок занадто великої громіздкості цієї системи поступово відмовилися. Можна буде відновити цю систему для окремих випадків, користуючись помилками для повідомлення кореспондентів…».

Після цього радянська торгівельна делегація в Лондоні одержала інструкцію пересилати свою кореспонденцію, по можливості, кур'єрською поштою до розробки нової системи шифру. Фетерлейн і його англійські колеги протягом декількох місяців не могли розгадати нові радянські шифри, введені в дію на початку 1921 року. Але вже до кінця квітня вони змогли розшифрувати значну частину радянського дипломатичного листування.

Радянські агентурні шифри були тоді слабші ніж дипломатичні. Так, завербований у паризькому центрі білогвардійського руху агент скаржився на слабкість і незручність шифрів, що використовувались. Найбільш пунктуального офіцера російської армії дратувало те, що шифровки наносилися тайнописом між рядків звичайних послань, а Москва нерідко забувала спеціальним чином по-

значити лист, що містив тайнопис, і він знищувався без прочитання. Більше того, виявлений поганим складом тайнописний текст зникав часом так швидко, що не вдавалося встигнути його скопіювати.

1 вересня 1920 року Чичерін написав листа наркому фінансів Крестинському про направлення в НКЗС співробітників для роботи в шифрувальному відділенні: «Наші шифрувальники були і раніше переобтяжені роботою, а зараз створилася повна невідповідність між їх складом і роботою. Збільшення складу наших шифрувальників є тепер завданням першорядної ваги».

А 16 вересня 1920 року він написав листа Леніну про «обережність із питання про персонал, пов'язаний з шифровками», і пропонував йому, щоб всі співробітники шифрувального відділення або шифрувальники «були ухвалені Оргбюро і Особливим відділом ВНК». На його думку, було особливо необхідно ретельно підбирати «самокатчиків», які розвозили б шифровки. У інших листах Леніну Чичерін порушив такі питання, як правила розсилки шифротелеграм, їх зберігання, охорони НКЗС, особливо охорони шифрувального відділу, для чого нарком пропонував призначити курсантів, «як це практикується у Кремлі».

Того ж місяця Політбюро російської комуністичної партії (далі – РКП) розглянуло «пропозицію т. Леніна вжити заходів щодо ускладнення шифрів і до більш суворої охорони шифрованих повідомлень». Політбюро ухвалило доручення наркому з військових і морських справ Троцькому, *«организовать комиссию из представителей Наркомвоена, Наркоминдела, ЦК РКП и Наркомпоштеля»*. Ленін, вивчивши досконало питання, знаючи думку НКЗС й інших зацікавлених відомств, доручив знайти шляхи наведення порядку в шифрувальній справі керівництву ВНК, хоча шифрувальні служби були й у інших наркоматах.

Одразу ж почала працювати Державна комісія з питання «постановки шифрувальної справи в Республіці». У зв'язку з цим Чичерін 25 вересня 1920 року доповідав у РНК, що «з понеділка у нас розпочне працювати т. Голуб, завдання якого полягатиме в перетворенні шифровок на офіційні папери для розсилки їх у такому абсолютно зміненому вигляді звичайним одержувачам».

А вже наприкінці 1920 року в НКЗС був розроблений «Циркуляр про шифри». 1 березня 1921 року завідувачем шифрувальною частиною був призначений І.М.Міхель, колишній завідувач канцелярією НКЗС.

В десятих числах січня 1921 року Колегія ВНК приймає рішення про скликання наради представників зацікавлених відомств для підготовки відповідних пропозицій щодо утворення єдиної криптологічної служби. В обговоренні питання брали участь представники ЦК РКП, ВНК і наркоматів. В результаті 28 січня 1921 року при ВНК був утворений Спеціальний відділ для координації та контролю відомчих шифрувальних служб і централізованої організації секрет-

ного діловодства у державних установах. Відділ очолив колишній голова Петроградської НК у 1918 році та повноважний представник ВНК у Туркестані у 1919-20 роках Гліб Іванович Бокій, який з 12 липня 1921 року увійшов за посадою до Колегії ВНК.

Колегія ВНК до березня підготовила пропозиції про створення міжвідомчої шифрувальної комісії при РНК, що складалася з представників Наркомата військових справ, ВНК, НКЗС і Наркомата зовнішньої торгівлі під головуванням представника ВНК – начальника Спеціального відділу. Проте розроблений ВНК проект діяльності цієї комісії прийнятий не був, оскільки стало очевидно, що в умовах, що створилися, за наявності у всіх наркоматів безлічі важких невідкладних власних завдань, всю роботу зі створення і організації діяльності спеціальної служби повинно узяти на себе одне відомство, а саме ВНК.

Було прийнято ухвалу, запропоновану Леніним: «Доручити начальнику шифрувального відділу ВНК прийняти заходи до здійснення нагляду, контролю і керівництва шифрувальною справою в Республіці і представити в Малу раду відповідний проект Ухвали, погодивши його з найбільш зацікавленими відомствами». 12 квітня на засіданні Малого РНК з проектом утворення єдиного у країні шифрувально-дешифрувального відділу виступив начальник Спеціального відділу при ВНК Бокій, людина, якій належало стати головним організатором криптологічної служби країни і її першим керівником.

Ось текст цього проекту:

«Маючи на увазі: 1) відсутність у Республіці центру, що об'єднує та спрямовує діяльність шифрувальних органів різних відомств, і пов'язані з цим безсистемність і випадковість у постановці шифрувальної справи; 2) можливість, завдяки цьому, при існуючому положенні широкого інформування ворогів Робітничо-селянської держави про таємниці Республіки, Рада Народних Комісарів ухвалила:

Утворити при Всеросійській Надзвичайній Комісії «Спеціальний відділ», штати в якому затверджуються Головою ВНК. Начальник Спеціального відділу призначається Раднаркомом.

У коло ведення Спеціального відділу при ВНК включити:

І. Постановку шифрувальної справи в РРФСР:

А. Наукова розробка питань шифрувальної справи:

а) аналіз всіх існуючих та існуючих російських і іноземних шифрів;

б) створення нових систем шифрів;

в) складання описів шифрів і інструкцій у шифрувальній справі та користуванні шифрами;

г) збирання архівів і літератури у шифрувальній справі для сконцентрування такого при Спецвідділі;

д) складання і видання керівництва з питань шифрування.

Б. Обстеження і вироблення систем шифрів:

1. Обстеження всіх шифрів, що діють у даний час, і порядку користування ними шифрорганами;

2. Остаточна обробка інструкцій у шифрувальній справі і користуванні шифрами та розробка правил роботи шифрорганов;

3. Розподіл знов вироблених систем шифрів між всіма відомствами.

В. Організація навчальної частини:

1. Розробка програми школи шифрувальників.

2. Створення школи шифрувальників.

3. Укомплектовування школи викладачами і учнями.

Г. Облік особового складу шифрувальних органів. Спостереження за закономірною постановкою шифрувальної справи. Інструктаж та інспекція шифрувальних органів:

1. Облік і перевірка всіх співробітників всіх шифрорганів.

2. Розподіл співробітників усіх шифрорганів між останніми залежно від індивідуальних якостей кожного працівника та фактичної потреби в працівниках у тому або іншому шифроргані, а також залежно від державної важливості кожної установи.

3. Чищення неблагонадійного і нездібного елементу зі всіх шифрорганів.

4. Спостереження за закономірною постановкою шифрувальної справи у всіх шифрорганах.

5. Інструктаж та інспекція всіх шифрорганів і проведення в життя Інструкції і правил у шифрувальній справі.

II. Постановка розшифрувальної справи у РРФСР:

1. Дослідження способів повсюдного вловлювання всіх радіо, телеграм і листів ворожих, іноземних і контрреволюційних.

2. Відкриття ключів ворожих, іноземних і контрреволюційних шифрів.

3. Розшифровка всіх радіо, телеграм і листів ворожих, іноземних і контрреволюційних.

Всі розпорядження і циркуляри Спеціального відділу при ВНК з усіх питань шифрувальної та розшифрувальної справи є обов'язковими до виконання всіма відомствами РРФСР».

Тим часом 4 квітня 1921 року наказом РВРР № 785/141 *«Региструпр»* ПШ РСРР був реорганізований у Розвідувальне Управління (далі – РУ) Штабу РСЧА. У його складі було створене шифрувальне відділення 2-го (агентурного) відділу, начальником якого став В.Я.Закіс.

А вже 5 травня 1921 року постановою Малого РНК № 672 була утворена єдина радянська криптослужба у вигляді Спеціального відділу при ВНК. Приведемо

текст цієї постанови:

«РНК, розглянувши питання про шифрувальні відділи, ухвалив наступне:

1) утворити при ВНК «спеціальний відділ»;

2) Спецвідділ ВНК поєднує всі шифрувальні органи, контролює й направляє всю діяльність таких органів;

3) всі розпорядження й циркуляри Спецвідділу ВНК із всіх питань шифрувальної та розшифрувальної справи є обов'язковими до виконання всіма відомствами Росії».

З того часу 5 травня вважається святом шифрувальників усіх міністерств і відомств. Начальником нової структури й одночасно членом колегії ВНК був призначений Гліб Іванович Бокій, який до цього керував Петроградською НК і завжди цікавився шифруванням, а свої записи про підпільні справи шифрував особистим математичним шифром.

З його ініціативи 25 серпня 1921 року у ВНК був виданий наказ, що пропонував усім підрозділам у центрі та на місцях «направляти в Спецвідділ всякого роду шифри, ключі до них і шифровки, виявлені при обшуках та арештах, а також добуті через агентуру або випадково».

Розміщався відділ не тільки на Малій Лубянці, але й у будинку № 21 на вулиці «*Кузнецкий мост*», у приміщеннях НКЗС, де займав два верхні поверхи. Офіційними його завданнями були масштабна радіо- і радіотехнічна розвідка, дешифрування телеграм, розробка шифрів, радіоперехоплення, пеленгація й виявлення ворожих шпигунських передавачів на радянській території.

Специфіка роботи Спецвідділу докорінно відрізнялася від усього того, що робилося у ВНК, а тому вимагала залучення людей, що володіли унікальними навичками. Це насамперед відносилося до криптологів, завданням яких було розгадування шифрів і ребусів.

Взагалі, серед особового складу дешифрувального відділу було багато колишніх російських аристократів, зокрема графів і баронів. Ця суперечність із державним устроєм того часу пояснювалася серйозним браком лінгвістів, які були потрібні для ведення дешифрувальних робіт. А сама професія дешифрувальника була настільки рідкісною, що навіть тоді, коли представники цієї професії потрапляли у в'язницю, їх все одно залучали до роботи за фахом.

Ось що розповів письменник Лев Разгон, який був зятем Бокія, а в 1930-і роки – співробітником Спецвідділу: «Бокій підбирав людей дуже різних і дивних. Як він підбирав криптографів? Адже це здатність, що дана від Бога. Він спеціально шукав таких людей. Пам'ятаю старого співробітника Охоронки статського радника (у чині полковника), що ще в Петербурзі, сидячи на Шпалерній, розшифрував таємне листування Леніна. У відділі працював і винахідник-хімік Євгеній Гоппіус. У ті часи найважчим у шифрувальній справі вважалося знищен-

ня шифрувальних книг. Це були товсті фоліанти, і потрібно було зробити так, щоб у випадку провалу або інших непередбачених обставин подібні документи не дісталися ворогу. Наприклад, морські шифрувальні книги мали свинцеве плетіння, і в момент небезпеки військовий радист повинен був кинути їх за борт. Але що було робити тим, хто знаходився вдалині від океану та не міг оперативно знищити небезпечний документ? Гоппіус же придумав спеціальний папір, і треба було тільки піднести до нього у відповідальний момент палаючу цигарку, як товста шифрувальна книга перетворювалася через секунду в купку попелу».

До служби у Спецвідділі у першу чергу залучались колишні «царські» криптологи. Так, у 1919 році перекладачем-дешифрувальником Особливого відділу ВНК був призначений відомий нам Володимир Іванович Крівош, а його син Роман - секретарем бюро з видачі перепусток у прикордонну зону Особливого відділу Московської НК. У цей час Володимир Іванович додав до свого прізвища слово «Неманіч» (скорочено - нема нічого), мабуть, підкреслючи цим своє матеріальне становище порівняно до царського часу. Тепер він мав прізвище - Крівош-Неманіч.

У 1920 році він разом із сином Романом був арестований ВНК за підозрою у організації незаконного перетинання кордону. Однак у тому же році Роман був звільнений за амністією, а Володимир Іванович - у 1922 році та прийнятий на службу у Спецвідділ у якості експерта. Цікаво, що його син Роман з 1 травня 1921 року вже працював перекладачем-дешифрувальником Спецвідділу.

У 1923 році Крівош-Неманіч був арестований за підозрою у шпигунській діяльності та висланий на 10 років у Соловецький концтабір. У 1928 році він вийшов на свободу та знову став працювати експертом у Спецвідділі. У 1935 році Крівош-Неманіч був звільнений на пенсію, а у 1937 році був арестований його син Роман, співробітник Спецвідділу ГУДБ НКВС.

Завдяки своїм високим професійним здібностям Роман до концтаборів висланий не був і знаходився у Бутирській в'язниці, де успішно працював криптологом. З початком Вітчизняної війни у 1941 році Роман був звільнений та разом з батьком мешкав у евакуації в Уфі. Роман Крівош продовжував свою службу як фахівець-криптограф Спецвідділу НКВС і у 1942 році був нагороджений медаллю «За трудову відмінність». Його батько Володимир Іванович Крівош-Неманіч помер 4 серпня 1942 року в Уфі.

Штатним співробітником Спецвідділу став і талановитий криптолог «охоронки» Іван Зибін. Ще довгі роки він успішно працював у криптослужбі, допомагаючи створювати вже радянську школу криптологів. Перед молодими співробітниками він не боявся розповісти, що у свій час дешифрував деякі листи Леніна! Утім, справа ця була не дуже складною... Подальша його доля на даний час залишається невідомою.

Робота Спецвідділу розпочалася з детального вивчення спадку, отриманого з архівів спеціальної служби дореволюційній Росії. Це були шифри, їх детальний опис, документи з дешифрування, матеріали шифроперехвату. Серед цих документів, зокрема були матеріали з дешифрування шифрів Туреччини, Персії, Японії, інших держав, а також копії і оригінали шифрів США, Німеччини, Японії, Китаю, Болгарії, навчальні посібники тощо.

Співробітники відділу ретельно вивчали ці матеріали, усвідомлюючи важливість своєї роботи. Велику роль в цей і подальший періоди зіграли знання і досвід Зибіна, Крівоша-Неманіча та інших «царських» криптологів. При їх активній участі при Спецвідділі були організовані 6-місячні курси, на яких вивчалися основи криптографії, вирішувалися завдання з дешифрування. На курси набирали людей здібних і грамотних. Перший випуск курсів складався з 14 осіб, п'ятеро з яких пришли на роботу в дешифувальне відділення відділу, останні – в інші відділення.

Необхідною умовою успішної роботи Спецвідділу була наявність матеріалів шифроперехвату. У способах їх отримання зберігалися традиції дореволюційних служб. Окрім зняття копій з шифровок іноземних держав, що проходили через Центральний телеграф або доставлялися дипломатичною поштою, чим займався відділ Політконтроля, було посилено перехоплення шифротелеграм, що передавалися по радіоканалах. З цією метою були задіяні військові радіостанції, надані в розпорядження Спецвідділу радіомовні станції, зокрема радіостанція Комінтерну. Однак недосконалість радіоприймальної апаратури, а також сильна зношеність не могли забезпечити високої достовірності текстів перехоплюваних шифротелеграм.

Таким чином до труднощів перших років роботи Спецвідділу, пов'язаних із невисокою загальною підготовленістю та нечисленністю особового складу, додавалися труднощі, пов'язані з недоліком і низькою якістю матеріалів для дешифрування. Перед керівництвом Спецвідділу постали завдання організації та налагодження роботи всіх ланок спеціальної служби в країні, включаючи здобуття шифроматеріалів і технічне оснащення радіостанцій. У зв'язку з цим Спецвідділом проводилася робота з розробки та виготовлення спеціальної техніки. У тісному контакті працював Спецвідділ з Закордонним відділом ВНК, контактуючи та маючи зв'язок з агентурою, орієнтованою на здобуття шифрів і кодів.

Зберігся звіт про роботу Спецвідділу за 1921 рік. У ньому, зокрема, було вказано, що з самого початку успішно проводилася розробка та виготовлення нових кодів і шифрів. Тільки за цей рік було введено в дію на різних лініях зв'язку 96 нових кодів. Ця робота співробітників Спецвідділу активно підтримувалася урядом. Характерною для того часу була телеграма секретаря ЦВК СРСР Єнукідзе Бокію, хоча і відносилася вона вже до 2 вересня 1924 року та була пов'язана з

закінченням роботи над телеграфним кодом:

«Поздоровляю тов. Г.І.Бокія з закінченням складання «Російського коду» – цієї величезної і складної праці.

«Буття визначає свідомість». Буття і необхідність сучасних стосунків, швидкий зв'язок і економія в часі штовхнули людей до створення цієї нової мови «коду», мови, не схожої ні на одну людську мову.

Як маленький шматочок радію при розкладанні випускає колосальну кількість енергії, так і слова «коду» – короткі, незрозумілі і невимовні для нашої мови, при розшифруванні розгортають перед нами ряд фраз і думок, що посилаються або отримуються нами здалеку.

Як стенографія стала необхідною для точного запису і розмноження людської мови, так і мова «код» стає і повинна стати необхідною в стосунках між людьми, що знаходяться на різних точках земної кулі.

Я упевнений, що «код» отримає широке застосування в усіх наших установах Союзу РСР.

Раз темп роботи Жовтневої революції нас привів до того, що ми вимушені були красиву та гнучку російську мову вимовляти зі скороченням складів, то по дротах і повітряних хвилях ми сміливо спілкуватимемося концентрованою мовою «код», тим паче, що вона доходитиме до адресатів у красивому, розгорненому і зрозумілому вигляді.

Я зі свого боку закликаю всі установи ввести у себе при спілкуванні по телеграфу і радіо мову «код». Єнукідзе».

На початку 1920-х років Спецвідділ включав 6, а пізніше – 7 відділень. Проте власне криптографічні завдання вирішували тільки три з них: 2-е, 3-є і 4-е. Так, співробітники 2 відділення займалися теоретичною розробкою питань криптографії, виробленням шифрів і кодів для ВНК і всіх інших установ країни (включаючи МЗС, Військове відомство тощо). Відділення в перші роки роботи складалося з 7 осіб, а його начальником був Федір Григорович Тіхоміров.

Перед 3 відділенням стояло завдання «ведення шифроробoти та керівництво цією роботою у ВНК». Складалося воно спочатку всього з 3-х осіб, керував відділенням старий більшовик, колишній латиський стрілець Федір Іванович Ейхманс, який одночасно був заступником начальника Спецвідділу. Ейхманс організовував шифрозв'язок із закордонними представництвами СРСР, спрямовував і координував їх роботу.

Співробітники 4 відділення, а їх було 8 осіб, серед яких був і Крівош-Неманіч, займалися «відкриттям іноземних і антирадянських шифрів і кодів та дешифровкою документів». Начальниками цього відділення були: з травня по грудень 1921 року – Ященко, з січня по серпень 1922 року – Горячов, з серпня 1922 по вересень 1923 року – Ельтман.

Перші успіхи радянських криптослужб незабарилися. Уже в 1921-22 роках удалося розкрити перші дипломатичні й військові турецькі шифри, до 1925 року проводилася активна й небезуспішна робота з шифрами 15 європейських держав, у 1927 році розпочалося читання японських повідомлень, а в 1930 році були розкриті деякі шифри США.

У травні 1921 року при Штабі РСЧА був також утворений свій спецвідділ – Центральний шифрувальний відділ (далі – ЦШВ) і було затверджене Положення про нього та його штат, а також штати шифрорганів штабів фронтів, округів, армій, дивізій, бригад, Центрального управління ВОСО і дисловідділення Управління зв'язку штабу РСЧА, Управління ВОСО і дисловідділень зв'язку штабів фронтів і армій. ЦШВ складався з 4-х відділень загальною чисельністю 27 осіб.

В той час столицею радянської України був Харків, тому в 1921 році в складі українських органів держбезпеки був створений Загальний відділ під керівництвом Ігнатова, одним із завдань якого було забезпечення таємного телеграфного зв'язку. Пізніше при ДПУ Української Радянської Соціалістичної Республіки (далі – УРСР) було організовано Шифрувальне бюро.

Співробітниками ЦШВ були розроблені перші радянські шифри *«74-й Ключ Наркомвоена», «Гелиос», «75-й Ключ Наркомвоена», «Советский»* та інші. У 1921 році ними було виготовлено й розіслано у війська та на флот 54 нові шифри і 2 радіокоди.

Коди та шифри того часу – «Око», «Кулемет», «Стрілок», «Пролетар», «Іскра», «Спартаківець» – згодом були витіснені більш серйозними – «УП Третій», «АРО Перший» та іншими. Це підвищило стійкість шифрованих повідомлень і збільшило безпеку застосування наявних каналів зв'язку.

З перших місяців свого існування Спецвідділ розпочав успішно проводити дешифрування іноземного листування. Колегія ВНК робила все для того, щоб організувати справу найкращим чином і забезпечити повну таємність. Був встановлений порядок, згідно з яким про всі розкриті шифри та здобуті відомості Спецвідділ доповідав ЦК партії, Раднаркому, голові ВНК і керівникам інших за-

цікавлених відомств.

Колегія ВНК надавала велике значення оперативному використанню таємного листування, що дешифрувалося. Всі термінові і особливо важливі дешифровані повідомлення доповідалися негайно. Вже у той час дешифровані матеріали активно використовувала радянська розвідка, НКЗС, деякі інші організації.

Перший позитивний результат був досягнутий у «розкритті» німецького дипломатичного коду, яким користувався повноважний представник німецького уряду в Москві. Це був цифровий 5-значний код з перешифруванням гамою багатократного використання. Починаючи з червня 1921 року, розшифровувалося все листування на лінії зв'язку Москва–Берлін.

З 1922 року Німеччина ввела на дипломатичних лініях зв'язку буквений код з перешифруванням гамою багаторазового використання. Коди та велика частина перешифрувальних засобів розкривалися аналітичним шляхом у Спецвідділі. Розкриття таких шифрів дозволило контролювати листування багатьох ліній дипломатичного зв'язку Німеччини та її консульств у Ленінграді, Києві, Одесі, Харкові, Тбілісі, Новосибірську, Владивостоку аж до 1933 року, коли кількість читаного листування різко скоротилася через те, що німці почали застосовувати гаму одноразового використання.

У серпні 1921 року було здійснено дешифрування перших турецьких дипломатичних телеграм. Вже на початку 1920-х років криптологи Спецвідділу добилися можливості читати листування внутрішніх ліній зв'язку Туреччини та окремих ліній зв'язку військових аташе. Турки застосовували головним чином 4-значні коди з перешифруванням короткою гамою, змінною через дві доби, а також коди без перешифрування. Дешифроване листування містило відомості, які представляли великий інтерес для радянської сторони, та активно використовувалося. Багато дешифрованих телеграм надсилалося, наприклад, в Закавказьку НК, і це давало можливість вжити заходи з припинення шпигунських дій іноземних, а у даному випадку турецької, розвідок. У 1921 році Спецвідділ розпочав розробляти англійське шифролистування.

Велику допомогу Спецвідділу надавав Іноземний відділ ВНК, розвідники якого у період 1920-30-х років добули більше 10 англійських кодів. По цих шифрах читалася частина дипломатичного листування, проте не вся, оскільки виникали складнощі з розкриттям перешифрування.

Серед «розкритого» листування було багато матеріалів, що представляли великий інтерес для радянського уряду, органів радянської розвідки та контррозвідки. Серед таких документів були, наприклад, телеграми про радянсько-англійські відносини, про продаж англійцями зброї країнам, що мали кордон з СРСР, про діяльність англійської розвідки у Середній Азії тощо.

Хоча робота з розкриття польських шифрів почала проводитися незабаром

після організації Спецвідділу, перші практичні результати були отримані лише у 1924 році, коли були розкриті 2 коди 2-го розвідувального відділу генерального штабу польської армії для зв'язку з військовими аташе в Москві, Парижі, Лондоні, Ревелі, Вашингтоні і Токіо.

Для органів державної безпеки особливу цінність мали дешифровані телеграми, що освітлювали шпигунську діяльність кадрових розвідників, що знаходилися під офіційним прикриттям іноземних дипломатичних, військових і консульських представництв у СРСР. Так, почате у 1924 році читання дешифрованого листування польських військових аташе дозволило отримувати таємні повідомлення польської розвідки, яка намагалася широко проводити шпигунську роботу на території СРСР. Радянська розвідка була дуже зацікавлена в отриманні подібної інформації.

Природно, що в початковий період своєї роботи Спецвідділу довелося зустрітися з великими труднощами. Досвідчених криптологів було мало, і кожному з них доводилося очолювати роботу по декількох напрямах. Молоді співробітники ще не володіли необхідними криптологічними та мовними знаннями. Перехоплення шифролистування по багатьох лініях зв'язку велося нерегулярно, можливості виділених технічних засобів були дуже обмежені. Всі роботи, пов'язані з аналізом шифроматеріалів, проводилися тільки вручну. Були й інші труднощі. Проте у міру зміцнення Спецвідділу, зростання майстерності його співробітників обсяг криптологічних досліджень з розкриття шифрів почав неухильно зростати. До 1925 року проводилася розробка шифрів вже 15 держав. У 1927 році почалося читання японського листування, а у 1930 році – листування деяких ліній зв'язку США.

Окрім розробки шифрів іноземних держав одним з актуальних завдань дешифрувального відділення Спецвідділу у цей період була розробка так званого внутрішнього шифрованого листування, тобто нелегального листування білогвардійських та інших контрреволюційних організацій, ворожих радянському ладу політичних угрупувань. Архівні документи свідчать, що фахівці 4-го відділення Спецвідділу змогли розкрити сотні різних шифрів, ключів і умовностей. Ними були прочитані тисячі всіляких листів, донесень і інших конспіративних документів, зокрема виконаних тайнописом.

На початку 1920-х років Спецвідділом досліджено багато шифроматеріалів царського Департаменту поліції і жандармерії. Було прочитано 90 документів, за якими складено 10 основних ключів. За дешифрованими матеріалами встановлено багато таємних агентів поліції і жандармерії, що працювали тепер на фабриках і заводах різних міст.

Однією з контрреволюційних організацій, шифролистування якої було вперше дешифроване у 1921 році, був «Народний союз захисту Батьківщини та сво-

боди» Бориса Савінкова. Аналізом ряду шифрованих документів встановлено, що члени цієї організації використовували шифри пропорційної заміни. Незабаром вони були розкриті.

Шифри організації Савінкова будувалися в квадраті 10х10 або були шифрами за словом на довжину алфавіту, рядки ключа чергувалися. Фактично виходили ключі до шифру або в прямокутнику 10х30, або виявлялася 10-значна перешифрувальна гама. Було розкрито 26 ключів до шифру та дешифровано більше 30 документів, що містили паролі та конспіративні явки.

У 1922-1924 роках головним чином «розкривалися» матеріали меншовицьких організацій. За ці роки було дешифровано 38 документів і розкрито 17 ключів до шифру. За цими матеріалами було встановлено 65 адрес із паролями та явками.

Перехоплювалося та доставлялося у Спецвідділ листування кримінального розшуку Китайської військової залізниці. Було дешифровано 355 телеграм, розкрито 33 ключі до шифру та один код на 900 величин.

6 лютого 1922 року на базі ВНК було утворене Державне політичне управління (далі - ДПУ) при НКВС. 1 грудня 1922 року був уведений новий штат центрального апарата ДПУ кількістю 2213 осіб, у складі якого залишився Спеціальний відділ з керівництва шифрувальною справою в країні, контролю за діяльністю шифрувальних органів і веденню радіоконтррозвідки (начальник Спецвідділу - Бокій, помічник начальника - Олександр Георгійович Гусєв, начальники відділень - Григорій Карлович Крамфус, Микола Якович Кліменков, Володимир Дмитрович Цибізов).

З того часу органи ДПУ почали приймати суворі заходи з дотримання вимог організації шифрувального зв'язку та забезпечення його безпеки. Спецвідділ ДПУ проводив розслідування фактів порушень порядку зберігання й використання шифрів і надавав рекомендації щодо покарання винних чиновників.

Так, у червні 1922 року Спецвідділ ДПУ розіслав по всіх губерніях повідомлення про недбале зберігання шифродокументів співробітником Володимирського губернського комітету компартії Щолоковим. Спецвідділ рекомендував покарати порушника 15-добовим арештом, причому виконання дисциплінарного стягнення покласти на Володимирський губернський відділ ДПУ.

Організаційний відділ ЦК РКП(б), розглянувши на засіданні 12 червня 1922 року це питання, висловив повну згоду із пропозицією Спецвідділу. Секретар ЦК Й.Сталін у супровідному листі, прикладеному до пакета документів про «володимирський інцидент», підтвердив, що й надалі «за всяке порушення інструкції з ведення шифролистування та зберігання шифродокументів, як і за порушення елементарних правил конспірації – винні будуть притягнуті до найсуворішої відповідальності».

15 березня 1923 року всім місцевим прокурорам була розіслана шифротелеграма відділу прокуратури Наркомату юстиції, де говорилося про суворе дотримання інструкцій шифрорганами. «Ніяких розмов про шифр із будь-ким без винятку не припустимо. Винні в порушенні цього будуть притягатися до відповідальності». Крім цього, співробітникам, що мали відношення до шифрорганів, заборонялося відвідувати іноземні місії, представництва та торгівельні консульства, а так само мати знайомства зі співробітниками цих органів.

26 травня того ж року був розісланий циркуляр Спецвідділу ДПУ з пропозицією максимально впорядкувати та законспірувати шифрувальну роботу, зокрема: керівникам взяти у осіб, що мають справу із шифродокументами, підписку про відсутність контактів з іноземними місіями та представництвами. У випадку наявності родичів або знайомих в іноземних місіях, співробітники шифрорганів повинні були сповістити про це шифрувальні відділення за місцем роботи.

Крім того, на початку 1923 року в країні були введені нові дипломатичні шифри, які вважались радянськими криптологами стійкими. Однак англійському криптоаналітику «Фетті» знадобилося всього лише кілька днів, щоб прочитати їхній скандальний зміст. Результатом цього став знаменитий «ультиматум Керзона» з вимогою припинити ворожі дії Москви проти Британії.

В опублікованому в травні 1923 року ультиматумі, у якому більшовики звинувачувалися в підривній діяльності, не тільки буквально цитувалися перехоплені радянські радіограми, але й відпускалися досить недипломатичні жарти на адресу росіян із приводу успішного розшифрування перехопленої англійцями їхньої кореспонденції: «У російському Комісаріаті іноземних справ напевно пригадають наступне повідомлення, датоване 21 лютого 1923 року, що було ними отримано від Ф.Раскольнікова... У Комісаріаті іноземних справ також повинні пригадати і радіограму, отриману ними з Кабула і датовану 8 листопада 1922 року... Очевидно, їм знайомо і повідомлення від 16 березня 1923 року, надіслане Ф.Раскольнікову помічником комісара іноземних справ Л.Караханом...».

Влітку 1923 року Москвою були введені нові шифри та коди, над якими Фетерлейну та його колегам знову довелося «поламати голову». Але до кінця 1924 року вони все ж таки знову змогли розшифрувати значну частину радянського дипломатичного листування.

4.2. Становлення криптослужб СРСР

6 липня 1923 року на території колишньої Російської імперії була утворена нова держава – Союз Радянських Соціалістичних Республік (далі - СРСР) та затверджена її Конституція. 2 листопада того ж року при РНК СРСР було утворене Об'єднане державне політичне управління (далі - ОДПУ), а 15 листопада затвер-

джено «Положення про ОДПУ». На підставі цього Положення ДПУ республік було виведене із підпорядкування республіканських НКВС і було перепідпорядковано безпосередньо ОДПУ при РНК СРСР.

12 листопада 1923 року згідно з новим «Положенням про НКЗС СРСР» його шифрувальна частина була названа «шифрувальною та таємною частиною». Вона вийшла зі складу Управління справами і стала структурною частиною Секретаріату Колегії НКЗС. Однак у цей же період відбувалося скорочення штатів державних установ.

В одному з листів у відповідні органи 31 липня 1923 року нарком Г.Чичерін писав: «*На шифрчасти чрезвычайно тяжело отражаются как колоссальные сокращения, произведенные у нас, так и ужасающе низкие ставки… Мы должны признать безграничную преданность тех партийных товарищей, которые в такой тяжелой обстановке тем не менее до изнурения работают, перенося непосильную тяжесть, лежащую на безмерно сокращенной шифрчасти*».

У цьому ж листі він повідомляв, що новопризначеному члену Колегії НКЗС СРСР В.Л.Коппу доручено «працювати над всіма питаннями з організації в НКЗС шифрувальної справи». Згідно з даними про виконану в 1924 році роботу 2-го відділення таємно-шифрувальної частини НКЗС СРСР значиться, що зашифровано було 309408, а розшифровано 479299 документів.

Що стосується України, то 10 вересня 1924 року Постановою РНК УРСР на базі Шифрувального бюро ДПУ УРСР був утворений Спецвідділ. На нього покладені обов'язки з керування шифрувальною роботою у всіх наркоматах і центральних установах УРСР (крім загальносоюзних), розробки та обліку шифрів, підбору та обліку особового складу шифрувальних підрозділів, загального нагляду за додержанням конспірації у шифрувальній роботі. Постановою РНК УРСР від 24 листопада 1924 року був затверджений його штатний розклад чисельністю у 5 осіб.

28 березня 1924 року на підставі наказу Революційної Військової Ради (далі – РВР) СРСР № 446/96 про реорганізацію Центрального апарату наркомату з військових і морських справ (далі – НКВМС) СРСР Центральний шифрувальний відділ Штабу РСЧА був реорганізований у Шифрувальний відділ при РВР СРСР.

У 1925 році начальник Спецвідділу ОДПУ Бокій завдяки своїм успіхам у сфері «таємної війни» зумів зайняти посаду заступника Голови ОДПУ. Він організував зразкову роботу з питань криптології та радіорозвідки. У 1926 році була введена в дію

«Інструкція з ведення секретного та шифрувального діловодства».

7 січня 1925 року комісія при таємно-шифрувальній частині НКЗС заслухала доповідь про роботу секретної частини та ухвалила об'єднати секретну й шифрувальну частини та назвати знов створену частину таємно-шифрувальною частиною НКЗС. Через два місяці, 7 березня 1925 року, було ухвалено рішення про ліквідацію секретної частини, а замість неї створити у складі шифрувальної частини 3-е відділення (секретне), а 9 березня 1925 року Колегія НКЗС затвердила це рішення.

У цьому ж році Нарком закордонних справ СРСР Г.Чичерін знов порушує питання про поповнення персоналу шифрувальників. 21 квітня і 8 травня 1925 року він звертається з цього питання в секретаріат ЦК РКП(б): «Недостатність персоналу нашої шифрочастини стає вже державною небезпекою».

У кінці 1925 року секретаріат колегії НКЗС почав функціонувати на правах управління, секретно-шифрувальна частина була перейменована в секретно-шифрувальний відділ, а три відділення, що входили в його склад, перейменовані в перший, другий і третій підвідділи відповідно.

У вересні 1926 року найменування управлінь Штабу РСЧА стали номерними. Військове Розвідувальне Управління перетворилося на IV Управління Штабу РСЧА. Шифрувальне відділення було виведене з складу 2-го (агентурного) відділу та реорганізоване у 1-у (шифрувальну) частину IV Управління, начальником якої став Закіс, а його помічником - Едуард Янович Озолін. Шифрувальний відділ при РВР СРСР був реорганізований у 2-й відділ Управління справами НКВМС і РВР СРСР.

9 грудня 1927 року наказом ОДПУ № 242/96 було затверджено Положення про спеціальні відділення при Повноважних представництвах (далі - ПП) ОДПУ. Ці відділення виконували такі завдання:

- організовували секретне та шифрувальне діловодство у всіх установах, розташованих на території ПП ОДПУ як місцевого, так і союзного значення;
- здійснювали контроль за порядком ведення і зберігання мобілізаційних і шифрувальних матеріалів;
- вели облік осіб, що відали секретним листуванням в радянських установах;
- виробляли шифри і забезпечували ними всі установи, розташовані на території повноважного представництва за винятком тих, які користувалися шифром, встановленим Спеціальним відділом ОГПУ.

У 1927 році шифрувальний відділ НКЗС, який складався з трьох підвідділів, був реорганізований у секретно-шифрувальний відділ у складі двох підвідділів. На базі 3-го

підвідділу був утворений секретний архів НКЗС.

1 грудня 1929 року наказом ОДПУ № 282 у складі ОДПУ, крім Спецвідділу, було утворене ще Центральне шифрувальне бюро (начальник – В.М.Колосов, він же – начальник 1 відділення Спецвідділу), яке відповідало за шифрований зв'язок.

У той час Спецвідділ складався з таких підрозділів:

- 1 відділення (спостереження за збереженням режиму секретності у всіх партійних, державних і громадських організаціях, начальник – В.М.Колосов);
- 2 відділення (створення шифрів і кодів для ОДПУ, НКВМС і НКЗС, радіоперехоплення, начальник – Федір Григорович Тіхоміров);
- 3 відділення (керівництво шифрувальною роботою в системі ОДПУ, зв'язок із закордонними резидентурами, а також керівництво таборами ОДПУ, начальник – Федір Іванович Ейхманс, він же помічник начальника Спецвідділу);
- 4 відділення (дешифровування перехоплених документів, начальник – Олександр Григорович Гусєв (з вересня 1923 по січень 1938 року), він же – помічник начальника Спецвідділу);
- 5 відділення (криптографічне обслуговування військового відомства, начальник – Володимир Дмитрович Цибізов);
- лабораторія (що у свій час іменувалася 7-м відділенням і займалася прикладною хімією і графологією, начальник – Євген Євгенович Гоппіус);
- технічне відділення (начальник – Антон Дмитрович Чурган);
- фотографія (начальник – П.Алексєєв).

Коло питань, що вивчалися підрозділами, які працювали на лабораторію Гопіуса, було надзвичайно широким: від винаходів усіляких пристосувань, пов'язаних із радіошпіонажем до дослідження сонячної активності, земного магнетизму й проведення різних наукових експедицій. Отут вивчалося все, що мало будь-який відтінок таємничості.

Контроль технічних нововведень радянської криптослужби здійснював заступник начальника її оперативного відділу Ейхманс. Всі фахівці-криптологи та радіотехніки проходили за таємним позаштатним розкладом. Загальна кількість особового складу Спецвідділу складала 189 осіб.

Цікаво, що начальник Спецвідділу Бокій робив спроби використовувати для криптологічної діяльності фахівців з окультних та містичних наук. Так, взимку 1924 року він залучив до роботи на Спецвідділ вченого-містика Олександра Барченка. Основні наукові інтереси цього дослідника були зосереджені в сфері вивчення біоелектричних явищ в житті клітини, в роботі мозку та живому організмі в цілому. Свої лабораторні досліди Барченко суміщав з посадою експерта Спецвідділу з психології та парапсихології. Зокрема, ним розроблялася методика виявлення осіб, схильних до криптологічної роботи та розшифровування кодів.

Вчений виступав і консультантом при обстеженні всіляких знахарів, шаманів, медіумів, гіпнотизерів і інших людей, які стверджували, що вони спілкуються з примарами. З кінця 1920-х років Спецвідділ активно використовував їх у своїй роботі. Для перевірки цих «екстрасенсів» один із підрозділів служби Бокія обладнав «чорну кімнату» в будівлі ОДПУ за адресою: Фуркасівський провулок, будинок 1.

Дослідження та методика Барченка застосовувалися і в особливо складних випадках дешифровування ворожих повідомлень – в таких ситуаціях проводилися навіть групові сеанси зв'язку з духами.

Барченко привніс в життя Бокія метафізичні теорії та умовив видного чекіста вступити в таємну окультну організацію «Єдине Трудове Братерство», що вивчала стародавню науку «Дюнхор», яка нібито перевершувала сучасне знання, але принципи якої були втрачені з часом.

До складу «Єдиного Трудового Братерства» увійшли, крім Бокія, ще такі особи: член ЦК ВКП(б) Моськвін, заступник наркома закордонних справ Стомоняков, працівник Спецвідділу Гоппіус, а також давні товариші Бокія по Гірському інституту інженери Міронов і Кострікін. Крім того, відомо, що на доповідях Барченка про «Дюнхор» були присутні в різний час співробітники Спецвідділу Гусєв, Цибізов, Філіпов і Леонов.

У кінці 1925 року для передачі езотеричного знання найбільш «гідним» представникам більшовицької партії Олександр Барченко за участю Бокія організував у «надрах» ОДПУ невеликий гурток із вивчення «Дюнхору». До нього увійшли провідні співробітники Спецвідділу: Гусєв, Цибізов, Кліменков, Філіпов, Леонов, Гоппіус, Плужніцов. Заняття із співробітниками Спецвідділу продовжувалися недовго, оскільки, за словами самого Бокія, учні виявилися «не підготовленими до сприйняття таємниць стародавньої науки». Врешті-решт, гурток Барченка розпався, але декілька разів його заняття відвідував і Генріх Ягода – майбутній шеф НКВС.

28 березня 1928 року на нараді у начальника 2-го відділу Управління справами НКВМС і РВР СРСР було прийнято ухвалу про організацію «військово-морської частини з дешифрування в Центрі, у Москві». Але справа просувалася украй поволі. Нова нарада, що відбулася 10 січня 1929 року та була присвячена тому ж питанню, на якому крім керівників ОДПУ і Спецвідділу, представників штабу РСЧА і Військово-морського флоту були також працівники морських штабів Балтійського та Чорного Морів, знов підтвердила необхідність організації відповідної дешифрувальної служби. Проте пройшов ще рік, а «військово-морська частина з дешифрування» ще не була створена.

Наприкінці лютого 1930 року Бокій підготував листа Ворошилову, в якому писав: «Спеціальний відділ при ОДПУ вважає такий темп, узятий штабом РСЧА у

вирішенні питання щодо організації військово-морської частини з дешифрування, дуже повільним. Бажано прискорити вирішення цього питання, тобто стосовно дешифрувальної служби РСЧА відстала від армій своїх можливих супротивників, у яких ця справа давно налагоджена».

І лише у серпні 1930 року був створений перший дешифрувальний підрозділ при штабі РСЧА. Знаходився він у оперативному підпорядкуванні Спецвідділу при ОДПУ і фактично входив у його склад. За штатом він називався 13-м сектором 7-го відділу Штабу РСЧА. Наказом РВР від 5 серпня 1930 року було затверджене «Положення про 7-й відділ».

В одному з пунктів цього Положення було записано, що на відділ покладалися питання організації дешифрувальної роботи, керівництво та контроль над нею. «Начальник 7-го відділу в спеціальному відношенні підпорядковується начальнику Спеціального відділу при ОДПУ». Начальником військово-морського дешифрувального сектора було вирішено призначити помічника начальника Спецвідділу при ОДПУ Павла Хрисанфовича Харкевича.

Розвиток військової дешифрувальної служби просувався швидкими темпами. Менш ніж через рік 13 дешифрувальний сектор був реорганізований у 5 відділ 4-го управління штабу РСЧА, але як і раніше залишився в оперативному підпорядкуванні Спецвідділу при ОДПУ. Всі працівники відділу мали хорошу мовну підготовку та зарекомендували себе здібними аналітиками. Провідними фахівцями у дешифруванні військових шифрів того часу були Борис Володимирович Звонарьов, Карл Густавович Тракман, Павло Матвійович Шунгський тощо.

15 листопада 1929 року були відкриті «Курси вдосконалення командного складу РСЧА», на яких готувалися офіцерські кадри шифрувальної служби. Тоді ж у Херсоні в найсуворішій таємності був організований відділ з підготовки офіцерів шифрувальної справи. Саме випускники херсонського відділу згодом брали участь у розробці малогабаритної дискової кодувальної машини К-37 «Кристал», що зробила дійсну революцію в шифрувальній справі.

У січні 1931 року були відкриті об'єднані дешифрувально-розвідувальні 3-місячні курси «спецпризначення» для підготовки криптологів дипломатичного та військового напрямів. Начальником курсів був призначений Харкевіч, а викладачами – Зибін, Ямченко, Аронський, Кильдишев. У 1934 році начальником цих курсів був призначений досвідчений криптолог Сергій Григорович Андреєв, який працював у Спецвідділі з 1921 року.

12 лютого 1930 року адміністративна комісія НКЗС розглянула питання про покращення роботи й зміну структури секретаріату колегії та ухвалила виділити зі складу секретаріату секретно-шифрувальний відділ як самостійний відділ та підпорядкувати його безпосередньо одному з членів колегії. 3 березня 1930 року Колегія НКЗС СРСР затвердила це рішення комісії.

У березні 1930 року начальником 1-ої (шифрувальної) частини IV (Розвідувального) Управління Штабу РСЧА був призначений Озолін, а дешифрувальний сектор 8-го відділу Штаба РСЧА був переведений до 5-го відділення Спецвідділу при ОДПУ для забезпечення спільної роботи над шифролистуванням іноземних держав.

У вересні 1930 року 2-ий відділ Управління справами НКВМС був реорганізований у 7-ий відділ Штабу РСЧА, а вже 13 жовтня 1930 року – у 8-ий відділ Штабу РСЧА. У штабах військових округів і морів шифроргани іменувалися 7-ми відділами, які у лютому 1931 року були перейменовані в військових округах у 8-і відділи, а на морях і флотах – 10-і відділи.

У березні 1931 року у складі IV Управління (з 22 листопада 1934 року – 5 Управління) Штабу РСЧА був утворений 5-ий (дешифрувальний) відділ (начальник – Харкевич). Військово-дешифрувальний сектор 5-го відділення Спецвідділу при ОДПУ був переведений до 5-го відділу IV управління Штабу РСЧА.

У зв'язку із збільшенням обсягу та підвищенням значення дешифрувальної роботи у 1932-1933 роках були створені дешифрувальні групи при повноважних представництвах ОДПУ у Києві, Тбілісі, Хабаровську, Ташкенті і Ленінграді, а потім у Читі і Владивостоку. Пізніше ці групи були перетворені у дешифрувальні відділення.

У 1931-1932 роках криптовідділи були утворені вже у всіх військових округах, а до середини 30-х років чисельність криптослужб СРСР у центрі й на місцях досягла приблизно 500 осіб, що цілком відповідало потребам того часу. Склалася досить ефективна система криптослужб, які дешифровували до 30% всієї перехопленої інформації, що було дуже гарним показником для того часу.

У 1932 році було утворене дешифрувальне відділення в Особливій Червонопрапорній Далекосхідній Армії, а у 1935-1936 роках – у Забайкальському, Середньоазіатському та Київському військових округах. Ці відділення, так само як і в центрі, знаходилися в оперативному підпорядкуванні ОДПУ.

7 червня 1934 року начальник IV Управління (розвідувального) Штабу РСЧА Берзін, куди входила у той час військова дешифрувальна служба, представив наркому з військово-морських справ, голові РВР маршалу Ворошилову доповідь про дешифрувально-розвідувальну службу (ДРС):

«Шифродокументи поступають від 52 країн, проте розробляються спільно із Спеціальним відділом при ОДПУ як тільки документи 22 країн... За 1933 р. при напруженій роботі часом за рахунок передчасного зносу розумових та фізичних сил працівників ДРС розроблено тільки 42% матеріалів, що є для розробки. 58% іноземних шифрованих документів, що можуть дати цінну додаткову інформацію, залишилися необробленими через нестачу кадрів».

У доповіді було висловлено прохання про посилення служби кадрами, зо-

крема пропонувалося збільшити чисельність кадрового складу на 10 чоловік і перевести 16 чоловік вільнонайманих у адміністративний склад. Не зважаючи на скромність прохань, викладених у доповіді Берзіна, вони не були у 1934 році задоволені, тому відділ продовжував працювати в колишньому чисельному складі.

У 1933 році шифрувальники Спецвідділу при ОДПУ працювали у великій кімнаті на 4-му поверсі обширної будівлі колишньої страхової компанії на вулиці *«Лубянка»* в Москві. А дешифрувальники займали верхній поверх колишньої будівлі НКЗС на розі вулиць *«Лубянка»* і *«Кузнецкий мост»*. Той факт, що нижні поверхи будівлі відвідувалися приватними особами і членами дипломатичного клубу, використовувався для маскування.

10 липня 1934 року ОДПУ увійшло до складу НКВС як Головне управління державної безпеки (далі – ГУДБ), а його регіональні органи увійшли до складу регіональних управлінь НКВС. Згідно з цим Спецвідділ ОДПУ був реорганізований у Спецвідділ ГУДБ НКВС.

22 листопада 1934 року було оголошено Ухвалу ЦВК і РНК СРСР про затвердження Положення про Народний комісаріат оборони (далі – НКО), згідно з яким у його склад увійшло Розвідувальне управління (далі – РУ), що раніше входило до складу штабу РСЧА. 15 грудня 1935 року був змінений і затверджений новий штат РУ РСЧА, згідно з яким 5-ий (дешифрувальний) відділ став 7-м відділом, а 1-а (шифрувальна) частина стала таємно-шифрувальним відділенням (іноді іменувалося відділенням «Ш»). Чисельність 7-го відділу складала 53 особи і 5 осіб постійного складу було виділено на Центральні курси ДРС.

Начальником 7-го відділу з лютого 1936 року по лютий 1939 року був полковник Харкевич, а його заступником – майор Звонарьов, який досконало володів чотирма іноземними мовами, трьома європейськими і японською. Начальником відділення «Ш» з січня 1935 року по листопад 1937 року був полковий комісар Озолін, а з вересеня 1938 року по травень 1939 року – майор Микола Олександрович Філатов.

У 1935 році за виконання спеціального завдання командування Звонарьов був нагороджений іменним золотим годинником наркома оборони, а у 1936 році – орденом Червоного Прапора. Річ у тому, що фахівці ДРС спільно з фахівцями Спецвідділу розкрили у жовтні 1935 року японський дипломатичний код, про що доповіли начальнику Розвідувального управління РСЧА С.Г.Урицькому. Останній написав рапорт заступнику наркома Гамарнику, а він, враховуючи важливість події, розпорядився доповісти про це особисто наркому Ворошилову. Ось доповідь Урицького Ворошилову:

«15 жовтня п. р. японський уряд відхилив свій основний код і ввів замість нього новий. Виникла загроза не мати інформації про військові заходи Японії

щодо лінії дешифрування японських шифротелеграм у потрібний момент. Помічник начальника... відділу РУ РСЧА т. Звонарьов Б.В. спільно з працівниками його підрозділу тт. Шунгським, Калініним, Мильниковим і працівниками Спецвідділу ГУДБ НКВС тт. Єрмолаєвим і Єрмаковою у мінімально короткий термін, у 6 днів, розкрили вказаний код і забезпечили безперебійне розшифрування японських шифротелеграм. Ці результати досягнуті завдяки систематичній підготовці т. Звонарьовим свого підрозділу до виконання завдань, що стоять перед ним. Безпосередньо при розкритті коду особливо важливу роль зіграли тт. Звонарьов і Шунгський. Клопочу про нагородження цінними подарунками... т. Звонарьова Б.В. і фахівців тт. Шунгського, Калініна і Мильникова...»

На цьому рапорті нарком оборони наклав резолюцію: «Нагородити т. Звонарьова золотим годинником, а решту тт. срібними (хорошими) годинниками. К.В. 27.XI.35 р.».

У 1935 році шифрувальники та дешифрувальники Спецвідділу переїхали в нову будівлю на вулиці імені Фелікса Дзержинського. Шифрувальний відділ був розділений на декілька відділень, які займалися забезпеченням секретного зв'язку з регіональними управліннями секретної поліції, з її прикордонними частинами і військовими формуваннями, з адміністраціями в'язниць і таборів, з нелегальною закордонною агентурою і з «легальними» резидентурами за кордоном.

За секретний зв'язок з «легальними» резидентурами відповідало 6-е відділення. Його начальник з прізвищем Козлов був знятий з посади під час репресій у 1937 році. А після того, як наступник Козлова був відправлений шифрувальником до США, начальником 6-го відділення стала людина, чиє ім'я придбало згодом скандальну популярність. Це був Володимир Петров, який у 1954 році разом з дружиною Євдокією отримав політичний притулок в Австралії.

Дешифрувальний відділ був розділений на відділення за географічним і мовним принципом – китайське, японське, англо-американське і так далі. Майбутня пані Євдокія Петрова (Дуся), яка протягом двох років вивчала японську мову в московській спецшколі, працювала в японському відділенні. Її колегами по роботі були:

- Віра Плотнікова, дочка професора японської мови, яка протягом багатьох років була резидентом японської розвідки у Москві;
- Галина Підпалова, настільки закохана у все японське, що, прийшовши додому, вона незмінно одягалася в кімоно;
- Іван Калінін, який час від часу запрошувався як консультант;
- професор Шунгський – головний авторитет відділення з питань японської мови, який служив ще в царській армії.

У 1938 році була проведена чергова реорганізація НКВС. В результаті для

ведення шифрованого листування у його структурі 9 червня був утворений 3-й спецвідділ, начальником якого став капітан держбезпеки Олександр Дмитрович Баламутов. 29 вересня Спецвідділ ГУДБ НКВС був перейменований у 7-й відділ начальником якого став той же Баламутов. У 1939 році до складу 7-го відділу ГУДБ НКВС було переведене дешифрувальне відділення Розвідувального відділу НКВМФ СРСР, яке було утворене у 1938 році. 9 квітня 1939 року начальником 7-го відділу був призначений капітан держбезпеки Олексій Іванович Копитцев. Станом на 1 січня 1940 року у складі 7-го відділу працювало 230 осіб.

У травні 1939 року був реорганізований і секретно-шифрувальний відділ НКЗС. Шифрувальний відділ був виділений з нього як самостійний відділ з безпосереднім підпорядкуванням заступнику наркома та перейменований у 10-й відділ НКЗС. Найменування посади «шифрувальник» було скасовано та були введені посадові назви «референт», прийняті в оперативних відділах НКЗС.

19 липня 1939 року відповідно до Постанови Комітету Оборони СРСР 8-й відділ ГШ РСЧА був перейменований у Відділ шифрувальної служби і включений на правах самостійного структурного підрозділу до складу Оперативного управління ГШ РСЧА.

У 1939 році у зв'язку з реорганізацією 5-го (розвідувального) Управління НКО шифрувальне відділення стало 9-м відділом, а 7-й (дешифрувальний) відділ став 11-м відділом. Начальником 9-го відділу до жовтня 1939 року був Філатов, а з жовтня 1939 року став майор Леонтій Сергійович Пілєвін. Начальником 11-го відділу з жовтня 1939 року став Філатов.

Наказом НКО СРСР № 0038 від 26 липня 1940 року 5-е (розвідувальне) Управління НКО увійшло до складу Генерального штабу (далі - ГШ) Червоної Армії (далі - ЧА) і почало називатися РУ ГШ ЧА. У його складі залишився 9-й (шифрувальний) відділ (начальник - майор Пілєвін), а 11-й (дешифрувальний) відділ став 10-м відділом (начальник - полковник Філатов). 18 серпня 1941 року на базі Відділу шифрувальної служби Оперативного управління ГШ ЧА було створено Управління шифрувальної служби ГШ ЧА загальною чисельністю 197 військовослужбовців і 50 службовців.

Указом Президії Верховної Ради (далі - ПВР) СРСР від 3 лютого 1941 року зі складу НКВС був виділений наркомат державної безпеки (далі – НКДБ). Шифрувально-дешифрувальна справа перейшла до 5-го відділу НКДБ, начальником якого став майор держбезпеки Копитцев. Для ведення шифролистування у складі НКВС наказом № 00198 від 22 лютого 1941 року було організовано 6-е відділення, начальником якого став Солодянніков.

Після початку Великої вітчизняної війни Указом ПВР СРСР від 20 липня 1941 року НКВС і НКДБ були знов об'єднані в єдиний НКВС. Шифрувально-дешифрувальна справа перейшла до 5-го спецвідділу НКВС, начальником якого став

майор держбезпеки Іван Григорович Шевельов, а його заступником - старший майор держбезпеки Копитцев. Спецвідділ станом на 20 травня 1942 року мав за штатом 683 одиниці та складався з 16 відділень, завдання яких були такими:

- 1 - дешифрувально-розвідувальна робота (далі - ДРР) по Німеччині;
- 2 - ДРР по Японії, Манчжоу-го; - 3 - ДРР по Англії, США;
- 4 - ДРР по Італії, Іспанії; - 5 - ДРР по Франції, Бельгії;
- 6 - ДРР по Балканах, Скандинавії, Фінляндії;
- 7 - ДРР по Туреччині, Ірану, Іраку, Афганістану;
- 8 - ДРР по Китаю;
- 9 - складання, дослідження та друкування кодів для НКЗС, НКВТ, НКВС, НКО і НКВМФ;
- 10 - складання та друкування блокнотів для НКО, НКВМФ, НКВС, НКЗС, НКВТ;
- 11 - здійснення шифрозв'язку оперативно-чекістських управлінь і відділів НКВС; зашифрування та розшифрування телеграм, облік і постачання шифрдокументів периферійним органам НКВС і їх інструктаж щодо шифрроботи;
- 12 - здійснення шифрозв'язку таборів НКВС, прикордонних, внутрішніх і оперативних військ НКВС, Прокуратури, Військової колегії Верховного суду СРСР;
- 13 - здійснення шифрозв'язку закордонної резидентури 1-го Управління НКВС;
- 14 - оперативно-чекістське обслуговування шифрорганів наркоматів і інших установ;
- 15 - перевірка та допуск осіб, що працюють з секретними, мобілізаційними та шифрувальними документами в установах і підприємствах; спецперевірка особового складу, що працюють на особливо режимних підприємствах;
- 16 - агентурно-оперативне.

16 лютого 1942 року наказом НКО № 0033 РУ ГШ ЧА було реорганізоване в Головне РУ (далі - ГРУ), а 23 вересня наказом НКО № 00222 з метою концентрації зусиль щодо «розкриття» шифролистування супротивника дешифрувальна служба ГРУ була передана до 5-го спецвідділу НКВС. 3 листопада наказом НКВС № 002424 на базі 5-го спецвідділу, до якого увійшли 7-й відділ (дешифрувальний) 2-го Управління ГРУ та частини спецслужби внутрішніх військ НКВС (радіорозвідка) було утворено 5-е управління НКВС. Його начальником став старший майор держбезпеки Шевельов, а його заступником - комісар держбезпеки Копитцев. У складі 5-го Управління була також утворена Криптографічна Рада для організації і координації наукових досліджень і підготовки наукових кадрів

у спецслужбі (за роки війни розглянула більше 60 питань і проблем за основними напрямами спеціальної роботи).

14 квітня 1943 року у зв'язку з наближенням радянських військ до кордонів СРСР рішенням Політбюро ЦК ВКП(б) № П 40/91 «Про утворення НКДБ СРСР» і ухвалою РНК СРСР № 393-129сс зі складу НКВС знову був виділений НКДБ. Шифрувально-дешифрувальна справа та спецзв'язок перейшли до 5-го Управління НКДБ. Його начальником став комісар держбезпеки Шевельов, а його заступниками - комісар держбезпеки Копитцев і старший майор держбезпеки Сергій Вікторович Покотіло.

Для ведення шифролистування у складі НКВС наказом № 00776 від 28 квітня 1943 року був утворений 2-й спецвідділ, начальником якого став підполковник держбезпеки А.Воробйов, а з 1944 року по 21 березня 1949 року був підполковник В.Романов. Станом на 1 квітня 1945 року спецвідділ мав по штату 52 одиниці, а в наявності - 49 осіб. 3 травня 1949 року наказом МВС № 544 начальником спецвідділу був призначений колишній заступник начальника Управління кадрів МВС полковник І.І.Філаткін.

Закінчення Другої світової війни та зміни у світовому геополітичному становищі підштовхнула радянський уряд до реорганізації органів влади та державної безпеки. Так, 15 березня 1946 року 5-а сесія Верховної Ради СРСР прийняла Закон про перетворення Ради Народних Комісарів СРСР в Раду Міністрів СРСР, а народних комісаріатів – у міністерства.

Таким чином, НКВС перетворився у Міністерство внутрішніх справ (далі - МВС), НКДБ - Міністерство державної безпеки (далі - МДБ), НКЗС - Міністерство закордонних справ (далі - МЗС), НКО - Міністерство оборони (далі - МО) тощо. Наказом НКДБ № 00107 від 22 березня 1946 року 5-е (шифрувально-дешифрувальне) Управління НКДБ стало 6-м Управлінням МДБ. Його начальником став генерал-лейтенант Шевельов, а його заступником - генерал-майор Копитцев.

20 серпня 1946 року Рішенням Політбюро ВКП(б) була затверджена нова концепція структури держбезпеки та її напрямків діяльності. Вона припускала подальший розподіл органів держбезпеки та створення незалежних та конкуруючих між собою спецслужб, причому Секретаріат ЦК ВКП(б) виступав у цій схемі як арбітр. На виконання даної концепції у травні 1947 року на базі 1-го ГУ МДБ і ГРУ ГШ ЗС було утворене нове розвідувальне відомство – Комітет Інформації при Раді Міністрів СРСР, який проіснував до 1951 року. До його складу увійшов і дешифрувальний відділ ГРУ ГШ ЗС, який був реорганізований у 7-е Управління Комітету Інформації.

19 жовтня 1949 року Постановою Політбюро ЦК ВКП(б) № П71/426 було прийнято найважливіше для радянської криптології рішення. Вся шифрувально-дешифрувальна робота з МДБ передавалася до ЦК ВКП(б) і, відповідно, 6-е Управління

МДБ ліквідовувалось. Це було оформлено наказом МДБ № 00369 від 15 листопада, а у складі ЦК ВКП(б) було створено Головне управління спеціальної служби (далі – ГУСС). Його начальником став генерал-лейтенант Шевельов, а начальником 1-го Управління (дешифрувально-інформаційного) - генерал-майор Копитцев.

4.3. Створення радянської шифротехніки

В даний час у закордонній і вітчизняній літературі є багато публікацій про закордонні електромеханічні шифрувальні машини, аж до описів принципів їхніх дій і фотографій. При цьому аналогічних публікацій про радянську шифрувальну техніку (також застарілої і знятої з експлуатації) дотепер дуже мало. Недостатність інформації з цього питання створює помилкове враження, що шифрувальна справа в СРСР у частині автоматизації найскладних процесів шифрування безнадійно відстала від передових країн світу. Але насправді це не відповідає дійсності.

Більш того, існуючий пробіл в історії вітчизняного спеціального приладобудування, як частини історії країни, незаслужено збіднює її в цілому, тому що створення у 1930-і роки в Ленінграді вітчизняної шифрувальної техніки та організація її промислового виробництва є досягненнями національного рівня. Це варто знати та пишатися нашими попередниками. Крім того, власний шлях еволюційного розвитку вітчизняних шифрувальних машин також являє історичну цінність, особливо в порівнянні з досягненнями передових у цій сфері західних країн того часу.

У молодій Радянській республіці ніякої шифрувальної техніки не існувало зовсім, але багато хто вже серйозно задумувалися над тим, як вирішити цю проблему. Саму активну позицію з цього питання займали фахівці 8-го (криптологічного) відділу ГШ РСЧА. Однак перша спроба створити електромеханічний шифратор була розпочата не криптологами та не шифрувальниками. Є дані, що це зробили в 1923 році фахівці Особливого технічного бюро з військових винаходів спеціального призначення (далі – ОТБ), що не мали до шифрувальної справи ніякого відношення.

Остехбюро було утворене 18 червня 1921 року Постановою Ради Праці й Оборони як філія московського науково-дослідного інституту (далі – НДІ) № 20, що займався розробками в сфері радіотехніки для армії і флоту. Очолив нове відомство талановитий російський винахідник В.Бекаурі.

В ті роки радянському керівництву вже стало зрозуміло, що наявні ручні системи й способи шифрування й кодування, скільки б їх не вдосконалювали й модернізували, не в змозі впоратися із все зростаючими потоками інформації в силу слабкої швидкості її обробки. Було загострено питання щодо механізації даного процесу.

У 1923 році в ОТБ був розроблений і, навіть, виготовлений діючий макет дискового шифратора. Більш докладні дані про нього відсутні, та й подальша розробка шифратора була припинена, тому що це відволікало фахівців від планової роботи термінового характеру. Після масових репресій 1937–1938 років в ОТБ та його наступної реорганізації зник і сам шифратор. Він, можливо, був просто знищений як не потрібний для людей, далеких від проблем криптології. Проте можна констатувати, що одна з перших спроб механізувати процес шифрування в Радянській республіці усе-таки відбулася.

Наступна спроба ініціювати розгляд питання щодо створення вітчизняної шифрувальної машини була розпочата шифрувальниками-моряками на нараді у 2-му відділі Управління справами Народного комісаріату з військових і морських справ, що відбулася в січні 1929 року. До порядку денного серед інших було включене питання про «машинізацію» шифрування (термінологія того часу), ретельно підготовлений морськими шифрувальниками. У результаті детального обговорення було докладно з'ясоване, яку саме моряки хотіли б бачити першу шифрувальну машину. Підсумки наради занесли до протоколу, наприкінці якого потенційним розробникам запропонували заглянути у майбутнє: «...Вважати бажаним і найбільш прийнятним для кораблів флоту введення такої шифрувальної машини, що одночасно самошифрує і передає радіоапаратом...». Показово, що вже в 1929 році радянські моряки порушили питання про створення не просто машини попереднього шифрування, а машини лінійного шифрування.

Учасники наради розуміли, що країна ще не вийшла з «розрухи» після громадянської війни і не мала реальної можливості для створення надійної шифрувальної машини. Однак звернення фахівців Спецвідділу ОДПУ і 8-го відділу ГШ РСЧА до керівництва НКО щодо утворення підприємства з розробки та виготовлення шифротехніки не дало позитивного результату. Наркомат не мав для цього необхідних ресурсів. Тоді фахівці 8-го відділу, що наполягали на розгортанні робіт з механізації шифрувальної справи, запропонували доручити цю роботу якому-небудь приладобудівному заводу, найбільш пристосованому для вирішення цього складного завдання.

Для вирішення цього питання наприкінці 1933 року в Москві була сформована робоча група з фахівців Спецвідділу і 8-го відділу, якій було доручено відібрати з підприємств Москви та Ленінграда найбільш придатні для розробки та виготовлення вітчизняної шифротехніки. Група повинна була, вибравши кілька заводів, проаналізувавши їхній стан на момент обстеження і спрогнозувавши перспективний потенціал кожного, рекомендувати керівництву НКВС і ГШ РСЧА конкретне підприємство. Далі цій же групі ставилася в обов'язок підготовка для обраного заводу пропозицій і рекомендацій з організації та фінансового забез-

печення промислового випуску шифротехніки.

Після громадянської війни більшість підприємств, хоча і працювало, але знаходилося у вкрай жалюгідному стані. Практично відразу ж були зняті з розгляду приладобудівні заводи Москви, відновлення яких йшло дуже повільно. Швидше усіх відновлювалися заводи, що були задіяні в затвердженій урядом «Програмі з військового кораблебудування на першу п'ятирічку» (1926–1932). У їхнє число входили ленінградські приладобудівні заводи імені Кулакова та «*Электроприбор*».

Після попереднього розгляду виробничо-технічних характеристик обох заводів більшість членів групи схилялося до того, щоб доручити розробку та випуск вітчизняної шифрувальної техніки заводу імені Кулакова, аргументуючи свої пропозиції таким чином:

- завод імені Кулакова був створений на базі «Електромеханічного заводу Гейслера і К°», заснованого у 1896 році. Його основну номенклатуру складала телеграфна і телефонна апаратура, телеграфні станції та телефонні комутатори. У процесі розвитку заводу до виробництва техніки, що вже випускалася, додалися електромеханічні прилади для ВМФ (різні види сигналізації, прилади керування артилерійським вогнем і торпедною стрільяниною, далекоміри, прилади точної механіки та електро- й радіотехніки). Тут працювали висококваліфіковані фахівці як у області розробки, так і у сфері виробництва електромеханічних приладів із застосуванням точної механіки.
- до 1928 року завод був цілком відновлений і навіть зміг виготовити для першої промислової виставки свою продукцію. Повним ходом йшла реконструкція, спрямована на подвійне збільшення виробничих площ, помітно збільшувався верстатний парк;
- вирішальним аргументом на користь заводу була наявність у його складі могутнього комбінату телеграфії, який до цього часу вже мав досвід розробки вітчизняних телеграфних апаратів.

Так, до 1929 року А.Шоріним був розроблений телеграфний апарат Ш-29, а до 1933 року завод став виготовляти кілька модифікацій цього сімейства, у тому числі й новітній телеграфний апарат Ш-33. У 1934 році головним конструктором Є.Міловідовим був розроблений нормальний одноканальний телеграфний апарат «*НОТА-34*». Роком пізніше М.Гагарін, узявши за прототип друкувальний пристрій телеграфного апарата Т-14 фірми «Моркрумкляйншмідт», створив власну оригінальну конструкцію вітчизняного стартстопного телеграфного апарата СТ-35 (рос. *советский телетайп 1935*). Апарат мав безліч модифікацій і проробив на лініях зв'язку до 60-х років.

У 1937 році під керівництвом С.Шендерова був розроблений рулонний одноканальний телеграфний апарат «*РОТА-38*». У 1938 році під керівництвом

начальника відділу І.Федорова був розроблений перший вітчизняний фототелеграфний апарат (більдапарат) у двох варіантах: настільний і чемоданний. Доведення конструкції більдапаратів було доручено С.Шендерову. Паралельно з цією роботою останній винайшов і сконструював апарат, що передавав фотозображення по радіо. Результати іспитів були оптимістичними. На дослідному зразку отримано чітке та контрастне зображення, цілком прийнятне при оперативній аерофотозйомці. На жаль, під час одного з іспитових польотів відбулася авіакатастрофа і С.Шендеров загинув. Довести апарат до виробництва без нього не вдалося, а з початком Великої Вітчизняної війни роботи були взагалі припинені.

Завод «*Электроприбор*» також був відновлений та випускав корабельні прилади для ВМФ, але практично не мав ніякого досвіду в розробці та виготовленні телеграфної апаратури, техніки конструктивно дуже близької до шифрувальної. В результаті було вирішено створити науково-виробничу структуру з розробки та виготовлення шифротехніки на заводі імені Кулакова.

Теоретичну основу створення шифротехніки вперше запропонував на засіданні наукової ради РСЧА 29 червня 1930 року інженер-конструктор Іван Павлович Волосок. Згодом саме він став провідним конструктором багатьох зразків шифрувальної та кодувальної техніки довоєнного й післявоєнного періодів. За основу був узятий принцип накладення комбінацій так званої гами нескінченного ключа на комбінації знаків відкритого тексту. У підсумку виходила криптограма з гарантованою стійкістю. Як носій знаків гами використовувалася перфострічка, виготовлена за допомогою спеціального пристрою, що одержав назву «Ікс». Це було оригінальним і вдалим винаходом, який дозволяв одержувати шифрострічку з гамою випадкової послідовності, що забезпечувало необхідну гарантовану стійкість шифрування будь-яких повідомлень.

У 1931 році при 8-му відділі ГШ РСЧА була утворена технічна лабораторія. У 1932 році розроблені та у лабораторії відділу виготовлені два роздільні шифруючі пристрої. Приблизно, це були спеціальні електромеханічні трансмітери для шифрувальних машин із зовнішнім носієм шифру. Одночасно з цим співробітники Спецвідділу НКВС, уже маючи у своєму арсеналі конкретні напрацювання, приступили разом з фахівцями 8-го відділу до складання проекту технічного завдання на конструювання вітчизняної шифромашини.

І вже у тому ж році під керівництвом інженера Волоска був створений перший дослідний зразок шифромашини, що одержала назву «ШМВ-1» (Шифрувальна Машина Волоска). Також були розроблені дослідні зразки механічних шифрувальних пристосувань до телеграфних апаратів, які, втім, не одержали подальшого розвитку. У силу своєї громіздкості й механічної ненадійності «ШМВ-1» не пішла в серію, однак послужила прототипом для наступного створення

нових серійних зразків.

Таким чином, група радянських фахівців, перебороwши всі технічні та організаційні труднощі, вклавши в створення машини усе своє уміння, винахідливість, знання, фізичну й моральну силу, розробила з «чистого аркуша» вітчизняну шифромашину. Враховуючи, що на організацію її серійного виробництва пішло менш року, це є унікальним випадком у світовій практиці, особливо, з урахуванням загального стану промисловості СРСР в ті роки. Необхідно звернути також увагу на те, що це могли зробити тільки люди, які пішли на це добровільно, і усвідомлюючи, що значить для держави наявність вітчизняної шифротехніки, вважали її створення своїм громадянським обов'язком.

Ця історія дозволяє також зрозуміти, як країна, ще не відновлена після руйнівної громадянської війни, змогла вирішити проблему не тільки створення вітчизняної шифротехніки, а й організувати її промисловий випуск. Необхідно відзначити, що вирішення такої проблеми по силах не кожній, навіть, розвинутій країні. Адже для цього, крім наявності необхідної кількості фахівців із криптології (причому фахівців вищого класу, жартівливо називаних «звіздарями»), потрібні були висококласні конструктори, інженери, технологи, організатори виробництва, робітники високої кваліфікації. Було потрібно спеціалізоване добре оснащене виробництво, спеціалізовані контрольноіспитові станції, лабораторії, самостійно зроблене діагностичне устаткування тощо.

У листопаді 1934 року на завод імені Кулакова (тоді він називався заводом № 209) приїхав начальник 2-го відділення 8-го відділу ГШ РСЧА капітан I рангу Волосок. Він повинен був особисто переконатися, чи зможе завод освоїти випуск нової продукції - шифрувальної техніки. Була затверджена перша група фахівців, які повинні були працювати над цією проблемою, у складі Домнічева, Ритова, Прімазової і Ізотової. Саме вони поклали початок новому напряму у вітчизняній техніці, що буде забезпечувати приховане управління військами. До кінця 1935 року (по суті, всього за шість місяців) групі вдалося вирішити всі принципові питання.

Як і планувалося, на початку 1936 року фахівці приступили до безпосереднього конструювання приладів, що повинне було завершитися випуском комплекту документації для передачі у виробництво. Робота була розподілена таким чином:

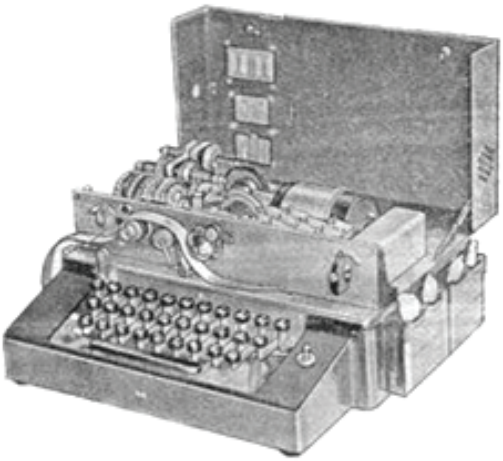
- шифрувальну апаратуру в цілому та дешифратор узяв на себе Домнічев;
- спеціальний трансміттер конструював Ритов;
- все 4 електромагнітні пристрої розробляв Андреєв, а конструював Шаригин;
- доопрацювання імпортної електромеханічної машинки «Мерседес» була доручена Прімазової;

🗝 доопрацювання серійних перфораторів (запозичених з телеграфної техніки) у вигляді окремих приладів здійснювала Ізотова.

Практично весь 1936 рік пішов на розробку конструкції приладів і пристроїв, а у 1937 році був завершений випуск конструкторської документації на шифромашину В-4. Комісія з проведення державних випробувань рекомендувала прийняти В-4 на озброєння, що одержала згодом назву «М-100». Відповідний наказ Народного комісара оборони СРСР був підписаний у середині травня 1938 року. Саме з цього зразка інженерно-криптологічної думки почався відлік створення серії шифромашин, що забезпечують й понині гарантовану стійкість застосовуваних шифрів.

До цього часу лабораторія 8-го відділу ГШ РСЧА переросла в досить потужне конструкторське бюро. У 1937 році в чорноморському санаторії Волосок познайомився з молодим офіцером-шифрувальником Михайлом Степановичем Козловим і, відчувши в ньому талант конструктора, запропонував продовжити службу в лабораторії 8-го відділу. З 1938 року 8-й відділ очолив Петро Миколайович Белюсов, який був талановитим адміністратором та прослужив на своїй посаді до 1961 року. Під його керівництвом перебувала «міцна» команда конструкторів перших радянських шифрувальних та кодувальних машин – Волосок, Судаков, Ритов, Строїтелєв, Гусєв, Шаригин, Козлов.

8 лютого 1938 року був утворений Комбінат особливої техніки, до якого увійшли відділ № 33 (що складався з конструкторського бюро, лабораторії спецтехніки таі групи технологів) і складальний цех спеціальної техніки, створений на базі дослідного виробництва. По суті, усередині заводу № 209 розмістилося невелике автономне підприємство техніки особливої секретності, яке очолив Г.С.Кукес.



Шифромашина В-4, що поступила в експлуатацію вже наприкінці 1938 року, була проста у використанні, мала мінімальний набір органів управління. Вона складалася із трьох основних вузлів (клавіатура з контактними групами, стрічкопротягувальний механізм із трансмітером і пристосування, встановлене на клавіатуру друкарської машинки) і семи додаткових. Загальна вага комплекту до-

сягала 141 кілограма. Тільки одні акумулятори для автономного живлення електричної частини машини важили 32 кілограми.

Для підвищення ефективності шифрувального зв'язку необхідно було мати декілька моделей, які б відповідали вимогам різних рівнів управління армією і флотом. Було ухвалено рішення розпочати попередні роботи з модернізації В-4 у двох варіантах. Варіант апаратури, в якій всі прилади шифромашини об'єднувалися в єдину конструкцію, запропонували провідні конструктори Валентин Миколайович Ритов і Павло Андріанович Судаков. Варіант, що складався з двох приладів, запропонував провідний конструктор Микола Михайлович Шаригин. У липні 1938 року роботу почали відразу по двох варіантах, і до кінця року обидва були готові.

Проте вже при розробці першого варіанту конструкції трансміттер і дешифратор по багатьох параметрах і характеристиках перевершили аналогічні вузли базового виробу В-4. При цьому конструктивно вони були більш компактними. У другому варіанті машина складалася з двох приладів: ТР-1001 і ПГ-1001. Шаригин проявив чудеса винахідливості та в нових конструкціях зміг застосувати максимальну кількість деталей з апаратури В-4. Але найістотнішим досягненням конструкторів в обох варіантах було створення вбудованих в шифромашину оригінальних друкуючих пристроїв їх власної розробки.

За основу для подальшої роботи був узятий другий варіант, а з першого використаний трансміттер, дешифратор і компактніший друкуючий пристрій. Під загальним керівництвом Волоска новий зразок шифромашини М-101 створювався провідним конструктором Шаригиним, а деякі її механізми винайшов і розробив особисто Козлов. У 1939 році Шаригин успішно завершив роботу, і з 1940 року шифромашина М-101 «Смарагд» почала поступати в експлуатацію. Вона складалася вже з двох основних вузлів і по габаритах була зменшена більш, ніж у 6 разів, а по вазі – більш, ніж удвічі.

Шифротехніка першого покоління (М-100/101) призначалися для штабів вищого рівня управління збройними силами там, де циркулював найбільший обсяг стратегічної та оперативно-стратегічної інформації. Дана техніка почала виготовлятися серійно та у 1938 році була успішно випробувана в бойових умовах на Хасані, в 1939 році – на Халхін-Голі, в Іспанії та під час фінської війни взимку 1939-40 року. Шифрований зв'язок у цих військових конфліктах здійснювався у ланці Генштаб – штаб армії.

У грудні 1938 року представник науково-випробувального інституту зв'язку та особливої техніки РСЧА імені Ворошилова привіз на завод технічні завдання на розробку шифруючих приладів-приставок: С-306 - до телеграфного апарату Морзе з живленням від електромережі, С-307 - для журналістів з живленням від акумуляторів, С-308 - до телеграфного апарату Бодо, С-309 - до телеграфного

апарату СТ-35. З інститутом був заключений договір, після чого почалися дослідно-конструкторські роботи.

Відповідальними розробниками шифруючих приладів були призначені: Прімазова - С-306 і С-307, Шаригин - С-308 і Ритов - С-309. У другому кварталі 1939 року роботи по шифруючих приладах були закінчені. Після випробувань С-308 і С-309 були прийняті на озброєння. З третього кварталу того ж року на заводі розпочався їх серійний випуск, який продовжився у 1942-44 роках на заводі № 707 у Свердловську. Наймасовішим шифруючим приладом-приставкою став С-308, які були встановлені на лінії Одеса-Київ одразу ж після її відкриття у 1939 році.

Разом з тим, необхідність розробки малогабаритної машини з метою заміни ручного кодування в оперативній ланці військового управління (армія – корпус – дивізія), ставала все більш очевидною. Тому було ухвалено рішення про фінансування дослідно-конструкторської роботи із створення кодувальної машини К-37 «Кристал» з дисковим шифратором. У 1939 році ця робота завершилася, і після військових випробувань «Кристал» був прийнятий на озброєння. З 1940 по 1941 роки машина випускалася заводом № 209, а під час вітчизняної війни - його філією у Свердловську (заводом № 707). Це був досить компактний пристрій, що складався з однієї упаковки вагою 19 кілограмів.

У 1939 році з метою підвищення конспірації в роботі шифрувальників та їхньої достатньої мобільності при передислокації військ в Америці були закуплені 100 автобусів «Студебекер». Після того, як вони були переобладнані під спецапаратні – шифроргани, стало можливим зашифровувати та розшифровувати телеграми не тільки під час зупинок, але й під час руху військових колон.

У 1940 році було випущено 100 комплектів К-37. А всього, до початку вітчизняної війни було прийнято на озброєння шифрорганів СРСР понад 150 комплектів К-37 та 96 комплектів М-100. До червня 1941 року всього на шифрувальній службі налічувалося 1857 чоловік. Шифрувальна техніка дозволила в 5-6 разів у порівнянні з ручним способом підвищити швидкість обробки телеграм, зберігаючи при цьому гарантовану стійкість переданих повідомлень.

У 1940 році конструктором Судаковим був розроблений військовий букводрукувальний стартстопний телеграфний апарат із знімним шифруючим блоком НТ-20. З січня 1941 року почалося серійне виробництво даної апаратури на заводі № 209, а у 1942-45 роках ці шифромашини, як і інші, згадані вище, виготовлялися на свердловському заводі. Для регламентації роботи даної апаратури незабаром після 22 червня 1941 року був виданий Наказ НКО № 0095 про засекречування передач по апарату Бодо.

Великий внесок у розробку радянських шифромашин того часу зробив Володимир Олександрович Котельников. У 1931 році він закінчив Московський

енергетичний інститут (далі - МЕІ) і, як одного з кращих випускників його залишили в аспірантурі. У тому ж році до початку занять в аспірантурі він декілька місяців працював в Науково-дослідному інституті зв'язку (далі - НДІЗ) РСЧА. Під час навчання в аспірантурі Котельниковим вперше була математично точно сформульована та доведена «теорема відліків», яка згодом була названа його ім'ям. Теорема Котельникова, яка була опублікована у 1933 році, увійшла до числа основоположних принципів теорії зв'язку та стала одним з «наріжних каменів» інформатики.

Після закінчення аспірантури у 1933 році Котельников, залишаючись викладати в МЕІ, поступив на роботу в Центральний науково-дослідний інститут зв'язку (далі - ЦНДІЗ) НКЗ на посаду інженера, а потім головного інженера. У 1938-39 роках в ЦНДІЗ була організована лабораторія під керівництвом Котельникова по засекречуванню телеграфної інформації.

У 1935 році під керівництвом Котельникова і за його участю була створена перша в наший країні багатоканальна букводрукувальна установка для роботи по радіо, яка значно перевершувала за своїми параметрами зарубіжні аналоги та згодом широко використовувалася в наший країні. У 1938 році йому був присуджений вчений ступінь кандидата технічних наук без захисту дисертації, що відбулося у Ленінградському електротехнічному інституті.

Він першим у СРСР розробив принципи побудови телеграфної апаратури засекречування шляхом накладання на повідомлення шифру, що було реалізовано в спецапараті «Москва». Запропонована схема накладання шифру на відкритий текст виявилася дуже привабливою та довгий час використовувалася в апаратурі засекречування наступних поколінь. Разом з тим, пристрій формування шифру, тобто шифратор, сконструйований на електромеханічних вузлах, був складним і громіздким.

4.4. Військова криптологія у 1940-50-і роки

Девід Кан у книзі «Війна кодів і шифрів» написав, що радянський військовий код у 1930-і роки був розкритий шведським криптологом Арне Берлінгом. Тому у період російсько-фінської війни шведи передавали фінам розвідувальні дані, отримані шляхом читання радянського шифролистування.

Радянська стратегія ведення цієї війни передбачала нанесення ударів по 5 напрямках у глиб території Фінляндії. Одне з угруповань радянської армії повинно було атакувати супротивника у районі невеликого сільця Суомусалмі, а інше, розташоване північніше, планувало наступ у напрямку села Салла. Однак розвідувальна інформація, отримана шведами з дешифрованого листування цих угруповань, допомогла фінам відбити обидва удари.

Фінський маршал Манергейм, який до революції 1917 року служив «вірою і

правдою» російському царю, зумів розгромити радянські війська під Суомусалмі. Зробив це він, в основному, завдяки тому, що завчасно одержав інформацію про висування туди 44-ї Московської ударної моторизованої дивізії. Маючи на руках ці дані, Манергейм направив до Суомусалмі необхідні підкріплення. Через два дні після того, як за наказом Манергейма 5 батальйонів прибули на місце, фінські солдати в білих маскувальних халатах, немов примари, атакували позиції радянських військ, зломили їхній опір і змусили відступити по льоду замерзлого озера Каянтоярві. Потім фінські лижники відрізали шляхи відходу 44-й дивізії та знищили її частинами у ході затяжних боїв, що продовжувалися аж до початку 1940 року. Фінами захоплено велику кількість радянського військового майна.

Шведськими криптоаналітиками була прочитана велика кількість криптограм радянських ВПС. Багато з них містили накази про нанесення бомбових ударів по столиці Фінляндії – Гельсінкі. Дуже часто ці криптограми дешифрувалися ще до моменту вильоту радянських бомбардувальників з аеродромів, розташованих у Латвії та Естонії. Завдяки цьому фінська влада мала достатній запас часу для того, щоб завчасно попередити населення міста про повітряні нальоти, і в результаті кількість жертв серед цивільного населення столиці було незначним, з огляду на величезну кількість скинутих бомб.

Однак маленька Фінляндія не могла зрівнятися за своєю військовою міццю та ресурсами з Радянським Союзом і, незважаючи на значну допомогу сусідів (у тому числі з криптоаналізу), у березні 1940 року вона була змушена підписати не зовсім прийнятний для себе мирний договір. Тому, коли роком пізніше Німеччина напала на Радянський Союз, Фінляндія охоче взяла участь у розпочатих бойових діях і приступила до активної взаємодії зі своїм новим союзником у сфері ведення шифроперехоплення.

Разом із тим, німецька радіорозвідка проти Радянського Союзу була малоефективною. У стратегічному відношенні вона взагалі не мала жодного помітного успіху. Німці виявилися не в змозі розкрити шифросистеми, що застосовувалися для засекречування листування вищого ра-

дянського військового командування. Таким чином, німецька дешифрувальна служба мало сприяла тому, щоб у командування вермахту склалася найбільш повна уява про радянську стратегію ведення війни проти Німеччини.

Значних успіхів у «розкритті» листування супротивника у 1942 році домоглися також і дешифрувальники ГРУ ГШ ЧА. Вони виявили можливості розшифровки німецьких телеграм, зашифрованих німецькою шифрувальною машиною «Енігма», і приступили до конструювання спеціальних механізмів, що прискорили це розшифрування. Таким чином, не тільки британська розвідка розкривала зміст перехоплених німецьких радіограм, зашифрованих «Енігмою».

Дешифрувальниками ГРУ було розкрито 75 шифрів німецької розвідки та прочитано понад 25 тисяч німецьких шифротелеграм. Отримані таким шляхом відомості про супротивника дозволили встановити дислокацію понад сто штабів з'єднань, розкрити нумерацію двохсот окремих батальйонів і інших частин німецької армії.

Так, у квітні 1942 року вийшов Указ ПВР СРСР «Про нагородження працівників НКВС СРСР за зразкове виконання завдань Уряду». Орденом Леніна були нагороджені два капітани державної безпеки: Борис Олексійович Аронський і Сергій Семенович Толстой, орденом Трудового Червоного Прапора – 6 співробітників, орденами Червоної Зірки і «Знак Пошани» – 13 співробітників, а медалями «За трудову доблесть» і «За трудову відзнаку» – ще 33 співробітники.

Пов'язано це було з тим, що вже в перші дні війни Аронським (за допомогою своїх помічників і перекладачів) були дешифровані кодовані повідомлення послів союзних Німеччині країн у Японії. За дорученням Імператора Японії посли доповідали своїм урядам про те, що Японія упевнена в їхній швидкій перемозі над Росією, але поки зосереджує свої сили на півдні Тихого океану проти США. Аналогічна інформація була отримана Толстим шляхом дешифрування листування вищих ешелонів влади Японії.

Ще у 1922 році Аронський був відряджений на службу до Спецвідділу. У Фінську кампанію 1939-40 років він був нагороджений орденами Червоного Прапора і «Знак Пошани», а під час вітчизняної війни – двічі орденом Леніна й орденом Трудового Червоного Прапора. Наприкінці війни займав посаду начальника відділу 5-го Управління НКДБ СРСР.

Постійно піклуючись про свою самоосвіту, Аронський поступово став знавцем російської та західної літератури, опанував французькою, англійською, німецькою, італійською і навіть японською мовами. Правда, ці знання були специфічними – досконало він знав мову та стиль дипломатичного листування, що в сполученні з природним аналітичним даром зробило Аронського блискучим «зломщиком»

кодів.

У зв'язку з відсутністю в ті роки спеціальної техніки все це робилося вручну. Проте багатомісячна робота колективу криптоаналітиків найчастіше приводила до аналітичного розкриття значної частки змісту кодової книги та можливості оперативного читання перехоплених кодотелеграм. Це й визначило успіх групи Аронського, що мало величезне значення в результаті битви за Москву.

Сергій Семенович Толстой, як і Аронський, почав служити у Спецвідділі з 1922 року, однак працював над аналізом не кодів, а шифрувальної техніки супротивника. У передвоєнні роки він очолював «японський» відділ дешифрувальної служби НКВС. Тому центром його інтересів були знамениті «червоні» та «пурпурні» японські системи. Свій перший орден «Знак Пошани» він одержав у 1940 році.

Під час Вітчизняної війни Толстой був нагороджений орденом Леніна, орденами Червоного Прапора і Трудового Червоного Прапора. Вже одне те, що безпосередні начальники Толстого й Аронського не мали стільки нагород, підтверджувало важливість дешифрованої ними інформації для Верховного командування. Тут доречно привести слова Генерального директора «*ФАПСИ*» генерал-полковника О.В.Старовойтова: «Нам була доступна інформація, що циркулювала в структурах Вермахту (майже вся!). Я думаю, нашим маршалам була зроблена істотна допомога в досягненні перелому в ході війни і, нарешті, остаточної перемоги. Наші польові центри дешифрування працювали досить успішно. Війну в ефірі ми виграли».

Не можна не відзначити і той факт, що Толстой у співавторстві з Аронським, Андреєвим і Копитцевим (останні двоє вищезазначеним Указом були нагороджені орденами Трудового Червоного Прапора) у 1939-1940 роках написали один із перших радянських підручників із криптографії, що зберігся усього в декількох екземплярах.

У той же час фашистська дешифрувальна служба також наполегливо працювала. Так, у 1943 році начальник штабу 48-го танкового корпуса полковник Мелентін, що брав участь у бойових діях у районі Радомишля в складі групи німецьких армій «Південь», писав:

«У ті дні ми успішно здійснювали перехоплення радіоповідомлень росіян. Ці повідомлення негайно дешифровувались, і їхній зміст своєчасно доповідався командуванню корпуса. Ми завжди були в курсі дій росіян, що починалися у відповідь на передислокацію наших сил, і у кожному конкретному випадку ми вносили відповідні зміни в наші плани. Спочатку росіяни недооцінили важливість нанесеного по них удару та підкинули на нашу ділянку занадто малу кількість протитанкових гармат. Потім поступово російське командування почало виявляти помітне занепокоєння. В ефірі стали з'являтися стривожені запити: «Тер-

міново уточніть, звідки наступає супротивник». Відповідь: «Довідайтеся в чортової бабусі. Як я можу довідатися, звідки наступають німці?» (Усякий раз, коли в російських радіограмах згадуються чорт і його найближчі родичі, можна було припустити, що назрівають серйозні події.) До середини дня 60-а армія росіян перестала виходити в ефір, але це вже не мало особливого значення, оскільки незабаром наші танки розгромили її штаб».

Мелентін також відзначав: «Червона Армія періоду Другої світової війни значно відрізнялася від імператорської російської армії 1914-1917 років, однак у двох аспектах росіяни нітрохи не змінилися. Вони продовжують віддавати перевагу масованим наступам і не перестають виявляти надзвичайну байдужність до забезпечення безпеки свого радіозв'язку».

Дешифровані радянські дані, як повідомлялося в доповіді про результати роботи німецької дешифрувальної служби за лютий 1944 року, «дозволили одержати відомості про оперативну обстановку, про райони зосередження, командні пункти, втрати та підкріплення, порядок підпорядкування та рубежах для атаки. Крім того, зміст цих повідомлень дав змогу виявити сім танкових частин супротивника та їхні номери, а також установити наявність ще дванадцяти танкових частин. За рідкісним винятком, весь матеріал оброблявся вчасно, та отримані відомості використовувалися на практиці».

Ці дані тактичного характеру могли у кращому випадку сприяти досягненню успіхів сугубо місцевого значення. У цілому, криптоаналітичні успіхи німців проти СРСР можна оцінити як украй слабкі, що визнав один з німецьких криптологів В.Фліку: «Я повинен зробити росіянам комплімент: у цій війні Росія була єдиною країною, чиї криптографічні системи не розкривалися практично, незважаючи на зусилля першокласних експертів в інших країнах розкрити них. Зокрема, криптографічні системи вищого військового командування та дипломатичне листування залишалися для іноземних криптографічних бюро «книгою за сіма печатями»… Після декількох років марних зусиль копіювання дипломатичного листування росіян у Німеччині було припинено. Для нефахівців це може здатися перебільшенням, але я наважуся завірити: Росія програла Першу світову війну в ефірі і виграла Другу світову війну в ефірі».

Полонені німецькі фахівці дешифрувальної служби розповідали, що наші машинні криптограми прочитати було неможливо, а з 1942 року вони, взагалі, більше не перехоплювалися. Було зрозуміло, що радянська система машинного шифрування може бути уразлива тільки при наявності самої шифртехніки та ключів до неї.

Гітлер видав спеціальний наказ по вермахту, в якому значилося: «…кто візьме в полон російського шифрувальника, або захопить шифрувальну техніку, буде нагороджений Залізним хрестом, відпусткою на батьківщину і забезпече-

ний роботою в Берліні, а після закінчення війни - маєтком в Криму». На виконання гітлерівського наказу, у 1942 році поблизу від окупованого фашистами Херсона, в Степановці, була організована розвідувально-диверсійна школа. Розташовувалася вона на території теперішньої психіатричної лікарні.

Перед курсантами однієї із спецгруп ставилося завдання: будь-що добути радянську шифрувальну техніку. Але наступальна кампанія Червоної Армії і надійна охорона радянськими спецслужбами своїх секретів так і не дали фашистам виконати наказ Гітлера до закінчення війни. Радянські шифрувальники завзято не хотіли попадати в полон, а якщо й попадали, користі від цього німцям було мало...

Приведемо один із таких прикладів. Так, офіцер спецзв'язку Л.Травцев віз секретні документи та шифри під охороною трьох танків і взводу піхоти. Колона потрапила в засідку та за декілька хвилин була практично знищена. В автобус із шифрами та документами потрапив німецький снаряд – Травцеву перебило обидві ноги. Стікаючи кров'ю, шифрувальник знайшов у собі сили розкрити сейфи, облити документи бензином і знищити їх. Потім він ще відстрілювався, поки не згорів разом з підірваною машиною.

У 1943 році німецькі зв'язківці віддали належне успіхам радянських криптоаналітиків, коли у прийнятому на конференції офіцерів зв'язку рішенні, записали: «Забороняється яким-небудь чином виділяти передані по радіо послання фюрера».

У всіх найважливіших боях Другої світової війни незримо брали участь шифрувальники: без їхньої підтримки ціна перемоги могла б стати набагато дорожчою. У романах, популярних статтях і спогадах ветеранів ми можемо прочитати про розвідника Кузнєцова, що назвав дату наступу німецьких військ під Курськом. Може й так, але остаточне рішення про цю битву було прийняте після того, як буквально за добу вітчизняні криптоаналітики розкрили шифрований наказ Гітлера про наступ.

Усе було начебто як завжди: перехопивши німецьку радіограму, радянські фахівці впізнали почерк радиста ставки головнокомандувача супротивника, а за характером передачі допустили, що вона містить дуже важливий наказ. Криптологи знали,

що мова може йти про великий наступ і припустили, що наприкінці документа знаходиться підпис єдиної людини, що міг видати цей наказ – Адольфа Гітлера. Далі застосовувалась «техніка взламування» шифру: через відому ділянку тексту «розкривався» ключ, а ключем розшифровувався весь інший текст. Можна було сумніватися в правильності повідомлення Кузнєцова: чи немає там дезінформації, гри контррозвідки супротивника, але не довіряти наказу військам уже не доводилося. «Цьому наступу, – говорив Гітлер в оперативному документі № 6, – надається вирішальне значення. Він повинен завершитися швидким і вирішальним успіхом...»

Для проведення операції, що одержала назву «Цитадель», на флангах Курського виступу були зосереджені 50 добірних дивізій, 10 тисяч гармат, 2700 танків і понад 2000 літаків. Дешифрування наказу встановило, що наступ почнеться вранці, тому в 2 години 20 хвилин почалася радянська артилерійська контрпідготовка. Через великі втрати ВПС під Курськом Німеччина змушена була надалі повністю відмовитися від дій своєї авіації по об'єктах нашого глибокого тилу.

У цей період великий внесок у радянську криптологію вніс учений Котельников, який ще у 1941 році сформулював і довів вимоги, яким повинна задовольняти математично недешифрована система. Дана робота та «теорема відліків» (теорема Котельникова) з'явилися основними в розвитку радянської криптології. Розробка шифратора мала оборонне значення, і для її завершення лабораторія під час війни була евакуйована до Уфи, куди також був евакуйована лабораторія ленінградського заводу «Красная заря». Разом вони увійшли до знову створеного Державного союзного виробничо-експериментального інституту «ГСПЭИ № 56». В інституті Котельников керував спочатку групою, а потім лабораторією. Розпочаті до війни роботи із створення апаратури телеграфного засекречування були продовжені та привели до створення необхідного шифратора до осені 1942 року. Створені під керівництвом Котельникова системи шифрозв'язку з успіхом використовувалися в 1942-1945 роках для зв'язку Москви з фронтами, у діючій армії, а також під час прийняття капітуляції Німеччини для зв'язку радянської делегації з Москвою.

У 1942 році був виданий Наказ НКО № 0093 про взяття на озброєння частинами зв'язку приладів «Селектор», що автоматично шифрували телеграми, передавані апаратом Бодо. На жаль, поки не вдалося знайти опис даного шифратора.

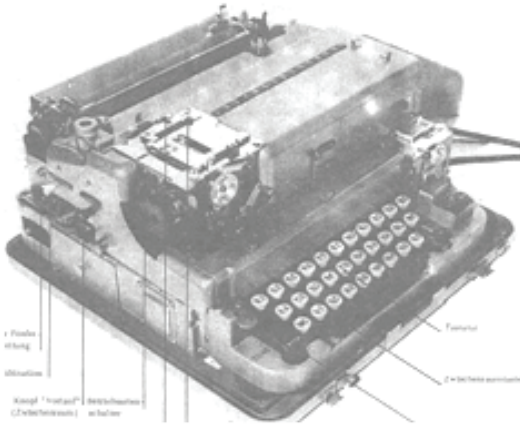
23 березня 1943 році Радою народних комісарів СРСР була прийнята Ухвала «Про присудження Сталінських премій за видатні винаходи за 1942 рік». Третю ступінь з винагородою у 50 тисяч карбованців за розробку нової апаратури спеціального

призначення отримали інженер-капітан 1 рангу Волосок Іван Павлович, конструктори заводу № 707 Судаков Павло Андріанович, Ритов Валентин Миколайович. Також орденами були нагороджені Шаригин, Козлов, Строітєлєв і Гусєв. Крім того, Волосок отримав учений ступінь кандидата технічних наук (без захисту дисертації), а 20 грудня 1943 року - звання генерал-майору військ зв'язку.

На машинний шифрзв'язок у роки війни лягло основне навантаження при передачі секретних телеграм. Тільки у 8-му (режимному) Управлінні ГШ за період з 1941 по 1945 роки було оброблено понад 1,6 мільйонів шифротелеграм і кодограм. Деколи навантаження на шифрувальників Управління доходило до 1500 телеграм на добу. У штабах фронтів нормою вважалося добове навантаження до 400 телеграм, в штабах армії - до 60. Разом з шифрами гаммування застосовувалися шифри багатоалфавітної заміни. За роки війни 8-м управлінням ГШ нижчестоячим штабам і військам було розіслано порядка 3,2 мільйонів комплектів шифрів.

До кінця 1944 року у 130 шифрорганах радянської армії були на озброєнні шифрувальні та кодувальні машини М-100/101 і К-7. Так, у 1943 році до військ було відправлено понад 90 комплектів М-101, а до кінця війни в експлуатації всього перебувало 396 комплектів техніки спеціального зв'язку. За час війни «Курси вдосконалення командного складу шифрослужби» і навчальні команди фронтів і військових округів підготували й відправили на фронт більше 5 тисяч фахівців-шифрувальників. Вони з честю впоралися з покладеними на них завданнями, забезпечуючи машинним шифрозв'язком Ставку Верховного Головнокомандуючого, Генеральний штаб, управління Наркомата оборони, Тегеранську, Ялтинську та Потсдамську конференції.

Офіцери-конструктори 8-го Управління у роки війни займалися не тільки створенням нових зразків шифротехніки. Впровадження її у війська та навчання роботі на ній – ось що було їхнім основним заняттям. Конструктор Козлов за військові роки був відряджений на фронт 32 рази! А вранці 9 травня 1945 року, одержавши терміновий припис держбезпеки й Генерального штабу, вилетів літаком «Дуглас» до Берліна для участі в роботі комісії з відбору й відправлення в СРСР найціннішого устаткування заводів і фабрик гітлерівської Ні-



меччини за репарацією. Тільки з Карл-Хорста й Потсдама для потреб майстерень з ремонту шифрувально-кодувальної техніки їм було вивезено 3 вагони устаткування.

Наприкінці 1945 року були підведені підсумки експлуатації шифрувально-кодувальної техніки в діючій армії. У цей же час проводилася дослідна робота з подальшого підвищення криптостійкості застосованої техніки, а також були запропоновані шляхи й напрямки зі створення нових моделей М-104 «Аметист» і М-105 «Агат». Поряд із шифром гамування все більше застосування знайшов шифр колонної заміни, технічна реалізація якого була закладена ще в 1930-і роки в кодувальній дисковій машині К-37.

У 1950-і роки на заміну машині М-105 «Агат» прийшла модель М-125 *«Фиалка»*, яка стала основною шифромашиною в СРСР та країнах Варшавського договору під час «холодної» війни до 1990-х років. Вона була заснована на принципі німецької «Енігми» та мала 10 роторів, установлених на одній вісі, з нанесеними на них 30 буквами російського алфавіту. Машини М-125 включали моделі «*М-125-МN*», а починаючи з 1978 року, більш складні моделі «*М-125-3МN*» і «*М-125-3МР3*» з багатомовною клавіатурою та регульованими роторами.

На відміну від «Енігми», на якій вихідні символи засвічувались лампочками, *«Фиалка»* друкувала символи на паперовій стрічці й одночасно перфорувала отвори на стрічці і тому була подібна телетайпу Бодо. «*Фиалка*» мала зчитувач встановленої перфокарти, за допомогою якого встановлювалось внутрішнє кодування параметрів машини. Також вона мала зчитувач паперової стрічки для

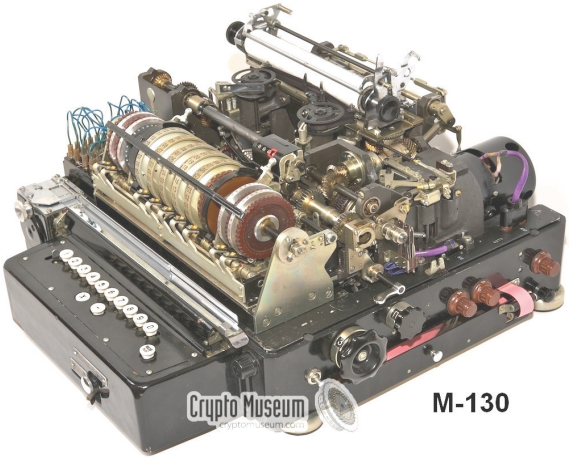
перетворення стрічки з друкованими символами в перфострічку.

«*Фиалка*» забезпечувала обертання кожного зі своїх 10 роторів у напрямку, що був протилежним сусідньому ротору. Крім роторів вона мала ще комутатор, що складався з двох комплектів 30-контактних смуг. Перфокарта вставлялася між двома комплектами контактів через отвір на лівому боці машини. Кожна перфокарта мала 30 отворів, що визначали установку 30 контактних ліній ротора.

Спочатку на машині встановлювалися тільки нерегульовані ротори з фіксованими кільцевими параметрами та фіксованою електропроводкою. З 1978 року на машині вже встановлювали регульовані ротори, що мали як електричні контакти, так і механічні штирки. Встановлення ключа визначала порядок розташування роторів на вісі та початкові параметри роторів. Зміни до параметрів роторів можна було вносити переставленням модулів внутрішньої проводки усередині роторів. Модуль будь-якого ротора можна було переставити в інший ротор у кожне з 30 можливих позицій, що давало в цілому 60 видів електричних ланцюгів.

Ключовий матеріал *«Фиалки»* складався з щоденної ключової книги, ключової книги повідомлень і книги ідентифікатора повідомлення. Щоденна ключова книга містила денні ключові дані на період одного місяця. Щоденний ключ складався з ключової таблиці й перфокарти, діяв протягом 24 годин і змінювався у 00:01. Щодня шифрувальник повинен був виривати карту з пакета та встановлювати її у зчитувач карти машини. Для фіксованих систем ротора ключова таблиця визначала порядок роторів на вісі та початкові параметри ротора. Ключ повідомлення повинний був використовуватися тільки одного разу.

Для шифрування даних про погоду у 1965 році на базі М-125 була сконструйована шифромашина М-130 *«Коралл»*, яка мала тільки цифрову клавіатуру. М-130 використовувалась для обміну шифрованими метеозведеннями як у СРСР, так і у країнах Варшавського договору.



М-130

4.5. Шифри радянської розвідки

В історії СРСР радянському розвіднику Ріхарду Зорге (псевдонім – Рамзай) призначено було зайняти особливе місце. Волею долі і завдяки своїм винятковим людським якостям він піднявся на вершину Олімпу радянської розвідки. Десятки книг, сотні статей, документальні і художні фільми, вулиці, названі на честь великого розвідника. Вивчаючи матеріали про нього і його товаришів, дуже складно було знайти правдиві матеріали про шифр його японської розвідувальної групи. Як, втім, і про шифри інших його товаришів – Леопольда Треппера, Шандора Раде, Рудольфа Абеля. А тим часом історія їхніх шифрів – одна з найчудовіших сторінок світової криптології.

«Тріумфом радянської розвідки» назвав її агентурні шифри відомий історик Девід Кан. Саме радянські шифри, розроблені поза сумнівом видатними фахівцями своєї справи, на десятиліття визначили вектор розвитку світової криптології в сфері так званих «ручних» шифрів.

Отже, шифр Рамзая – зразок радянської шифрувальної техніки тридцятих років XX століття. Першою його частиною був так званий «квадратний» шифр. Чомусь західні публіцисти постійно пов'язують історію цієї системи криптології з революціонерами Росії, називаючи її шифром «нігілістів». Але для цього немає ніяких підстав, а метод, застосований у системі Зорге (як і в інших радянських розвідників), відходить до XVI століття, коли абат Трітемій вперше виклав його в своїй книзі «Поліграфія». І революціонерами він у Росії практично не використовувався.

Відомо, що свої шифровки Ріхард Зорге складав виключно англійською мовою. Тому як ключ для побудови шифру він вибрав слово «*SUBWAY*», що перекладається як «підземний хід». Ключ виписувався у верхньому рядку квадратної таблички. А в клітинки, що залишилися, по порядку проставлялися букви англійського алфавіту, що не увійшли до слова «*SUBWAY*». Таким чином, ми отримаємо таку сітку:

S	U	B	W	A	Y
c	d	E	f	G	h
I	j	к	L	m	N
O	p	q	R	T	v
x	z	.	/		

У кінці алфавіту в таблиці додано два знаки. Це крапка і знак індикатора «/» – для позначення переходу на цифровий текст. Але про це докладніше нижче.

Проте таблиця в подібному вигляді використовувалася тільки для додання символам нових цифрових позначень, що увійшли до неї. Відомо, що частота

появи тих або інших букв у різних мовах світу різна. Стосовно англійської мови вона зведена в таку таблицю:

A	B	C	D	E	F	G	H	I	J	K	L	M
57	9	17	26	116	28	14	46	58	1	5	34	14
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
57	53	18	3	49	55	91	25	9	11	1	18	1

Тут 8 англійських букв, що найчастіше трапляються, можна представити у вигляді анаграми «ASINTOER», яку і використовував Зорге як другий крок побудови свого шифру. Для цього він нумерував вхідні в анаграму букви в своїй табличці по порядку зверху вниз і отримував нову таблицю:

S=0	U	B	W	A=5	Y
з	d	E=3	f	G	h
I=1	j	до	L	m	N=7
O=2	p	q	R=4	T=6	v
x	z	.	/		

Кінцевою метою Зорге було складання такого «квадратного» шифру:

	0	1	2	3	4	5	6	7	8	9
-	s	i	o	e	r	a	t	n	-	-
8	c	x	u	d	j	p	z	b	к	g
9	.	w	f	L	/	g	m	y	h	v

Зрозуміти систему його побудови неважко. У верхньому рядку ми бачимо букви, що найчастіше трапляються в англійській мові, яким дані цифрові позначення від 0 до 7. У два рядки, що залишилися, виписана по порядку решта букв з таблиці «SUBWAY» (зверху вниз). Вони отримують позначення у вигляді двійкових чисел від 80 до 99. Як видно, у верхньому рядку клітини під номерами 8 і 9 порожні. Ці цифри стають номерами рядків у ключовій таблиці.

Таким чином, тут ми маємо втілення ідеї пропорційного шифру, що дозволяє різко зменшити кількість вхідних в шифрограму знаків. А це було дуже важливо для ускладнення можливого дешифрування та зменшення часу передачі радіограм. Відділення ж в тексті однозначних знаків від двозначних (звичайно, при знанні кодової таблиці) не завдає ніяких труднощів. Це була абсолютно видатна ідея невідомого нам радянського криптолога, що мала потім у світовій криптології широке розповсюдження.

Припустимо, потрібно зашифрувати фразу: «51 DIVISION HAS 80 TANKS» (51-

ий дивізіон має 80 танків). Ігноруємо останню букву «S» для все того ж ускладнення дешифрування та округлення кількості цифр, а решту букв і знаків беремо з ключової таблиці.

В результаті отримуємо: 945511948319910127985094880094657 88.

Цей короткий запис дозволяє зрозуміти, як йшла передача цифрового тексту. Цифри виділялися в шифрограмах індикатором 94 з двох сторін, а самі цифри писалися здвоєними: 51 = 94551194, а 80 = 94880094.

Тепер розділяємо отриманий числовий набір на групи цифр по п'ять кожна: 94551|19483|19910|12798|50948|80094|65788.

Тут ми підійшли до головного секрету Зорге. Первинна шифровка тексту далі кодувалася методом накладення на нього нескінченної одноразової цифрової гами за модулем 10. Спосіб отримання її міг бути абсолютно різним: починаючи від використання так званих одноразових шифрувальних блокнотів до перетворення букв певного книжкового тексту в цифри. І той, і інший спосіб мали в розвідці найширше застосування. Але для Зорге завдання значно спростили. Як шифрувальна книга був обраний товстенний «Німецький статистичний щорічник за 1935 рік», у величезній кількості наповненому всілякими цифрами.

Причому розташовувалися числові дані довідника у вигляді акуратних колонок, роблячи з книги ідеальний шифроблокнот. Він мав тільки один недолік – не був одноразовим, що дозволило японській поліції надалі захопити книгу при провалі розвідгрупи та прочитати все перехоплене листування Зорге з Москвою. Отже, цифри гами по черзі вибиралися з довідника та виписувалися під цифрами шифротекста, потім йшло позначкове складання цифр клера і ключа за модулем 10. Тобто, при складанні цифр до уваги приймалися тільки одиниці суми, а десятки відкидалися. Наприклад:

клер	94551	19483	19910	12798	50948	80094	65788
ключ	23467	56439	13257	56744	87682	33248	21675
шифр	17918	65812	22167	68432	37522	13232	86353

Місце довідника, з якого починалася вибірка чергової гами, позначалося п'ятизначною групою і додавалося в текст шифрограми. Перші дві цифри були номером сторінки, потім дві цифри позначали рядок, а остання цифра – номер колонки на сторінці, де розташовувалися потрібні цифри. Проте вставлялася ключова цифрогрупа не безпосередньо, а ховалася в тексті шифру. Наприклад, якщо Зорге починав вибірку гами з 75 сторінки, 12 рядка і 3 колонки, то позначав він це як 75123.

Для зашифровуваної цієї групи бралися третя і п'ята цифрогрупи шифрогра-

ми, які додавалися до ключової групи знову ж таки за модулем 10. Суму, що вийшла, поміщали на початку криптограми як індикатор до розшифровки всього тексту. В результаті маємо таку шифрограму: 24702 17918 65812 22167 68432 37522 13232 86353.

Тут початкова група є індикатор: 24702. Якщо ми з цих цифр послідовно віднімемо третю (22167) і п'яту (37522) цифрогрупи телеграми, то отримаємо групу 75123, що позначає місце вибірки гами в німецькому довіднику.

Ось таким був знаменитий шифр не менш легендарного розвідника Ріхарда Зорге. Перехоплення радіоповідомлень Зорге велося японською поліцією багато років, колонки загадкових п'ятизначних груп акуратно підшивалися в досьє не спійманих ще шпигунів. Але до самого кінця японські експерти не змогли прочитати ні єдиної їх шифрограми. І лише арештований радист групи Макс Клаузен восени 1941 року пояснив контррозвідці систему цього шифру.

Не вдаючись до причин цього сумного факту, акцентуємо свою увагу на іншому – коли ж був обумовлений цей шифр і чим він принципово відрізнявся від інших книжкових шифрів радянської розвідки?

Зорге прибув до Японії зі своєю секретною місією в 1933 році, але зрозуміло, що тоді він мав абсолютно інший ключ до шифру. Адже його статистичний довідник був датований 1935 роком! Саме літом 1935 року резидент виїхав до Москви для короткочасного відпочинку, консультацій і вирішення практичних завдань, що стояли перед його розвідгрупою. Немає сумніву, що саме у цей момент ГРУ забезпечило його новою системою шифру, яка протягом наступних шести років захищала Зорге від наполегливих пошуків контррозвідки Японії.

Тільки з середини 1939 року до дня арешту власний радист Зорге Макс Кла-

узен зашифрував і передав в ефір 106 тисяч груп цифрового тексту, понад 2 тисячі радіограм, тобто в середньому – 600 радіограм у рік або по 2 радіограми в день. Інтенсивнішого радіообміну в умовах конспірації важко собі уявити. При наростаючому потоці інформації з Токіо, припустити, що сам Зорге був здатний займатися складною довгою і монотонною справою зашифровування телеграм, просто неможливо!

Помилкою Зорге було об'єднання в одній особі функцій радиста і шифрувальника, але у нього, напевно, не було іншого виходу. Японія – не Європа, де кадрова проблема вирішувалася в розвідці значно простіше.

Також розглянемо криптологічну діяльність інших резидентур радянської розвідки.

Так, 26 червня 1941 року, через чотири дні після початку Великої Вітчизняної Війни, радист пеленгаторної установки абверу почув сигнали, приналежність яких він не зумів визначити. Йому були знайомі позивні всіх шпигунських радіостанцій Європи, проте цей передавач, що кілька разів повторив код «РТХ», він чув уперше.

Близько трьох годин і п'ятдесяти хвилин ранку невідома рація «вистрілила» в ефір радіограму. «*KLK из PTX 2606 0330 32WES N14KBV*» – записав оператор, потім послідували 32 п'ятизначні групи цифр, що закінчувалися підписом: «*AR 50 385 KLK из PTX*».

Весь цей день і наступний фахівці з абверу стежили за «РТХ», проте так нічого і не змогли зрозуміти, крім того, що передавальна станція знаходиться десь на північному заході від німецько-радянського кордону. Але незабаром вони зробили важливе відкриття: хтось відповідав «РТХ». Місцезнаходження цієї станції не викликало сумнівів: вона була поряд з Москвою. Через декілька днів в ефірі запрацював інший радіопередавач, який передавав такі ж п'ятизначні групи сигналів. І йому також відповіла станція, розташована під Москвою. Всім абверовським радіопостам у Південній Німеччині було наказано «тримати пеленг».

В результаті було встановлено, що одна із станцій з позивними «РТХ» знаходиться в Брюсселі, а інша – в Парижі. У подальші два тижні в ефір один за одним виходили нові передавачі (у тому числі і в Берліні!), що використовують ті ж самі п'ятизначні групи чисел. І всім їм відповідала Москва. У абвері всі ці станції охрестили «Die Rote Kapelle», що в перекладі означає «Червона капела». У липні 1941 року на Москву запрацювали також три радіопередавачі з нейтральної Швейцарії. Їм, у свою чергу, дали назву «Червона трійка».

Звістка про виявлену широку радянську шпигунську мережу швидко дійшла до керівника абверу адмірала Канаріса. Його суперник Гейдріх, що очолював службу безпеки Третього рейху, також дізнався про це. А через декілька днів про «червоних музикантів» знав вже і сам Гітлер. Фюрер був розгніваний, особливо

тим фактом, що шпигуни діють в самому Берліні. Абверу і «СД» в окупованих країнах Західної Європи, так само, як і гестапо в Німеччині, було наказано за всяку ціну вийти на слід невідомих «піаністів». За декілька перших місяців війни вони передали до Москви декілька сотень повідомлень. Ніч за ніччю і день за днем станції пеленгацій абверу ловили зашифровані п'ятизначні сигнали, проте найдосвідченіші німецькі шифрувальники не могли «розкрити» радянський шифр.

У грудні 1941 року була запеленгована перша радіостанція «Червоного оркестру». 13 грудня загін солдатів безшумно піднявся на другий поверх будинку 101 по вулиці Атребатів у Брюсселі. Вони увірвалися в одну з кімнат і заарештували там радиста-шифрувальника та двох інших радянських агентів. Дивом з рук фашистів вислизнув радянський резидент Леопольд Треппер. У каміні будинку німці виявили обвуглений клаптик паперу, списаний цифрами.

Зрозуміло, що це були записи, зроблені в процесі шифрування якогось повідомлення, і німецькі дешифрувальники негайно взялися за його вивчення. Фраза, записана на знайденому клаптику паперу, була французькою мовою і більше схожа на частину ключа, ніж на відкритий текст. У цій фразі було присутнє слово «ПРОКТОР». Служба радіорозвідки допитала господиню, наївну немолоду вдову, яка перерахувала 11 книг, які читав її постоялець. На 286-ій сторінці науково-фантастичного романа французького письменника Ги де Терамона «Диво професора Вальмара» дешифрувальники знайшли дійову особу з ім'ям Проктор. Вони зуміли правильно зрозуміти важливість цього збігу.

Роман Терамона дав їм можливість прочитати 120 шифровок, які належали одній з найактивніших радіостанцій «Червоної капели». У прочитаних повідомленнях говорилося про весняний наступ німців на Кавказі, давалися дані про стан німецьких ВПС, повідомлялися відомості про споживання пального, про втрати і містилася деяка інша важлива інформація. Але всі імена розвідників, згадані в цих повідомленнях, були псевдонімами, а три заарештовані на вулиці Атребатів агенти не хотіли або не могли дати про

них інформацію. Служба радіоконтррозвідки подвоїла зусилля. Адже тільки запеленгувавши станції і схопивши радистів, фашистські контррозвідники могли розраховувати, що ними ціною тортур і зради вдасться пробитися через «броню» радянського шифру.

Відомий на Заході історик «Червоної капели» Хайнц Хене описав систему одного з радянських шифрів у своїй книзі «Пароль – Директор», що була видана у Німеччині у 1971 році. Для цього він скористався мемуарами Отто Пюнтера – члена швейцарської розвідгрупи, відомої на Заході як «Червона трійка». Журналіст, директор і власник інформаційного агентства в Женеві, Пюнтер мав в своєму розпорядженні широкі зв'язки як у журналістських, так і дипломатичних колах і навіть у швейцарських урядових органах. За своїми переконаннями Пюнтер був соціаліст лівого напряму і симпатизував Радянському Союзу. Він сам погодився допомагати радянській розвідці з ідейних спонук, вважаючи боротьбу з фашизмом своїм громадянським обов'язком.

У кінці 1942 року, перед явною загрозою окупації Швейцарії Німеччиною, радянський резидент Шандор Радо отримав дозвіл Центру навчити шифру найближчих своїх помічників, у тому числі і Пюнтера, що носив кодове ім'я Пакбо. З цієї миті і до самого кінця існування групи Пюнтер брав найбезпосереднішу участь у шифруванні телеграм, які потім йшли до Москви через підпільні передавачі. У 1967 році в своїх мемуарах «Секретна війна в нейтральній країні» Пакбо додав гласності подробиці свого колись абсолютно секретного шифру.

Припустимо, він хотів повідомити до Москви, що «Лейбштандарт СС Адольф Гітлер прибув до Варшави». Для кодування свого послання Пюнтер скористався путніми замітками шведського дослідника Свена Хидіна «Від полюса до полюса» і виписав випадкове речення із сторінки 12: «Документальні зйомки припинені, але незабаром будуть відновлені знову». Оскільки для ключового слова йому було потрібно тільки 10 букв, він використовував частину першого слова «Dokumentar» (по-німецьки). Пюнтер записав ключове слово прописом і нижче за нього у два рядки букви алфавіту, що не містяться в слові «*Dokumentar*». По лівому краю трьох рядків він проставив свої умовні цифри (461), а над ключовим словом виписав порядкові номери відповідних букв у латинському алфавіті (все той же метод Трітемія!).

В результаті кожна буква визначалася двозначним числом: *A – 14, B – 26, C – 76* (перша цифра – стовпець, друга – рядок у таблиці).

	2	7	4	0	5	3	6	9	1	8
4	D	O	K	U	M	E	N	T	A	R
6	B	C	F	G	H	I	J	L	P	Q

1	S	V	W	X	Y	Z	.	/		

Тепер Пюнтер міг кодувати своє послання. Він скоротив його до найкоротшої телеграфної форми: «*Hitlerstandarte in Warschau***»** (Гітлершдандарт у Варшаві), перевів це в цифри, вказані ключовим словом, і мав в своєму розпорядженні групи по п'ять цифр. В результаті отримав такий шифротекст:

56369 49634 84219 41464 24148 49434 36644 11484 21765 61404

Потім настала черга повторного шифрування. Пакбо записав все речення: «Документальні зйомки припинені, але незабаром будуть відновлені знову» (звичайно, по-німецьки) і перевів його в цифри, але за системою, що відрізнялася від первинного кодування, яка використовувала однозначні цифри для позначення букв, а не двозначні. Друга цифра просто опускалася. Таким чином А ставала одиницею, В – двійкою, С – сімкою і так далі. В результаті виходила одноразова псевдовипадкова гама. Нарешті Пюнтер складав числа першого і другого кодування за модулем 10. Тепер послання було «закрите» двічі.

В кінці повідомлення розвідник додавав останню групу, призначену для адресата в Москві, який, безумовно, знав, де шукати в книзі Свена Хидіна ключове слово. Остання група в посланні про «Leibstandarte» була «12085», що позначала: «сторінка 12, рядок 8, слово 5».

Двічі зашифровані таким чином радянські кодовані «шаради» майже не піддавалися розшифруванню. Та все ж у них було одне слабке місце: якщо потрапляло до супротивника ключове слово або навіть сама книга, питання розшифрування ставало справою часу.

А зараз пригадаємо найпершу телеграму «Червоного оркестру», перехоплену в Східній Пруссії у червні 1941 року: *«KLK из PTX 2606 0330 32WES N14KBV… (32 п'ятизначні групи цифр) …AR 50 385 KLK из PTX».*

Тепер все в ній стає зрозумілим. *KLK* – позивні московського радіоцентру. *PTX* – позивні групи Леопольда Треппера. 2606 – 26 червня, 0330 – час початку передачі, 32 – кількість передаваних груп № 14 – черговий номер телеграми. Анаграми *WES, KBV, AR* – умовні телеграфні позначення. Наприклад, Шандор Радо для своєї радіостанції в Лозанні використовував схожі коди: *MSG* – звичайні радіограми, *RDO* – термінові, *VYRDO* – блискавки. І найважливіше – група цифр 50385 – індикатор, що позначає місце початку вибору буквеної гами в кодовій книзі розвідників.

І тут є прямий зв'язок розвідгруп Леопольда Треппера і Шандора Радо. Відомо, що заступник Треппера Анатолій Гуревіч за завданням Центру в 1940 році виїжджав до Швейцарії для навчання Радо шифрувальній справі.

Крім системи, описаною Пюнтером, очевидно були й інші її варіанти. Ось, наприклад, радіограма, направлена в квітні 1943 року до Швейцарії для іншої помічниці Радо (Альберта) Рашель Дюпендорфер (Сісі): «23.4.43. Циці. Повідо-

мляємо назву нової книги для вашого шифру. Придбайте її, і ми дамо вам правила користування. Альберт не повинен знати нової книги. Вона називається «Буря над будинком», видавництво Еберс, 471-а сторінка. Директор».

Виходить, що для шифру тут використовувалася тільки одна сторінка книги. Хоча, ймовірніше, що вказана сторінка планувалася лише для першої шифрограми розвідниці, з подальшим переходом на звичайний спосіб. Про нього повідомляє в своїх мемуарах і Шандор Радо: «код щодня мінявся. І якщо нацисти не встигали прослуховувати і записати перші цифрові групи, які були початком коду, то, навіть маючи в руках потрібну кодову книгу, їм дуже важко було, якщо взагалі можливо, розшифрувати радіограму».

Шифр швейцарської розвідгрупи був звичайною системою для радянських розвідників військової пори. Варто тільки порівняти її з шифром Зорге, як ми знайдемо в ній багато схожого. Звичайно, шифр Рамзая був обумовлений ще в 1935 році і часова відстань до шифру Пюнтера у 1943 році складала майже 8 років. Але система радянського шифру була настільки вдала, що ще і довгі роки після війни її складові елементи широко застосовувалися в криптології.

А тепер перенесемося за океан у Сполучені Штати Америки, де з подачі радянських розвідників розігрувалася ще одна драматична історія криптологічної війни під назвою «Венона» (англ. *Venona*). Радянський Союз надійно забезпечував безпеку свого дипломатичного і розвідувального листування, застосовуючи для її зашифрування одноразові шифроблокноти, що використовуються вже з 1930 року. Тому будь-які плани, які СРСР міг виношувати проти тих, хто в кінці війни повинен був стати їх супротивниками, так і залишилися б найбільш недоторканними з його секретів.

Однак увечері 5 вересня 1945 року в Оттаві «втік на захід» 26-річний шифрувальник радянського посольства в Канаді Ігор Гузенко. Він передав канадцям і американцям не тільки списки всіх відомих йому радянських агентів, але й систему шифрування, прийняту в ГРУ і КДБ. Інформація Гузенка стала у пригоді американським контррозвідникам. Вже протягом декількох років вони робили невдалі спроби проникнути в таємницю російських шифровок, які удосталь йшли з вашингтонського посольства до Москви. Під ім'ям «Венона» ця найтаємніша операція американської розвідки нині відома у всіх своїх подробицях. Нас же тут цікавлять виключно системи шифрів радянських розвідників, які в деталях змалював американцям зрадник Гузенко. Скористаємося тут книгою Льва Лайнера (Бориса Сиркова) «Венона» – найсекретніша операція американських спецслужб» (2003). І якщо раніше в центрі нашої уваги були агентурні шифри розвідників, то тепер ми звернемося вже до шифрів держави.

Донесення, призначене для відправки до Москви, посольський шифруваль-

ник спочатку перетворював на послідовність чотиризначних цифр з використанням так званої кодової книги. Кодова книга є різновидом словника, в якому кожній букві, складу, слову або навіть цілій фразі зіставляються числа. Такі ж числа зарезервовані і для знаків пунктуації, і для цифр. Якщо слово або фраза в кодовій книзі відсутні, то вони, як правило, розбиваються на склади або букви, які, у свою чергу, замінюються числами згідно з кодовою книгою. Для імен і географічних назв, для яких в донесенні до Москви необхідно було привести їх точне написання з використанням латинського алфавіту, була передбачена окрема кодова книга. Її називали «таблицею вимови».

Допустимо, слід було зашифрувати повідомлення такого змісту: ««Гном» передав звіт про винищувач». Шифрувальник перетворював 5 слів тексту телеграми за допомогою кодової книги в послідовність 5 груп чотиризначних чисел: 8045 3268 2240 4983 3277.

Потім він перегруповував цифри в цій послідовності, розбиваючи їх на 4 групи по 5 цифр в кожній: 80453 26822 40498 33277. А після цього брав до рук так званий одноразовий шифроблокнот. Одноразовим він називався тому, що для зашифрования донесення його можна було використовувати тільки один раз. Кожна сторінка шифроблокнота містила 60 п'ятизначних цифр. Шифрувальник вибирав першу п'ятизначну групу, розташовану в лівому верхньому кутку сторінки шифроблокнота (37584), і записував її як першу групу шифровки. Ця група, що звалася індикатором, повинна була допомогти його колезі в Москві, який займався розшифруванням донесень з Вашингтона, за допомогою такого ж шифроблокнота, визначити, яку саме сторінку цього шифроблокнота слід було використовувати.

Далі шифрувальник виписував наступні за індикатором п'ятизначні групи з шифроблокнота під групами, які у нього вийшли після кодування телеграми за допомогою кодової книги. Він складав всі пари чисел між собою зліва направо, при цьому якщо в результаті складання у нього виходило число більше 9, то 1, що позначала десяток, відкидалася (наприклад, 6 плюс 8 давало 4, а не 14, оскільки 1 була відкинута). В результаті шифрувальник обчислював нову послідовність п'ятизначних груп, які він записував відразу услід за індикатором:

Після кодування: 80453 26822 40498 33277
З шифроблокнота: 37584 67439 30842 46793 34809
Шифровка: 37584 47882 56664 86181 67076

На завершальному етапі, п'ятизначні цифрові групи перетворялися в п'ятизначні буквені групи з використанням такої таблиці:

0	1	2	3	4	5	6	7	8	9

O	I	U	Z	T	R	E	W	A	(?)

У більшості дипломатичних шифросистем, якими Радянський Союз користувався під час Другої світової війни, як індикатор задіювався номер сторінки шифроблокнота, який застосовувався для зашифрования повідомлення (зазвичай у шифроблокноті було 35 або 50 сторінок). Радянська розвідка дотримувалася цього правила аж до 1 травня 1944 року, після чого замість номера сторінки почала застосовувати п'ятизначну цифрову групу, з якою починалася сторінка шифроблокнота.

Перетворення цифр у букви служило, швидше за все, для того, щоб скоротити витрати на передачу шифровки у вигляді телеграфного повідомлення. У свій час передавати по телеграфу букви було дешевше, ніж цифри. І хоча в 1940-і роки, з погляду оплати, було вже неважливо, з букв або ж з цифр складалося телеграфне повідомлення, росіяни як і раніше відправляли свої телеграми в буквеному вигляді.

В результаті вийшла така шифровка:

ZWRAT TWAAU REEET AEIAI EW0WE RWWEO 12315.

У кінець цієї шифровки додавалася п'ятизначна цифрова група, що йшла у шифроблокноті за групою, яку шифрувальник використовував останньою (57760 або RWWEO), а також ще п'ять цифр, перші три з яких позначали порядковий номер шифровки (123), а останні два числа, яким вона датувалася (15).

У Москві шифрувальник перетворював п'ятизначні буквені групи отриманої шифровки в п'ятизначні цифрові групи:

(37584) 47882 56664 8618167076 (57760).

Перша з цих п'ятизначних груп підказувала московському шифрувальнику, яку сторінку одноразового шифрболокнота слід використовувати, а остання допомогала переконатися, що жодна п'ятизначна група не була пропущена при передачі донесення. Далі він по черзі «віднімав» цифри, приведені на відповідній сторінці шифроблокнота, з цифр шифровки (при цьому, якщо від'ємник виявлявся більше зменшуваного, останнє збільшувалося на 10). Таким чином обчислювалась початкова цифрова послідовність п'ятизначних груп:

80453 26822 40498 33277.

Після розбиття цієї послідовності на групи з чотирьох цифр шифрувальник у Москві відновлював початковий відкритий текст донесення, застосувавши зворотне перетворення відповідно до кодової книги:

8045 3268 2240 4983 3277 – «Гном» передав звіт про винищувач.

Насправді процес кодування і шифрування донесення, а також перетворення отриманої цифрової послідовності в буквену не був дискретним. Це була разова операція, оскільки шифрувальнику не дозволялося переписувати

як відкритий текст донесення, так і п'ятизначні групи з шифроблокнота, що використовувалися для шифрування. Таким чином це запобігало їх випадковому включенню в текст шифровки з подальшою передачею у складі телеграфного повідомлення. Найбільша складність для шифрувальника була у відстежуванні місця, з якого в процесі шифрування слід було брати чергову п'ятизначну групу. Для цього шифрувальник просто викреслював групи у шифроблокноті у міру їх використання для зашифрування повідомлення.

Таким чином, донесення, які радянські розвідники відправляли з Вашингтона до Москви, спочатку кодувалися за допомогою кодової книги, а потім шифрувалися з використанням одноразового шифроблокнота. Застосування одноразового шифроблокнота робило радянську шифросистему не розкриваною. Навіть якщо б американці яким-небудь чином роздобули кодову книгу і дізналися б в деталях про радянську шифросистему, все одно вони мало б просунулися в її «розкритті». Стійкість такої шифросистеми визначається, по-перше, випадковістю (тобто непередбачуваністю) послідовності знаків, з яких складається шифроблокнот, а по-друге, унікальністю цієї послідовності. Останнє означає, що кожна сторінка шифроблокнота використовується для зашифрування і розшифрування донесень лише один раз. При суворому дотриманні цих умов «зламати» шифросистему, побудовану на основі одноразового шифроблокнота, неможливо.

Проте така абсолютна стійкість цієї криптосистеми давалася дуже дорогою ціною. Оскільки кожне розвідувальне донесення після кодування доводилося додатково шифрувати за допомогою унікальної цифрової послідовності, для засекречування сотень тисяч повідомлень кількість сторінок в шифроблокноті повинна була обчислюватися тими ж сотнями тисяч. Адже щоб забезпечити абсолютну надійність, кожна сторінка шифрболокнота могла бути використана тільки один раз. У 1940-і роки, за відсутністю швидкодіючих комп'ютерів, які можна було б використовувати для автоматизації процесу створення шифроблокнотів, вручну виготовити абсолютно випадкову цифрову послідовність завдовжки декілька сотень тисяч знаків було просто неможливо.

Це робило застосування системи одноразових блокнотів страшно витратним і зумовило неможливість широкого використання їх у військовий час у стратегічній агентурній розвідці. Результатом цієї обставини і було масове застосування для отримання шифрувальних гам текстів тих або інших книг. І лише на рівні посольських резидентур можна було піти на одноразовий абсолютний шифр. Проте помилки розвідників, що багато разів використовували для шифрування повідомлень сторінки з одних і тих же шифроблокнотів (через неможливість забезпечити їх потрібну кількість у Вашингтоні), привели до злому американськими криптологами багатьох шифрограм радянської розвідки.

Однак найбільших втрат радянська криптологія назнала через зрадників,

одним з яких став радянський агент Рейно Хейханен – радист і шифрувальник резидента радянської розвідки в США Рудольфа Абеля (Марк). Ручний шифр, яким користувався Хейханен, увійшов до історії західних спецслужб під назвою «ВІК» (англ. *VIC* – по перших буквах його псевдоніма Віктор).

Ця історія розпочалася влітку 1953 року, коли Джеймс Бозарт, 14-річний продавець газет, отримав здачу від одного зі своїх клієнтів у Брукліні. Це була монета в 25 центів і п'ять п'ятицентових монет. Джеймс розповідав: «Я йшов по сходах, і дрібниця раптом вислизнула у мене з рук. Коли я почав підбирати гроші, одна з монет розпалася на дві частини. Я підібрав шматочки – в одному з них лежала мікроплівка. Це був малюнок документа або візитної картки. На ній був ряд цифр» – 210 п'ятизначних груп цифрового тексту.

Джеймс відніс свою знахідку в поліцію, де його похвалили за кмітливість. Якби він не спіткнувся на сходинках, за цю монету і зараз можна було б купити газету. Поліція Нью-Йорка передала мікроплівку ФБР, звідки вона потрапила до шифрувальників, які так і не змогли розкрити секрет шифру. Монета залишалася загадкою до весни 1957 року, коли Хейханен несподівано сам здався американським властям. Він з'явився з повинною в американське посольство в Парижі, де опинився, прямуючи на «заслужений відпочинок» до СРСР, куди його відправив Рудольф Абель, що розчарувався в своєму помічнику.

Крім видачі Марка, Хейханен в подробицях виклав співробітникам ФБР шифросистеми та ключі, що застосовувалися ним у листуванні з Москвою. Влітку 1957 року експерт ФБР Майкл Леонард здогадався застосувати отримані від Хейханена відомості для читання матеріалу на мікроплівці, знайденою Бозартом, і переконався, що багаторічні спроби криптоаналітиків розкрити використовувану Хейханеном шифросистему, маючи на руках один тільки шифротекст, були абсолютно марними.

Шифр був складною системою перестановки шифрованих знаків і був заснований на чотирьох ключах, що легко запам'ятовувалися: російському слові «снігопад», патріотичній даті, куплеті російської народної пісні і цифрі 13. Першим у системі підстановки йшло слово «снігопад», дата – 3 вересня 1945 року – день перемоги СРСР над Японією, перші двадцять букв російської народної пісні і цифра 13 використовувалися для подальших підстановок. Це був особистий шифр Хейханена, яким користувався він і його керівники в Москві.

Шифр «*VIC*», який буде пояснений нижче, адаптований під англійську мову (хоча використовувався радянськими розвідниками російською мовою) і починався він процедурою отримання десяти псевдовипадкових цифр.

Для цього агент повинен був знати напам'ять 6 ключових цифр (які запам'ятовувалися у формі якої-небудь дати), 20 букв ключової фрази (у Хейханена вона була початком популярної пісні), а також придумати п'ять випадкових цифр, що

використовувалися як індикатор повідомлення.

Якщо як ключ використати дату 4 липня 1776 року, то він записується цифрами: 741776. Насправді російські розвідники використовували тут своє звичне написання – спочатку дата, а потім номер місяця і рік, але це не має принципового значення.

У якості ж індикатора використаємо таку групу цифр: 77651.

1. Першим кроком виконаємо віднімання за модулем 10 з індикатора 77651 перших п'яти цифр ключової дати 74177 (остання цифра 6 буде використана вже в самому кінці шифрування).

77651 – 74177 = 03584

2. Тепер перетворимо 20 ключових букв на 20 цифр, розділивши їх на дві половини. Букви в кожній групі пронумеруємо окремо за місцем знаходження їх в англійській азбуці. Таким чином, якщо як ключ вибрана фраза «I dream of Jeannie with t», то потрібні дві групи букв виглядатимуть так:

I D R E A M O F J E A N N I E W I T H T

6 2 0 3 1 8 9 5 7 4 1 6 7 4 2 0 5 8 3 9

3. Наступною дією буде так званий ланцюг доповнень, що перетворює нашу, отриману в п.1, цифрову групу 03584 у десятизначну. Для цього, підсумовуючи дві цифри, що стоять поряд, дописуватимемо їх результат далі (подібний метод застосовуватиметься нами надалі на постійній основі).

У нас група: 03584. Тепер: 0+3=3, 3+5=8, 5+8=3 (за модулем 10), 8+4=2, 4+3=7.

В результаті отримуємо десятизначную групу: 0358438327.

4. Далі проведемо підсумовування цифр, що відповідають ключовим буквам «IDREAMOFJE», із знов отриманою групою: 6203189574 + 0358438327 = 6551517891.

5. Тепер беремо другу ключову десятибуквену групу «ANNIEWITHT» і перекодуємо відповідні їй цифри наступним очевидним способом (верхній рядок підстановки відповідає порядковим номерам нижніх знаків):

1 2 3 4 5 6 7 8 9 0

1 6 7 4 2 0 5 8 3 9

6. Використовуючи це перекодування, трансформуємо знов отриману нами в п. 4 групу цифр:

6 5 5 1 5 1 7 8 9 1

0 2 2 1 2 1 5 8 3 1

7. Останні десять цифр і є наш кінцевий результат, за допомогою якого ми, використовуючи метод ланцюга доповнень (див. п.3), генеруємо 50 псевдовипадкових цифр,

потрібних нам у подальшій побудові шифру.

0 2 2 1 2 1 5 8 3 1
2 4 3 3 3 6 3 1 4 3
6 7 6 6 9 9 4 5 7 9
3 3 2 5 8 3 9 2 6 2
6 5 7 3 1 2 1 8 8 8
1 2 0 4 3 3 9 6 6 9

8. Завершальні 10 цифр таблиці застосуємо для отримання іншого ряду цифр, потрібних для побудови квадратного шифру. Для цього виписуємо:

1 2 0 4 3 3 9 6 6 9
1 2 0 5 3 4 8 6 7 9

Нижній рядок є порядковими номерами цифр з верхнього рядка і застосовується в нижчеприведеній таблиці для перейменування букв англійського алфавіту:

	0	1	2	3	4	5	6	7	8	9
	A	T		O	N	E		S	I	R
0	B	C	D	F	G	H	J	K	L	M
8	P	Q	U	V	W	X	Y	Z	.	/

Тут ми бачимо повну аналогію з іншими шифрами радянської розвідки, зокрема, з шифрм Ріхарда Зорге. У верхньому рядку присутні букви англійського алфавіту, що найчастіше трапляються, потім йдуть букви (метод Трітемія), що по порядку залишилися, в кінці таблиці виписана крапка й індикатор (/), який вказує, що далі йде числовий текст. Але в цьому поясненні не все історично вірно. Російські розвідники складали свої тексти на рідній мові (розкрита американцями за допомогою зради Хейханена криптограма була російськомовною).

Отже, таблиця ця мала інший вигляд, але будувалася за тими ж правилами на основі слова «СНІГОПАД» (у російській мові найбільш поширені букви можна представити анаграмою «СЕНОВАЛІТР»). Знову тут варто провести аналогію з системою Зорге, що використовує для основи свого шифру ключ «SUBWAY». Але все вищесказане не має прямого відношення до пояснення нашого прикладу, хоча і робить шифр «*VIC*» ще стійкішим.

9. Тепер маємо все, щоб приступити до зашифровування конкретного тексту. Хай ми хочемо «закрити» такий текст: «*We are pleased to hear of your success in establishing your false identity. You will be sent some money to cover expenses within a month*». Його можна перекласти приблизно так: «Ми раді чути про ваші успіхи в утворенні вашого легального прикриття. Ви отримуватимете гроші на покриття витрат протягом одного місяця».

Використовуючи нашу таблицю перетворення букв, отримаємо такий шиф-

ротекст:

W EAREP L EASED TOH EAROF Y OU RSU C C ESSINESTAB L ISH ING
834194810741640025044195058858096800202466734621010776047303
Y OU RF AL SEID ENTITY Y OU W IL L B ESENTSOM EM ONEY TOC O
88580905107647004327288885808370707014643265094095348825025
V EREX P ENSESW ITH INAM ONTH
85494848143646837204731095320 4.

10. Пригадаємо, що метод «VIC» полягав у використанні при шифровці складної подвійної перестановки. Для цього у агента був ще невеликий особистий номер, наприклад, цифра 8 (насправді ним у Хейханена було число 13). Це число використовувалося для визначення розмірів двох перестановочних таблиць (їх ширина). З 50-значной гами (див. п.7) бралися дві останні цифри (6 і 9), які по черзі підсумовувалися з особистим номером. Для першої таблиці 8+6=14 стовпців, і 8+9=17 стовпців для другої перестановочної таблиці. Окрім ширини стовпців нам потрібно знати ключовий набір цифр. Він витягувався з отриманої нами 50-значной таблиці:

0 2 2 1 2 1 5 8 3 1
2 4 3 3 3 6 3 1 4 3
6 7 6 6 9 9 4 5 7 9
3 3 2 5 8 3 9 2 6 2
6 5 7 3 1 2 1 8 8 8
1 2 0 4 3 3 9 6 6 9

Для двох перестановочних таблиць нам потрібні в сумі 14+17=31, які ми і випишемо по черзі з таблиці згідно з верхньою її нумерацією: 36534 69323 39289 47352 36270 39813 4.

Варто також пояснити, навіщо ми отримували в таблиці 50 знаків. У Хейханена особистим номером було число 13. Максимально можлива цифра, яку можна додати до 13 є 9. В сумі це 22. Для двох таблиць – 44 знаки. Отже для «VIC» було важливо мати як ключ саме 50 цифр.

Таким чином, для першої перестановки використовуємо перші 14 цифр: 36534 69323 3928. Випишемо в нашу 14-колонну таблицю по рядках весь зашифрований у п.8 текст:

36534693233928
83419481074164
00250441950588
58096800202466
73462101077604
73038858090510
76470043272888
85808370707014

64326509409534
88250258549484
81436468372047
3109532049

У зв'язку з тим, що у нас в шифровці було 149 знаків, додамо для округлення ще одну цифру (9), враховуючи, що надалі ми перетворимо шифрограму на набір п'ятизначних груп. Тепер з таблиці випишемо цифри по стовпцях, знову ж таки згідно з верхньою її нумерацією і отримаємо проміжне шифрповідомлення:

09200274534 6860181384 80577786883 15963702539 11018309880
75079700479 4027027992 90628086065 42040483240 30833654811
44818035243 4864084447 84005470562 1546580540.

11. Для другої перестановки тексту ми беремо наступні 17 цифр ключової групи, отриманої нами в п.10: 9 47352 36270 39813 4. Тут ми маємо складну нерівномірну колонну перестановку. У першому рядку ми виписуємо 14 цифр тексту, потім 15, 16 і 17 цифр в другому, третьому і четвертому рядку відповідно. Починаючи з п'ятого рядка ми додаємо кількість цифр, що відповідає номеру потрібного рядка. Отримуємо таку таблицю для перших 97 знаків тексту:

<u>94735236270398134</u>
09200274534686
018138480577786
8831596370253911
01830988075079700
47940
270279
9290628
08606542
040483240

Кількість стовпців визначається з розрахунку загального числа цифр у тексті (150) і ширини таблиці (17). Тобто 9 рядків (17x9=153). У пропуски таблиці, що залишилися, пишемо цифри шифротекста, що залишилися:

<u>94735236270398134</u>
09200274534686308
01813848057778633
88315963702539116
01830988075079700
47940548114481803
27027952434864084
92906284478400547
08606542056215465

04048324080540

Тепер залишається ще раз вибрати цифри шифрограми по колонках, згідно з верхньою нумерацією таблиці:

36178054 289959253 507014400 011342004 746845842 675048425
03100846 918177284 83603475 035007668 483882424 283890960
350713758 689914050 008042900 873786014 472544860.

Або, при розбитті на п'ятизначні групи:

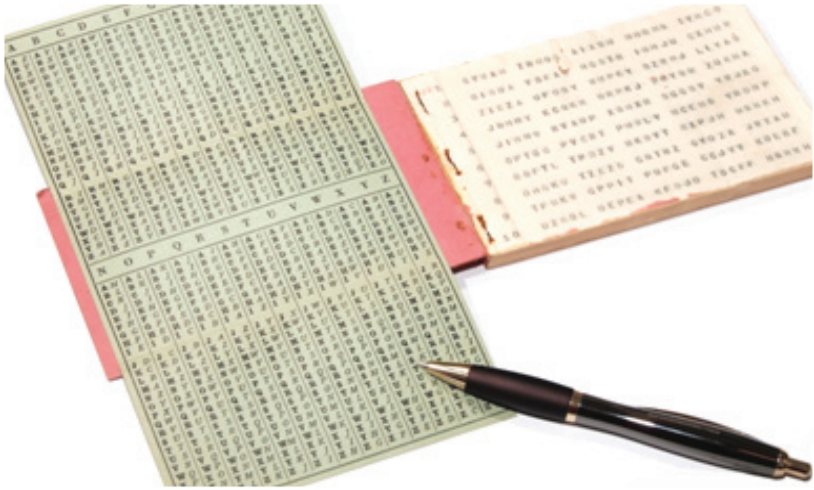
36178 05428 99592 53507 01440 00113 42004 74684 58426 75048
42503 10084 69181 77284 83603 47503 50076 68483 88242 42838
90960 35071 37586 89914 05000 77651 80429 00873 78601 44725
44860.

У отриману нами криптограму вставлений наш індикатор повідомлення 77651 (див. п.1). Він стоїть у шостій групі з кінця шифру і його положення вказує остання цифра з використаної нами як один із ключів дати «4 липня 1776 року» (див. п.1).

Ось таким був цей легендарний шифр «*VIC*», що отримав свою назву за ім'ям зрадника Рейно Хейханена (Віктора). Саме він видав американцям найскладнішу з відомих «ручних» систем шифрування, таку, що категорично не піддавалася розшифруванню.

Розшифрований у ФБР текст із п'ятицентової монети свідчив: «Вітаємо вас із благополучним прибуттям. Підтверджуємо одержання вашого листа за адресою «V», повторюваний «*V*» і прочитання листа номер 1.

Для організації «прикриття» ми віддали розпорядження про переклад



вам трьох тисяч у місцевій (валюті). Проконсультуйтеся з нами, перш ніж вкладати гроші в яку-небудь справу. Повідомте про характер цієї справи.

На ваше прохання ми передамо спосіб приготування м'якої плівки і окремо – новини разом із листом (вашій) матері.

Дуже рано посилати вам гами (*одноразові шифроблокноти – прим.*). Короткі послання зашифровуйте, а довгі робіть зі вставками. Дані про вас, про місце роботи, адреса і так далі не повинні передаватися в одному зашифрованому посланні. Передавайте вставки окремо.

Посилки були вручені особисто вашій дружині. У вас у сім'ї все гаразд. Бажаємо вам успіху. Поздоровлення від товаришів. Номер 1, 3 грудня».

Цей текст криптограми, надісланий Хейханену з Москви і так невдало переданий йому Абелем в Нью-Йорку, можна знайти в літературі в різних варіантах. Нагадаємо, що тут ми маємо подвійний переклад. Спочатку російський текст криптограми для західних читачів переклали на англійську, а потім вже для нас – на російську мову. Тепер трохи статистики. У листі Москви ми налічуємо близько 710 знаків (без пропусків). Відомо, що в самій криптограмі було 210 п'ятизначних груп. Якщо припустити, що для шифрування кожної букви було б потрібно два знаки (при звичайному квадратному ключі), то в криптограмі повинно бути 710 х 2 = 1420 цифр. Але фактично ми маємо 210 х 5 = 1050. На 25% менше! Це, звичайно, приблизні розрахунки, але зовсім не випадкові. Саме метод пропорційного позначення букв дає такі результати. І до цифри 25% ми повернемося в нашому останньому розділі.

Цікаво, що Хейханен на судовому процесі у справі Абеля надав присяжним пояснення про систему свого шифру. Але адвокат Абеля Джеймс Донован нічого в ньому не зрозумів і написав в своїй книзі «Незнайомці на мосту», що *«він недоступний розумінню»*. Не зважаючи на свою безперечну надійність, шифр «*VIC*» був складний і довгий в застосуванні, можливі були в ньому і звичайні людські помилки, що робили його результат абсолютно нечитаним. Незручно було складати за допомогою подібного перестановочного шифру довгі криптограми. Текст доводилося шифрувати частинами. Адже максимальна кількість клітин під цифри шифру в перестановочній таблиці Хейханена могла бути не більше 500, що дозволяло одночасно шифрувати близько 300 букв (при 25% економії знаків!).

А, наприклад, у вищерозглянутій криптограмі Москви ми маємо вже більше 700 букв. Це, природно, створювало для розвідників зрозумілі проблеми. Саме тому Центр радив Віку довгі повідомлення шифрувати зі вставками, залишаючи частину тексту нешифрованою, а вставки пересилати окремо. І саме тому Хейханен просив у свого керівництва одноразові шифрувальні блокноти (гами). Але в цьому Віку на той момент було відмовлено. За 5 років перебування в США леда-

чий Хейханен відправив до Центру не більше 30 повідомлень, а отримав у відповідь приблизно 25. Важко назвати такий шифрооборот інтенсивним. Так або інакше, але в 1956 році перестановочна система «*VIC*» Центром була скасована, залишившись в історії розвідки найбільш складним ручним шифром.

На питання суддів про шифр самого Рудольфа Абеля Вік пояснив: «Марк розповідав мені, що він шифрував і розшифровував іншим способом, що він користувався спеціальними невеликими книжками, за допомогою яких зашифровувати було значно легше, ніж за допомогою цього методу».

Дійсно, Рудольф Абель застосовував для свого листування з Москвою шифроблокноти у формі брошур розміром всього з поштову марку. Співробітники ФБР виявили один із них 21 червня 1957 року в сміттєвому кошику в кімнаті готелю «Латам» у Нью-Йорку під час обшуку після арешту Абеля. Шифр виявився досить простим – цифри в ньому просто заміщали букви повідомлення. В той же час цей шифр не можна було зламати. До кожної групи чисел додавалася випадкова цифра, тому зашифроване повідомлення виглядало абсолютно безглуздим.

Крім того, Абель говорив своєму помічнику про те, що записує інформацію, яка поступає з Центру, на магнітофон, потім переписує її на папір і розшифровує. Після арешту Абеля американські контррозвідники стежили за радіопередачами відповідно до розкладу, знайденого у Абеля в порожнистому кінці олівця, і двічі перехоплювали радіограми, що складалися з п'ятизначних цифрових груп.

Одноразові шифроблокноти були захоплені при арешті ще декількох радянських агентів. На початку 1961 року в передмісті Лондона було знайдено з півдюжини шифроблокнотів у вигляді згорнутих трубочок паперу. Англійські поліцейські відшукали їх в запальничці на дачі Олени і Пітера Крогер – двох радянських агентів, що видавали себе за сімейну американську пару, Лону і Моріса Коен. Решту шифроблокнотів витягли з іншої запальнички, виявленої на лондонській квартирі їх керівника, – радянського резидента в Англії, відомого під вигаданим ім'ям Гордона Лонсдейла (полковника Конона Трохимовича Молодого).

У своїх спогадах провідний технічний спеціаліст британської контррозвідки «*MI-5*» Пітер Райт, який брав участь у арешті, пише:

«Незважаючи на незграбну роботу поліцейських, що проводили обшук, було очевидно, що будинок буквально напханий шпигунським устаткуванням. Два комплекти різних шифрів-блокнотів були закамуфльовані в запальничці для сигарет, схожій на ту, що використовувалася Г.Лонсдейлом. Були також виявлені таблиці для прийому повідомлень із Москви по трьох різних каналах, засоби тайнопису, а також приналежності для виготовлення мікрокрапок: солі хромової кислоти і целофан.

Місіс Крогер намагалася знищити умови зв'язку з іншими агентами, викинувши вміст своєї сумочки в унітаз, але була зупинена пильною жінкою-поліцейським.

Але найцікавішою знахідкою, поза всяким сумнівом, був план швидкісного радіозв'язку з Москвою. У банці з-під печива ми знайшли скляночку з магнітним порошком, що дозволяв зробити видимими неозброєним оком крапки й тире на магнітній стрічці, що застосовувалася для прискореної радіопередачі. При цьому відпадала необхідність у складному спеціальному магнітофоні для уповільненого відтворення прийнятих і переданих повідомлень».

У 1963 році в лондонському аеропорті був заарештований англійський вчений-атомник Джузепе Мартеллі, якому було пред'явлене обвинувачення в шпигунстві на користь Радянського Союзу. Він носив при собі два шифроблокноти, що були заховані в пачці сигарет. Сім сигарет у пачці були неторкнуті, а шість інших виявилися склеєними одна з одною та частково вирізаними з метою звільнення місця для шифроблокнотів.

Таким чином, очевидно, що в п'ятдесяті роки минулого століття основним шифром радянських розвідників був одноразовий шифроблокнот. Зовнішній вигляд одноразового шифроблокнота був різним. Він міг являти собою товсту прямокутну брошуру розміром з поштову марку, а іноді – згорнуті смужки папера розміром із сигаретний недопалок. Причому зовнішній вигляд радянських шифроблокнотів мав чітку тенденцію до зменшення.

Так, шифроблокнот, захоплений у 1954 році, містив 40 рядків по 8 груп з 5 цифр. У іншому шифроблокноті, доступ до якого був отриманий у 1958 році, було 30 рядків по 10 груп. У шифроблокнотах, захоплених у 1957 і 1961 роках, було 20 рядків по 4 і 5 груп відповідно. Групи, рядки і сторінки пронумеровані. Ще один шифроблокнот складався з 250 сторінок, виготовлених з матеріалу, що нагадував металеву фольгу. Зазвичай одна половина шифроблокнота друкувалася червоним шрифтом, а інша – чорним. Ймовірно, це робилося, щоб розрізняти гаму, яка використовувалась для зашифрування і розшифрування. Розмноження шифроблокнотів здійснювалося простим фотографуванням, яке вважалося найкращим способом скопіювати гаму для агента.

Більше того, папір, з якого виготовлялися шифроблокноти, робився з нитроклетчатки – матеріалу, який застосовувався для виробництва фотоплівки на зорі кінематографа. Цей матеріал дуже легко займався, а за допомогою марганцевокислого калія, який у шпигунів був завжди під рукою, звичайне горіння можна було перетворити майже на вибух, який швидко і повністю знищував шифроблокнот, не залишаючи навіть прихованого зображення на попелі.

Як відзначав Девід Кан, «радянським агентам не загрожує небезпека бути викритими через слабкість вживаних ними шифрувальних засобів». Така оцінка

відомого історика світової криптології є дуже цінною. Очевидно, але факт: мистецтво радянських криптологів у складанні агентурних шифрів стало надбанням навіть ворожих нам світових розвідок.

4.6. Від ГУСС до ГУКДБ

19 жовтня 1949 року Постановою Політбюро ЦК ВКП(б) № П71/426 було прийнято ряд найважливіших для радянської криптології рішень, суть яких була такою:

- на базі 6-го Управління МДБ і дешифрувально-розвідувальної служби ГШ ЗС було створене Головне управління спеціальної служби (далі - ГУСС) при ЦК ВКП(б) (з 13 жовтня 1952 року - КПРС);

- здійснювалися заходи щодо залучення учених як для виконання оперативних завдань криптослужби, так і в ролі викладачів для підготовки нових висококваліфікованих кадрів;

- створювалися Вища школа криптографів (далі – ВШК) і «закрите» відділення механіко-математичного факультету (далі – мехмат) Московського державного університету (далі – МДУ).

Згідно секретного додатку № 1 до цієї Постанови склад і завдання ГУСС були такими:

УПРАВЛІННЯ № 1 (дешифрувально-інформаційне) веде роботу з аналітичного розкриття шифрувальних машин, шифрів і кодів США, Англії та інших іноземних держав, а також читання іноземного дипломатичнго, військового, комерційного та агентурного шифролистування.

1. Перший відділ - дешифрування американських шифроматеріалів.
2. Другий відділ - дешифрування англійських шифроматеріалів.
3. Третій відділ - дешифрування шифроматеріалів європейських країн.
4. Четвертий відділ - дешифрування шифроматеріалів решти країн.
5. П'ятий відділ - машинна обробка шифроматеріалів.
6. Шостий відділ - інформаційний.

УПРАВЛІННЯ № 2 (вітчизняного шифрованого зв'язку) веде розробку та виготовлення шифрувальних машин, апаратури секретної топографії і телефонії, шифрів і кодів для міністерств, відомств і організацій, що мають шифрований зв'язок, а також контроль за організацією шифрувальної роботи та використанням засобів шифрувального зв'язку в міністерствах, відомствах і організаціях.

1. Перший відділ - контрольно-інспекторський.
2. Другий відділ - розроблення ручних шифрів і кодів.
3. Третій відділ - виготовлення шифрувальних і перешифрувальних документів.
4. Конструкторське бюро - розроблення машин незалежного шифрування, се-

кретної телеграфії, телефонії і машин для виготовлення ключів.

5. Друкарня.

УПРАВЛІННЯ № 3 (радіоперехоплення) веде радіоперехоплення шифрованого листування іноземних держав, а також розроблення та виготовлення спеціальної радіоперехоплюючої апаратури.

1. Перший відділ - служба радіоперехоплення.

2. Другий відділ - технічний.

3. Третій відділ - оргстройової та бойової підготовки.

4. Четвертий відділ - політичний.

5. П'ятий відділ - військового постачання.

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ веде розробку: теоретичних основ дешифрування, головним чином машинних шифраторів Америки і Англії; теоретичних основ і аналізу стійкості вітчизняних шифрів; проблем зі створення та використання швидкодіючих рахунково-аналітичних машин і проблем щодо нових методів перехоплення повідомлень.

1. Вчена рада.

2. Відділ теоретичної криптографії.

3. Відділ рахунково-аналітичної техніки та нових методів перехоплення.

4. Науково-дослідні лабораторії.

5. Аспірантура.

6. Бібліотека.

ДОСЛІДНИЙ ЗАВОД з виготовлення шифрувальної і дешифрувальної техніки.

ШКОЛА ПІДГОТОВКИ КРИПТОГРАФІВ.

КУРСИ ПЕРЕПІДГОТОВКИ І ВДОСКОНАЛЕННЯ РАДІОРОЗВІДНИКІВ І ШИФРУВАЛЬНИКІВ.

ВІЙСЬКА СПЕЦІАЛЬНОЇ СЛУЖБИ.

ДЕШИФРУВАЛЬНІ ВІДДІЛИ У ЛЕНІНГРАДІ, ТБІЛІСІ, ХАБАРОВСЬКУ І КИЄВІ.

Згідно секретного додатку № 2 до цієї Постанови завдання різних відомств були такими:

1. Зобов'язати Комітет Інформації при МЗС СРСР (тов. Зоріна) підсилити розвідувальну роботу за кордоном щодо здобичі матеріалів і відомостей з іноземних шифрів і нових технічних засобів шифрозв'язку і забезпечити своєчасну передачу цих даних ГУСС.

2. Зобов'язати МДБ СРСР (тов. Абакумова) забезпечити своєчасну передачу ГУСС отримуваних по чекістській лінії даних, що стосуються іноземної шифрувальної техніки та шифрів, а також даних про недоліки в шифрувальній роботі міністерств, відомств і організацій, що отримуються в результаті чекістського обслуговування їх шифрувальних органів.

3. Зобов'язати ГУСС (т. Шевельова) створити школу підготовки криптографів

на 250 чоловік з терміном навчання 2 роки та курси перепідготовки і удосконалення радіорозвідників і шифрувальників на 150 осіб з терміном навчання 1 рік.

4. Зобов'язати т.т. Булганіна і Шевельова підібрати в Москві відповідний науково-дослідний інститут, близький за своїм профілем до ГУСС з тим, щоб на цій базі організувати науково-дослідний інститут цього Управління, а також завод для виготовлення шифрувальної та дешифрувальної техніки.

До речі, треба відзначити, що аналогічна спецслужба в США – АНБ – була створена тільки у 1952 році. Утворення ГУСС зіграло величезну роль для істотної перебудови всієї криптослужби СРСР і подальшого її розвитку. Ще в 1946 році до роботи в криптослужбі була притягнута група наукових і інженерних працівників з МДУ й інших навчальних закладів, що зробили значний внесок у вирішення актуальних завдань вітчизняної криптографії та підвищили її науковий рівень. Ця обставина визначила напрямок подальшого комплектування підрозділів криптослужби.

Начальником ГУСС при ЦК ВКП(б) став генерал-лейтенант Шевельов, а начальником 1-го Управління (дешифрувально-інформаційного) - генерал-майор Копитцев. У період з 28 червня 1952 року по 12 березня 1953 року начальником ГУСС був Іван Тіхонович Савченко.

11 січня 1950 року для забезпечення власного шифрувального зв'язку та дешифрування в МДБ наказом № 0035 був утворений шифрувальний відділ, який з 18 серпня згідно наказу МДБ № 00443 почав іменуватися як Відділ «С». Його начальником став М.П.Шаріков, а у період з 2 листопада 1951 року по 14 березня 1953 року був В.П.Семенов.

25 квітня згідно ухвали РМ СРСР № 1701-660сс «Про заходи щодо забезпечення збереження державної таємниці при передачі відомостей по радіо» наказом МВС № 00489 від 5 серпня 1950 року у складі МВС планувалось утворення Відділу зв'язку. Однак наказ в частині організації Відділу зв'язку виконаний не був, а наказом МВС № 00609 від 4 жовтня 1950 року штат 2-го спецвідділу був збільшений на 29 осіб і склав 111 осіб.

30 червня Постановою Секретаріату ЦК ВКП(б) № СТ-515/246С в ГУСС замість Криптографічної Ради була створена Вчена Рада в кількості 9 осіб під головуванням Копитцева. 9 січня 1952 року Рішенням ЦК ВКП(б) № П85/228 було передбачене утворення нових частин спецслужби, для них введені нові штати та одночасно проведені зміни в загальній структурі частин спецслужби: збільшено більше, ніж на 50% кількість постів в частинах, чисельність особового складу зросла удвічі, підвищені службові категорії та посадові оклади офіцерському складу.

11 серпня хвалою Секретаріату ЦК ВКП(б) у складі ГУСС була створена Вища школа криптографів (далі - ВШК) і віднесена до вищих учбових закладів 1-ої категорії. Положення про ВШК було затверджене начальником ГУСС при ЦК ВКП(б) 6 вересня 1950 року. Школа мала кафедри криптографії, радіорозвідки, мате-

матики, соціально-економічних дисциплін та іноземних мов, а також курси з підготовки техніків-криптографів. Термін навчання складав 2 роки - на денному відділенні та 3 роки - на вечірньому. Чисельність слухачів була встановлена в 250 осіб.

Навчання у ВШК (нині – Інститут криптографії, зв'язку та інформатики Академії ФСБ Росії) почалося на початку лютого 1951 року. Навчання за спогадами Л.Кузьміна дійсно була непростим: математика на університетському рівні сполучилася з електро- і радіотехнікою на рівні Інституту зв'язку. До цього додавалися майже щоденні заняття з англійської мови та марксистської філософії. Рівень математичної підготовки визначався складом педагогів: вищу алгебру і теорію чисел читав автор відомого підручника професор Леопольд Якович Окунєв, аналіз і теорію імовірностей – провідні молоді доценти МДУ Микола Петрович Жидков і Андрій Сергійович Монін (останній пізніше став академіком).

Першими спецдисциплінами були «Коди» і «Основи криптографії». Основні лектори з цих дисциплін, полковник Борис Олексійович Аронський і підполковник Михайло Спиридонович Одноробов, представляли два покоління радянських криптологів. Ще в квітні-травні 1941 року в радянську криптослужбу було мобілізовано близько півсотні молодих учених із МДУ – математиків, фізиків і випускників Військової академії зв'язку. Вони не тільки змогли швидко знайти в ній своє місце, але і привнесли в криптоаналітичну роботу нові ідеї.

Якщо «старі» криптоаналітики уміли копітко, крок за кроком накопичувати відомості про ключ шифру супротивника, то математики, аналізуючи логічні побудови лише частково відомого ключа, знаходили алгоритми його істотного поповнення. Інженери і фізики почали створювати і впроваджувати в аналіз шифрів допоміжну техніку. Ці два фактори сприяли здійсненню якісного стрибка в «розкритті» ключів, що часто змінювалися. Чималий внесок у становлення цих методів зробив М.Одноробов, а також кандидати фізико-математичних наук Г.Пондопуло і М.Соколов, що викладали нові математичні методи аналізу шифрів і дешифрування шифролистування.

Лекції М.Одноробова складалися з двох частин. Перша містила систематизований опис класичних шифрів з аналізом їхніх слабкостей і підходів до їх злому, друга ж знайомила з тільки-но опублікованою в західній пресі математичною теорією стійкості секретних систем Клода Шеннона. Практичні заняття за курсом складалися у дешифруванні усе більш складних шифрів. Починаючи з третього семестру з'явилися спецдисципліни, у яких знайшли відображення нові віяння – механізовані способи шифрування, що народилися вже після Першої світової війни. Ці способи поділялися за принципом сполучення з приймально-передавальною технікою зв'язку на два класи.

Один клас містив у собі шифртехніку лінійного шифрування або техніку за-

секречування. Інший містив у собі шифртехніку попереднього шифрування, що дозволяла швидко зашифрувати або розшифровувати криптограму незалежно від типу передавальної техніки. Перша (особливо телефонна) була надзвичайно оперативною, але більш складною та дорогою, друга була простішою та дешевшою. Курс, присвячений лінійній апаратурі, вів Є.Щукін. Його лекції були засновані на майже 10-літньому досвіді створення й аналізу техніки засекречування для телеграфного зв'язку, що виявили цілу низку слабкостей телеграфної лінії при грубому вторгненні. Є.Щукін звертав особливу увагу на можливості використання таких слабкостей при дешифруванні, з одного боку, та технічні шляхи їхнього подолання – з іншого.

Курс «Техніка попереднього шифрування» у ту пору складався з двох розділів. Перший із них полягав у всебічному вивченні особливостей механічної портативної шифртехніки, винайденої в 1930-і роки шведом російського походження Борисом Хагеліном, який встиг ще до війни налагодити її виробництво та продати ліцензії на кілька модернізацій у багато країн світу. Полковником М.Нестеренком і підполковником Д.Трускановим було продемонстровано, що розрекламований критерій стійкості шифру – величезна кількість ключів до нього – не завжди гарантує неможливість його розкриття. Виявлені уразливості цих машинок поряд з їхнім широким поширенням досить довго дозволяли забезпечувати керівництво СРСР корисною інформацією.

Другий розділ курсу вів молодий криптограф-математик майор Василь Іванович Бобилєв, що прийшов у службу під час війни. Цей розділ базувався на аналізі класу пристроїв, родоначальницею якого була винайдена наприкінці 20-х років німецьким інженером Шербіусом електромеханічна шифромашина «Енігма». Наші криптографи побудували математичну теорію таких шифрів, що дало можливість ще в ході війни створити вітчизняні машини подібного класу, позбавлені слабкостей «Енігми», та обґрунтувати неможливість їхнього дешифрування за допомогою надпотужної для того часу обчислювальної техніки.

На останньому, четвертому семестрі ВШК разом з іншими спецдисциплінами викладалася «Допоміжна техніка криптоаналізу», про що розповідав полковник Володимир Степанович Полін. Ця техніка в той час являла собою окремі релейні або, навіть, багатолампові пристрої, що полегшували криптологу трудомісткі процеси статистичного аналізу шифроперехоплення.

Доречно сказати декілька слів про першого начальника кафедри криптографії ВШК Михайла Івановича Соколова. На початку 1941 року він був призваний до армії та направлений до ГУСС. Під час війни він зробив істотний внесок у розробку алгоритмів відновлення ключів деяких шифрів фашистської Німеччини і, віддаючи багато сил аналізу шифротехніки супротивника, розкрив деякі її ключові елементи, що не завжди, однак, приводило до регулярного читання відпо-

відного листування.

Цілком закономірним було його призначення на посаду начальника кафедри криптографії. Закінчував службу Соколов знову в аналітичних підрозділах, вніс багато важливого в теорію оцінки параметрів якості шифрів, виховав декількох молодих криптографів, довівши їх до захисту кандидатських дисертацій.

Крім того, з метою забезпечення навчання співробітників радянських криптологічних підрозділів наказом начальника ГУСС від 17 грудня 1952 року, згідно з рішенням ЦК КПРС від 10 грудня 1952 року, було організовано вечірнє відділення з підготовки інженерів-криптографів із 4-річним терміном навчання. Заняття на вечірньому відділенні розпочалися 18 лютого 1953 року.

Навчальний план вечірнього відділення був розглянутий на Вченій раді ГУСС і затверджений начальником ГУСС у вересні 1952 року. У його основу був покладений навчальний план фізико-математичних факультетів педагогічних інститутів, термін навчання на яких також складав 4 роки, з доповненням дисциплін, знання яких було необхідне в практичній діяльності різних оперативних підрозділів Управління.

Планом передбачалося вивчення 24 дисциплін. Із загального числа 2216 годин (лекцій – 1350 годин, групових занять – 866 годин) на вивчення спеціальних дисциплін відводилося 316 годин. Провідне місце в навчальному плані відводилося вивченню математичних дисциплін – 47 % годин. На відміну від денного відділення, де слухачам після закінчення навчання присвоювалася кваліфікація «інженер-криптограф» і диплом на руки не видавався, а залучався до особистої справи, випускники вечірнього відділення отримували диплом єдиного для всіх вузів зразка з присвоєнням кваліфікації «інженер-обчислювач» за фахом «прикладна математика». У разі закінчення річних курсів присвоювалася кваліфікація «технік-криптограф», свідоцтво на руки не видавалося, а залучалося до особистої справи. У зв'язку з цим випускники нерідко потрапляли в скрутне становище, якщо бажали продовжити освіту у цивільному вузі.

ВШК, що підготувала впродовж 1951-1953 років молодих висококваліфікованих фахівців і створила умови для подальшого розвитку спецслужби, навіть в умовах її нерозумного скорочення і роздроблення, піддалася сильному скороченню на початку 1953 року (при ліквідації ГУСС). Під демобілізацію потрапили навіть слухачі першого курсу. Замість Соколова, що залишив у час цієї реорганізації кафедру, начальником був призначений його соратник Пондопуло, що раніше курирував спеціальні групи підготовки криптологів на закритому відділенні мехмату МДУ.

У програму цього відділення входили курси з додаткових розділів теорії ймовірностей і математичної статистики, вищої алгебри, теорії груп, теорії чисел, теорії кінцевих різниць, спеціальних застосувань обчислювальної техніки та

курси з криптографії.

За час свого функціонування у 1949-1957 роках на «закритому» відділенні мехмату МДУ пройшли навчання близько 200 осіб. Їхній прихід на початку 50-х років до криптослужби значною мірою сприяв процесу «математизації» радянської криптології. Поряд з розробкою нових методів криптоаналізу шифросистем істотний розвиток одержала теоретична криптологія, у якій одну з провідних ролей став грати математичний апарат.

Широке застосування в криптології знайшли теоретико-ймовірнісні та статистичні методи, що пояснювалося, з одного боку, випадковим характером відкритих і шифрованих текстів і застосовуваних для шифрування ключів, а з іншого боку, широким використанням для вивчення складних детермінованих процесів різних теоретико-ймовірнісних моделей.

Застосування алгебраїчних і теоретико-числових методів у криптології для вивчення процесів шифрування засновано на використанні функціональних особливостей елементної бази для побудови шифраторів, що реалізовували низку алгебраїчних операцій. Це дозволяло проводити аналіз шифросистем на основі застосування методів теорії груп, теорії кінцевих полів і кілець, лінійної алгебри, а пізніше – й методів алгебраїчної геометрії та алгебраїчної теорії чисел.

Для вивчення різноманітних дискретних моделей шифраторів широке застосування в криптології знайшли комбінаторні методи. При цьому в криптології виникли як завдання з побудови комбінаторних конфігурацій з заданими властивостями, так і завдання з їхнього перерахування, при вирішенні яких використовуються теоретико-ймовірнісні методи та методи асимптотичного аналізу.

Одним із найважливіших завдань того періоду стало створення датчиків випадкових чисел і суворе математичне обґрунтування випадковості й рівноймовірності одержуваних за їхньою допомогою послідовностей, а також методів статистичного контролю їхньої криптологічної якості. Це завдання було успішно вирішене колективом криптологів і інженерів під керівництвом В.Козлова. Надалі великий внесок у розвиток цього напрямку зробили П.Беляєв і В.Пярін. Відзначимо, що у зв'язку з вирішенням цього завдання були отримані перші результати в теорії ймовірнісних розподілів на групи, що мала у подальшому досить широкий розвиток.

Наприкінці 1952 року Й.Сталін ще раз хотів реорганізувати розвідку й контррозвідку, санкціонувавши утворення в МДБ Головного управління розвідки, що мало б у своєму складі розвідувальне і контррозвідувальне управління. Однак 5 березня 1953 року Й.Сталін помер, тому ця реорганізація була зупинена. Першим заступником Голови Ради міністрів СРСР і міністром внутрішніх справ був призначений Л.Берія.

Того ж дня на спільному засіданні Пленуму ЦК КПРС, РМ СРСР і ПВР СРСР було ухвалено рішення про повернення МДБ до складу МВС. 23 квітня 1953 року наказом МВС № 00142 відповідальність за шифрувально-дешифрувальну справу було покладена на 8-е Управління МВС. Його начальником став полковник Савченко, а його заступником - генерал-майор Копитцев. Також в Управлінні була створена Науково-технічна рада (далі - НТР), до якої перейшли функції Вченої ради ГУСС.

У тому же році 8-м Управлінням МВС було видано 2 частини підручника криптографії: «Частина перша. Курс розкриття шифрів заміни, гамування і перестановок» (автор М.І.Соколов) і «Частина друга. Курс розкриття кодованих текстів і їх ускладнень» (автори – Б.А.Аронський, В.Ф.Самсонов, І.В.Гусаков, В.І.Садіков, Н.А.Циганков і А.Г.Вигодський).

24 квітня 1953 року ГУСС Постановою РМ СРСР була ліквідована та розділена на три частини: Спеціальна служба органів державної безпеки (8-е Управління МВС), Спеціальна служба ГШ Збройних сил (далі – ЗС) і Спеціальна служба Головного штабу ВМФ. ВШК перейшла у підпорядкування 8-го Управління і стала називатися Вищою школою 8-го Управління МВС. Однак її штатний розклад і списки викладацького та навчально-допоміжного складу збереглися без змін.

6 червня 1953 року був арештований Міністр внутрішніх справ Л.Берія. Указом ПВР СРСР він був позбавлений повноважень депутата Верховної Ради, знятий з посади першого заступника голови РМ СРСР і Міністра внутрішніх справ, позбавлений всіх звань і нагород, а справа про його «злочинні дії» передана на розгляд Верховного Суду СРСР. Одночасно з Л.Берія арештовані або усунені з посади Б.Кобулов, С.Гоглідзе, Л.Влодзимирський, Б.Обручніков, М.Сазикін, Л.Райхман, П.Судоплатов, П.Лорент і ряд інших керівників МВС.

13 березня 1954 року Указом ПВР СРСР був утворений Комітет державної безпеки (далі – КДБ) при РМ СРСР. 8-е Управління МВС стало 8-м Головним Управлінням (далі – ГУ) КДБ при РМ СРСР. Його начальником став генерал-майор Василь Андрійович Лукшин, а його заступником - генерал-майор Копитцев. «Положення про КДБ при РМ СРСР» було затверджене Президією ЦК КПРС і введене в дію Постановою РМ СРСР від 23 грудня 1958 року.

16 березня 1954 року у МВС для забезпечення власного шифрувального зв'язку був знову створений 2-й спецвідділ, начальником якого став полковник І.І.Філаткін. 24 квітня 1956 року начальником спецвідділу наказом МВС № 387 був призначений колишній інструктор Відділу адміністративних органів ЦК КПРС полковник К.Є.Єлісеєв. Станом на 25 березня 1959 року у спецвідділі працювало 38 осіб.

8-е ГУ КДБ повинно було виконувати дві основні функції: по-перше, розробка шифрів і систем криптографії для КДБ і МЗС; по-друге, забезпечення надій-

ності і безпеки урядових ліній зв'язку на території СРСР. Крім того, персонал його перехоплює і намагається розшифровувати радіообмін між іноземними урядовими установами, використовуючи штучні супутники Землі, спеціальні судна та апаратуру, розміщену в будівлях радянських посольств.

8-е ГУ складалося з таких основних підрозділів:

- Управління «А» - забезпечення безпеки дипломатичного листування;
- Управління «В» - розробка шифрів;
- Управління «С» - інженерно-криптографічний захист;
- Науково-дослідний інформаційно-аналітичний інститут;
- Вища школа (до 1960 року).

8-е ГУ у різні періоди часу очолювали:

1. Лукшин Василь Андрійович (27.03.1954 - 16.03.1961).
2. Лялін Серафим Миколайович (16.03.1961 - 18.10.1967).
3. Ємохонов Микола Павлович (02.07.1968 - 08.07.1971).
4. Усіков Георгій Артемович (серпень 1971 - серпень 1975).
5. Андреєв Микола Миколайович (серпень 1975 - 1991).

29 квітня 1954 року начальником 8-го ГУ було затверджено нове «Положення про курси удосконалення офіцерського складу частин Спецслужби при Вищій школі 8-го Головного Управління». На Вищу школу (далі - ВШ) додатково були покладені функції робочого апарату Науково-технічної ради (далі – НТР) 8-го ГУ, підготовка наукових кадрів, науково-технічна інформація, редакційно-видавнича і бібліотечна робота. Крім того, на ВШ була покладена організація та проведення чекістської і мовної підготовки у 8-му ГУ. Після скасування підготовки криптографів на денному відділенні єдиним місцем підготовки криптологів залишилося вечірнє відділення.

У червні 1954 року Голова КДБ Іван Сєров затвердив нове «Положення про вечірнє відділення Вищої школи 8-го Головного Управління з підготовки інженерів-криптографів». У цьому Положенні вказувалося: «Вечірнє відділення є відділенням закритого типу з 4-річним терміном навчання і має на меті підготовку криптографічних кадрів для роботи у 8-му Головному Управлінні».

Комплектування вечірнього відділення проводилося з кола співробітників 8-го ГУ у віці до 40 років, що мали закінчену середню освіту і досвід практичної роботи за фахом у дешифрувальній службі. Тим, хто закінчив вечірнє відділення, присвоювалася кваліфікація «інженера-криптографа» за фахом «ручні і машинні шифросистеми».

Значне місце в роботі ВШ займали курси з підготовки та перепідготовки криптологів різних профілів з кола спів-

робітників, вже зайнятих на криптологічній роботі, а головне – для тих, хто знов прийшли, зокрема закінчили закрите відділення мехмату МДУ, де з 1954 року спецдисципліни не викладалися. На курсах були групи як для осіб з вищою освітою, так і для осіб, що мали середню освіту. Термін навчання на курсах встановлювався від 3-х місяців до півтора року. Ці курси функціонували з 1954 по 1964 рік.

На курсах навчалися не тільки співробітники 8-го ГУ, але й проводилася підготовка криптологів для спеціальних служб ГРУ ГШ ЗС, ВМФ, а також для Головного управління гідрометеослужби при РМ СРСР.

У січні 1960 року був прийнятий закон «Про нове значне скорочення ЗС СРСР», відповідно до якого істотно скорочувалися і кадри КДБ. У зв'язку з цим ВШ 8-го ГУ КДБ, маючи у своєму складі профілюючі кафедри, аспірантуру, вечірнє відділення і курсову систему, вливалася (у скороченому вигляді) як 4-й (технічний) факультет у ВШ КДБ.

Спочатку факультет готував за повною вузівською програмою тільки інженерів-математиків для Державного комітету з радіоелектроніки на вечірньому відділенні. Однак успіхи спецслужб швидко піднімали його авторитет, і в 1961 році знову була прийнята урядова постанова про підготовку криптологів вищої кваліфікації.

Перед факультетом було поставлене нове завдання: набирати обдарованих математиків з числа випускників середніх шкіл на 5-річне навчання. За пропозицією авторитетних науковців служби очолити цю роботу був запрошений професор математики Іван Якович Верченко.

У 1960 році за пропозицією 8-го ГУ і ОТУ КДБ Вчена рада 8-го ГУ була скасована, а замість неї була створена Спецрада № 1 Вищої школи КДБ під головуванням А.М.Куренкова, якій були передані всі функції Вченої ради 8-го ГУ КДБ.

У травні 1962 року на факультеті було створено денне відділення з підготовки інженерів-математиків, а з 1 лютого 1970 року розпочалася підготовка військових інженерів для частин спеціальної служби.

Досить вчасно завершилася робота зі створення перших підручників з основних криптологічних курсів. Зокрема, книга Л.Кузьміна обсягом понад 500 сторінок була присвячена аналізу дискових (роторних) шифраторів, а книга Б.Антонова – лінійному шифруванню телеграфних повідомлень. По цих підручниках протягом декількох років випускники факультету вивчали тонкощі криптології.

Перший випуск нової хвилі молодих криптологів відбувся в 1966 році. Уже через кілька років їхнє число перевищило сотню, і вони стали відігравати істотну роль у спецслужбах КДБ, Радянської Армії, ВМФ і промисловості. Найсильніші з них регулярно поверталися на факультет як аспіранти, що зміцнювало зв'язок

кафедри з оперативними підрозділами.

Начальниками факультету у різні періоди часу були:

1. Баженов Євгеній Фомич (1960 - 1963).
2. Верченко Іван Якович (травень 1963 - 1972).
3. Бондаренко Володимир Іванович (січень 1972 - 1988).
4. Погорєлов Борис Олександрович (1989 - 1991).

Спецкафедру (криптографії) № 7 очолювали:

1. Пондопуло Георгій Іванович (1960 – 1976).
2. Шанкін Генріх Петрович (1977 – 1991).

4-й (технічний) факультет ВШ КДБ набирався досвіду і заслужив помітний авторитет у спецслужбах країни. У 1970-х роках Колегія КДБ двічі приймала рішення про перетворення його в самостійний вищий військовий навчальний заклад. Після першого з них Верченко «по гарячих слідах» розробив пропозиції, згідно з якими факультет повинен був перетворитися в навчальний заклад зі статусом Військової академії.

Однак ця пропозиція не знайшла підтримки ні в керівництва ВШ, ні в Управлінні кадрів КДБ, оскільки ставило факультет у більш привілейоване положення в порівнянні з «материнською» Школою. Верченко був розсерджений, посварився з начальством і відмовився від продовження керівництва факультетом, хоча і продовжував читати на ньому свій лекційний курс.

Начальником факультету був призначений генерал-майор Володимир Іванович Бондаренко – заступник начальника ГУ КДБ, що пройшов Велику Вітчизняну війну і командував раніше декількома підрозділами ГУСС. Для якнайшвидшого вирішення виниклих проблем Бондаренко став шукати собі надійного помічника, і у квітні 1972 року Л.Кузьмін був призначений заступником начальника рідного факультету замість Є.Баженова, який пішов у відставку. Так почався новий етап розвитку Технічного факультету ВШ КДБ і його кафедри криптографії. Випускники цього періоду і зараз грають ведучі ролі у російських криптослужбах.

Під керівництвом Юрія Володимировича Андропова на посаді голови КДБ в період з 1967 по 1982 рік, органи держбезпеки істотно укріпили і розширили свій контроль над всіма сферами життя держави і суспільства. Посилився їх політичний вплив в партійній номенклатурі: Андропов був вибраний членом Політбюро ЦК КПРС, потім секретарем ЦК партії і згодом зайняв вищий партійний пост генерального секретаря ЦК КПРС. А 5 липня 1978 року підвищилася позиція КДБ в системі органів державного управління: КДБ був перетворений з відомства при РМ СРСР в центральний орган державного управління СРСР з правами державного комітету і перейменований в КДБ СРСР, що втім не торкнулося системи і структури органів державної безпеки.

У цей період радянські криптослужби, що знаходилися у структурах КДБ, МЗС і ГШ ЗС, зміцніли, одержавши необхідну техніку та теорію. Попри все те дуже зросла й складність розв'язуваних нею завдань. Саме в той час почали використовувати винятково машинні шифри багатоалфавітної заміни, ускладнені перестановкою з ключами дуже великої довжини, які відповідали найвищим вимогам таємності. Тому шифри недавніх союзників були настільки «міцним горішком», що розколоти їх не було ніякої можливості, якщо тільки шифрувальниками не допускалися грубі помилки. Для вирішення складних дешифрувальних завдань в 16-му Управлінні КДБ був утворений та використовувався суперкомп'ютер «Булат».

Останнім російським політиком, що відкрито цитував «розкриту» чужу дипломатичну пошту, був у 1964 році тодішній партійний лідер Микита Сергійович Хрущов. Він хвастався тим, що регулярно читає листування між американським президентом і американським послом у Москві.

З часом структура 8-го ГУ КДБ змінювалась та у 1980-і роки складалося з трьох великих підрозділів – управлінь «*A*», «*B*» і «*C*», з яких управління «*A*» відповідало за безпеку дипломатичного листування, управління «*B*» – за безпечне виготовлення ключів і своєчасне забезпечення ними всіх, хто має потребу, а управління «*C*» - Спецуправління - за контрольний криптоаналіз старих шифрів, за розробку нових перспективних шифрів, за інженерно-криптографічний захист, за нормативну базу при роботі з шифрами, за зв'язок з промисловістю тощо.

Основна частина Спецуправління розміщувалася у Кунцеві, в будівлі, що нагадувала відому будівлю Ради Економічної Взаємодопомоги (далі – РЕВ) на Арбаті, – розкриту книгу. Тільки «сторінки» цієї книги були не вигнутими, як у оригінальному РЕВ, а прямими, і їх було не дві, а три, та й поверхів трохи менше.

У Спецуправлінні було декілька відділів, кожен з яких спеціалізувався на якомусь певному колі криптографічних завдань. 5-ий відділ Спецуправління займав особливе положення: знаходився не в основній будівлі, а у відособленій старовинній будівлі в'язничного типу. Це був Теоретичний відділ, в якому начальником був Вадим Євдокимович Степанов. В ньому працювало близько 50 чоловік, три відділення по 15-20 осіб у кожному. Основним завданням відділу було проведення контрольних криптоаналізів діючої шифрапаратури, виявлення її можливих недоліків і потенційних небезпек, пов'язаних з постійним розвитком обчислювальної техніки і криптологічних методів аналізу шифрів.

Згідно з чинними у ті часи положеннями будь-яка шифрапаратура, що знаходилася в експлуатації, повинна була піддаватися контрольному криптоаналізу не рідше, ніж один раз у 5 років. Це досить розумне положення, оскільки дати 100% гарантію стійкості на всі часи ніхто не міг, криптоаналіз постійно розвивав-

ся, з'являлися нові методи, нові люди, «свіжі» погляди. Сам криптоаналіз тривав, як правило, близько року і проводився таким чином.

Групі експертів з 3-5 осіб давали всі попередні звіти з аналізу даної апаратури, докладний опис її криптосхеми, умов експлуатації, вимог, що висувалися замовником апаратури, і впродовж року треба було спробувати знайти якісь нові методи криптоаналізу цієї схеми, які дозволили б скинути з попередніх оцінок декілька порядків стійкості. Робота майже завжди була чисто абстрактною, оскільки цю апаратуру експерти часто зовсім не бачили. Звичайно ж, якість проведеного криптоаналізу дуже сильно залежала від кваліфікації експертів, від їх криптологічного світогляду, ерудиції, уміння знайти та застосувати якісь нетрадиційні, нетривіальні підходи, відзначити те, що було пропущене на попередніх експертизах.

На початку 1980-х років розклад «криптологічних сил» у 5-му відділі був таким:

🗝 1 відділення – «криптографічні законотворці», ті, хто займався розробкою нових вимог до перспективної шифрапаратурі, а також розробкою радянського стандарту шифрування, заснованого на схемі типу «*DES*». Кузня кадрів для майбутніх криптологічних чиновників.

🗝 2 відділення – «ймовірники», ті, хто спеціалізувався на статистичних методах аналізу шифрів. Їх улюбленими об'єктами були традиційні електронні шифратори (фахівці називали їх «балалайками»), що працювали з бітами на елементній базі 1960-х років.

🗝 3 відділення – «алгебраїсти», ті, хто спеціалізувався на методах алгебри криптоаналізу. Тут, крім аналізу традиційних «балалайок», були люди, що займалися розробкою шифрів на новій елементній базі, а також, ті, хто вивчав і аналізував нові американські ідеї відкритих ключів.

В основному, у 5-му відділі працювали порівняно молоді хлоп'ята, що ще не втратили смаку до криптології як до науки. Всіляко підтримувалися і заохочувалися різні семінари, диспути, спори, здорова конкуренція за кращу ідею, за скинуті порядки з оцінок стійкості. Степанов прагнув дотримуватися балансу: половина людей у відділі закінчувала 4-й факультет ВШ КДБ, інша половина – МДУ. Це були дві різні команди, в яких «школярі» (4-й факультет) володіли тією перевагою, що були вже знайомі з криптологією, оскільки людині, що приходила на роботу, потрібно було декілька років на засвоєння всіх тонкощів криптологічних методів.

Крім контрольних криптоаналізів відділ вів ще декілька перспективних науково-дослідних робіт (далі – НДР), в яких намагалися передбачити можливості розвитку криптографії і обчислювальної техніки в майбутньому, появу нових напрямів в аналізі і синтезі шифрів, проблеми штучного криптографічного

інтелекту.

Разом з тим, КДБ була налагоджена плідна співпраця зі спецслужбами соціалістичних країн, що входили до «Варшавського договору». Так, у січні 1975 року 16-м Управлінням (радіоелектронної розвідки) КДБ була складена та затверджена «Інструкція з принципів і напрямків співробітництва зі службами безпеки соціалістичних держав у сфері операцій із дешифрування». Цей документ містив такі основні положення: по-перше, спільні операції з дружніми спецслужбами повинні проводитися під керівництвом КДБ; по-друге, передана союзникам інформація «не повинна розкривати рівень останніх радянських досягнень у сфері криптоаналізу».

Зокрема, в інструкції говорилося: «З огляду на той факт, що в даний час відповідні служби наших друзів накопичили значний досвід роботи по цілях з використанням методів електронного криптоаналізу, то існує деяка ймовірність того, що в майбутньому наші друзі можуть також спробувати використовувати ці методи самостійно проти інших цілей. В цих умовах істотно важливого значення набуває зміцнення подальшого співробітництва між 16-м управлінням і відповідними службами наших друзів для того, щоб виключити можливість проведення неконтрольованих нами операцій, що можуть завдати непоправної шкоди 16-му управлінню в тому, що стосується використання методів електронного криптоаналізу».

Цікаво, що у 1986 році видавництво «Радіо і зв'язок» у плані видань на 1987 рік опублікувало анонс книги Д.Конхейма «Основи криптографії». В ній містилися тільки загальновідомі поняття, опис американського криптостандарту «*DES*», найтривіальніші підходи до його криптоаналізу. Реакція 8-го ГУ КДБ була однозначною: заборонити. Весь тираж був «закритий» грифом обмеження доступу «Для службового користування» і направлений в закриті спецбібліотеки управлінь КДБ.

Відповіддю 8-го ГУ КДБ на американський стандарт став злегка «перефарбований» його варіант – радянський стандарт 1989 року, названий «алгоритм ГОСТ 28147-89».

Шифри на новій елементній базі, математична основа яких була закладена на 4-му факультеті ВШ у другій половині 1970-х років у рамках НДР «Проба», хоча і не стали загальнонаціональним стандартом, але внесли дуже вагомий внесок до розвитку цивільної криптології в Росії. В результаті фахівцями НДІ Автоматики була розроблена схема блокового шифру, що працював на основі байтового регістра зрушення та використовував тільки найтиповіші операції з байтами, які були закладені в архітектуру мікропроцесорів, що з'являлися у той час. Цю схему назвали «Ангстрем-3».

З появою перших персональних комп'ютерів «*IBM PC XT - 86*» з'явилися і

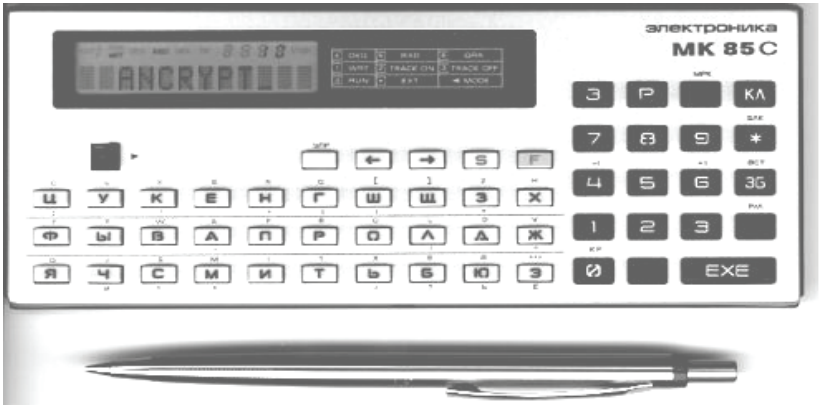
перші спроби реалізувати за їх допомогою криптологічні процедури, засновані на ГОСТ 28147-89. Але тут, навіть не дивлячись на ті фантастичні (на ті часи) можливості, які відкривав перед криптологами персональний комп'ютер, швидкість роботи радянського стандарту виявилася настільки повільною, що було прийняте рішення створити спеціалізовану плату для «IBM PC», на якій ГОСТ реалізовувався апаратними засобами. Так з'явився радянський криптопристрій «Кріптон».

Звичайно ж, із зростанням продуктивності персональних комп'ютерів міняліся погляди і на можливості реалізації з їх допомогою криптографічних алгоритмів. З появою «*IBM PC AT - 286*» швидкість ГОСТ стала вже не такою актуальною, але «маховик» радянської промисловості був запущений, Зеленоградський завод «Ангстрем» почав випускати «Кріптони».

У 1980-х роках активно розробляється й впроваджується шифрапаратура на базі електронно-обчислювальної техніки, створюється й починає експлуатуватися перша загальносоюзна система шифрованого зв'язку «Исток». Її розробники та творці одержали Державну премію, урядові нагороди.

У 1986 році фахівці заводу «Ангстрем» і 8-го ГУ КДБ вирішили зробити шифратор на базі портативного мікрокалькулятора «Електроніка МК-85», який серійно випускався на заводі «Ангстрем». Ними був розроблений шифратор «Ангстрем-3», який став основою програми, призначеної для реалізації за допомогою калькулятора «Електроніка МК-85». Цю програму треба було записати у програмно-записуючий пристрій (далі – ПЗП) калькулятора замість серійної програми, призначеної для побутових цілей.

Модернізований калькулятор назвали «Електроніка МК-85С». Він вже не виконував ніяких функцій калькулятора, але в нього можна було ввести секретний ключ завдовжки 100 десяткових цифр і з його допомогою здійснювати симетричне зашифрування та розшифрування текстової або цифрової інформації,



що вводилася з клавіатури, а шифровка або відкритий текст висвічувалися на екрані. Ніякі периферійні пристрої, окрім мережевого адаптера, до цього калькулятора не підключалися.

Цими калькуляторами спочатку передбачалося оснастити Радянську Армію, де довгий час використовувалися дуже громіздкі та незручні переговорні таблиці, призначені для засекречування переговорів на низових рівнях: відділення, взвод, рота. Також причиною його появи стала війна в Афганістані, коли незручні переговорні кодові таблиці в критичних ситуаціях вимушували солдатів передавати дані взагалі відкритим текстом, що приводило до трагічних подій.

Але поступово плани використання «МК-85С» все розростались і було потрібно забезпечити програмну реалізацію цього калькулятора на персональному комп'ютері, а також програмну систему для вироблення секретних ключів до калькулятора. Перший портативний шифратор «Електроніка МК-85С» був виготовлений у кінці 1990 року.

Його новизна полягала в тому, що працював цей шифратор не з бітами і не з байтами, а із звичайними десятковими цифрами. Основним критерієм була швидкість шифрування. «Електроніка МК-85С» – це, фактично, побутовий програмований калькулятор «Електроніка МК-85», в якому була реалізована проста мова «*BASIC*».

Крім того, значним досягненням 8-го ГУ КДБ у сфері дешифрування у 1989 році було «розкриття» криптосистеми аналогової апаратури засекречування телефонних переговорів АНБ США «*STU-II*», в результаті чого КДБ змогло прослуховувати телефонні розмови між Білим Домом і штаб-квартирою НАТО у Брюсселі.

Впродовж усієї історії СРСР органи державної безпеки, внутрішніх і закордонних справ, військового управління та розвідки під впливом зовнішніх обставин та зростанням обсягу завдань постійно реорганізовувалися, змінювали свою структуру та назву. Відповідно змінювалася структура та назва радянських криптологічних підрозділів:

1) в органах державної безпеки і внутрішніх справ

Дата утв.	*Найменування підрозділу*
05.05.1921	Спецвідділ при ВНК РРФСР
06.02.1922	Спецвідділ при ДПУ при НКВС РРФСР
02.11.1923	Спецвідділ при ОДПУ при РНК СРСР
10.07.1934	Спецвідділ при ГУДБ НКВС СРСР
25.12.1936	9 відділ ГУДБ НКВС СРСР
28.03.1938	Секретно-шифрувальний відділ НКВС СРСР
19.06.1938	3 Спецвідділ НКВС СРСР

29.09.1938	7 відділ ГУДБ НКВС СРСР
26.02.1941	5 відділ НКДБ і 6 відділення НКВС СРСР
31.07.1941	5 спецвідділ НКВС СРСР
03.11.1942	5 управління НКВС СРСР
14.04.1943	5 управління НКДБ і 2 спецвідділ НКВС СРСР
04.05.1946	6 управління МДБ СРСР
19.11.1949	Головне управління спеціальної служби при ЦК ВКП(б) (з 13.10.1952 - КПРС)
11.01.1950	Відділ «С» МДБ СРСР
14.03.1953	8 управління МВС СРСР
13.03.1954	8 ГУ КДБ при РМ СРСР (з 05.07.1978 - КДБ СРСР) і 2 спецвідділ МВС СРСР

2) в органах закордонних справ

Дата утв.	*Найменування підрозділу*
12.1917	Відділ шифрувальний і друкарський НКЗС РРФСР
29.04.1918	Шифрувальний відділ НКЗС РРФСР
1922	Шифрувальна частина Управління справами НКЗС РРФСР
01.1923	Секретний відділ Управління справами НКЗС РРФСР
12.11.1923	Шифрувальна і секретна частина Секретаріату Колегії НКЗС СРСР
09.03.1925	Шифрувальна частина Секретаріату Колегії НКЗС СРСР
кінець 1925	Секретно-шифрувальний відділ Секретаріату Колегії НКЗС СРСР
12.02.1930	Секретно-шифрувальний відділ НКЗС СРСР
05.1939	10 відділ НКЗС СРСР
18.03.1946	10 відділ МЗС СРСР
1989	Управління зв'язку МЗС СРСР

3) в органах військового управління

Дата утв.	*Найменування підрозділу*
13.11.1918	Шифрувальне відділення звітно-організаційного відділу Організаційного управління ВГШ РСЧА
10.05.1921	Центральний шифрувальний відділ Штабу РСЧА
28.03.1924	Шифрувальний відділ при РВР СРСР
09.1926	2 відділ Управління справами НКВМС СРСР
10.09.1930	7 відділ Штабу РСЧА

13.10.1930	8 відділ Штабу РСЧА
19.07.1939	Відділ шифрувальної служби Оперативного управління ГШ РСЧА
18.08.1941	Управління шифрувальної служби ГШ ЧА
19.11.1949	Головне управління спеціальної служби при ЦК ВКП(б)
24.04.1953	Управління ГШ Збройних Сил Радянської Армії
1955	Управління ГШ Збройних Сил СРСР

4) в органах військової розвідки

Дата утв.	*Найменування підрозділу*
08.11.1918	«Завідувач шифром» РУ ПШ РВРР
19.06.1919	Шифрувальна частина РУ ПШ РВРР
09.1920	Шифрувальне відділення РУ ПШ РВРР
04.04.1921	Шифрувальне відділення II відділу РУ Штабу РСЧА
11.1922	Шифрувальне відділення РВ II частини Штабу РСЧА
28.03.1924	Шифрувальне відділення II відділу РУ Штабу РСЧА
09.1926	I частина IV Управління Штабу РСЧА
03.1931	1 частина і 5 відділ IV Управління Штабу РСЧА
22.11.1934	1 частина і 5 відділ 5 Управління РСЧА
11.1935	Шифрувальне відділення і 7 відділ 5 Управління РСЧА
05.1939	9 відділ і 11 відділ 5 Управління НКО СРСР
26.07.1940	9 відділ і 10 відділ РУ ГШ Червоної Армії
16.02.1942	Відділ спецзв'язку і 7 відділ 2 Управління ГРУ ГШ Червоної Армії
03.11.1942	7 відділ 2 Управління ГРУ увійшов до складу 5 управління НКВС СРСР
19.04.1943	8 відділ РУ ГШ Червоної Армії
06.1945	8 відділ ГРУ ГШ Червоної Армії
03.1946	8 відділ ГРУ ГШ Збройних Сил СРСР
30.05.1947	7 Управління Комітету Інформації при РМ СРСР
19.11.1949	Головне управління спеціальної служби при ЦК ВКП(б)
24.04.1953	Відділ зв'язку ГРУ ГШ Збройних Сил Радянської Армії
1955	8 відділ ГРУ ГШ Збройних Сил СРСР

Однак, незважаючи на всі реорганізації, в цілому радянськими криптослужбами були розроблені й впроваджені у війська та державні органи ручні шифри високого ступеня стійкості, що забезпечували необхідний захист будь-яких повідомлень.

4.7. «Полювання» за шифрами

Розвідка завжди активно вела «полювання» за криптологами та шифрами супротивника. Розкриття складніших кодів і шифрів, зазвичай, залежало не тільки від здібностей дешифрувальників, але й від допомоги розвідників. Починаючи з сорокових років XVIII століття розвідка час від часу користувалася перехопленням дипломатичної кореспонденції як джерелом інформації.

Ставилося й більш важке завдання – впровадити агента до служби супротивника, пов'язані з шифрами та кодами. Часто розкриттю шифрів і кодів сприяли отримані агентурним шляхом відкриті тексти, які можна було прив'язати до відповідних шифрованих повідомлень. Для кодів, наприклад, це відразу давало деяке число розкритих кодових груп, після чого значно полегшувалася робота з дешифрування.

Царська «охоронка» стала першою сучасною розвідувальною службою, що ставила перед собою завдання з викрадання іноземних дипломатичних кодів і шифрів, а також оригінальних текстів дипломатичних телеграм, які можна було б згодом порівняти з перехопленими шифровками. Для цього в МЗС був створений секретний відділ «з метою одержання доступу до архівів іноземних місій у Санкт-Петербурзі».

Нерідко коди й шифри просто купувалися та продавалися. Європейським центром подібної діяльності у той час був Відень. Там вироблялися всілякі угоди з купівлі та продажу копій таємних документів, листів, карт, кодів, планів, креслень тощо. Співробітник російського ЧК С.Майський писав, що Росія купувала коди й шифри у Відні, Парижі та Брюсселі. Торговцям кодами можна було навіть робити «попередні замовлення».

Цими методами активно користувалися розвідки Німеччини, Австро-Угорщини й інших країн. Коди, що представляли менший інтерес, грецький, болгарський або іспанський, можна було легше дістати. Вони коштували дешевше – 1,5-2 тисячі карбованців, у той час як німецькі, японські або американські – десятки тисяч. Ціни шифродокументів інших країн коливалися між 5 і 15 тисячами.

У Брюсселі шифри й коди здобувалися у відомого авантюриста де Верніна. Його основним заняттям було викрадення шифрів і кодів з посольств за допомогою працюючих там і підкуплених ним лакеїв, швейцарів, денщиків тощо. Де Вернін робив фотографії украдених документів і продавав їх. Таким чином, у російській криптослужбі була велика кількість іноземних кодів і шифрів. У порядку взаємодопомоги МЗС Росії навіть «ділився» інформацією з морськими і сухопутним генеральними штабами.

У 1800 році член колегії МЗС Росії М.Панін писав своєму послу в Берліні: «Ми маємо у своєму розпорядженні шифри листування короля (Пруссії) з його повірником у справах тут. Якщо Ви запідозрите Хаугвиця (міністра закордонних справ

Пруссії) у віроломстві, знайдіть привід для того, щоб він направив сюди повідомлення з даного питання. Як тільки повідомлення, послане ним або королем, буде розшифровано, я негайно повідомлю Вам про його зміст».

Наприкінці XVIII століття російське посольство в Парижі через свого секретаря Мешкова завербувало одного з чиновників МЗС Франції. У такий спосіб були отримані шифри та ключі до них, якими користувався міністр закордонних справ Франції граф Монморсі та французький повірник у справах у Росії Жені. У результаті Росія одержувала секретну інформацію тривалий час.

Наприкінці XIX століття російським агентом був завербований німецький підданий К.Маукіш, що займав посаду перекладача китайського адміралтейства. За його допомогою були отримані таємні сигнальні (кодові) книги Японії.

У 1902 році начальник відділу австрійської розвідки та контррозвідки полковник Альфред Редль за велику суму продав Росії копію єдиного військового словникового коду Австрії, так само як і австрійські плани ведення війни на Східному фронті.

У другій половині 1904 року співробітниками «Спеціального відділення з розшуку про міжнародне шпигунство», створеного в Особливому відділі ДП Російській Імперії та яким керував Іван Федорович Манасевич-Мануйлов, «агентурним шляхом» були добуті американський, китайський, шведський та японський дипломатичні шифри.

З березня 1905 року цей підрозділ став іменуватися «IV (секретним) відділенням дипломатичної агентури» Особливого відділу ДП, котрий очолив Аркадій Михайлович Гартінг (Гекельман). А завідувачем Закордонною агентурою ДП з вересня того ж року став Михайло Степанович Комісаров. На протязі свого існування до 1906 року співробітники секретного відділення здобули 12 дипломатичних шифрів і кодів. Така активна їхня діяльність не залишилася непоміченою супротивниками.

Так, у червні 1904 року Чарльз Хардінг, що займав посаду посла Великобританії в Санкт-Петербурзі з 1904 по 1906 рік, доповідав у британське МЗС, що він був «надзвичайно засмучений», дізнавшись про те, що начальнику його канцелярії була запропонована величезна сума в 1000 фунтів за те, щоб він викрав копію одного з дипломатичних шифрів. Він також повідомив, що один видний російський політик сказав, що йому «все одно, наскільки докладно я передаю наші з ним бесіди, якщо це робиться в писемній формі, але він благав мене ні в якому разі не пересилати мої повідомлення телеграфом, оскільки зміст усіх наших телеграм їм відомий».

Усі зусилля, спрямовані на модернізацію досить примітивної системи безпеки британського посольства, не принесли ніяких результатів. Секретар англійського посольства Спрінг Райс доповідав у лютому 1906 року: «От уже протягом деякого часу з посольства зникають папери... Кур'єр та інші особи, пов'язані роботою з посольством, перебувають на утриманні поліцейського департаменту і, крім того,

одержують винагороду за доставку паперів». Спрінг Райс стверджував, що йому вдалося встановити організатора секретних операцій проти посольства Великобританії. За його словами, це був Комісаров, співробітник «охоронки», за наказом якого «біля посольства вечорами постійно знаходяться поліцейські емісари для того, щоб здобути папери, які доставляються».

Незважаючи на те, що в посольстві був установлений новий сейф, в архівні шафи врізані нові замки, а співробітники одержали найсуворішу інструкцію нікому не передавати ключі від канцелярії, дипломатичні папери продовжували зникати. Два місяці потому Спринг Райс одержав докази того, що «до архівів посольства існує доступ, який дозволяє виносити папери та робити їхню зйомку в будинку Комісарова». Швидше за все, це була справа рук підкупленого співробітника посольства, який, зробивши воскові відбитки з замків архівних шаф, одержав дублікати ключів від «охоронки». Щось подібне відбувалося й у посольствах Сполучених Штатів, Швеції та Бельгії.

Протягом усього періоду правління Миколи II Росія була лідером у сфері перехоплення та розшифрування дипломатичної пошти. Великобританія, Німеччина, Сполучені Штати та більшість менш впливових держав узагалі не мали подібної служби аж до Першої світової війни. Єдиним серйозним конкурентом Росії в цій сфері була її союзниця Франція. Протягом двадцяти років до початку Першої світової війни ЧК МЗС Франції та служби безпеки «Сюрте» успішно працювали над розшифруванням дипломатичних кодів і шифрів більшості провідних держав. У той час, як росіянам удавалося розгадувати деякі французькі дипломатичні коди і шифри, російське дипломатичне листування залишалося зовсім недоступним для французів (хоча вони й домоглися деяких успіхів у розшифруванні кодів і шифрів закордонної агентури).

Улітку 1905 року, в останні дні російсько-японської війни та франко-німецької кризи в Марокко, Росія та її союзниця Франція протягом короткого періоду співробітничали в області перехоплення та розшифрування таємної інформації. У червні 1905 року російський посол за вказівкою свого уряду передав французькому прем'єр-міністру копію розшифрованої німецької телеграми, пов'язану з марокканською кризою. Для Франції ця телеграма мала настільки велике значення, що «Сюрте» отримало вказівку передати іноземному відділу російської «охоронки» все японське дипломатичне листування, що тільки вдалося перехопити та розшифрувати ЧК французької служби безпеки.

Телеграми, що були послані Манасевичем-Мануйловим та містили розшифровані японські документи, у свою чергу, були перехоплені та розшифровані ЧК французького МЗС. Не знаючи про те, що ці документи були передані Росії за вказівкою прем'єр-міністра, у МЗС вирішили, що відбувся серйозний витік інформації в системі безпеки кодування та шифрів, і відділу шифровок був відданий наказ припинити

всі контакти з аналогічним відділом «Сюрте». За результатом безглуздої помилки, породженої коротким періодом співробітництва між французькою та російською службами перехоплення, ЧК МЗС і «Сюрте» протягом наступних шести років напружено працювали абсолютно незалежно один від одного, іноді перехоплюючи та розшифровуючи ті ж самі дипломатичні телеграми. З того часу Росія та Франція жодного разу не обмінювалися перехопленою інформацією.

Це прикре непорозуміння, що виникло за результатом плутанини в діях французьких служб перехоплення, негативно вплинуло на роботу російської служби дешифрування. Аж до початку Першої світової війни росіянам удавалося розшифровувати значну частину дипломатичного листування практично всіх провідних держав, за винятком Німеччини. Нерозсудливі дії французів під час франко-німецької агадирської кризи 1911 року призвели до того, що німці змінили свої дипломатичні коди та шифри. У результаті цього російські дешифрувальники протягом двох років з 1912 по 1914 рік не могли прочитати ні однієї німецької шифровки.

У 1919 році в арештованого у Москві офіцера контрреволюційного «Національного центра», тісно пов'язаного з білогвардійською армією генерала Денікіна, був вилучений папірець з викладеним у ній шифром змовників: «Візьміть російське Євангеліє від Луки, главу 11 (де «Отче наш») – текст пишеться цифрами в два і три цифрові знаки; праворуч завжди означає порядок букви у вірші, а інші цифри означають номер вірша...»

Однією з перших радянських спецоперацій було вилучення шифру з китайського посольства в 20-х роках, яка була проведена талановитим розвідникомсамоучкою Петром Леонідовичем Поповим, механіком з канонерського човна «Манджур», що охороняла рибні промисли в районі Камчатки. Користуючись завойованим авторитетом у китайської влади і посла Китаю в СРСР Чи Тьяао, Попов одержав вільний доступ у китайське посольство в Москві. Вивчивши обстановку там, він склав план одержання зліпків з ключів від сейфа, у якому знаходилися шифродокументи. Відключивши опалення будинку посольства перед черговим візитом туди, Попов на прохання господарів зайнявся перевіркою всієї опалювальної системи й одержав доступ у зону безпеки. Перевіряючи там опалювальні батареї, він улучив момент і зняв потрібні зліпки з ключів, що лежали на столі шифрувальника. Маючи ключі від сейфа, вилучення шифру було здійснено без утруднень.

У 1921 році радянська спецслужба здобула шифри антирадянських організацій у Лондоні та Парижі. Перехоплені та розшифровані телеграми цих центрів надали серйозну допомогу у виявленні та знешкодженні ворогів молодої республіки.

У 1924 році співробітнику ОДПУ Василю Івановичу Пудіну вдалося через завербовану агентуру в Харбіні отримати японські дипломатичні шифри. У той час

японці вважали, що їх мова настільки складна, що, навіть володіючи шифрами, не можна зрозуміти текстів шифролистування. Тому деякі японські дипломати і шифрувальники готові були продати відомі ним шифри.

У 1925 році радянському військовому аташе в Ірані, колишньому офіцеру царської армії, Бобріщеву вдалося завербувати всіх шифрувальників головного штабу Ірану, завдяки чому він знав не тільки дислокацію іранської армії, але був в курсі всіх змін в іранській армії та її руху.

У середині 1920-х років співробітникам ОДПУ в Ташкенті вдалося умовити афганського консула продати шифри і таємне листування консульства. Консул вимагав за це 10 тисяч рублів золотом. Оскільки грошей не було, чекісти розробили наступну операцію. Вибравши день, коли в консульстві залишилися тільки консул і секретар, консула запросили на вечерю, а секретаря викликала до себе його подруга. В кінці бенкету консулу підсипали в стакан снодійного і, коли він заснув, у нього з годинного ланцюжка зняли ключі від сейфу. Швидко проникнувши в консульство, чекісти сфотографували шифри і все таємне листування.

У 1926 році резиденту ОДПУ на Близькому Сході Агабекову вдалося завербувати шифрувальника при Раді міністрів Персії. Завдяки послугам цього шифрувальника російський уряд мав можливість отримувати всі інструкції, що посилалися персидським урядом своєму представнику в Москві.

У 1927 році радянська спецслужба завербувала експерта з шифрів Кабінету Міністрів Ірану. Крім того, радянська розвідка зуміла роздобути ключ до шифрів вірменської націоналістичної партії «Дашг накцутюн» («Союз»). Діяльністю «дашнаків» керували з-за кордону – іранського міста Тебріза. Радянський резидент у Тебрізі встановив зв'язок з одним з чиновників поштової служби Ірану та незабаром отримав достатню інформацію, що дозволяла йому вчасно дізнаватися про всі заплановані заходи «дашнаків».

У 1928 році у радянське представництво в Парижі прийшов відставний офіцер швейцарської армії Россі та запропонував купити у нього за 200 тисяч франків коди і шифри Італії. Пізніше радянською розвідкою було встановлено, що ця торгівля шифрами була організована міністром закордонних справ Італії графом Чиано.

20 червня 1929 року шифрувальник управління зв'язку британського МЗС Ернест Холовей Олдхем, перебуваючи з торгівельною делегацією у Парижі, прийшов у радянське посольство та запропонував купити у нього за 2 тисячі доларів англійський дипломатичний шифр. Протягом трьох років від Олдхема одержували англійські шифри та коди, щотижневі збірники шифротелеграм британського зовнішньополітичного відомства.

Талановитий радянський розвідник-нелегал Дмитро Олександрович Бистролєтов, працюючи у 1927 році в радянському торгівельному представництві у Празі, успішно здійснив «розробку» співробітниці посольства Франції, що мала

безпосередній доступ до листування та шифрів французького МЗС. У результаті проведеної роботи у 1928 році від неї були отримані доповіді та шифри французького посла в Чехословаччині.

Крім того, Бистролєтов, одержавши вказівку здобути шифри фашистської Італії, закохав у себе італійську графиню, єдину в історії фашистської Італії жінку-посла, та одержав через неї необхідні шифри. У середині 30-х він добув німецькі шифри й установив оперативний контакт зі співробітником військової розвідки Франції, від якого згодом були отримані австрійські, італійські та турецькі шифрувальні матеріали.

Бистролєтов також регулярно отримував таємні документи та інформацію від високопоставленого чиновника англійської розвідки, фахівця з розробки шифрів і дешифрування. Він на початку 1930-х років з'явився до російського військового аташе в Лондоні та запропонував купувати у нього копії з щоденних листів, які з різних країн надходять до британського зовнішньополітичного відомства. 17 листопада 1932 року Бистролєтов за зразкове виконання завдань керівництва радянської розвідки був нагороджений іменною зброєю.

З 1929 року у німецькій таємній поліції розпочав свою службу Віллі Леман, що був радянським розвідником, який мав кодове ім'я «А-201» і псевдонім «Брайтенбах». Його останньою посадою в «РСХА» була посада начальника контррозвідки на заводах рейха. Від нього в Москву надходили тексти шифротелеграм різних відомств рейха з їх розшифровкою, що допомогли радянській дешифрувальній службі одержати ключ до деяких німецьких кодів. У Москві високо оцінювали результати діяльності «Брайтенбаха». Так, у 1940 році німецький відділ розвідки НКВС, складаючи довідку про цього агента вищому керівництву, доповідав: «За час співробітництва з нами з 1929 року «Брайтенбах» передав нам надзвичайно велику кількість справжніх документів і особистих повідомлень...»

У 1930 році високопосадовець румунської поліції в знак протесту проти свого несправедливого зниження в посаді передав радянській розвідці секретний код Румунії. У 1930-і роки радянська розвідка на Далекому Сході мала агента «*Кротова*», через якого, крім великого обсягу важливої інформації, добувала шифрувальні таблиці та кодові книги не тільки японської військової розвідки, але й США, Китаю та Німеччини.

У травні 1935 року був завербований шифрувальник МЗС Великобританії Джон Герберт Кінг. Інформація, що надходила від нього, була надзвичайно важливою. За допомогою переданих телеграм Спецвідділу НКВС удалося розкрити шифри британського МЗС, так що чекісти могли читати навіть ті телеграми, до яких Кінг не мав доступу. На жаль, провал Кінга відбувся з вини Вальтера Кривицького, що «втік на захід» у 1937 році та видав його англійській владі. У вересні 1939 року Кінг був арештований та засуджений за шпигунство на 10 років ув'язнення.

У 1936 році заступник резидента НКВС в Болгарії Пудін, використовуючи накопичений раніше досвід оперативної роботи по японцях, завербував крупного японського дипломата. В результаті за винагороду від нього були отримані шифри МЗС Японії, які це зовнішньополітичне відомство застосовувало в ті роки в Європі. Це дозволило в перші роки Другої світової війни читати шифролистування між Токіо і Берліном та бути в курсі їх планів відносно СРСР.

Улітку 1936 року радянська військова розвідка одержала доступ до шифролистування військового аташе Японії в Берліні з японським Військовим міністерством у Токіо. Фотокопії шифротелеграм були надані в розпорядження московського експерта, що володів японською мовою. Він дешифрував їх за допомогою кодового блокнота, добутого радянською розвідкою, і перевів на російську мову. Прочитані японські шифровки стосувалися діяльності країн, що приєдналися до так називаного антикомінтернівського пакту, що, безсумнівно, становило величезний інтерес для батьківщини III Інтернаціоналу.

Крім того, у 1935 році радянська розвідка в Голландії, у 1938 році в Австрії та у 1940 році у Швейцарії зуміла здобути англійський дипломатичний шифр, що дозволив їй мати доступ до таємного листування МЗС Англії та британської розвідки. Завдяки цьому радянський уряд знав про підготовку «мюнхенської змови» Англії та Франції з Німеччиною й Італією «за спиною» СРСР.

У 1942 році співробітник британського міністерства фінансів Джон Кернкросс, завербований радянською розвідкою ще в 1930-і роки, був переведений на роботу в британську дешифрувальну службу в Блетчлі-Парку для спостереження за розшифруванням британськими контррозвідниками донесень, що були зашифровані з використанням німецької машини «Енігма». Протягом майже трьох років він кожного тижня передавав радянській розвідці матеріали дешифрувальної служби Британії. У 1944 році Кернкросс був переведений у Лондон у штаб-квартиру «*SIS*», де координував роботу британської розвідки в Югославії. Інформація, що надходила від нього, освітлювала плани і наміри Англії і США в цій країні.

У 1945 році був заарештований відповідальний співробітник Головного Управління імперської безпеки Німеччини Гельмут фон Паннвіц, який передав радянській контррозвідці розкритий німцями код, що використався у листуванні між Черчиллем і Рузвельтом.

У 1946 році росіянами був завербований американський шифрувальник Вільям Вейсбанд. На початку 1950-х років був завербований шифрувальник британського військово-морського аташе у Варшаві Гарі Фредерик Хоутон, якого у січні 1961 року «здав» ЦРУ підполковник польської розвідки Михайло Голенієвський, зрадивший свою державу.

У лютому 1953 року у Східному Берліні був завербований писар-реєструвач таємної частини розвідувального відділу Берлінського командування армії США

сержант Роберт Лі Джонсон, який пізніше, у свою чергу, залучив до співробітництва свого друга кур'єра збройних сил в аеропорті Орлі сержанта Джеймса Мінткенбау. В період з грудня 1962 року по кінець квітня 1963 року Джонсон регулярно двічі на місяць чергував у диспетчерському центрі військового відомства США в Європі, де розкривав сейфи та передавав радянським розвідникам пакети, що містили цілком таємну інформацію американського військового відомства, у тому числі, матеріали щодо шифросистем, що використовувались в армії США і НАТО. Ці шифрувальні матеріали дозволяли читати особливо важливе листування США та їхніх союзників з НАТО. Крім того, протягом декілька років радянські фахівці були в курсі розвитку американської криптології та практичних удосконалень у цій сфері, у тому числі, сучасної шифрувальної апаратури. Зрештою Джонсон був схоплений у 1964 році у зв'язку зі зрадництвом Носенка.

У 1957 році з радянськими спецслужбами почав співробітничати Нельсон Корнеліус Драммонд, корабельний писар 1-го класу, а потім – клерк у штабі ВМС США в Лондоні, який мав доступ до абсолютно секретної інформації. У 1958 році він служив у США, де впродовж чотирьох років передавав інформацію про військово-морські бойові і шифрувальні системи, протичовнову електроніку і матеріально-технічне забезпечення підводних човнів. Американською контррозвідкою був арештований у вересні 1962 року та засуджений до довічного вироку.

Наприкінці 1959 року були завербовані радянською розвідкою фахівці-криптологи Вернон Фергюсон Мітчел і Вільям Гамільтон Мартін, які працювали в АНБ з 1957 року і найбільше повно розкрили її діяльність з перехоплення та дешифрування іноземних ліній таємних комунікацій. Приблизно через рік, 6 вересня 1960 року вони з'явилися в Москві, де в Будинку журналістів відбулася прес-конференція за їхньою участю. Вони викрили підривну діяльність АНБ, розповіли, як ця американська спецслужба перехоплювала та читала зашифровану кореспонденцію та повідомлення не тільки супротивників, але й союзників США.

Серед останніх вони називали Італію, Францію, Туреччину, Югославію, Індонезію, Уругвай, Об'єднану Арабську Республіку. Вони стверджували, що АНБ регулярно читало таємну кореспонденцію більш ніж сорока держав. Знаходячись у Москві, вони передали дуже важливу інформацію про роботи АНБ в сфері криптології. Обидва потім упродовж довгих років були цінними консультантами для радянських спецслужб з питань, що стосувалися АНБ.

Навесні 1960 року в радянське посольство у Вашингтоні прийшов співробітник АНБ Джек Данлеп і запропонував таємні документи АНБ. Данлеп мав можливість добувати різні настанови, посібники з ремонту, математичні моделі і плани науково-дослідних робіт щодо таємних шифромашин США. 22 липня він скоїв самогубство та з усіма військовими почестями був похований на Арлингтонському національному цвинтарі. Про його зрадництво так ніколи і не довідалися, якби

місяць по тому його вдова не знайшла схованку з цілком таємними документами, які він не встиг передати КДБ. Провівши розслідування, АНБ прийшло до висновку, що за своєю важливістю відомості, видані Данлепом КДБ, у багато разів перевершували інформацію, передану Мартіном і Мітчелом, разом узятими.

У серпні 1962 року співробітник криптографічного підрозділу розвідки США в Парижі Джозеф Хелміч передав агентам радянської розвідки за винагороду в 130 тисяч доларів таємну інформацію про американські шифри. Вона дозволила КДБ перехоплювати зв'язок американських військ у період війни у В'єтнамі.

У тому ж році в США був завербований підполковник Вільям Генрі Валлен, який керував шифрувальним відділом у Комітеті начальників штабів міністерства оборони США. Протягом двох років від нього надходила важлива інформація про ядерну зброю, ракети, детальні плани командування стратегічної авіації США і плани дій американських військ у Європі. Однак у 1966 році Валлена заарештували агенти ФБР, і у тому ж році суд засудив його до 15 років тюремного ув'язнення.

20 червня 1963 року колишній криптоаналітик АНБ Віктор Гамільтон, пропрацювавши два роки в цьому відомстві на арабському напрямку, знаходячись проїздом у Празі, прийшов до радянського посольства та попросив політичного притулку. А 23 липня у вечірньому випуску газети «Известия» був опублікований лист Гамільтона, у якому він розповів про американське радіошпигунство.

Будучи досвідченим арабістом, він займався з матеріалами АНБ щодо Об'єднаної Арабської Республіки, Іраку, Лівану, Йорданії, Сирії, Південної Аравії, Ємену, Лівії, Марокко, Тунісу, Ірану, Ефіопії та Греції. Усе шифроване листування, наприклад, Єгипту з єгипетськими посольствами у всіх країнах, за ствердженням Гамільтона, розшифровувалася в АНБ і направлялося до Держдепартаменту США. Крім цього, він повідомив радянській розвідці усю відому йому інформацію щодо структури АНБ, шифрів, імен керівників тощо.

Восени 1965 року молодий солдат Роберт Стивен Липка, який служив в АНБ та знищував таємні документи, усвідомивши цінність минаючих через його руки документів, прийшов у посольство СРСР у Вашингтоні та запропонував продавати ці таємні матеріали. Пропозиція була негайно прийнята. Усього за період з 1965 по 1967 рік з Липкою було проведено близько 50 операцій зв'язку, під час яких було одержано більш 200 важливих документів АНБ, ЦРУ, Держдепартаменту та інших урядових відомств США.

У 1966 році був арештований штаб-сержант ВПС США Герберт Вільям Бекенхаупт, який з 1965 року служив радистом у Пентагоні і мав доступ до абсолютно секретних документів. Він передавав радянській розвідці сигнальні та кодові книги, а також інші документи щодо електроніки та криптосистем ВПС США.

На початку 1968 року в прибережних водах КНДР було затримано американське судно радіорозвідки «Пуебло». На борту знаходилися фахівці-криптологи

США, а також секретна техніка, у тому числі і шифратори. Знищити апаратуру і документи команда не встигла. Північні корейці отримали важливі матеріали і апаратуру, зокрема американські шифратори «*KW-7*», «*KWR-37*» і «*KG-14*», а також ключі до них. Ці відомості стали надбанням радянської криптослужби та надали імпульс до дешифрування військово-морського листування США.

У січні 1968 року старший уорент-офіцер Джон Ентоні Уокер, старший черговий офіцер із зв'язку в штабі командуючого підводним флотом США в Атлантичному регіоні, приїхавши до Вашингтона, прийшов до радянського посольства та продемонстрував місячні ключові установки для шифромашини «*KL-7*». Він заявив, що має необмежений доступ до шифрувальних апаратів і ключів, і попросив за свої послуги тисячу доларів у тиждень.

Вже в лютому того ж року на зустрічі, що відбулася за межами США, Уокер знову передав уже кілька ключів для шифру у виді спеціальних карток. Передачу шифроключів Уокер робив систематично впродовж свого співробітництва з СРСР і, в цілому, кількість їх за оцінкою американської спецслужби після його арешту було достатньою для «розкриття» та прочитання більш мільйона зашифрованих повідомлень, що проходили по лініях комунікацій ВМФ США.

Цілих 17 років радянські фахівці ретельно аналізували хід розвитку американської криптології, так що будь-які нові перетворення в цій сфері могли бути розгадані радянськими фахівцями на основі цього багаторічного досвіду. Таємний шифрований зв'язок підводних човнів, що повідомляли своєму командуванню про місцезнаходження та напрямок руху, усе це знаходилося під контролем завдяки отриманим розвідкою через Уокера шифрам і ключам до них.

Разом із Джорданом Уокером на СРСР працював і Альфред Джеррі Уітворт, співробітник відділу постачання бази морської авіації в Лос-Аламітос і навчального центра ВМФ у Сан-Дієго. Він передавав радянській розвідці таємну військову інформацію, у тому числі криптографічні матеріали, шифрувальні ключі та посібники з експлуатації військових систем зв'язку. У червні 1985 року після арешту та засудження Уокера Уітворт під впливом публічного процесу добровільно здався ФБР.

У січні 1968 року капрал британських збройних сил Джефрі Артур Прайм попросив, щоб з ним зв'язалися представники радянської розвідки. У той час він працював у Західному Берліні на станції перехоплення радянських комунікацій. Надалі йому вдалося влаштуватися у Штаб-квартирі урядового зв'язку Великобританії (далі – ШКУЗ). Восени 1969 року він закінчив навчання, здав іспити з мови та приступив до роботи на посаді шифрувальника ШКУЗ.

Перші шість з половиною років Прайм провів у лондонській групі обробки – спеціальному дешифрувальному підрозділі, що знаходився в Сент-Данстанз Хілл. Навесні 1975 року його, тепер уже визнаного в ШКУЗ фахівця з російської мови, направили на роботу з космічного перехоплення всіх ліній зв'язку Радянського

Союзу. До вересня 1975 року Прайм доставив у Відень велику кількість знятих ним на фотоплівку цілком таємних матеріалів ШКУЗ.

Хоча впродовж цього часу він давав розвідці менше криптологічних таємниць, ніж інформації про практичне застосування їх у ШКУЗ, але у 1975 році він досяг поставленої мети. Від Прайма стали надходити такі матеріали, що він перетворився в повноцінне джерело знань про британську криптологію, а отже, і про американські таємниці у цій сфері у зв'язку з тісною взаємодією ШКУЗ і АНБ.

У листопаді 1982 року розвідувальна діяльність цього агента закінчилася арештом і осудженням його на цілих 38 років тюремного ув'язнення. Великий термін підтверджує той величезний збиток для безпеки британських таємних ліній зв'язку, що нанесло співробітництво Прайма з радянською розвідкою. І не тільки їм, а й іншим західним спецслужбам, і в першу чергу, АНБ і ЦРУ.

У 1973 році польська розвідка отримала шифр однієї з латиноамериканських республік. Цим придбанням вона поділилася з СРСР. Вказана країна представляла інтерес для радянської розвідки, оскільки було відомо, що ЦРУ США використовувало посольство цієї країни в Москві для прикриття дій американських розвідників. Шифр незабаром був змінений, і виникла необхідність в придбанні нових шифрів посольства. Радянська спецслужба спільно з поляками провела акцію проникнення в посольство цієї країни у Варшаві та отримала необхідні шифродокументи.

У 1974 році в результаті спільних операцій з дружніми спецслужбами соціалістичних країн 16-му Управлінню КДБ удалося одержати шифроматеріали із семи посольств у Празі, з п'яти – у Софії, із двох – у Варшаві і двох – у Будапешті.

У квітні 1975 року були завербовані співробітники АНБ Крістофер Бойс і Ендрю Лі. Батько Бойса, що був співробітником ФБР, рекомендував сина для роботи в АНБ, куди він і був прийнятий клерком у ЧК, надзвичайно засекречений, навіть, у системі самого АНБ шифрувально-кодовий підрозділ, звідки по спеціальних зашифрованих лініях зв'язку направлялася цілком таємна інформація до ЦРУ та інших відомств і спецслужб США.

Ця інформація зашифровувалася в ЧК на спеціальних шифромашинах, ключі до яких і шифри змінювалися щодня. Бойс займався обслуговуванням шифрованого зв'язку з космічними супутниками та мав доступ до самих «чуттєвих», тобто суворо охоронюваних таємниць АНБ. Через його руки проходили щоденні ключі до шифрувальних машин, що використовувалися на всіх каналах зв'язку в американських спецслужбах, у тому числі від АНБ до ЦРУ та у зворотньому напрямку.

Радянська розвідка одержувала від Бойса плівки з фотокопіями карт-ключів для шифромашин на місяць наперед і масу конкретної інформації, що стосувалася всієї системи супутникової розвідки США та іншої діяльності АНБ. Успішна робота з цими агентами продовжувалася до середини 1977 року, коли відбувся провал кур'єра, та агенти були арештовані. У липні 1977 року Чи був засуджений до дові-

чного ув'язнення, а Бойс у вересні 1977 року – до сорока років ув'язнення.

У середині 1970-х років радянська розвідка, використовуючи підкуп, завербувала шифрувальника японського МЗС. Крім передачі секретних послань МЗС Японії, що проходили через його руки, він поставляв інформацію, що дозволяла радянським криптоаналітикам швидко помічати та розгадувати зміни в японських дипломатичних шифросистемах.

На початку 1980-х років радянською розвідкою за допомогою розвідуправління МДБ НДР був завербований сержант армії США Джеймс Холл. У 1982 році він проходив службу в західному Берліні, вийшов на зв'язок з КДБ і запропонував свої послуги – інформацію з бази радіошпигунства в Тойфельсберзі, де мав доступ до надсекретної інформації. За 4 роки служби в Тойфельсберзі Холл передав КДБ сотні надсекретних документів, зокрема інформацію за проектом «Троян» – світовою мережею електронного спостереження. Крім того, в результаті діяльності Холлу була виведена з ладу комп'ютерна програма, яка мала на меті визначення слабких місць у системі радянських військових комунікацій. У 1989 році Холл був засуджений до 40 років перебування у військовій в'язниці.

У 1980-х роках ГРУ була завербована співробітниця шифрувального центру прем'єр-міністра Канади Макензі Кінга.

Наприкінці 1970-х років шифрувальник посольства США в Боготі Джеффрі Барнет продав співробітнику радянської розвідки за 100 тисяч доларів копії відкритих текстів шифротелеграм резидента ЦРУ в Колумбії. Порівняння копій з відповідними зашифрованими варіантами дозволило криптоаналітикам зробити такий «пролом» у системі забезпечення безпеки зв'язку американського посольства, що залатати його можна було тільки за допомогою повної заміни посольських шифромашин. Видав Барнета у червні 1979 року завербований резидентурою ЦРУ в Джакарті підполковник КДБ Володимир Пігузов.

15 січня 1980 року сам запропонував свої послуги резидентурі КДБ у Вашингтоні Рональд Вільям Пелтон, що працював в АНБ із 1964 по 1979 рік. Майже шість років до його арешту (у листопаді 1985 року) Пелтон подавав докладну інформацію про діяльність і елементи системи безпеки АНБ у сімдесяті роки. Пелтон склав документ на 60 сторінках, названий ним як «Папка параметрів зв'язку», де були розглянуті засоби зв'язку, що вважалися АНБ найбільш важливими, процедура їхнього аналізу та результати.

Розвідка організовувала зустрічі з Пелтоном фахівців з 8-го Головного Управління КДБ, що тижнями записували повідомлення агента. Він повідомляв їм детальну інформацію про наявні в АНБ системи перехоплення та дешифрування й інші всілякі подробиці американської електронної розвідки. Саме він розкрив діючу операцію під кодовою назвою «Дзвіночки плюща» (Ivybells), у ході якої американці здійснювали знімання інформації з радянських підводних кабелів, що

були прокладені дном Охотського та Баренцева морів.

Після свого звільнення з АНБ в 1980 році і до 1984 року його постачав надсекретною інформацією його друг – математик з Управління безпеки зв'язку АНБ. У 1985 році Р.Пелтон був арештований та засуджений до трьох довічних термінів ув'язнення та ще десяти років. В історії американського судочинства це був найбільш тривалий термін за шпигунство.

У деяких випадках співробітникам КДБ удавалося проникати безпосередньо на територію іноземних представництв. Найважливішою з таких операцій було таємне відвідування посольства Японії, де клерк шифрувального відділу повідомив про кодові ключі до сейфів посольства та японські дипломатичні шифри. З усіх шифрів основних держав радянським дешифрувальникам найчастіше вдавалися розкодувати японські шифри, причому починаючи ще з двадцятих років.

На початку 1960-х років радянська розвідка провела операцію «Карфаген», метою якої було агентурне проникнення в диспетчерський центр зв'язку американського військового відомства у Франції. В ході цієї операції вдалося отримати відомості про шифри, що використовувались армією США і військами НАТО. У операції брав участь, вже згадуваний нами сержант армії США Роберт Лі Джонсон, який і визначив успіх всієї операції. Працюючи в зовнішній службі охорони, Джонсон забезпечив проникнення в секретний сейф центру зв'язку.

Після операції «Карфаген» була здійснена нова операція радянської розвідки – «Олімп». Об'єктом операції були посольства і представництва іноземних держав в Австрії. В ході операції був завербований співробітник австрійської державної поліції, що мав доступ до секретних документів. До проведення операції був залучений раніше завербований фахівець у сфері електронного захисту іноземних посольств. Він, у свою чергу, завербував шифрувальника одного з іноземних посольств у Відні. В результаті операції були отримані шифри цього посольства, що дозволило радянському керівництву зробити правильні висновки про політику країни на міжнародній арені.

У середині 1960-х років радянська розвідка провела операцію таємного проникнення в будівлю посольства США. Операція зайняла достатньо багато часу. В останню мить, після розкриття сейфа шифрувальника, виникла несподівана проблема. Шифроблокноти були забезпечені спеціальним захистом: кожен по краях був обшитий українською вишиванкою. Малюнок вишиванки був складений з переплетених ниток п'яти квітів. Довелося перервати операцію та створити аналогічну вишиванку. Потім операція знову була відновлена, в результаті чого вдалося перлюструвати декілька шифроблокнотів, не залишивши доказів.

У 1960-х роках співробітники КДБ при сприянні болгарських колег проникнули в посольство Італії в Софії та зняли копії із шифроблокнотів «Калабрія» і «Сардинія», за допомогою яких обслуговувався інформаційний відділ НАТО. А трохи

пізніше у французькому посольстві в Болгарії представниками КДБ були скопійовані кодові книги резидентур спецслужб Франції.

У 1970-х роках співробітникам КДБ удалося завербувати клерка в шифрувальному відділі японського МЗС, що виявив таку ж готовність до співробітництва, як і його колега з московського посольства двадцять років тому. У такий же спосіб КДБ удалося одержати доступ до сейфів і шифрів шведського посольства: одна з «ластівок» спокусила нічного чергового, а увагу собаки відвернули величезними шматками м'яса. На початку 1950-х років таким же чином удалося проникнути в посольства Туреччини, Єгипту, Сирії, Ірану й інших країн Близького Сходу.

Розповідаючи про агентурне проникнення до іноземних посольств з метою здобуття шифрів, треба відмітити, що в другій половині минулого сторіччя спецслужби стали також використовувати електронну апаратуру для перехоплення сигналів ПЕМВН під час роботи шифрувальних машин з метою прочитання зашифрованих та дешифрованих ними повідомлень. Тобто таке підслуховування вело до кінцевого результату щодо розкриття шифру.

Радянською розвідкою такий електронний пристрій був таємно прикріплений до шифромашини західнонімецького посольства в Москві. Ще до того, як текст повідомлення був зашифрований машиною, друкований його текст від впровадженого електронного пристрою надходив на прийомний пристрій поза будинком посольства. Таким чином, готове повідомлення для Бонна або розшифровані вказівки з Бонна з'являлися на столі радянських керівників. А оскільки копії всіх шифроповідомлень посольства по радіо, телеграфу та телексу автоматично надходили в розпорядження радянських криптослужб, залишалося тільки накласти уже відомі відкриті тексти телеграм на зашифровані, і таким чином отримати ключ до шифромашини. У вересні 1964 року цей пристрій був знайдений німецьким фахівцем Хорстом Шваркманом.

Інший приклад використання методу перехоплення випромінювань шифромашини відноситься до періоду середини 1970-х років, коли японське посольство в Москві проводило заміну своїх шифромашин. Знаючи про це, фахівці КДБ уважно стежили за тим, як нові машини будуть транспортуватися, тому що через їхню громіздкість посилати машини диппоштою було неможливим. За лічені години КДБ стало відомо, що опечатаний дипломатичними печатками вантажний автомобіль доставить шифромашини з Фінляндії через Виборг поблизу від Ленінграда та проїде без зупинки до Москви, тобто проїде відстань у 600 кілометрів. Оскільки ні водій вантажівки, ні супроводжуючі вантаж японські дипломати не стежили за тим, що відбувалося позаду них, то фахівці служби № 1 КДБ розкрили печатки на вантажівці, проникли до шифромашин і встановили на них електронні пристрої. Після цього можна було слухати все шифроване листування японців, принаймні, впродовж десяти років.

У 1976 році та на початку 1977 року для французького посольства в Москві залізницею були направлені шість апаратів телекса без усякого супроводу. Саме в цей період спецслужби КДБ змогли розкрити опечатані шухляди та підмінити конденсатори телексів іншими, спеціально обладнаними електронними пристроями, які передавали шифровану інформацію з посольства. Від кожного пристрою відходило два тонких проводки, які безпосередньо з'єднувалися через силовий кабель телекса з зовнішньою електричною мережею. По цій мережі сигнали працюючого телекса перехоплювалися КДБ, у результаті чого його служба дешифрування могла одержувати відкриті тексти переданих телексами повідомлень ще до їхнього зашифрування. У січні 1983 року, після того як встановлений у бюро французького посольства в Москві ще в 1976 році телекс зажадав ремонту, електронні пристрої у корпусах його конденсаторів були виявлені.

У 1984 році майстри з 16-го Управління КДБ вмонтували «закладки» у 30 нових друкарських машинок, призначених для посольства США в Москві та американського генконсульства в Ленінграді.

У 2010 році за інформацією співробітника розвідувальних служб США стало відомо, що АНБ в обстановці глибокої секретності знову шукає серед своїх співробітників агента, що працює на російську розвідку. Пошук ведеться в штаб-квартирі організації у Форт-Міді (штат Меріленд), до внутрішнього розслідування у цій справі вже підключилося ФБР. За словами джерела, в АНБ вважають, що російська Служба зовнішньої розвідки (СЗР) використовувала російських нелегалів для зв'язку з одним або декількома агентами в цьому відомстві. Шпигунську мережу, за деякими даними, здав колишній співробітник СЗР полковник Олександр Потєєв, який втік у США. Так що «холодна» війна продовжується...

4.8. «Втрати» російської криптології

У січні 1664 року шведський представник у Москві в повідомленні своєму королю писав про те, що в нього з'явився таємний і цінний інформатор. Цим інформатором був Г.К.Котошихін, службовець Наказу таємних справ (Посольського наказу), що займався, у тому числі, і питаннями криптозахисту дипломатичних повідомлень. Котошихін одержував скромне грошове забезпечення, але досить сумлінно виконував свої службові обов'язки. Однак за невелику помилку в царському документі (неточне іменування царських регалій) за найвищим указом був «біт кийками».

Образа на царя і недостатнє матеріальне забезпечення підштовхнули Котошихіна на бік шведів – тодішніх супротивників Росії, які щедро оплачували його інформацію. Однак незабаром він був змушений «бігти» у Швецію, де прожив однак недовго. У 1667 році Котошихін був страчений за вироком місцевого суду за навмисне убивство шведського підданого.

19 серпня 1888 року з Російської місії у Пекіні були викрадені примірники росій-

ських ключів: біграмного № 356 і словарного № 336, а останнього ще й у 1891 році – у Вашингтоні. Цікаво, що у 1898 році один з примірників ключа № 356 був втрачений начальником Адріатичної ескадри.

Напередодні російсько-японської війни 1904-1905 років у Порт-Артурі разом з планами фортеці були викрадені шифри, що використовувалися російським військовим командуванням. Крадіжка була здійснена під керівництвом відомого Сіднея Рейлі, що знаходився у Кореї з розвідувальними дорученнями. Після крадіжки Рейлі спішно відправився до Японії, де продав здобуті документи за великі гроші японцям.

У грудні 1910 року був викритий німецький шпигун Юліус Рейхак, який прослужив у російському посольстві у Швейцарії більше 20 років на посаді старшого канцелярського службовця та мав доступ до усіх приміщень посольства й ключі від усіх сейфів. Крім того, він сам упаковував і возив на вокзал усю дипломатичну пошту посольства, тим самим значно полегшуючи роботу німецької розвідки з перлюстрації російської дипломатичної пошти.

У 1919 році в літаку, що летів з Німеччини до Радянського Союзу та зробив аварійну посадку в Латвії, місцеві прикордонники знайшли три шифровані повідомлення. Не зумівши їх дешифрувати, уряд Латвії передав ці повідомлення в розпорядження американського консула в Ризі, що у свою чергу переправив їх до США. Там вони були досить швидко прочитані. Виявилося, що повідомлення послали в Москву німецькі комуністи, які застосували для засекречування шифр вертикальної перестановки, а у якості ключа використовували рядки з вірша німецького поета Генріха Гейне «Лорелея». У шифровках було прохання надіслати побільше грошей, обговорювався провал з'їзду комуністів у Голландії та говорилося про арешт відомої німецької комуністки Клари Цеткін.

У 1925 році зникли шифродокументи з радянського посольства в Шанхаю. Російський білогвардієць, який був запідозрений у крадіжці, при нез'ясованих обставинах зник з корабля, на якому повинен був відплисти з Шанхая.

У травні 1927 року в Англії зник шифрувальник радянської розвідки Міллер. Після цього частина радянського розшифрованого дипломатичного листування була опублікована, а відносини з Радянською Росією розірвані. Радянський Союз був вимушений витратити великі засоби, щоб змінити всю систему безпеки радянських представництв в Англії.

У 1935 році радянський службовець викрав шифри з посольства СРСР у Празі, і хоча вони згодом були чемно повернуті чеською поліцією їх законним власникам, ніщо не могло похитнути впевненості працівників посольства в компрометації цих шифрів.

У жовтні 1937 року відмовився повернутися до Радянського Союзу директор Лондонського відділу «Інтурист» Арон Шейнман, що був наркомом зовнішньої й

внутрішньої торгівлі СРСР, головою правління Держбанку та замнаркома фінансів СРСР. Шейнман добре знав всі «прикриття» радянських розвідників у системі зовнішньої торгівлі та мав прямий доступ до шифролистування.

У тому ж році був викрадений код, що застосовувався для засекречування листування між Москвою та Міністерством національної оборони іспанських республіканців, що одержували допомогу з СРСР у боротьбі проти режиму Франко.

29 травня 1938 року з території Монголії, скориставшись автомобілем, утік до японців працівник штабу 36-ї мотострілкової дивізії майор Фронтямар Францевич, який користувався військовим комплексом шифролистування.

12 червня 1938 року начальник Управління НКВС по Далекосхідному краю Генріх Люшков, що відповідав за ведення контррозвідувальної роботи в армії, дислокованої на Далекому Сході, перейшов державний кордон і здався японській окупаційній владі Маньчжурії. Він, крім усього іншого, передав японцям відомості про організацію шифрувального зв'язку. Правда, збиток, заподіяний СРСР утечею Люшкова, не був занадто великим, оскільки радянські агенти за рубежем вчасно інформували Москву про ті дані, що стали надбанням японців. Пізніше Люшков став громадянином Японії під ім'ям Ямогучи Тосікадзу. Коли радянські війська в 1945 році вступили в Маньчжурію, його ліквідували японці як небажане джерело інформації про методи японської розвідки.

12 липня 1938 року, побоюючись арешту, втік у США резидент Іноземного відділу НКВС в Іспанії Олександр Орлов (Лейба Фельбінг). Він знав дуже багато чого про організацію шифророботи радянської розвідки. Орлов після втечі під ім'ям Берга мешкав у США, де й помер у 1974 році.

У жовтні 1938 року ще один працівник у Франції, Швейцарії та Іспанії нелегал Іноземного відділу Матвій Штейнберг відмовився виконати наказ про повернення до Москви через побоювання арешту та залишився на Заході.

У тому же році двоє російських емігрантів Володимир і Марія Азарови таємно вивезли з СРСР, як потім було зазначено в матеріалах судового висновку, «секретну кодову книгу, що містила діючий у Радянському Союзі код, передбачений для ведення листування». Їхні речі, у тому числі й кодова книга, спочатку були доставлені на борт вантажного судна, а потім вивантажені у Ризі, у результаті чого виявилися безповоротно загубленими. Азарови в судовому порядку пред'явили пароплавній компанії позов на 511 900 доларів США: 11 900 доларів – за загублене особисте майно, а інші півмільйона – за код, що згідно з заявою Володимира Азарова на суді, «точно відповідало ринковій вартості кодової книги на момент її пропажі». Справа була улагоджена поза судом. Тому ніхто так і не довідався, яка сума була виплачена Азаровим як відшкодування вартості кодової книги.

У червні 1941 року фашистами був захоплений в полон радянський льотчик,

який видав їм одну з шифросистем, що використовувалися в листуванні радянських ВПС. В результаті отримана з дешифрованих повідомлень інформація допомогла фашистським ВПС знищити сотні радянських літаків на землі й у повітрі в ході великого бою в небі над Мінським.

Згідно з документами третього рейху, які зберігаються у Національному державному архіві США у Вашингтоні, німецькій розвідці вдалося сфотографувати загальновійськовий командирський код № 5 «ОКК-5» 1938р., перекладну таблицю чергового радиста «ПТ-38А» лінії зв'язку РСЧА 1938р., правила користування кодом «Четвертий», оперативно-тактичний код «Третій» (набірно-розбірна книга), постовий код «СН» і «С» Північного флоту 1940р., ключову таблицю № 14 1940р., Інструкцію органам НКВС з ведення шифрроботи від 07.10.1942р., Інструкцію з організації зв'язку в авіаз'єднаннях і авіачастинах (на 50 сторінках) 1943р. і кодову таблицю «ВС-22» 1948р.

У листопаді 1944 року Управління стратегічних служб (далі – УСС) – попередник ЦРУ США здобуло 1500 сторінок шифрувальних зошитів радянської держбезпеки, захоплених фінами. Самі по собі зошити великого значення для західних криптологів не мали. Шифрувальник резидентури держбезпеки при зашифруванні послань спочатку кожне слово або, навіть, букву записував у вигляді 5-значного числа з шифрувального зошита. Але потім він додавав у кожну групу ще 5 знаків із серії випадково відібраних цифр, зазначених у «разовому зошиті», другий примірник якого був тільки у Московському центрі. Якщо використовувати «разовий зошит» лише один раз, як того і вимагали інструкції Центра, шифр «розколоти» було практично неможливо. Але в останній рік війни кількість інформації, переданої резидентурами зі США та Англії, була настільки великою, що Центр іноді направляв «разові зошити» вдруге. Наприкінці війни було ще два випадки порушення звичайно дуже суворого шифрувального режиму. У 1944 році ФБР перехопило незашифровані тексти декількох повідомлень резидентури з Нью-Йорка до Москви.

Хоча оригінал з настійної вимоги президента Рузвельта повернули до Москви, УСС зберігло копію. Підгоріла книга була передана особисто радянському послу у Вашингтоні Громико, і більше ніхто в радянському посольстві про її існування не знав. У травні 1945 року НКДБ замінило шифри, а копія старого зошита, що УСС залишило собі, віддаючи оригінал, використовувалася до 1948 року для розшифрування деяких повідомлень НКДБ в останній рік війни, завдяки чому вдалося згодом розкрити радянських агентів часів війни. Якби отримання зошита удалося сховати від росіян у 1944 році, її цінність для американського перехоплення була б значно вище.

У вересні 1945 року здався канадській владі шифрувальник радянського посольства в Оттаві Ігор Гузенко, який після своєї втечі розповів про принципи шифрування, що застосовувалися НКДБ і ГРУ. Крім того, він розповів про радянське шпигунство так багато, що канадський уряд заснував спеціальну Королівську ко-

місію з питань шпигунства. Комісія виявила імена 14 осіб, що входили в агентурну мережу радянської розвідки.

Дуже чутливий удар радянська шифрувальна служба одержала в жовтні 1948 року. Американські криптоаналітики під керівництвом Мередіта Гарднера змогли прочитати радіограми НКДБ, які були перехоплені американською контррозвідкою протягом 1944-1945 років та зберігалися у надтаємному досьє «Венона» (Venona). У цьому досьє було зібрано більше 2000 документів радянського посольства та резидентур радянської розвідки у США.

Протягом 1948 року йому удалося розгадати деякі фрагменти шифровок НКДБ до Центра та з Центра, переданих в останній рік війни. В наступні роки було цілком або частково дешифроване кілька тисяч шифровок НКДБ. Таємницю «Венони» та методи Гарднера з її дешифрування видав росіянам у 1948 році американський шифрувальник Вільям Вейсбанд, завербований МДБ за два роки до цього.

Частково проблему вирішив і радянський розвідник Гарольд Андріан Рассел «Кім» Філбі, який з 1940 року служив у британській розвідці «*SIS*», у 1944 році став заступником начальника її контррозвідки, а з 1949 по 1951 роки очолював місію зв'язку «SIS» у Вашингтоні. Аж до свого від'їзду у червні 1951 року Філбі завдяки своєму доступу до матеріалів «Венони» завжди встигав попередити Центр про те, що навколо когось з агентів стискується «петля».

У 1954 році залишився в Австралії дипломат, співробітник КДБ СРСР Петров Володимир Михайлович. На початку своєї служби в КДБ він був шифрувальником, потім працював у радянських посольствах в Швеції і Австралії. Після розстрілу Берії в 1953 році Петров боявся, що його запідозрять у причетності до змов Берії. Це і спонукало його до втечі. З собою Петров захопив ряд документів, що стосуються радянської розвідувальної діяльності в Австралії, які розглядалися парламентською комісією, але не були розсекречені австралійцями. Також він передав західним спецслужбам відомі йому шифри СРСР.

У 1957 році Рейно Хейханен, помічник радянського розвідника Рудольфа Абеля, відправлений ним на «заслужений відпочинок» до СРСР, з'явився у американському посольстві в Парижі. Хейханен передав до ФБР шифросистему «VIC», якою він користувався у листуванні з Москвою, та ключі до неї. Шифр, до речі, був настільки стійким, що ні АНБ, ні ШКУЗ не могли прочитати зашифровані ним повідомлення, які перехоплювалися ФБР з 1953 року.

У травні 1963 року в Москві відбувся суд над полковником ГРУ ГШ ЗС СРСР Пеньковським Олегом Володимировичем. Він був засуджений до розстрілу за зраду Батьківщини. Проте зрадник встиг передати ЦРУ США важливі відомості не тільки про ЗС СРСР, а також про діяльність радянських криптослужб. Суд встановив, що з квітня 1961 по осінь 1962 року полковник Пеньковський передав ЦРУ 110 касет фотоплівки – більше 5 тисяч знімків документації і більше 7

тисяч сторінок секретних матеріалів.

У 1972 році під час американо-радянських переговорів щодо скорочення озброєнь, за ствердженням західних джерел, через помилки радянського шифрувальника АНБ змогло читати все листування між радянською делегацією у Вашингтоні та Москвою.

У середині 1970-х років КДБ СРСР викрив польську розвідку у перехопленні побічних електромагнітних випромінювань і наведень (далі – ПЕМВН) силових ліній військового об'єкта у Москві. Проведені КДБ дослідження щодо методів перехоплення радіовипромінювань з використанням рентгенівського та радіоізотопного випромінювань, підтвердили уразливість шифрувальних машин. З метою запобігання витоку інформації за рахунок ПЕМВН їх не помістили в сталеві кожухи з генераторами шуму та автономними двигунами-генераторами.

У 1976 році став перебіжчиком шифрувальник і радист радянського посольства у Республіці Нігер (Африка) старший лейтенант Анатолій Дмитрович Семенов.

У жовтні 1979 року ініціативно встановив контакт з американською розвідкою під час відрядження у Польщу співробітник відділу захисту шифрованого зв'язку 8-го Головного Управління КДБ майор Віктор Шеймов, який відповідав за безпеку всіх закордонних шифрувальних служб зовнішніх установ СРСР, а також знав все про апаратуру захисту ліній комунікацій шифрованого зв'язку. У Москві Шеймов мав кілька зустрічей зі співробітниками резидентури ЦРУ, яким передавав інформацію про свою роботу. Побоюючись викриття, Шеймов із дружиною Ольгою та малолітньою дочкою Оленою за допомогою західних спецслужб у 1980 році зумів виїхати зі СРСР до США. КДБ шукав його п'ять років, вважаючи, що Шеймов пропав безвісти. Лише у 1985 році стало відомо, що він втік на «захід». Усі ці п'ять років системи шифрування в КДБ не змінювалися, і про них знали в ЦРУ.

Використовуючи інформацію, отриману від Шеймова, армійський підрозділ електронної розвідки США в Західній Німеччині, відомий за назвою «Група швидкого реагування», здійснив у квітні 1981 року операцію щодо закладки підслуховуючих пристроїв в автомашини, що належали радянському військовому аташе в Західній Німеччині. При цьому в шасі замовлених на заводі фірми «Опель» (Opel) у Руссельсхаймі 12 автомобілів установили апаратуру, яку можна було виявити тільки зруйнувавши машини. У результаті американці розкрили кілька радянських агентів і розшифрували ряд кодів радянської військової розвідки.

Цікаво, що Віктор Шеймов після втечі і роботи на АНБ, у 1991 році почав судитися з ЦРУ, заявляючи, що йому не виплатили обіцяного мільйона доларів за надану інформацію. Замість цього йому була призначена виплата у 27 тисяч доларів у рік. Оскільки права перебіжчиків прописані в американському законодавстві, суд став на захист Віктора Шеймова. Це привело до того, що в 1999 році ЦРУ улагодило з ним фінансові питання «полюбовно».

У травні 1985 року співробітник 16-го Управління КДБ лейтенант Віктор Макаров ініціативно запропонував свої послуги британській розвідці «*MI-6*» і передав інформацію про дешифрування канадських, грецьких і німецьких повідомлень, що містили відомості про НАТО і Європейський союз. Засуджений у 1987 році на 10 років таборів, він був звільнений за амністією через 5 років, і «*MI-6*» переправила його до Англії, де обіцяла «гарне» життя. Однак цікавим виявилося те, що він подав позов до суду на керівництво «*MI-6*» з причини недостатньої для «гарного» життя пенсії, яка була йому встановлена.

4.9. Історія радіорозвідки

Вперше у світі радіорозвідка та радіоелектронна боротьба була застосована у період російсько-японської війни 1904-1905 років. Пріоритет у використанні цих нових видів бойових дій належав російським ВМС. Майже відразу після винаходу радіо Морське міністерство Російської імперії розпочало роботу з його використання для добування інформації про ВМС ймовірних супротивників, з'ясування характеру їхньої бойової діяльності у відкритому морі, що агентурними методами було зробити неможливо.

Перші радіостанції надійшли на озброєння російського флоту у травні 1900 року. Крім власне забезпечення зв'язку виявилися й інші напрямки використання радіостанцій: радіорозвідка, перехоплення та наступне дешифрування радіограм іноземних флотів і баз, створення в ефірі радіоперешкод з метою придушення діяльності радіостанцій супротивника на випадок початку воєнних дій.

Початок активної діяльності на цих напрямках, також як і радіофікація флоту, був покладений адміралом Макаровим. Після його призначення на посаду були здійснені енергійні кроки щодо ведення радіорозвідки: до березня 1904 року було організоване постійне несення вахт радіорозвідки, а 7 березня був виданий наказ № 27, що з'явився законодавчою базою подальшого розвитку радіорозвідки і радіомаскування ВМС. Приведемо витяг з цього наказу:

«Приймальна частина телеграфу повинна бути увесь час замкнута так, щоб можна було стежити за депешами, і якщо буде виявлятися ворожа депеша, то негайно ж доповісти командиру та визначити, по можливості, закриваючи прийомний дріт, приблизний напрямок на ворога та доповісти про це. При визначенні напрямку можна користуватися, повертаючи своє судно і заслоняючи своїм рангоутом прийомний провід, причому по виразності можна судити про напрямок на ворога. Мінним офіцерам пропонується провести в цьому напрямку всякі корисні досвіди».

Слід зазначити, що цим же наказом уперше у світі був уведений принцип режиму радіомовчання (без дозволу командира корабля або командувача флотилією заборонялося відправляти будь-які радіограми).

На жаль, загибель адмірала 31 березня на броненосці «Петропавловськ», який

підірвався на японській міні, істотно сповільнила втілення цих планів у життя. До речі, при аналізі обставин затоплення «Петропавловська» було з'ясувано, що саме недостатня робота радіорозвідки, яка не змогла виявити факт встановлення японцями мін на зовнішньому рейді Порт-Артура, стала основною причиною трагедії.

Проте ведення радіорозвідки продовжувалося, і її роль при розкритті планів супротивника була досить важливою. Так, на початку квітня 1904 року японське командування прийняло рішення про проведення чергової бойової операції під Порт-Артуром силами 12 кораблів. Уже 9 квітня морський похідний штаб царського намісника на Далекому Сході адмірала Алексєєва сповістив штаб фортеці: *«Сьогодні ранком на ескадрі були розібрані (дешифровані – авт.) японські телеграми по бездротовому телеграфу, з яких можна припустити, що намічається нова атака...».*

Російське командування відразу ж підсилило пильність. 15 квітня японці, закінчивши необхідні приготування, провели в акваторії порту-фортеці рекогносцировку з метою ознайомити капітанів кораблів з районом майбутніх дій. У цю же ніч радіотелеграфісти броненосця «Полтава» перехопили і дешифрували телеграму супротивника, що підтвердила його плани, і операція, що відбулася в ніч на 20 квітня, закінчилася для японців невдачею.

Під час Першої світової війни справа перехоплення та розшифровування ворожих радіограм була продовжена. Наприкінці 1915 року на Північному фронті перехоплювалися ворожі шифровані радіограми, що відправлялися потім у Петроград (нині – Санкт-Петербург) до спеціального бюро Головного управління Генерального штабу. Однак практичних результатів робота цього бюро не дала.

Незрівнянно краще була поставлена справа радіорозвідки на російському флоті. Розшифрування німецьких морських радіограм розпочалося з часу отримання нашими водолазами таємних документів, у тому числі і радіотелеграфних шифрів, із загиблого восени 1914 року поблизу Оденхольмського маяка у Балтійському морі німецького крейсера «Магдебург». У тому же році на прохання Адміралтейства Великобританії були відряджені для зв'язку з ними капітан І-го рангу Кедров і капітан ІІ-го рангу Смірнов, тому що у британців на той час була думка проникнути частиною свого флоту до Балтійського моря.

Цим офіцерам було доручено передати британцям цей морський шифр, який вони особисто вручили Першому лорду Адміралтейства (морському міністру) Вінстону Черчиллю у присутності Першого морського лорда (начальника Морського Генерального штабу) принца Людвіга Баттенбергського та начальника штабу контр-адмірала Олівера.

З цього часу розшифрування німецьких морських радіограм була організована належним чином, причому росіяне працювали у повному зв'язку з британцями. Для цього і у Балтійському морі, і у Севастополі були побудовані спеціальні станції радіоперехоплення. Варто помітити, що турецький флот користувався тим

же німецьким шифром. За словами старшого лейтенанта Стеблін-Каменського, декілька разів німці й турки змінювали свій шифр, не змінюючи його системи, і всякий раз його розкривали.

Найінтенсивніше і успішно робота з радіоперехоплення та розшифрування німецьких морських радіограм розвернулася у моряків на Балтіці. Так, на узбережжі Балтійського моря вже у серпні 1914 року було виділено: у південному районі – 3 радіоприймачі (Гапсаль, Кильконд, Даггерорт), у північному районі – 3 в Гельсингфорсі і 1 в Гангу, у західному районі – також 3 радіоприймачі (Абор, Престе, Уте).

Пеленгаторні станції (компасного типу – 32 промені) були встановлені у Гангу, на о.Реншер, о.Езель і у Гапсалі.

У перший період систематизації і обробки матеріалів перехоплення безпосередньо на станціях організовано не було. Всі шифровки передавалися на районні центральні станції, де, як правило, матеріал залежувався через відсутність або брак криптологів або просто не оброблявся.

Цінність окремих розшифрованих телеграм незабаром показала, що необхідно створити спеціальний інформаційний центр і станції особливого призначення – дешифрувальний центр. Морським Генеральним штабом були затверджені штати таких станцій. До штату кожної станції входили 73 особи, з них: начальник станції – капітан 1-го рангу, чергові офіцери і дешифрувальники – 10-12 осіб на чолі з начальником дешифрувальної групи – дійсним статським радником.

До серпня 1915 року у Штітгамні було закінчене будівництво станції особливого призначення, працівники якої одразу приступили до ретельної обробки німецьких шифрованих телеграм. Німці у війну застосовували морський трибуквений код з перешифруванням. Російські дешифрувальники достатньо швидко «розкривали» нові ключі та читали німецькі повідомлення і накази.

Завдяки роботі невеликої групи експертів (начальник станції капітан 1-го рангу Петров, лейтенанти Барльовен і Ізмалков, мічмани Марков і Тімофеєвський, надвірний радник Павлович, статські радники Орлов і Проффен) військове командування майже завжди було обізнане про діяльність німецьких кораблів. Мінні поля і банки, про які німці повідомляли всі свої кораблі після їх встановлення, також ставали відомі росіянам.

Не менш вражаючими були результати розшифрування німецьких радіограм Чорноморським флотом. Так, одна з розшифрованих ворожих радіограм сповіщала вночі, що на зорі, тобто через кілька годин, дві турецькі моторні канонерки, йдучи з Бургаса в Константинополь, підійдуть до європейського мису Карабурну. О 8-й годині ранку російський крейсер «Пам'ять Меркурія» повідомив: «Потопив двох турецьких канонерок».

Оскільки турки продовжували робити всі оперативні розпорядження по радіотелеграфу, то цим же шляхом росіяне довідалися про загибель на їхніх мінах ні-

мецьких човнів у Босфорі та Варні. Так, у вересні 1916 року турки протралили прохід уздовж азіатського узбережжя для великого транспорту, що повинний був пливти з вантажем вугілля, якому про цей шлях і було повідомлено по радіо. Негайно ж російські міноносці закидали мінами протралений канал, а пізніше з перехопленої ворожої радіограми стало відомо, що транспорт цей затонув на російській міні.

У грудні 1916 року штаб Чорноморського флоту одержав інформацію, що при відступі нашої армії з Констанци лівий її фланг обстрілювався німецькою канонеркою. У той же день росіянами був розшифрований наказ цьому човну повернутися в Константинополь, використавши для цього тільки що протралений канал. Негайно ж із Севастополя вийшли міноносці для встановлення мін у протраленому каналі, а через 48 годин з розшифрованої радіограми стало відомо, що цей німецький човен затонув на поставлених мінах.

Офіційна історія радянської радіорозвідки розпочалася з 13 листопада 1918 року, коли було створено перший військовий підрозділ радіорозвідки – приймально-контрольна радіостанція в Серпухові. Вона підпорядковувалась Реєстраційному (розвідувальному) управлінню Польового Штабу Революційної Військової Ради Республіки. Незабаром були сформовані такі ж станції для фронтів, і до 1920 року на фронтах Громадянської війни вели радіорозвідку 8 пеленгаторних, 17 приймально-інформаційних і більше 50 зв'язкових радіостанцій.

На початку 1920 року на Чорноморському флоті було прийняте рішення про формування служби радіоспостереження та зв'язку у складі Одеського, Очаковського, Херсонського та Маріупольського районів, начальником якої був призначений С.Касаткин. Головне Управління служби спостереження та зв'язку спочатку мало у своєму складі оперативний відділ з чотирма шифрувальниками та двома перекладачами. Наявність перекладачів говорить про те, що вони займалися перехопленням іноземного радіообміну.

5 травня 1921 року була утворена єдина радянська криптослужба у вигляді Спеціального відділу при ВНК, офіційними завданнями якої були також масштабна радіо- і радіотехнічна розвідка, дешифрування телеграм, розробка шифрів, радіоперехоплення, пеленгація й виявлення ворожих шпигунських передавачів на радянській території.

Перша пеленгаторна мережа розміщалась на дахах багатьох державних установ, і в такий спосіб здійснювалося спостереження за радіоефіром. У сфері уваги Спецвідділу знаходилися не тільки автономні неофіційні передавачі, але й передавальні пристрої посольств та іноземних місій. У них встановлювалася підслуховуюча апаратура та відслідковувалися телефонні розмови.

По лінії командування Червоної Армії у травні 1921 року в кожному штабі фронту та військового округу було виділено по одній з приймальних радіостанцій для перехоплення шифрованих телеграм, що передавались іноземними польови-

ми та стаціонарними раціями. Такі радіостанції з того часу почали називати радіостанціями особливого призначення (рос. скор. *ОСНАЗ*).

Спочатку в штабах Московського і Тверського військових округів, а потім у ряді прикордонних міст були утворені підрозділи «*ОСНАЗ*», які були оснащені могутніми приймальними станціями та займалися перехопленням радіопереговорів супротивників. Одночасно у ряді прикордонних міст країни були розгорнуті приймально-інформаційні радіостанції.

Співробітники радіостанцій «*ОСНАЗ*» перехоплювали телеграми закордонних радіостанцій, забезпечуючи розвідувальні та контррозвідувальні органи цінною інформацією. Всі матеріали з перехоплення негайно прямували до Москви - безпосередньо до Спецвідділу, який очолював і направляв всю цю роботу.

У 1922 році крім тих, що вже існували у Москві, Твері і деяких прикордонних містах, з'явилася радіостанція безпосередньо при Спецвідділі. Вона складалася з 4-х найбільш сучасних для того періоду приймачів, а обслуговувало її 20 осіб. Разом з мережею армійських радіостанцій «*ОСНАЗ*» вона забезпечувала Спецвідділ даними радіоперехоплення. У оперативному відношенні всі радіостанції підпорядковувалися Спецвідділу та відповідним губернським відділам ДПУ за місцем їх дислокації.

Для роботи на станціях «*ОСНАЗ*» відбиралися найбільш перевірені та добросовісні радіотелеграфісти, в основному, з комуністів і комсомольців. У Спецвідділі затверджувалося призначення кожної кандидатури. Головна увага радіостанцій «*ОСНАЗ*» була сконцентрована на перехопленні шифротелеграм від радіостанцій основних капіталістичних держав. Вже в перші роки своєї діяльності радіостанції «*ОСНАЗ*» перехопили багато цінних радіограм з відомостями про наміри та дії ворогів Радянської республіки.

Так, з березня 1924 року почалося прослуховування переговорів польського генерального штабу з армійськими і корпусними штабами. Це дозволило органам держбезпеки отримати дані про окремі антирадянські задуми польської розвідки. Так, з перехопленої 6 вересня того ж року радіограми стало відомо, що Англія, Франція і Америка поставляли зброю меншовикам Грузії для боротьби з Радянською владою.

Проте до створення власної радіолабораторії, в цей період діяльності органів безпеки справа не дійшла. Апаратуру купували за кордоном. Дослідні роботи з питань технічного забезпечення підслуховування телефонних розмов розпочав проводити з 1926 року Науково-випробувальний інститут зв'язку (далі – НВІЗ) РСЧА. А у 1929 році в структурі НВІЗ були утворені такі спецлабораторії:

- секретного телеграфування відділу радіопередавачів,
- пеленгаторна відділу радіоприймачів,
- телефонної апаратури і секретного телефонування телеграфно-телефон-

ного відділу,

- станцій прослуховування телеграфно-телефонного відділу,
- відділу застосування.

Наприкінці 20-х років співробітники Спецвідділу взяли активну участь в організації дешифрувальної роботи в РСЧА. Підсумком цих зусиль стало створення у березні 1931 року об'єднаного підрозділу радіорозвідки: 5-ої частини 4-го (розвідувального) Управління Штабу РСЧА. З червня 1931 року його начальником був призначений Я.Файвуш. У листопаді 1934 року цей підрозділ був реорганізований у 3-й відділ, а у листопаді 1935 року – 6-й відділ Розвідувального управління ЧА.

У січні 1933 року НВІЗ був реорганізований в науково-випробувальний інститут зв'язку і електромеханіки (далі – НВІЗЕМ) у складі 10 відділів, серед яких були відділ спеціального телеграфно-телефонного й радіозв'язку (начальник – І.Г.Кляцкін) та відділ радіорозвідки (начальник – В.М.Никітін).

У січні 1935 року НВІЗЕМ був реорганізований у два інститути: Науково-дослідний інститут зв'язку (далі – НДІЗ) РСЧА з тематики зв'язку і радіорозвідки, підпорядкований Управлінню зв'язку РСЧА і науково-випробувальний технічний інститут (далі – НВТІ) РСЧА з тематики «особливої техніки», підпорядкований Технічному управлінню РСЧА.

Відділ спеціального телеграфно-телефонного й радіозв'язку (начальник – М.І.Болховітін) та відділ радіорозвідки (начальник – С.І.Андреєв) увійшли до складу НДІЗ, де у січні 1936 року був утворений новий відділ радіорозвідувальних засобів (начальник – С.Андреєв).

У 1936 році криптоаналітики Спецвідділу разом з підрозділом перехоплення виїхали в Іспанію, де після прибуття відразу почали роботу в складі Генштабу республіканської армії. Поступово справа налагодилася, і республіканське військове командування разом з радянськими військовими радниками стали одержувати все більше важливої інформації.

Інша особлива оперативна група з числа співробітників Спецвідділу була відряджена до Китаю для надання дешифрувальної допомоги у війні проти Японії. Щомісяця цій групі вдавалося дешифрувати близько 200 японських шифротелеграм, а всього за 1,5 року роботи в Японії нею були розкриті 10 військових шифрів Японії.

В утвореному 30 грудня 1937 року Наркоматі ВМФ в Управлінні розвідки передбачалося 7-е відділення (у подальшому – 11-й відділ), до завдань якого входила організація дешифрувальної роботи у ВМФ і керівництво нею. Криптологічні курси, що були організовані при Академії ГШ РСЧА, у травні 1939 року та лютому 1941 року направили на флот понад 40 фахівців, що стали «ядром» морської ДРС під час війни.

У травні 1938 року НДІЗ і НВТІ були об'єднані в єдиний науково-випробувальний інститут зв'язку і особливої техніки (далі - НВІЗТ) РСЧА, який з 1939 року розпочав роботи щодо «закриття» телефонних розмов по радіо й дротових лініях

зв'язку та дослідження в сфері радіорозвідки для вирішення завдання створення автоматизованої радіопеленгаторної системи й розробки автоматизованого електронно-променевого пеленгатора.

У травні 1939 року підрозділ радіорозвідки РСЧА був реорганізований у 7-й відділ 5-го (розвідувального) управління НКО СРСР, начальником якого був призначений Ф.П.Малишев. 26 липня 1940 року цей відділ наказом НКО № 0038 став 8-м відділом РУ ГШ РСЧА, а його начальником – І.М.Артем'єв. У червні 1939 року до складу 5-го (розвідувального) Управління НКО увійшов також Інститут оперативної техніки під керівництвом В.С.Четверікова.

Досвід, отриманий радіорозвідкою РСЧА в 1930-і роки, підтвердив її важливу роль у забезпеченні розвідувальними даними органів управління військами різних рівнів. Так, у 1938 році частка даних радіорозвідки в загальній кількості всіх розвідувальних даних про воюючі Озброєні Сили Японії склала 30-35%. Радіорозвідка надавала до 75% даних про переміщення військ з Японії до Китаю і Манчжурії, про дислокацію в зоні бойових дій.

За її допомогою були отримані цінні відомості про підготовку фашистської Німеччини до нападу на Радянський Союз. Так, 18 травня 1941 року радіорозвідка Закавказького військового округу перехопила повідомлення англійського резидента з Туреччини до Лондона про те, що за достовірними даними, що є у нього, Німеччина розпочне військові дії проти СРСР 15 червня.

Окрема радіорозвідувальна станція, що працювала на західному напрямі, доповіла про переміщення німецьких поліцейських частин і про приведення в бойову готовність поліцейських батальйонів у містах Пултуськ, Плоцьк і Тільзіт.

18 червня центральна розвідувальна радіостанція перехопила важливу японську радіограму наступного змісту: «З Берліна в Токіо. Начальнику Генерального штабу. Термінова. У Східній Пруссії відмічена концентрація від 120 до 130 німецьких дивізій».

19 червня 1941 року інша розвідувальна радіостанція перехопила радіограму німецької розвідки про те, що напад німецько-фашистських військ на СРСР почнеться 22 червня 1941 року.

Під час Великої Вітчизняної війни відбулося становлення ДРС Наркомату ВМФ як одного з найважливіших елементів розвідки ВМФ. Досить незначна за чисельністю, що не перевищувала 150 осіб, ДРС ВМФ показала дивну результативність і ефективність. Не маючи на озброєнні навіть елементарного устаткування для механізації трудомістких процесів, працюючи в прифронтовій смузі при постійному бойовому впливі супротивника, ДРС ВМФ безупинно видавала достовірні розвідувальні дані найрізноманітнішого змісту, у тому числі й стратегічного значення.

Ранок 22 червня 1941 року виявилося пам'ятним для ветеранів ДРС Чорноморського флоту (далі – ЧФ) зміною всіх контрольованих до цього шифрозасобів супротивника. Але впевненість у своїх силах, цілеспрямованість і професійна май-

стерність допомогли: після безперервного тридобового «штурму» неприступна «цитадель» нових шифрів супротивника була узята – 25 червня розпочалося читання їхніх шифровок.

Найбільш важливим джерелом інформації з'явилися зносини румунського ГШ зі своєю місією зв'язку при фельдмаршалі Манштейні. В результаті читання листування командування ЧФ мало вичерпну інформацію не тільки про поточну бойову обстановку, але й про деякі стратегічні задуми ворога. Ось декілька прикладів отриманої інформації від криптологів ЧФ:

- бойові накази про штурм Одеси, Севастополя, Новоросійська;
- напрямок головного удару, що планувався, у районі Курська у майбутній літній кампанії 1943 року;
- підготовка замаху на глав урядів союзних держав під час майбутньої Тегеранської конференції;
- умови, при яких Туреччина вступить у війну з Радянським Союзом;
- план відведення (або знищення) румунського флоту, розроблений фашистами у зв'язку з наступом радянських військ.

Уже влітку 1942 року Верховний головнокомандуючий Й.Сталін високо оцінив роботу ДРС ЧФ, заявивши: «Якби не було розвідки Чорноморського флоту, я не знав би обстановки на Півдні».

ДРС Балтійського флоту (далі – БФ) за період 1941-1943 років було розкрито 256 шифрів і кодів Німеччини і Фінляндії, завдяки чому прочитано 87 362 криптограми, а це близько 100 повідомлень у день.

Читання листування берегових постів німецької, фінської і шведської служб радіоспостереження дозволяло одержувати найцінніші дані про фарватери, вільні для плавання, про мінну, гідрографічну та метеообстановку на Балтійському морі, про інтенсивність руху судів і системи їхнього захисту, що становило першорядний інтерес для командування флоту при плануванні бойової діяльності підводних човнів і морської авіації.

У цілому, криптологи ДРС БФ працювали цілеспрямовано й ефективно, навіть коли знаходилися в блокадному Ленінграді. Основні зусилля були зосереджені на Німеччині (напрямок очолював капітан-лейтенант Семенов). Накопичувався досвід, з'являлася можливість більш поглибленого аналізу шифрозасобів, дослідження яких раніше не велося через недолік сил і засобів. Однак розпочаті роботи були припинені після закінчення війни, а ДРС БФ була ліквідована.

Бойові завдання, що були поставлені перед ДРС Північного флоту (далі – ПФ), визначалися цілями, переслідуваними ПФ, роль якого у війні на морі виявилася досить своєрідною в порівнянні з іншими флотами – крім активної боротьби на морських комунікаціях супротивника, доводилося здійснювати захист наших зовнішніх морських шляхів з Англією і США у виділеній операційній зоні.

Найбільш нечисленний загін криптологів ДРС ПФ (за усю війну через службу пройшло всього 15 осіб) упорався з усіма завданнями. Головним об'єктом ДРС флоту була авіація супротивника. Усього за роки війни було розкрито 9 кодів і 575 їхніх варіантів та перешифрувальних засобів, прочитане понад 55 000 криптограм, що дозволило цілком контролювати все «закрите» листування ВПС фашистської Німеччини.

За роки війни ДРС Північного флоту аналітичними методами було розкрито 26 шифрів, 13 кодів, що використовувалися силами берегової оборони, аварійно-рятувальною, маяковою і радіонавігаційною службами, та прочитано близько 3 000 криптограм.

Радянська радіорозвідка так само активно працювала за Полярним кругом. Радіоперехоплення вели спеціальні берегові радіостанції, морські судна, у тому числі і цивільні, полярні станції. Отримана інформація ретельно аналізувалася розвідкою ПФ. У результаті цих заходів вдалося установити райони дії німецьких підводних човнів. Маршрути конвоїв стали прокладати в обхід небезпечних ділянок. При неможливості обігнути небезпечна ділянка туди направлялися додаткові протичовневі сили та підсилювалася охорона транспортних судів. Ці заходи дозволили істотно знизити втрати наших судів від дій німецьких підводників, а в деяких випадках і знищити ворога.

Свій внесок у перемогу над Японією зробила і ДРС Тихоокеанського флоту (далі – ТОФ), найстарша з усіх флотських ДРС. Вже у середині 1934 року у Хабаровську функціонувала «військово-морська частина», що здійснювала дешифрувально-розвідувальну роботу. Роль далекосхідних підрозділів ДРС ВМФ звелася, в основному, до добування й узагальнення достовірної інформації, необхідної для підготовки ударів, що визначили нищівний розгром японських збройних сил на. Після перемоги над Японією ДРС ТОФ була розформована.

Після початку війни під військові цілі була реорганізована й робота НВІЗТ, в якому з метою забезпечення перехоплення та аналізу різних систем зв'язку супротивника були утворені 2 науково-дослідні відділи: НДВ-1 і НДВ-2. У складі НДВ-1 розпочала роботу лабораторія з розробки апаратури для розвідників-радистів, що планувалися для роботи за лінією фронту, і радіовузлів розвідки фронтів, а у складі НДВ-2 – лабораторія телефонії, телеграфних систем і фототелеграфії.

16 лютого 1942 року наказом НКО СРСР № 0033 про реорганізацію Розвідувального управління (далі – РУ) Генерального штабу (далі – ГШ) в Головне РУ (далі – ГРУ) ГШ Червоної армії (далі – ЧА) 8-й відділ (радіорозвідки) РУ ГШ ЧА був реорганізований у 8-й відділ 1-го (агентурного) Управління ГРУ ГШ ЧА.

23 жовтня 1942 року наказом НКО СРСР № 00222 про реорганізацію ГРУ ГШ ЧА в ГРУ НКО і Управління військової розвідки (далі – УВР) ГШ ЧА дешифрувальна служба військової розвідки і 8 окремих радіодивізіонів особливого призначення (скорочено російською – «*ОСНАЗ*») були передані до НКВС, де були утворені по-

льові управління спеціальної служби, а дивізіони переформовані в окремі дивізіони спецслужби, центральну й окрему радіостанції військ НКВС.

Більша частина фахівців НДВ-2 НВІЗТ ЧА з тематики радіорозвідки також була переведена до НКВС. А у листопаді 1942 року НВІЗТ був реорганізований у науково-випробувальний інститут зв'язку (далі – НВІЗ) ЧА.

19 квітня 1943 року наказом НКО СРСР № 0071 про реорганізацію УВР ГШ ЧА в РУ ГШ ЧА у складі РУ ГШ ЧА, крім основних відділів, були утворені 5-й відділ (радіорозвідки), відділ спецрадіозв'язку і відділення спецзв'язку для навчання агентів і розвідників з питань використання шифрів і підтримки зв'язку з ними.

У червні 1945 року РУ ГШ ЧА і ГРУ НКО були знов об'єднані в ГРУ ГШ Червоної Армії (з 1946 року – Збройних Сил), у складі якого радіорозвідкою почав займатися 2-й відділ.

У вересні 1947 року ГРУ увійшло до складу знов створеного Комітету Інформації при Раді Міністрів СРСР, у ведення якого були передані всі розвідувальні служби країни. А у січні 1949 року військова розвідка була знов повернута до Збройних Сил (далі – ЗС): на базі 6-го Управління КІ було утворено 2-е (розвідувальне) ГУ ГШ ЗС (з 1953 року – ГРУ ГШ ЗС).

На початку 1950-х років сфера діяльності радянської радіорозвідки стала значно розширюватися. Зокрема, велися активні науково-дослідні роботи з пошуку шляхів доступу до джерел, що користується ультракороткохвильвими (далі – УКХ) і надвисокочастотними (далі – НВЧ) діапазонами.

Разом з тим, одержала подальший розвиток радіотехнічна та електронна розвідка, що здобувала дані про радіоелектронні засоби іноземних держав. Займалися цим відділ радіорозвідки ГРУ, який у травні 1955 року був реорганізований у 6-е Управління ГРУ ГШ ЗС, і 8-е ГУ КДБ СРСР.

21 червня 1973 року наказом КДБ № 0056 зі складу 8-го ГУ КДБ було виділене самостійне 16-е Управління КДБ, завдання якого були такими: вести перехоплення повідомлень з ліній зв'язку іноземних представництв і нелегалів на території СРСР; займатися встановленням місцезнаходження радіоапаратури та дешифруванням перехоплених повідомлень; здійснювати технічне проникнення в іноземні посольства та представництва як у СРСР, так і за кордоном; одержувати інформацію за кордоном в урядових і військових лініях зв'язку іноземних держав, а також з використанням прослуховуючої апаратури та інших технічних засобів.

Начальниками Управління у різні періоди були:

1. Андреєв Микола Миколайович (липень 1973 - серпень 1975).

2. Маслов Ігор Васильович (серпень 1975 - 1991).

Чисельність співробітників Управління в кінці 1970-х років досягала 2-х тисяч осіб. Склад Управління був таким:

- 1 відділ - займався розкриттям шифрів, для чого використовував ЕОМ «Бу-

лат» – одну з наймогутніших у СРСР;

- 2 відділ - функції невідомі;
- 3 відділ - відповідав за переклад прочитаної кореспонденції на російську мову, що потім надходила до 4-го відділу;
- 4 відділ - редагував і постачав пояснювальними коментарями матеріали, що надходили з 3-го відділу, та відбирав з них ті, які призначалися для відправлення споживачам. Матеріал оформлявся у вигляді 2-х брошур. При цьому, одну з них одержували тільки деякі члени Політбюро ЦК КПРС, а з другою знайомилися начальники 1-го (зовнішня розвідка) і 2-го (контррозвідка) ГУ КДБ;
- 5 відділ - займався аналізом шифросистем і здійснював зв'язок з відповідними спецслужбами країн-учасниць Варшавського договору і союзних держав;

Служба 1 - відповідала за закладки й інші технічні способи проникнення в іноземні посольства. При цьому, 1-й відділ Служби здійснював аналіз іноземної апаратури шифрозв'язку на предмет виявлення в ній закладок, розробляв методи уловлювання сигналів, що випромінювались цією апаратурою. 2-й відділ займався перехопленням цих сигналів і їхньою обробкою. 3-й відділ підтримував контакти з митними органами та іншими установами, за допомогою яких проводилися операції щодо встановлення та вилучення «жучків». 5-й відділ «очищав» перехоплені сигнали від перешкод.

Тут необхідно відзначити, що головним об'єктом уваги Управління з перших днів його існування були США. Так, начальник американського відділу 8-го ГУ КДБ Селезньов відразу ж зажадав, щоб співробітники 16-го Управління негайно приступили до збору даних про американські шифри, розкриття яких було головною задачею його підрозділу.

Для здійснення радіоперехоплень 16-е Управління мало у своєму розпорядженні численні станції на території СРСР. Крім того, з 1960-х років були утворені пости радіоперехоплення в резидентурах Першого ГУ (далі – ПГУ) КДБ в іноземних державах. Найперший такий пост був організований у 1963 році в Мехіко та одержав кодове найменування *«Радар»*. Через 3 роки аналогічний пост за назвою *«Почин»* заробив у посольстві СРСР у Вашингтоні, а у 1967 році почав функціонувати пост *«Проба»* у Нью-Йорку.

До 1970 року пости *«Почин-1»* (у посольстві), *«Почин-2»* (у житловому комплексі посольства), *«Проба-1»* (у будинку радянського представництва в ООН) і *«Проба-2»* (на дачі радянського посольства на Лонг-Айленді) уже могли перехоплювати послання дипломатів Аргентини, Бразилії, Канади, Франції, Португалії, Іспанії та деяких інших країн, а також деякі повідомлення, передані по американських військових лініях зв'язку. При цьому велика частина отриманої інформації одержала високі оцінки міністра закордонних справ СРСР Андрія Громико і радянського представника при ООН Якова Маліка.

Голова КДБ СРСР Юрій Андропов 15 травня 1970 року ухвалив план розгор-

тання постів радіоперехоплення у 15 резидентурах ПГУ, а до кінця 1980 року за кордоном уже діяло більш 30 таких постів. Крім вищезгаданих постів *«Почин-1»* і *«Почин-2», «Проба-1»* і *«Проба-2»*, це були:

«Весна» у Сан-Франциско, *«Венера»* у Монреалі, *«Радар»* у Мехіко, *«Термит-С»* у Гавані, *«Клён»* у Бразилії, *«Остров»* у Рейк'явіку, *«Меркурий»* у Лондоні, *«Север»* в Осло, *«Юпитер»* у Парижі, *«Центавр-1»* у Бонні, *«Центавр-2»* у Кельні, *«Тироль-1»* у Зальцбурзі, *«Тироль-2»* у Відні, *«Эльбрус»* у Берні, *«Кавказ»* у Женеві, *«Старт»* у Римі, *«Алтай»* у Лісабоні, *«Радуга»* в Афінах, *«Тюльпан»* у Гаазі, *«Вега»* у Брюсселі, *«Парус»* у Белграді, *«Радуга-Т»* в Анкарі, *«Сириус»* у Стамбулі, *«Марс»* у Тегерані, *«Орион»* у Каїрі, *«Сигма»* у Дамаску, *«Заря»* у Токіо, *«Краб»* у Пекіні, *«Амур»* у Ханою, *«Дельфин»* у Джакарті, *«Крым»* у Найробі.

Крім того, 25 квітня 1975 року Постановою Ради міністрів СРСР було санкціоновано утворення поста радіоперехоплення 16-го Управління на базі ГРУ МО в Лурдесі на Кубі. Пост, який одержав назву *«Термит П»*, почав функціонувати в грудні 1976 року. Він був оснащений 12-метровою стаціонарною параболічною та встановленою на відкритій вантажівці 7-метровою мобільною параболічною антенами. Вони дозволяли перехоплювати повідомлення у НВЧ-діапазоні, що передавалися з американських супутників, а також контролювати переговори між вежами НВЧ-зв'язку. Пізніше такі ж пости були введені в дію на військовій базі *«Камрань»* (В'єтнам) і в Південному Ємені.

Утім, із усіх постів найважливішими вважалися пости в Нью-Йорку та Вашингтоні. Так, у 1975 році *«Почин-1»* і *«Почин-2»* перехопили 2,6 тисячі повідомлень, а у 1976 році – уже 7 тисяч. Серед останніх варто відзначити ті, що стосувалися поїздки міністра оборони США Дональда Рамсфелда на засідання групи ядерного планування НАТО, зустрічей держсекретаря Генрі Кіссінджера з керівниками Великобританії, Франції, Німеччини і Північно-Африканської Республіки.

Вдалося також прослухати розмови, що велися через авіабазу *«Ендрюс»* між Вашингтоном і Президентом, держсекретарем США, іншими американськими високопосадовцями, що літали з візитами на президентському літаку закордон (за що один зі співробітників поста *«Почин-1»* був нагороджений орденом Червоної Зірки). На основі цих перехоплень було підготовлено та відправлено до Москви 800 повідомлень.

Однак здобутком постів *«Почин-1»* і *«Почин-2»* була інформація не тільки політичного, але й військового характеру. Вона стосувалася, зокрема, балістичних ракет *«Трайдент», «МХ», «Першинг-2»*, крилатих і зенітних ракет, літаків «*F-15*», «*F-16*», «*F-18*», «*B-52*» і «*B-1*». Починаючи з 1973 року, нью-йоркські пости «Проба-1» і «Проба-2» змогли одержувати досить важливу науково-технічну інформацію.

Ними, наприклад, був перехоплений декілька факсимільних повідомлень Брукхевенської національної лабораторії, компаній «Боїнг», «Ферчайлд», «Дженерал Дайнемікс», «Грумман», «Хьюз», «Локхід», «*IBM*», ще деяких провідних

фірм американського військово-промислового комплексу (далі – ВПК). Так вдалося отримати дуже важливі дані про конструкцію та розробку літаків «*A-10*», «*B-1*», «*F-14*», інших машин, про програми протиракетної та протичовневої оборони. А введений в дію у 1976 році у Сан-Франциско пост «Весна» тримав під контролем факсимільний і телефонний зв'язок підрядчиків Пентагона, а також найбільш великих компаній, розташованих на західному узбережжі США.

Крім постів радіоперехоплення в резидентурах ПГУ у Вашингтоні, Нью-Йорку та Сан-Франциско були також радіопости (*«Зефир», «Ракета» і «Рубин»* відповідно), що прослухували засоби зв'язку ФБР, відслідковуючи проведені американською контррозвідкою операції. Наприклад, у 1970-і роки пост *«Ракета»* у Нью-Йорку постійно контролював такі канали радіозв'язку:

- між машинами спостереження та 6 постами ФБР, що спостерігали за переміщеннями співробітників радянських представництв;
- між машинами спостереження та відділом розслідування пограбувань банків;
- між агентами ФБР, що спостерігали за переміщеннями співробітників представництв при ООН ряду близькосхідних і західних держав;
- між агентами ФБР, що займалися іншими карними розслідуваннями;
- між диспетчерськими центрами ФБР у Нью-Йорку та Нью-Джерсі;
- між нью-йоркським диспетчерським центром і машинами ФБР.

Результати діяльності поста радіомоніторингу «Ракета» у 1973 році співробітники нью-йоркської резидентури ПГУ оцінили таким чином: «Пости спостереження ФБР і групи зовнішнього спостереження використовують для зв'язку прості коди, сленгові вирази та умовні фрази, що легко розшифровуються оператором «Ракети». Переговори між постами спостереження та групами зовнішнього спостереження являють собою короткі діалоги, якими пост інформує групу про номер машини об'єкта спостереження та напрямку, у якому він рухається до перехрестя і після нього.

Щоденне радіоперехоплення повідомлень диспетчерського центра ФБР дозволяє скласти уявлення про оперативну обстановку та про те, як ФБР проводить операції у місті. Коли резидентура ПГУ КДБ проводить міську операцію, оператор «Ракети» здійснює моніторинг за роботою радіоцентра ФБР; у разі потреби оперативний працівник може одержати сигнал небезпеки до виходу до місця проведення операції або йому можна наказати припинити операцію, якщо він потрапив під зовнішнє спостереження. Пост «Ракета» реєструє всіх місцевих громадян, що потрапили в поле зору ФБР, і їхні прізвища заносяться у файли системи «Контакт».

У 1980-і роки пости радіоперехоплення та моніторингу були вже у всіх резидентурах ПГУ КДБ за кордоном. При цьому, кожний з них у листопаді повинний був передавати в Центр річний звіт, у якому докладно викладався зміст перехоплених зашифрованих і відкритих повідомлень, відсоток оперативно значимих перехоплень,

виявлені нові канали зв'язку, що являли розвідувальний інтерес, характеристики стану в країні з погляду радіорозвідки, ступінь виконання постом поставлених завдань, заходи щодо забезпечення безпеки й таємності та плани роботи поста на наступний рік.

Крім 16-го Управління КДБ радіотехнічною та електронною розвідкою в СРСР займалося ще 6-е Управління ГРУ ГШ ЗС. Офіцери даного Управління входили до складу резидентур у столицях іноземних держав і займалися перехопленням та розшифруванням передач по урядових і військових інформаційних мережах. Крім того, у підпорядкуванні цього Управління знаходилися полки електронної розвідки, дислоковані на радянській території, а також служби електронної розвідки військових округів і флотів.

6-е Управління мало Центр космічної розвідки, який знаходився на Волоколамському шосе та називався «Об'єкт К-500». Він складався з 4-х відділів:

🗝 1 - радіорозвідки займався перехопленням і дешифруванням повідомлень із каналів зв'язку іноземних держав. Він керував підрозділами «ОСНАЗ», що входили у військові округи і групи радянських військ в Угорщині, Німеччині, Польщі та Чехословаччині. Під керівництвом відділу радіорозвідки «ОСНАЗ» виконував функції перехоплення повідомлень з комунікаційних мереж закордонних країн – об'єктів радіорозвідувального спостереження з боку ГРУ. Для цього у розпорядженні 1-го відділу знаходилося 300 осіб плюс 1,5 тисячі інших військових і цивільних службовців.

🗝 2 - радіотехнічної розвідки користувався послугами тих же станцій перехоплення і здійснював спостереження електронними засобами за тими ж країнами, що і 1-й. Однак метою 2-го відділу були радіо, телеметричні й інші електронні сигнали, що випромінювались апаратурою військового призначення. Для перехоплення цих сигналів він задіював «ОСНАЗ» у військових округах і групах військ Міністерства оборони.

🗝 3 - технічного забезпечення займався обслуговуванням станцій перехоплення, устаткування яких розміщалося в будинках радянських посольств, консульств і торговельних місій по усьому світі, а також окремо розташованих станцій перехоплення на Кубі, у В'єтнамі, Бірмі та Монголії.

🗝 4 - спостереження цілодобово відслідковував всю інформацію, що здобувалася засобами радіорозвідки. Основним завданням відділу було спостереження за військовою ситуацією у світі та особливо за істотними змінами в Збройних Силах США. Кожен офіцер відділу відповідав за свій об'єкт спостереження: такими об'єктами були американське командування стратегічною авіацією, командування тактичною авіацією США тощо. На основі даних, отриманих з відділу спостереження, оперативний черговий 6-го Управління щодня складав інформаційні відомості, що, у свою чергу, входили у підсумкові інформаційні відомості усього ГРУ.

Крім того, веденням радіорозвідки займалися ще деякі технічні підрозділи ГРУ:

- командний пост ГРУ, що здійснював цілодобове спостереження за появою ознак підготовки нападу на СРСР і користувався при цьому інформацією, що надходила до 6-го Управління;
- дешифрувальна служба, що займалася криптоаналізом і читанням перехоплених шифрованих повідомлень з тактичних військових мереж зв'язку. Вона перебувала у прямому підпорядкуванні начальника ГРУ і знаходилася у Москві на Комсомольському проспекті;
- спеціальний комп'ютерний центр, що знаходився у населеному пункті Соколовський у 40 км під Москвою та обробляв отриману від радіорозвідки інформацію;
- лабораторія технічних проблем радіорозвідки, що знаходилася в Кунцево;
- Центральний НДІ у Москві, одним із завдань якого була розробка нового обладнання для радіорозвідки;
- Управління інформаційного забезпечення, що виконувало роботу з оцінки розвідданих, що надходили з 6-го Управління.

Що стосується Управління космічної розвідки ГРУ, то воно збирало розвідувальні дані за допомогою супутників. Управління керувало діями «*ОСНАЗ*», що були підпорядковані 1-му і 2-му відділам 6-го Управління, функціями яких була радіо- і радіотехнічна розвідка. Аналіз і обробка отриманої таким чином інформації були покладені на так називану «систему Дозор», що знаходилася в центральному будинку ГРУ на Хорошевському шосе («Об'єкт К-200»).

Крім того, на Воробйових горах знаходився Особливий радіодивізіон (далі – ОРД), за допомогою якого ГРУ підтримувало радіозв'язок зі своїми секретними агентами, розкиданими по всьому світу. Офіційна ця установа називалася Науково-дослідним інститутом з проблем золотодобування. Фахівці ОРД приймали криптограми від радянських агентів і передавали їм розпорядження за підписом «Директор».

Для агентів це було практично єдиним надійним засобом зв'язку з ГРУ, за наказами якого вони ризикували своїм життям. В ОРД були фахівці, які розробляли частотні розклади для забезпечення якнайкращої чутності при проведенні сеансів зв'язку з різних точок земної кулі, а також співробітники, що займалися розподілом радіопозивних серед закордонної агентури.

Об'єктами, які мала на своєму балансі служба радіорозвідки, були:

- Центр радіо- і супутникового зв'язку, розташований у селищі Ватутінки під Москвою. У ньому приймали, у тому числі й по супутникових каналах зв'язку, інформацію від 11 комплексів стратегічної електронної розвідки, що знаходилися в СРСР, і від 4 закордонних;
- Центральна станція радіорозвідки, розташований у місті Клімовськ під Москвою, де цілодобово працювала служба відстеження та первинної обробки даних радіорозвідки;
- Центри радіоперехоплення та електронної розвідки в Лурдесі (Куба), бухті

Камрань (В'єтнам), Рангуні (Бірма) і в Монголії.

Інформація з усіх центрів радіоперехоплення та електронної розвідки зосереджувалася в центральній станції радіорозвідки.

Інформаційні потоки з центральної станції радіорозвідки, з об'єктів тактичної розвідки у військових округах, групах військ і на флотах направлялися до апарату 6-го Управління, де на їхній підставі готувались щоденні відомості, які надходили на командний пост ГРУ, утворений у 1962 році під час Кубинської кризи, а також включалися в щоденні розвідувальні відомості ГРУ. Крім того, відомості 6-го Управління направлялися до служби інформації ГРУ, де вони накопичувалися та аналізувалися.

Особливо варто сказати про радіорозвідувальний флот СРСР, що нараховував 62 корабля. Так, у районі Східного Середземномор'я у 1970-і роки поза межами видимості з берегів Ізраїлю постійно курсували на вигляд нічим не примітні три радянські кораблі – «Кавказ», «Крим» і «Юрій Гагарін». Вдень і вночі вони патрулювали узбережжя Ізраїлю.

Під час війни в Югославії у квітні 1999 року в Адріатичному морі відкрито з'явився розвідувальний корабель ЧФ *«Лиман»*, якого через декілька місяців замінив корабель *«Кильдин»*. На таких кораблях не було ні ракетного, ні артилерійського, ні торпедного озброєння. Єдиною їхньою метою було ведення радіорозвідки, для чого вони мали тільки засоби радіо-, радіотехнічної, електронної та гідроакустичної розвідки.

Радіорозвідувальні кораблі СРСР фіксували всі радіопереговори та телефонні розмови. Незважаючи на те, що радянські експерти, що знаходилися на кораблях-розвідниках, могли самостійно аналізувати інформацію, що перехоплювалася, велика її частина відправлялася в Москву. Контакт із нею підтримувався цілодобово, у тому числі й за допомогою супутникового зв'язку.

Якщо говорити про космічну розвідку, то її історія почалася наприкінці 1950-х років, коли перед «ОКБ-1» академіка С.П.Корольова поставили завдання створити супутник-розвідник і пілотований орбітальний корабель. Це завдання було вирішено після створення супутника *«Зенит»*, що легко був переобладнаний в корабель *«Восток»*. Перший розвідувальний супутник *«Зенит»* вивели на орбіту 26 квітня 1962 року. Офіційно він називався *«Космос-4»* і пробув на орбіті 3 доби.

Супутники *«Зенит»* на довгий час стали основою системою космічної фоторозвідки. Зрозуміло, вони неодноразово модернізувалися та пристосовувалися до конкретних завдань: оглядової зйомки великих площ, детального фотографування районів особливого інтересу, стереоскопічної зйомки, однак базова конструкція зберігалася протягом 30 років.

Починаючи з супутника *«Космос-12»*, запущеного в грудні 1962 року, тривалість польоту супутника-розвідника була визначена у 8 діб, а частота запуску з

1964 року досягла 9 супутників у рік. З 1966 року для запуску фоторозвідувальних супутників стали використовувати стартові комплекси космодрому *«Плесецк»* із ракетами «8А92». В результаті кількість запусків супутників збільшилося до 20 і більше у рік, а їхнє виведення на нові орбіти дозволило їм «бачити» всі населені райони земної кулі.

До середини 1970-х років здійснювалося вже по 30-35 запусків щорічно, однак навіть при такій інтенсивності сумарний час польотів розвідувальних супутників ледь досягав 400 діб у рік. Утім, це ні скільки не применшує досягнень космічної розвідки. Так, саме її дані дозволили точно установити, що Китай працює над створенням власного супутника, запуск якого був успішно здійснений у 1970 році.

Тут треба відзначити, що при виникненні міжнародних криз і конфліктів кількість запусків розвідувальних супутників різко зростала. Так, під час радянсько-китайського конфлікту на острові Даманському з 25 лютого по 25 квітня вивели 10 фоторозвідників, а влітку 1969 року під час конфлікту біля озера Жаланашколь менше ніж за три місяці було запущено 15 супутників.

У 1975 році у розпорядженні ГРУ з'явилися супутники так називаного 4-го покоління, що знаходилися на орбіті близько 30 діб. А на початку 1980-х років тривалість їхнього польоту збільшилася з 45 до 55-59 діб. Відзнята з цих супутників плівка поверталася на Землю в спеціальних капсулах.

Була розпочата спроба вести космічну розвідку і з орбітальних станцій. Створенням таких розвідувальних орбітальних пілотованих станцій (далі – ОПС), що одержали назву *«Алмаз»*, займалося Конструкторського Бюро (далі – КБ) академіка В.Н.Челомея, а їхні іспити проходили у період з 1972 по 1977 роки. Правда, у повідомленнях ТАСС *«Алмаз»* називався *«Салютом»* та камуфлювалися під цивільні орбітальні станції.

Усього на орбіту вивели три станції *«Алмаз»*. Станція *«Алмаз-1»* була запущена 3 квітня 1973 року та знаходилася на орбіті 26 днів, після чого через розгерметизацію корпуса 29 квітня ввійшла в щільні шари атмосфери та згоріла. Станція *«Алмаз-2»* (офіційна назва «Салют-3») була запущена 25 червня 1974 року та пролітала 213 днів (до 25 січня 1975 року). На станції 14 днів працював військовий екіпаж у складі П.Поповича та Ю.Артюхина, а на борті був встановлений унікальний комплекс оптичних засобів розвідки. Відзнята інформація доставлялася на Землю в спеціальній капсулі, відстріленої зі станції під час її прольоту над територією СРСР.

Станція *«Алмаз-3»* (*«Салют-5»*) була запущена 22 червня 1976 року та пролітала 441 день – до 8 серпня 1977 року, коли за командою з Землі її затопили. На станції працювали два військових екіпажі. Перший у складі Б.Волинова та В.Жолобова пробув на станції 48 днів, а другий екіпаж у складі В.Горбатко та Ю.Глазкова – 17 днів. Третій екіпаж, що прибув до станції 14 жовтня 1976 року на кораблі *«Союз-23»*, зістикуватися з нею не зміг. Однак у 1978 році роботи по *«Алмазам»* були припинені, тому що в ГРУ прийшли до висновку, що автоматичні

розвідувальні системи переважніше пілотованих.

Після розпаду СРСР і ліквідації КДБ у 1991 році 16-е Управління КДБ увійшло до складу Російської Федеральної агенції урядового зв'язку та інформації (скорочено російською – *«ФАПСИ»*) і стало називатися Головним управлінням радіоелектронної розвідки засобів зв'язку (далі – ГУРР).

Крім того, у складі *«ФАПСИ»* була створена Криптографічна служба, що займалася шифруванням та зовнішньою радіоелектронною розвідкою. Слід особливо зазначити, що вона збирала та здійснювала первинну обробку розвідувальної інформації, направляючи її до Ситуаційного центру, інших спецслужб та правоохоронних органів. Найбільш важлива інформація доповідалася особисто Президенту Росії.

У березні 2003 року *«ФАПСИ»* була ліквідована. Частина ГУРР, що була пов'язана з розвідувальною діяльністю за кордоном, увійшла до складу Служби зовнішньої розвідки (далі – СЗР). Інша частина радіоелектронної розвідки – робота усередині країни разом з військами радіоелектронної розвідки – увійшла до складу Федеральної служби безпеки (далі – ФСБ).

22 вересня 2003 року міністр оборони Росії Сергій Іванов виступив із заявою, що демонтаж російських військових баз на Кубі (Лурдес) і у В'єтнамі (Камрань), що почався в грудні 2001 року, цілком завершений. Причому разом з військовими базами були ліквідовані й розташовані на їхній території центри радіоелектронної та радіотехнічної розвідки, що істотно позначилося на можливості російських спецслужб одержувати важливу інформацію.

4.10. Спецзв'язок Росії

Після невдалої спроби державного перевороту в СРСР 19 серпня 1991 року Указом Президента СРСР за № УП-2484 від 29 серпня 1991 року на базі відділів і служб Управління урядового зв'язку КДБ був створений Комітет урядового зв'язку при Президенті СРСР. 10 жовтня 1991 року Президентом СРСР було затверджене «Положення про Комітет урядового зв'язку», який визначався як союзно-республіканський комітет. До складу Комітету ввійшли:

- Головне управління урядового зв'язку (далі – ГУУЗ);
- Головне управління безпеки зв'язку (далі – ГУБЗ);
- Науково-технічний центр (у складі ГУБЗ);
- Головне управління радіоелектронної розвідки засобів зв'язку (далі – ГУРР);
- Управління урядового зв'язку РСФСР (за узгодженням із Президентом РСФСР);
- Інформаційно-аналітичне управління;
- Управління по роботі з особовим складом;
- Академія криптографії;

- Орловське вище військове командне училище зв'язку;
- Господарське управління;
- Військово-будівельне управління;
- Фінансово-планове управління;
- Організаційно-мобілізаційний відділ;
- Юридичний відділ;
- Служба безпеки;
- Науково-технічна рада;
- Комерційна служба;
- Секретаріат тощо.

Однак цей Комітет проіснував не більше 3-х місяців. Після остаточного «розпаду» СРСР на незалежні держави Указом Президента Росії за № 313 від 24 грудня 1991 року була створене *«ФАПСИ»* на базі 8-го ГУ, 16-го Управління КДБ і Комітету урядового зв'язку при Президенті СРСР, а також Державного інформаційно-обчислювального центра при Державній комісії з надзвичайних ситуацій і Московського НДІ електротехніки Науково-виробничого об'єднання «Автоматика».

Нова спецслужба була розділена на п'ять головних управлінь:

- Головне адміністративне управління, що було штабом *«ФАПСИ»*;
- ГУУЗ, що було утворено на базі Управління урядового зв'язку КДБ СРСР для забезпечення безпеки 100 абонентів президентського зв'язку; 1000 абонентів АТС-1, призначеної для великих урядових чиновників; 7000 абонентів АТС-2 (звичайні урядові зв'язки), а також 5000 абонентів урядового міжміського зв'язку, призначеного для спілкування з регіонами;
- ГУБЗ, що було утворено на базі 8-го ГУ КДБ, яке контролювало всі шифрувальні служби, включаючи службу МЗС, Уряду та Президента СРСР;
- ГУРР, що було утворено на базі 16-го Управління КДБ;
- Головне Управління інформаційних ресурсів (далі – ГУІР), яке через Ситуаційний центр поставляло Президенту Росії близько 80% інформації та відповідало за інформаційне та інформаційно-технологічне забезпечення всіх зацікавлених органів державної влади від Ради безпеки до ФСБ, включаючи і регіональний рівень.

Генеральний директор *«ФАПСИ»* був також командуючим військами Федеральної агенції, у склад яких входили війська урядового зв'язку, частини радіорозвідки та інженерно-будівельні частини. Відомо, що штат *«ФАПСИ»* нараховував кілька десятків тисяч чоловік, серед яких було близько 70 генералів. При *«ФАПСИ»* функціонува-

ла також Академія криптографії Російської Федерації.

Зміцнюючи законодавчу основу діяльності російських шифрувальників, президент Росії видав ряд правових актів, що регламентували цю сферу забезпечення загальнонаціональної російської безпеки. Так, 24 вересня 1992 року розпорядженням глави держави за № 536-рп у складі *«ФАПСИ»* був заснований Науково-технічний центр правової інформації «Система».

Указами Президента Російської Федерації від 28 вересня та 29 жовтня 1992 року була створена виділена система президентського зв'язку. При цьому комплекси технічних засобів та особовий склад президентського зв'язку були передані з *«ФАПСИ»* до Головного управління охорони Російської Федерації (далі – ГУО). Там було створено Управління президентського зв'язку, яке очолив заступник начальника ГУО Ю.П.Корнєв. У червні 1996 року ГУО було реорганізоване у Федеральну службу охорони Російської Федерації (далі – ФСО).

У лютому 1993 року був прийнятий Закон «Про федеральні органи урядового зв'язку й інформації» та відкритий для відвідування Музей урядового зв'язку на базі Орловського Військового інституту урядового зв'язку, який у жовтні 1996 року був перетворений у Музей *«ФАПСИ»*.

У 1994 році було затверджене *«Положение о ФАПСИ»*, відповідно до якого у веденні агенції знаходилися чотири питання: спецзв'язок; криптографічна безпека шифрованого зв'язку; розвідувальна діяльність у системі спецзв'язку та спеціальне інформаційне забезпечення вищих органів влади.

3 квітня 1995 року Президент Росії підписав Указ № 334 «Про заходи щодо дотримання законодавства в області розробки, виробництва, реалізації й експлуатації шифрувальних засобів, а також надання послуг в сфері шифрування інформації та прийнятих заходів щодо забезпечення інформаційної безпеки в інформаційній телекомунікаційній системі спеціального призначення», згідно з яким був створений Федеральний центр захисту економічної інформації при *«ФАПСИ»*.

Станом на 1997 рік в Росії урядовим зв'язком було охоплено близько 300 міст і спецоб'єктів, таємний телефонний зв'язок був наданий більше 20 тисячам абонентів, а шифрованим документальним зв'язком було охоплено понад 1600 органів влади і різних організацій. У 79 містах функціонували комплекси радіозв'язку з рухомими об'єктами, що обслуговували понад 3 тисячі абонентів.

ГУУЗ забезпечувало вищі органи державної влади Російської Федерації, органи державної влади суб'єктів Російської Федерації, центральні органи федеральної виконавчої влади, Раду безпеки спеціальними видами зв'язку. У розпорядженні ГУУЗ були так звані Центри урядового зв'язку, розташовані в найбільших містах Росії. Спецзв'язком був забезпечений, навіть, президент Чечні Аслан Масхадов – у січні 1998 року *«ФАПСИ»* закінчило в Грозному монтаж вузла спецзв'язку, що повинен був забезпечувати його та інших посадових осіб республіки урядовим зв'язком.

15 грудня 1998 року вийшла Постанова уряду Росії № 1492 про створення Воронезького військово-технічного училища *«ФАПСИ»*. А навесні 2000 року Орловський Військовий інститут урядового зв'язку був перетворений в Академію «ФАПСИ» при Президенті Російської Федерації.

Агенція мала один із самих могутніх інформаційних потенціалів у Росії. В активі ГУІР, наприклад, був величезний масив баз даних: відповідно до законодавства Росії різні відомства безкоштовно надавали у розпорядження *«ФАПСИ»* у вигляді «контрольного примірника» свою інформаційну продукцію.

Справа в тому, що ще в 1996 році вийшла постанова російського уряду щодо створення глобальної бази даних Росії, згідно з якою всі державні бази даних підлягали обов'язковому обліку та реєстрації, а інші – добровільному. Реєстрацію вели три державні установи, дві з яких – НТЦ «Система» та «Контур» – були підвідомчі *«ФАПСИ»*. Крім того, агенція створила при своїх регіональних центрах особливі підрозділи, що працювали як обчислювальні комплекси. Вони займалися всією центральною, регіональною та закордонною пресою, статистичною та оперативною інформацією з регіонів, аналізуючи соціально-економічний стан на місцях. Усе це осідало у власних базах «*ФАПСИ*» (таких як «Барометр», «Ельбрус» тощо).

Однак із приходом на посаду Президента Росії Володимира Путина, колишнього співробітника КДБ, настав час реформування правоохоронних структур і спецслужб. У березні 2003 року такий інформаційний «монстр» як *«ФАПСИ»* був ліквідований та поділений між наявними трьома відомствами: ФСБ, СЗР і ФСО. Як пояснили в Центрі суспільних зв'язків ФСБ Росії, «ліквідується паралелізм», оскільки «ті самі або дуже схожі функції, що з 1991 року виконувалися різними відомствами, тепер будуть зосереджені в єдиній структурі».

Але справа, мабуть, була не тільки у цьому. Так, 12 квітня 1996 року був заарештований начальник Фінансово-економічного управління *«ФАПСИ»* генерал-майор Валерій Монастирецький за обвинуваченням у присвоєнні довіреного йому майна та зловживанні владою. У його особистому депозитарії в «Рато-Банку» чекісти вилучили саквояж, наповнений доларами і марками загальною сумою у півтора мільярда карбованців. Крім того, він мав квартиру ціною у 1320 тисяч доларів і парк шикарних іномарок.

На початку 1997 року обвинувачення було скориговане: ст. 290 - 4 п. «м» Кримінального кодексу – одержання хабара у великому розмірі, ст. 160 ч.3 п. «б» – розкрадання майна у великому розмірі, ст. 222 ч. 1 – незаконне збереження зброї та боєприпасів. У кримінальній справі фігурувала німецька компанія «Сіменс», московський «Рато-Банк» і фірма «Роскомтех», яку очолювала дружина Монастирецького.

А починалась справа у 1992-1993-х роках, коли «*ФАПСИ*» обрало собі як генерального постачальника велику німецьку фірму «Сіменс Нікздорф Остєвропа». Аб-

солютна більшість проектів *«ФАПСИ»* робилася від того часу на базі «Сіменс». Німецькі фахівці брали участь у роботі Агенції по повній програмі. «Сіменс Ніксдорф Остєвропа» була створена після об'єднання Німеччини на базі східного «Роботрона» та західного «Сіменс» спеціально для співробітництва з країнами Східної Європи, у першу чергу, з Росією. Зрозуміло, що німці були дуже зацікавлені в дружбі з *«ФАПСИ»*. Контракт на п'ятсот із зайвим мільйонів марок, який вони уклали з Агенцією, зобов'язував постачати Агенцію комплектуючою технікою та розробками.

Але в Росії, утім як і в інших слов'янських державах, свої порядки: «не підмажеш – не поїдеш». Так з'явився ще один контракт – «Рішення про проведення робіт з консультування і надання сприяння фірмі «Сіменс Ніксдорф Остєвропа» з постачання устаткування та послуг». Пункт другий угоди говорив: «Як винагороду за проведені роботи фірма «Сіменс» забезпечує сплату АТ «*MKL*» 5% від суми реалізованого обороту, а також переклад вищезгаданої суми на розрахунковий рахунок «MKL» у банку «Ліхтенштейн Ландесбанк». 5% «від суми реалізованого обороту» – це 26 мільйонів марок. Контракт був підписаний 28 вересня 1994 року в Дрездені.

Просто так віддавати гроші якійсь фірмі «*MKL*» німці би не стали. Фірма АТ «*MKL*» була створена 10 вересня 1993 року в столиці Ліхтенштейну Вадуці. В її установчому договорі сказано: «Метою АТ є виробнича і комерційна діяльність усіх видів, надання послуг, а також будь-які інші види діяльності».

Отже, це була звичайна офшорна компанія, чий установчий договір був підписаний трьома особами. У тому числі і Монастирецьким, який був не тільки співзасновником, але й співвласником «*MKL*». 100% пакет акцій АТ був розбитий на 13 частин. Перша – з 10 акцій – належала Старовойтову. Другий пай (10%) був у Монастырецкого. Ще 7 акцій було записано на сина Старовойтова Дмитра. Дісталося 10% акцій і другу Старовойтова, тодішньому заступнику голови Російського фонду федерального майна Олександру Яковлеву.

Споконвічно, коли ще тільки вирішувалося питання, хто буде генеральним постачальником, у *«ФАПСИ»* розглядали пропозицію декількох фірм: німецької «Сіменс», французьких «Алькател» і «Шлямберже», американської «Нетрікс». Кожний із претендентів мав свої переваги та однозначно був кращим за «Сіменс». Попередник Монастирецького на посаді головного фінансиста «*ФАПСИ*» генерал-майор Володимир Малінін згадував, як у 1992 році йому принесли контракт із «Сіменс». Вивчивши його та проконсультувавшись з фахівцями Міністерства зовнішньої економіки, він відмовився підписувати документ. Мало того, що ціни на устаткування були непомірно завищені, у випадку яких-небудь з'ясовувань контракт зобов'язував вирішувати всі питання через іноземний суд, що не міг похвалитися особливою об'єктивністю.

Колишній заступник Старовойтова генерал-лейтенант Анатолій Куранов також розповів, що з погляду безпеки зв'язку кращою за всіх була фірма «Алькател».

По-перше, французи давали нам повний «листінг», тобто опис програм і систем, по-друге, це було їхнє «ноу-хау», а по-третє, вони бралися доробити усе під російські стандарти. В той час, як у «Сіменс» не було нічого: ні «листінгу», ні «ноу-хау», ні бажання «підганяти» під стандарти.

На той час німецька компанія фактично одержала можливість контролювати значну частину систем *«ФАПСИ»*. Справа була в тому, що за німецьким законодавством фірми не мають права продавати іноземним спецслужбам «математику» – опис програм, їхню таємницю – винятково готові вироби. Тобто «*ФАПСИ*» одержувала тільки «чорні шухляди», причому вони встановлювались тільки німецькими фахівцями. Внутрішня «начинка» німецької техніки залишалася для росіян таємницею.

Щоб було зрозуміло, які гігантські перспективи відкрилися перед «Сіменс», треба назвати тільки декілька спільних проектів: Інформаційно-телекомунікаційна система спецпризначення, Центральна і регіональні інформаційні системи податкових служб, Інформаційна система для керування земельними ресурсами. Брав участь «Сіменс» і в оснащенні Ситуаційного центра Президента Росії, у системах, призначених на особливий період.

З джерел у російській контррозвідці відомо, що наприкінці 1995 року німецька розвідка «БНД» узяла Монастирецького в активну розробку. А в січні 1996 року генерал, що вже потрапив «під ковпак» ФСБ, спробував втекти в Німеччину. Його зняли з борта літака... Правда, у вересні 1997 року його звільнили з-під варти, але який збиток таємницям російського шифрозв'язку був при цьому непомірному збагаченні завданий, не повідомлялося.

В результаті *«ФАПСИ»* було ліквідовано та розділено таким чином: основним її спадкоємцем стала ФСО. Сюди відійшло практично усе: ГУУЗ, війська урядового зв'язку, ГУІР (забезпечення роботи органів влади) і інформаційних систем (проведення моніторингів з будь-яких питань), значна частина ГУБЗ, що відало всією інформаційною сферою та створенням закритих засобів зв'язку, а також «соціалка» (будинки відпочинку, автобази), Орловська академія та Воронезький інститут.

Відповідно до Указу Президента Росії від 14 липня 2003 року № 774 на базі *«ФАПСИ»* при ФСО була створена Служба спеціального зв'язку та інформації (далі – ССЗІ), у подальшому названа як «Спецзв'язок Росії». Управління *«ФАПСИ»* федеральних округів були перетворені в Управління ССЗІ у федеральних округах. Центри урядового зв'язку (далі - ЦУЗ) суб'єктів Російської Федерації були перетворені у ЦУЗ ССЗІ. Військові частини військ *«ФАПСИ»* були перетворені у підрозділи зв'язку спеціального призначення ССЗІ.

7 серпня 2004 року ССЗІ увійшла до складу ФСО. Керівником ССЗІ, який є одночасно першим заступником керівника ФСО, був призначений генерал-лейтенант Ю.П.Корнєв, який більше 30 років прослужив у КДБ. У 1991-м році, після

розвалу КДБ, Корнєв перейшов до ГУО. З його ініціативи там було створене Управління президентського зв'язку, що за прикладом закордонних аналогів забезпечувало конфіденційним зв'язком перших осіб держави (так звані системи «*АТС-ПС*» і «*АТС-1*»). У найкоротший термін із групи ентузіастів у декілька десятків чоловік народилося могутнє управління з підрозділами у всіх регіонах Росії, де служать тепер майже 3 тисячі співробітників. За впровадження нових принципів зв'язку Ю.П.Корнєву була присуджена Премія Уряду в сфері науки та техніки.

Вищезазначеним Указом було також затверджено «Положення про ССЗІ ФСО РФ», згідно з яким Спецзв'язок Росії є федеральним органом спеціального зв'язку й інформації, який здійснює в межах своїх повноважень організацію та забезпечення експлуатації, безпеки, розвитку й удосконалення систем урядового та інших видів спеціального зв'язку (далі – спеціальний зв'язок) та інформації для федеральних органів державної влади, органів державної влади суб'єктів Російської Федерації та державних органів (далі – державні органи).

Основними завданнями Спецзв'язку Росії є:

- організація та забезпечення експлуатації, безпеки, розвитку й удосконалення спеціального зв'язку для державних органів;
- участь у розробці і проведенні державної політики в сфері інформаційної безпеки;
- інформаційно-аналітичне забезпечення державних органів, технічне обслуговування і програмний супровід телекомунікаційних систем і ситуаційних центрів, а також інформаційне забезпечення керування державою у воєнний час і при надзвичайних ситуаціях;
- участь у здійсненні заходів державної охорони при наданні спеціального зв'язку й інформації об'єктам державної охорони.

ФСБ отримала від «*ФАПСИ*», крім підрозділів внутрішньої радіоелектронної розвідки усередині країни, ще й ГУБЗ (криптологічні підрозділи) разом з науковими установами.

Згідно з «Положенням про ФСБ РФ та її структуру», що було затверджено Указом Президента Росії від 11 серпня 2003 року № 960, зазначені такі її функції:

- організація та здійснення шифрувальної роботи в органах і військах;
- організація та забезпечення експлуатації, безпеки, розвитку й удосконалення відкритого та засекреченого зв'язку;
- регулювання в сфері розробки, виробництва, реалізації, експлуатації, ввезення в Російську Федерацію і вивозу з Російської Федерації шифрувальних

(криптографічних) засобів і захищених з використанням шифрувальних засобів систем і комплексів телекомунікацій, а також у сфері надання на території Російської Федерації послуг із шифрування інформації та виявлення електронних пристроїв, призначених для негласного одержання інформації, у приміщеннях і технічних засобах;

- розробка та виробництво ключових документів до шифрувальних засобів і ручних шифрів, забезпечення ними федеральних органів державної влади, органів державної влади суб'єктів Російської Федерації; реалізація шифродокументів і шифрувальних засобів, нормативно-технічної документації на виробництво та використання шифрувальних засобів.

Частина 5.

Історія секретної телефонії в СРСР

5.1. Народження телефонного зв'язку

Якщо звернутися до довідників, то можна прочитати, що телефон винайшов в 1874 році американський інженер-конструктор Грехем Белл, який працював у знаменитій і могутній того часу компанії «Вестерн Юніон». Ним у 1876 році був отриманий патент на винахід «телеграфу, за допомогою якого можна передавати людську мову». Перша розмова по телефону відбулася 10 березня 1876 року:

Белл: «Ідіть сюди, містер Ватсон, Ви мені потрібні».

Ватсон: «Містер Белл! Я чітко чую кожне вимовлене Вами слово!!!».

Однак влітку 2002 року американські законодавці відновили історичну справедливість у справі «телефонного авторства» і офіційно визнали винахідником телефону геніального флорентійця Антоніо Меучи.

Виявляється насправді, в 1860 році А.Меучи, витративши свої останні гроші, опублікував в італійській газеті Нью-Йорка повідомлення про те, що він винайшов технічну новинку – «телетрофон». Замітка потрапила на очі клерку компанії «Вестерн Юніон», той відшукав винахідника та за скромну плату купив усі креслення й іншу документацію про телетрофон. Після цього на всі запити А.Меучи представники «Вестерн Юніон» безапеляційно відповідали, що всі документи загублені, а винайшов телетрофон інженер Грехем Белл. Тільки за два роки до своєї смерті, в

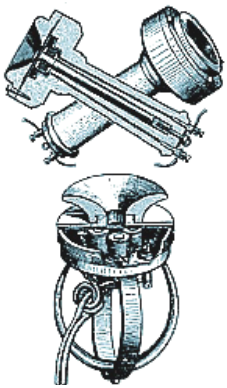
1887 році, А. Меуччи вдалося одержати з архіву «Вестерн Юніон» свій патент на винахід.

Але в Росії, виявляється, теж був свій винахідник телефону. Це був інженер Павло Михайлович Голубицький, що народився 16 березня 1845 року у селі Почуєві Таруського повіту Калузької губернії. В 1870 році він закінчив фізико-математичний факультет Петербурзького університету й працював інженером на залізниці. В 1878 році у майстерні залізничного вузла Бендери Павло Михайлович створив свій оригінальний телефон – так званий телефон-вібратор. Але це був лише перший результат його кропіткої роботи.

Почуєво було з'єднано телефонної лінією з Тарусою, де телефон був установлений на міській пошті. Перший опис телефону Голубицького зробив французький академік Лю-Монсель в 1882 році у журналі «Електричне світло». Він був свідком того, як вдало пройшли іспити телефонів Голубицького між Нансі та Парижем на відстані 353 км. Телефони ж Белла діяли тільки на відстані до 10 км.

Апарати Голубицького отримали визнання як у Росії, так і за кордоном. Зокрема, комісія французького морського міністерства визнала їх неперевершеними. Голубицький запропонував настільний телефонний апарат із важелем перемикання «виклик – розмова». При звичайному положенні слухавки контактний важіль підтримував апарат у стані готовності до прийому виклику, а при знятті слухавки схема апарата автоматично приводилася в стан готовності для ведення переговорів. Ця ідея – комутація електричних кіл залежно від положення слухавки – застосовується й у сучасних апаратах.

Дотепер використовується й принцип, покладений в основу створеного Голубицьким першого мікрофонного капсуля з вугільним порошком. Винахідник указав, що мікрофон з вугільними стрижнями спотворював мову через іскріння в контактах. Для усунення цього явища необхідно було максимально зменшити опір мікрофона та збільшити його поверхню, яка вібрувала під дією звукової хвилі. В 1883 році він сконструював і запатентував мікрофон з вугільним порошком. Однак у Росії до цього винаходу віднеслися з деякою недовірою. Тому Голубицький через обмеженість фінансування на продовження досліджень продав права на його використання французькій телефонній компанії. А для російських чиновників, що замовляли Голубицькому телефонні апарати для залізниць і не полюбляли порошкових мікрофонів, він створив «гребешковий» мікрофон – зі звичними вугільними паличками, але з більшим, ніж раніше, числом контактів.



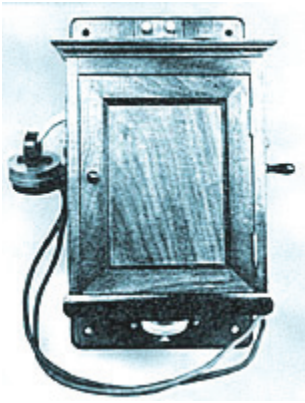
Долю мікрофона з вугільним порошком згодом розділила й система живлення мікрофонів абонентів від загаль-

ної батареї, що була розташована на місцевій телефонній станції. Голубицький розробив свою систему в 1886 році, і це дозволило створювати великі телефонні мережі міст. Але спроби впровадження її в Росії залишалися протягом двох років безуспішними. І тоді Павло Михайлович змушений був поступитися правом на експлуатацію системи Загальній телефонній компанії в Парижі.

До винаходів Голубицького відносився й комутатор, що дозволяв попарно з'єднувати між собою кілька телефонних ліній. Далі в ході робіт з устаткуванням станцій у Калузі й Катеринославі (1882-1885) він увів багато вдосконалень. Зокрема, щоб звільнити руки телефоністок, які працювали за комутатором, він запропонував гарнітуру – комплект навушника й мікрофона. Павлу Михайловичу належить авторство ідеї селекторного зв'язку на залізничному транспорті та її впровадження. І знову ж першим у Росії, в 1881 році, у своєму родовому маєтку біля Таруси він створив телефонну майстерню, де виготовив більше 100 апаратів.

Голубицький постійно брав участь зі своїми приладами на електротехнічних виставках, російських та закордонних, завойовуючи медалі й призи. Він виступав з лекціями та демонстрував роботу своїх апаратів. Винахідник систематично пропонував свої послуги з телефонізації міст і залізниць, але всі концесії на це були віддані іноземцям. Наполегливість і популярність дозволили йому все ж таки здійснити низку проектів на основі телефонної техніки, створеної ним у Почуєві. Ось основні з них:

- 1883 - введення в експлуатацію телефонної станції для правління Курсько-Харково-Азовської залізниці;
- 1884-1888 - встановлення десяти телефонів на Миколаївській залізниці;
- 1885 - введення в експлуатацію телефонного зв'язку в Катеринославі;
- 1885 - введення в експлуатацію телефонного зв'язку в Калузі;
- 1886 - введення в експлуатацію телефонної станції в Головному штабі в Петербурзі;



- 1888-1889 - випробування потяжного телефонного апарата на Миколаївській залізниці.

Виявлена в Державному архіві Калузької області *«Справа про пристрій телефонного сполучення в м. Калузі»* розкриває багато сторінок організації зв'язку та техніку її виконання. Спочатку пристрій телефонного зв'язку був доручений механіку урядового телеграфу Семенову, а потім, через незадовільну якість зв'язку, губернатор Калуги запросив для виконання робіт Голубицького. Винахідник надав проект у двох варіантах – з «центральним бюро», тобто комутатором, і без нього. Серед переваг варіанта з «центральним бюро» він відзначив більшу кількість можливих

з'єднань абонентів і перспективу розширення мережі. Кожна «абонентська станція», тобто телефонний апарат, монтувалася на полірованій цінній деревині, всі металеві частини були нікельовані. Повна станція коштувала 96 карбованців і за кошторисом вартість усього проекту складала 1824 карбованці. Після здачі мережі в експлуатацію у вересні 1885 року Голубицький здійснював також її обслуговування.

Роботи в Почуєвській майстерні, безумовно, були вершиною творчості винахідника, що викликало заздрість і злість іноземних конкурентів. Неодноразово Голубицький одержував від них пропозиції продати свої патенти й техніку, але незмінно відмовляв. 16 березня 1892 року майстерня в Почуєві була кимось підпалена та згоріла вщент. Пожежа знищила все устаткування, документи, готові телефонні апарати. Голубицький був «зломлений» цим ударом, і це позначилося на його роботі. В 1901 році він покинув Почуєве та переїхав у маєток своєї другої дружини (з першою він розлучився через її подружню невірність) у село Салтиково Таруського повіту. Тут Голубицький продовжував займатися телефонією, а 27 січня 1911 року помер після важкої хвороби.

Великий внесок у справу військового телефонного зв'язку зробив підполковник В.Якобі (син академіка Б.Якобі). У 1878 році він успішно провів іспити щодо використання телеграфного кабелю для встановлення телефонного зв'язку на далекі відстані. В результаті телефонна техніка була прийнята на озброєння російської армії, а всі телеграфні парки одержали наказ провести іспити телефонів для з'ясування тактико-технічних умов використання нового засобу зв'язку. У 1881 році Якобі розробив мініатюрний телефонний апарат («телекаль»), що призначався для воєнно-польового зв'язку.

Розвиток міжміського телефонного зв'язку в Росії розпочався у 80-х роках XIX століття, раніше, ніж у деяких інших країнах Європи. Восени 1881 року компанія Белла розпочала будівництво телефонних вузлів і мереж у Москві, Петербурзі, Ризі й Одесі. Перша міжміська лінія була побудована між Петербургом і царськими резиденціями в Гатчині (1882), Петергофі (1883) і Царському Селі (1885). В 1885 році московські промисловці профінансували будівництво однодротових сталевих ліній телефонного зв'язку між Москвою й Богородським, Пушкіним, Хімками, Одинцовом, Коломною, Подільським та Серпуховом. У той час зв'язок із цими містами називали «позаміським».

Експлуатація ж справжнього міжміського зв'язку почалася після вдосконалення методів одночасного телеграфування й телефонування. Заслуга в цьому належить телеграфному фахівцю Г.Ігнатьєву та інженеру Є.Гвоздьову. Ігнатьєв винайшов пристрій, що розділяв телеграфні й телефонні струми за допомогою встановлених у електричному колі конденсаторів і котушок індуктивності. Його система була введена в дослідну експлуатацію в 1881 році на повітряній лінії довжиною 14,5 кілометра, що з'єднувала табори Київського військового округу.

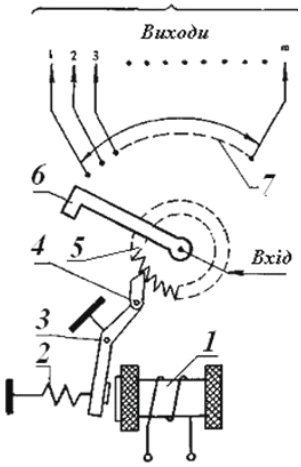
Гвоздьов запропонував зосередити на станціях набори ємностей та індуктивностей різних параметрів і розробив схеми паралельного й послідовного їх встановлення у різних випадках. Створене ним Телефонне товариство в 1888-1889 роках на Рибінсько-Бологоєвській залізниці успішно провело випробування приладів Гвоздьова для одночасного телеграфування й телефонування на відстані у 295 кілометрів.

Дослідження з метою автоматизації телефонного зв'язку велися з самого початку поширення телефону. Перший патент на найпростішу автоматичну телефонну станцію (далі – АТС) був отриманий в 1879 році групою американських винахідників. Через два роки автори вдосконалили свою систему імпульсним реле для трансляції імпульсів. Значний внесок в автоматизацію телефонного зв'язку зробив російський винахідник К.Мосцицький.

Він уперше висунув ідею релейної (без шукачів) АТС у 1887 році й розробив схему станції на шість номерів. Але це ще не була АТС у сучасному розумінні, оскільки комутація з'єднань, хоча й виконувалася без телефоністок, але управлялася абонентами. Абонент посилав через станцію позивні абонента, якого він викликав, і цей сигнал надходив в усі телефонні апарати, увімкнуті в станцію.

Американець Строуджер створив у 1888 році працюючу модель свого декадно-крокового шукача, коли йому було 49 років. На цей пристрій ним був отриманий патент (US Patent № 447918 10/6/1891). Протягом десятків років даний пристрій був основним елементом АТС. Побудовані за системою Строуджера АТС були досить надійні й експлуатувалися у всіх країнах світу аж до 70-х років минулого століття. Така АТС працювала й на станціях урядового зв'язку.

Строуджер винайшов і номеронабирач у вигляді обертового диска, що також протягом десятиліть використовувався в телефонних апаратах, які випускалися промисловістю. У винаході комутатора Строуджер не був піонером. Подібний пристрій був винайдений ще в 1879 році американськими інженерами Конолі і Мактайтом. Однак саме завдяки ентузіазму та наполегливості Строуджера ідеї автоматичної комутації одержали зрештою практичне застосування.



Перша ручна телефонна станція Московської міської телефонної мережі на 800 номерів була відкрита в 1882 році у будинку № 6 на Кузнецькому мості. У списку її телефонних абонентів значилося 26 осіб. Це були в основному багаті комерсанти, промисловці, здатні дозволити собі таку «розкіш».

Телефонна станція працювала з однопровідними абонентськими лініями та використанням до-

шок системи Гілеланда ємністю 50 номерів кожна. Цей пристрій являв собою ручний комутатор з вертикальною панеллю та горизонтальним столом, на якому розташовувалися подовжні і поперечні латунні смуги товщиною у півміліметра. Ці смуги з'єднувалися вставним штепселем. Між вертикальною дошкою та горизонтальним столом розміщалися 50 (по одному на кожен номер) викличних клапанів, розташованих у два ряди.

Абонентські лінії підключалися до клем на зворотньому боці комутаторної дошки. Кожна з них з'єднувалася з електромагнітом відповідного викличного клапану та відповідних смуг на горизонтальному столі й вертикальній панелі. По мірі розширення станції до кожної дошки Гілеланда вмикалися сполучні лінії для зв'язку з іншими дошками станції. Наприклад, московська станція до кінця XIX століття мала 16 дошок з 90 сполучними лініями в кожній.

Абонентські пристрої в той час складалися з трубки Белла, мікрофона Блейка, індуктора і дзвоника Гілеланда та батареї елементів Лекланше. Ці телефонні апарати, що одержали назву Белла-Блейка, викликали масу дорікань, зокрема, через незручність розміщення мікрофона (він був вмонтований у корпус апарата, і щоб говорити, приходилося нахилятися), а також через велику взаємну індукцію однопровідних абонентських ліній та недосконалої підоймової системи, що найчастіше давала збої.

Користуючись своїм монопольним правом, компанія Белла встановила високу плату за користування телефоном – 250 карбованців у рік і, забезпечивши себе надвисоким прибутком, не прагнула вкладати кошти в удосконалення побудованої системи, навіть незважаючи на численні скарги. Нерідко абонент не міг з'єднатися з другим абонентом протягом декількох годин.

На кожній станції працювало одночасно декілька телефоністок. Одна з них, одержавши сигнал виклику, запитувала абонента, з ким він бажає встановити зв'язок. Якщо необхідний номер був увімкнутий до іншого комутатора, перша телефоністка голосно сповіщала про це іншу. Та, у свою чергу, переконавшись, що номер не зайнятий, з'єднувала його з вільною сполучною лінією, що вела до першого комутатора, і голосно оповіщала про це його телефоністку. І тільки після цього телефоністка, що одержала викличний сигнал, з'єднувала абонента. Внаслідок голосних розмов телефоністок, що створювали на станції шум і плутанину, часто виникали помилки у з'єднаннях.

На початку листопада 1901 року закінчився контракт компанії Белла на володіння московською телефонною мережею та за результатами закритого конкурсу (сучасними словами – тендеру) усі права

перейшли до Шведсько-Датсько-Російського акціонерного товариства, що почало свою діяльність з розширення та корінної реконструкції станційних і лінійних споруд мережі.

У Києві перші телефони було встановлено у 1884 році, які знаходились у ресторані «Семаден» і в магазині Попова, використовувались лише для внутрішнього зв'язку. А у 1885 році в місті розпочали створення першої телефонної станції в приміщенні поштової контори за адресою: вулиця Хрещатик, будинок № 24/26.

Днем народженням київського телефонного зв'язку стало 1 квітня 1886 року, коли урочисто була відкрита перша телефонна станція міста Київ. У день відкриття станції запрацювало 60 телефонів, а до кінця року їх було вже 175, з яких 10% знаходилися у квартирах, а 55% – у торгівельних фірмах, промислових закладах і адміністративних органах. Пізніше у Києві були відкриті 5 «говорильних» пунктів, де за 25 копійок можна було придбати 3-х хвилинну розмову з будь-яким абонентом. З 1895 року плату за розмови знизили до 15 копійок.

У 1893 році було закінчене будівництво першої в Україні міжміські телефонні лінії зв'язку між Одесою та Миколаєвом довжиною у 138 кілометрів. У 1898 році під керівництвом інженера Новицького було закінчене будівництво міжміської телефонної лінії зв'язку між Петербургом і Москвою, яка функціонувала на підвішених мідних дротах. Її довжина складала 618 верст. У той час вона була найдовшою в Європі. Комутатори для першої міжміської станції були закуплені в Бельгії. Аналогічні станції в наступні 20 років з'явилися в Одесі, Варшаві, Ризі й Лодзі. За забезпечення зв'язку російського імператора відповідали Управління начальника військових сполучень і Чергового генерала при Головній квартирі Його Імператорської Величності.

Основою для проектування АТС став створений російським винахідником Фрейденбергом у 1895 році предшукач і його принцип вільного шукання. Він, працюючи над автоматизацією зв'язку, прагнув знайти рішення, що би зробило АТС рентабельніше ручної станції такої ж ємності. У 1896 році Фрейденберг створив лінійний шукач на 1 тисячу ліній із загальним багаторазовим полем для групи шукачів, а потім – груповий шукач. Макет АТС останньої системи, що була названа «машинною», пройшов успішні випробування в Парижі у 1898 році. Перша така АТС була створена у 1900 році в США.

У червні 1902 року в Москві у Милютинському провулку (нині – вул. Мархлевського) було розпочате спорудження нового багатоповерхового будинку Центральної телефон-

ної станції ємністю 60 000 номерів. У ньому брали участь шведські фахівці, що застосували досвід будівництва аналогічної станції в Стокгольмі. До 1913 року телефонний зв'язок по мідних двопроводових лініях був встановлений між Москвою та Харковом, Рязанню, Нижнім Новгородом і Костромою, між Петербургом і Ревелем, Гельсінгфорсом і між Баку та Тифлісом. Усього ж тоді функціонувало 87 міжміських телефонних ліній.

До 1917 року єдиним видом комутаторного устаткування далекого зв'язку, виробленого в Росії, були ручні «земські» комутатори російського акціонерного товариства «Еріксон». На первісному етапі розвитку телефонії вони цілком відповідали необхідним вимогам. Але зі зростанням кількості абонентів розпочалося районування телефонних мереж – встановлення станцій у кожному районі міста.

Використання так званих «ручних» станцій погано вписувалося в цей процес через ряд значних недоліків. Станції з'єднувалися за принципом «кожна з кожною», і при великій кількості районних станцій знижувалося використання устаткування міжстанційних сполучних ліній. До цього варто додати й більші витрати кабелю, а отже, і фінансові витрати.

У Києві у 1892 році нараховувалось вже 409 абонентів та 479 телефонних апаратів, а станція мала 9 комутаторів, і все це господарство обслуговувалось 37-ми працівниками. На кожен комутатор припадало до 200 з'єднань за добу. У 1893 році була споруджена ще одна станція на Подолі, що мала 300 номерів.

Історичною для Києва стала весна 1901 року, коли була змонтована перша телефонна каналізація. У траншею укладались циліндричні бетонні труби на 12 та 24 канали, діаметр кожного з яких був 90 міліметрів. Колодязі телефонної каналізації будувались «серйозно та надовго».

В подальші роки модернізація продовжувалась. В 1904-1912 роках ємність кабельних мереж зросла до 4000 пар, а ємність станції до 4200 номерів. Покращилась також і якість зв'язку. Але попереду виникли нові ускладнення – попит на телефонний зв'язок значно перевищував технічні можливості телефонної мережі, і вже у 1912 році всі ємності були задіяні та технічні можливості для розвитку вичерпано. На той час телефонна щільність складала

0,9 телефону на 100 киян.

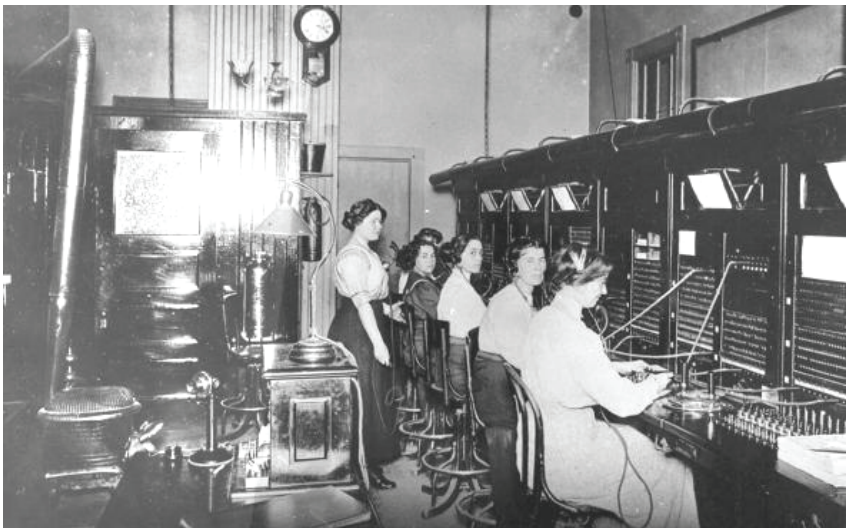
Новим етапом розвитку електрозв'язку було закладення фундаменту нового приміщення Міської телефонної мережі замість старого за тією ж адресою. Сталося це 12 липня 1912 року. Слід зазначити, що ця будівля стоїть і досі та розміщується там Державна Радіокомпанія України.

Роботу з реконструкції приміщення було закінчено у жовтні 1914 року. Незабаром якість зв'язку покращилась, а попит значною мірою був забезпечений. У цьому ж році телефонна щільність уже склала 1,6 апарата на 100 мешканців Києва. Киян тоді було 261 тисяча, а телефонів в мережі – 4178.

АТС із машинним шукачем у Росії почали поширюватися тільки з 1929 року з відкриттям у Ростові-на-Дону першої АТС ємністю 6 тисяч номерів, а у 1930 році – двох АТС у Москві на 8 і 7 тисяч номерів. Побудову цих станцій здійснював Ленінградський завод «Червона зоря» за технічною та технологічною документацією шведської фірми «Еріксон».

24 червня 1934 року Київ став столицею України, та з цього моменту для розвитку українського електрозв'язку наступив новий етап – більш жвавого та інтенсивного розвитку. Саме в той час і виникло окреме підприємство – Київська міська телефонна мережа (КМТМ). Вже у липні 1934 року була введена в експлуатацію АТСДК на 900 номерів. Ця АТС безпосередньо обслуговувала урядові установи. Проектом реконструкції КМТМ передбачалось будівництво 4-х АТС та оновлення лінійно-кабельного господарства.

У жовтні 1935 року з введенням в експлуатацію АТС ємністю 10 тисяч номерів,



на неї були переключені всі 6650 абонентів з ручної телефонної станції «ЦБ». Друга АТС машинної системи на 6 тисяч номерів, що знаходилась на вул. Хрещатик, почала працювати в 1937 році. Третя станція такого ж типу, ємністю 1500 номерів, що знаходилась на вул. Грушевського, була введена в експлуатацію в наступному році. В тому ж році запрацювала і станція на 4 тисячі номерів на вул. Нижній Вал.

У 1937 році телефонна щільність збільшилась із 1,2 після громадянської війни до 3,5 номера на 100 мешканців столиці. У кінці 1939 року ємність АТС в Києві складала 22400 номерів, магістральна кабельна мережа нараховувала 25000 пар. До 1 січня 1941 року на телефонній мережі діяло близько 19 тисяч телефонів та 10 тисяч були включені в різні відомчі станції та мали можливість виходу на мережу міста.

6 листопада 1943 року в столиці були змонтовані підстанції ручного обслуговування типу «ЦБ» ємністю 200 та 300 номерів. У січні 1944 року запрацювала ручна телефонна станція «ЦБ» ємністю 1000 номерів. Одночасно монтувалась АТС машинної системи на 4 тисячі номерів, яка була здана в експлуатацію 24 серпня того ж року. А в січні 1945 року вже розвернулось будівництво АТС декадно-крокової системи.

Наступний етап удосконалення вітчизняних АТС почався в 1947 році, коли радянські фахівці розробили нову систему АТС – декадно-крокову (АТС-47). Її впровадження в експлуатацію відбулося в 1949 році. Основними комутаційними елемен-

тами АТС декадно-крокової системи стали столінійні підйомно-обертальні шукачі *(ДШИ-100)*, обертальні шукачі *(ШИ-11)* і пласкі телефонні реле *(РПН)*.

А світова телефонна індустрія в цей час працювала над створенням більш сучасних АТС. Для керування АТС застосовувалися безконтактні комутаційні елементи – електронні та іонні лампи, електронно-променеві трубки, напівпровідникові прилади тощо. У 1954 році в Осло була введена в експлуатацію механо-електронна АТС на 2 тисячі номерів, що була запропонована бельгійськими інженерами. У тому же році в Англії був випробуваний перший макет АТС, повністю побудованої на електронних приладах. Так починалася нова ера телефонії – електронна.

5.2. Народження урядового зв'язку

Велику роботу з організації зв'язку революціонери-більшовики провели напередодні жовтневого збройного повстання у 1917 році. Для керівництва збройним повстанням Петроградська Рада робітничих і селянських депутатів утворила Військово-революційний комітет (далі – ВРК) під головуванням М.Подвойського, який розміщався у Смольному інституті. До складу ВРК увійшов відділ зв'язку, що відповідав за роботу центральної телефонної станції Смольного інституту та підтримку прямих ліній зв'язку з регіонами можливих військових дій.

З перемогою революції Петроградська Рада стала головним виконавчим органом нового уряду. Змінилося і призначення засобів зв'язку: із засобів керування збройним повстанням вони перетворилися в засоби керування державним апаратом. Зв'язок «Смольного» став, власне кажучи, урядовим зв'язком, тому що він став використовуватися винятково для обслуговування вищих державних органів влади. У систему цього зв'язку ввійшли центральна телефонна станція «Смольного», локальні станції, телеграф «Смольного» та Царскосельська радіостанція.

Після утворення вищих органів державного управління – Всеросійського Центрального Виконавчого Комітету (далі – ВЦВК) і Ради Народних Комісарів (далі – РНК) – колишній відділ зв'язку ВРК увійшов у повному складі в апарат ВЦВК. Головним завданням відділу, керівником якого став М.Ф.Андреєв, тепер було забезпечення телефонним і телеграфним зв'язком ВЦВК і РНК. У той час у кожному відомстві не було можливості мати своїх фахівців зв'язку, тому кожен надійний зв'язківець був на особливому рахунку.

Голова РНК В.Ленін наполягав на тому, щоб урядовий зв'язок діяв безперебійно в будь-яких ситуаціях, був якісним і, найголовніше, забезпечував таємність переговорів. Для виконання цих вимог в основу орга-

нізації зв'язку були покладені наступні принципи: забезпечення зв'язку по дротах, спеціальний відбір обслуговуючого персоналу, встановлення суворого порядку користування засобами зв'язку, застосування спеціальних шифрів і умовних сигналів.

Під час громадянської війни в Радянській республіці активно розвивався військовий зв'язок. Були проведені заходи з метою забезпечення централізованого керівництва військовим зв'язком і чіткою взаємодією органів військового зв'язку з установами Народного комісаріату пошти і телеграфів (далі - НКПіТ). У травні 1918 року до складу НКПіТ був введений відділ військового та військово-морського зв'язку.

Основа урядового зв'язку була закладена в 1918 році при переїзді Радянського Уряду до Москви. Силами фахівців відділу зв'язку ВЦВК, НКПіТ, а також Московської міської телефонної мережі була спроектована та побудована мережа урядового зв'язку в Кремлі. У вересні 1918 року в телефонній кімнаті Кремля був встановлений 100-номерний концентратор прямих проводів «ЦБ-100/20».

У січні 1919 року для роботи на концентраторі, що був встановлений у телефонній кімнаті Голови РНК, були введені 3 посади телефоністок. Із цього моменту концентратор став спеціальним комутатором мережі зв'язку уряду, до якої були включені 104 абоненти. У серпні 1920 року було прийнято «Положення про відділ зв'язку» Кремля.

У вересні того ж року з метою покращення керівництва військовим зв'язком була введена посада Надзвичайного комісара пошт і телеграфів при Головнокомандувачу Збройними Силами республіки. У той же час при штабах фронтів були створені поштово-телеграфні відділи НКПіТ, що відповідали за забезпечення зв'язку Головкому, штабів фронтів і армій. Військовим зв'язком у вищій ланці займалися Центральне управління військових повідомлень, НКПіТ і Головне військово-інженерне управління.

Місяцем пізніше РНК був затверджений вищий орган з керівництва зв'язком у країні – Верховна комісія телеграфного зв'язку (Верхкомтель). У 1918 році активно створювалися радіомагістралі, що зв'язали Москву з найбільшими адміністративними центрами республіки, а також зі столицями Франції, Німеччини та Туреччини.

Наприкінці 1918 року нарком пошти і телеграфів В.Подбельський вніс пропозицію до Управління справами ВЦВК про виведення переговорної станції Кремля з підпорядкування ВЦВК і злиття її з міським телеграфним відділенням при РНК в одне відділення зв'язку. Керівник справами ВЦВК погодився з

пропозицією, і до кінця січня 1919 року зявилось 29-е міське відділення зв'язку.

Таким чином, відділ зв'язку перетворився на орган, що відав тільки телефонним зв'язком уряду, що підтверджувалося рядом рішень, прийнятих Президіумом ВЦВК у жовтні 1920 року та стосувалися, зокрема, відділу зв'язку Кремля. Змінився і статус відділу: після виділення з його складу телеграфного переговорного пункту РНК він ставав підвідділом зв'язку ВЦВК, який відповідав за забезпечення керівників партії та уряду телефонним зв'язком і ставився в подвійне підпорядкування: з питань обслуговування керівників партії та уряду - РНК і ВЦВК, а з технічної політики в частині перевлаштування мережі і підвищення якості зв'язку Кремля - Управлінню Московської телефонної мережі (далі - УМТМ).

При цьому начальник зв'язку Кремля, що був відповідальною особою за роботу зв'язку уряду, призначався ВЦВК; телефоністки, які обслуговували «верхній» і «нижній» комутатори, входили, відповідно, до штатів РНК і ВЦВК; штат працівників, призначених для обслуговування лінійно-кабельного господарства, визначався УМТМ. Кадри, укомплектовані за цим штатом, виділялися відділу зв'язку Кремля на правах прикомандированих - старший групи (механік або технік) прикомандированого складу входив у відділ зв'язку Кремля на правах помічника або заступника начальника зв'язку Кремля.

Військовий зв'язок радянської республіки також розвивася. Так, 20 листопада 1919 року був виданий наказ Революційної Військової Ради (далі – РВР) про створення Управління зв'язку РСЧА. На фронтах були сформовані управління зв'язку фронтів, в арміях і дивізіях – відділи зв'язку, введені посади начальників зв'язку фронту та армії. Цей день вважається датою створення військ зв'язку РСЧА як самостійних військ.

До кінця 1919 року в телефонній кімнаті Кремля з'явилися телефонні апарати прямого зв'язку з фронтами. У лютому 1920 року сформований спеціальний загін зв'язку Штабу РСЧА, а в травні того ж року – радіотелеграфний дивізіон для забезпечення зв'язку у вищій ланці керівництва фронтами та арміями.

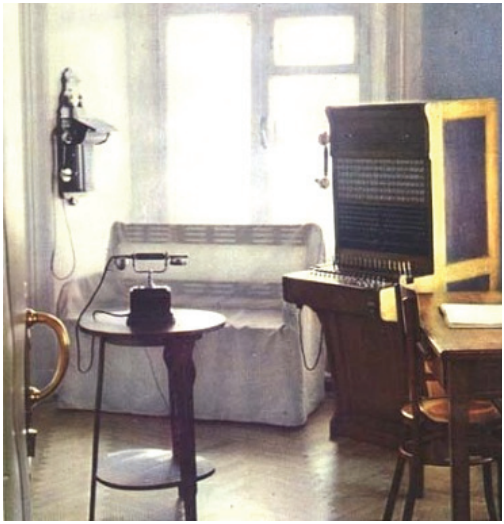
До кінця 1920 року для керування фронтами, арміями та укріпленими районами було сформовано: 1 спеціальний потяг зв'язку, 13 окремих батальйонів

зв'язку, 18 окремих телеграфно-телефонних дивізіонів, 40 телеграфно-експлуатаційних рот, 75 телеграфно-телефонних рот, 13 окремих рот зв'язку, 3 радіобази, 16 окремих радіодивізіонів, 38 окремих радіостанцій, 8 рот «летючої» пошти, 21 склад зв'язку, 25 майстерень зв'язку, 26 дислокаторних поштових відділення.

Незважаючи на значну перевагу радіозв'язку в порівнянні з проводовими засобами зв'язку, для яких були необхідні постійні повітряні лінії великої довжини, майже весь зв'язок вищого військового керівництва того часу базувався на використанні повітряних ліній зв'язку та окремих проводів. Часткова відмова від радіозв'язку було обумовлена тим, що стало відомо про успіхи білогвардійських служб радіоперехоплення та дешифрування. Саме тому зв'язок Штабу РВР зі штабами фронтів і армій здійснювався по окремих проводах через польові телеграфні контори, як правило, з використанням апаратів Бодо, Юза та Уітстона. Телефонний зв'язок застосовувався на невеликі відстані, в основному, в оперативній ланці.

17 серпня 1920 року РНК було прийняте рішення про закупівлю за кордоном першої АТС та монтаж її в Кремлі. 20 вересня 1921 року фірма «Сіменс» поставила замовлене устаткування, однак технічної документації у пакувальних ящиках не виявилося. Крім того, АТС була 3-проводовою, як і усі на Заході, тому протягом 1922 року її довелося самотужки переробляти на 2-проводовий режим роботи. 17 лютого 1923 року перша АТС ВЦВК була введена в дію. Це був початок системи АТС-1, яка стала відомою як «вертушка». На відміну від звичайної телефонної мережі, де у той час з'єднання відбувалося через телефоністку, абоненти з'єднувалися один з одним за допомогою АТС і дискового номеронабирача.

В середині серпня 1921 року були затверджені положення та інструкції управлінь і установ ВЦВК, в яких було визначено місце та функції кожного підрозділу найвищого законодавчого органу держави. Згідно «Положенню про підвідділ зв'язку», останній був підпорядкований Управлінню справами ВЦВК і забезпечував функціонування «верхнього» і «нижнього» комутаторів, а також АТС Кремля, роботи з монтажу якої у той час вже велися. Це означало, що будь-які розпорядження організаційно-технічного характеру (зокрема підключення телефонних апа-



ратів до мережі ВЦВК) могли виходити тільки від керівника справами ВЦВК або його заступника.

Зміна штатній чисельності підвідділу зв'язку (вона зросла до 31-ї одиниці за рахунок введення посад механіків з обслуговування АТС Кремля) і ускладнення виконуваних завдань в результаті введення в його підпорядкування Кремлівської АТС не вплинули на зміну статусу підвідділу. По мірі налагодження роботи АТС підрозділ піддавався неодноразовим скороченням. Так, рішенням комісії зі скорочення штатів службовців апарату ВЦВК від 7 травня 1923 року підвідділ зв'язку був скорочений на 3 одиниці зі встановленням штату у 26 одиниць.

Крім істотних зрушень в якісних і кількісних характеристиках інфраструктури електрозв'язку країни, 1920-і роки ознаменувалися цілим рядом реорганізацій структур спеціального зв'язку уряду. Це було обумовлено, перш за все, утворенням СРСР, внаслідок чого на порядок денний встало завдання розмежування повноважень законодавчих і виконавчо-розпорядчих органів влади РРФСР і новостворюваних аналогічних союзних органів. У структур, покликаних забезпечувати зв'язком вищі ешелони влади, обсяг завдань в цей час істотно зріс.

По мірі створення загальносоюзних органів управління вони ставали абонентами урядової мережі зв'язку. Поки йшло становлення союзних органів влади, а потім - робота комісій з розмежування повноважень між союзними і республіканськими органами влади, технічні служби владних структур РРФСР несли тягар турбот щодо забезпечення функціонування та обслуговуванню як своїх, російських органів, так і всесоюзних. Це вимагало від нечисленного підвідділу зв'язку ВЦВК постійної і кропіткої роботи. Разом з тим, штат його продовжував залишатися таким же.

Робота з розмежування функцій союзних і республіканських органів, результати якої безпосередньо торкнулися підвідділу зв'язку ВЦВК, була розпочата у 1923 році заходами щодо скорочення штатів технічних і допоміжних служб ВЦВК і впорядкуванню їх діяльності. Проміжним результатом цих зусиль з'явилося скасування 1 грудня 1923 року Управління справами ВЦВК і Управління Кремлем і будинками ВЦВК з передачею їх функцій знов організованому адміністративно-господарському відділу (далі - АГВ) ВЦВК.

АГВ, у свою чергу, складався з трьох підвідділів: адміністративного, господарського і житлово-експлуатаційного (далі - ЖЕП). Статус підвідділу зв'язку знижувався, він ставав відділенням зв'язку у складі ЖЕП. Услід за загальною реорганізацією установ ВЦВК було проведене також істотне їх скорочення. Якщо до цього ЖЕП налічував у своєму складі 563 людини, то після реорганізації - тільки 185. Примітно, що цей процес не торкнувся підрозділу зв'язку Кремля.

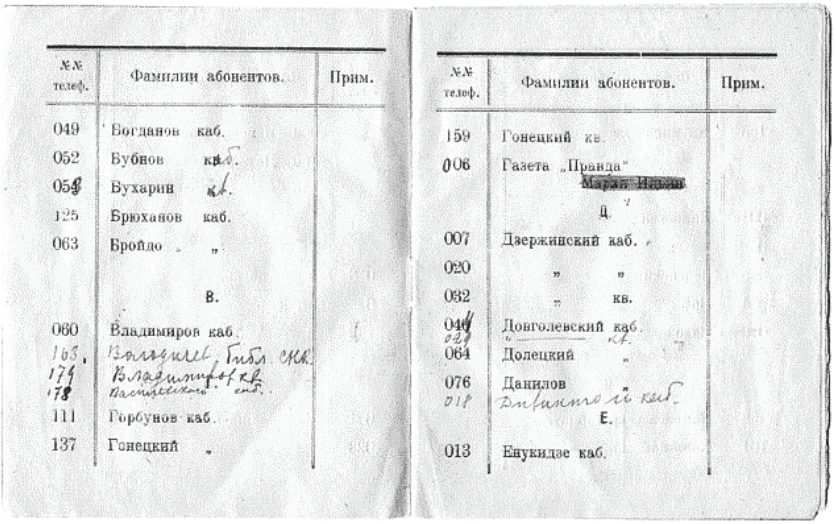
У грудні 1924 року штат відділення зв'язку був навіть збільшений і доведений до 34 одиниці. А 7 липня 1926 року АГВ ухвалою секретаріату Президіума ВЦВК був

перейменований у господарський відділ (далі - ГВ). Відділення зв'язку на той момент налічувало в своєму складі 33 людини, а всього у 1926 році у ГВ працювало 210 співробітників. Начальником відділення, як і раніше, був М.Ф.Андреєв.

До 1928 року всі організаційні узгодження між республіканськими та союзними органами державної влади були завершені. Відділення зв'язку ВЦВК передавалося у ведення союзного ЦВК, а штати його збільшувалися за рахунок механіків і монтерів АТС, внаслідок чого чисельність відділення була доведена до рівня, необхідного для нормального функціонування урядової мережі зв'язку. Організаційно цей підрозділ, знов реорганізований у підвідділ зв'язку, додавався цивільному відділу Управління Коменданта Московського Кремля (далі - УКМК) НКО, службовці якого вже у той час перебували на службі в ОДПУ.

В результаті наступних реорганізацій підвідділу, в структурі УКМК у 1935 році був утворений відділ технічного зв'язку, який у 1936 році був переданий разом з УКМК до складу НКВС. Надалі, вже в післявоєнні роки, цей відділ був об'єднаний з відділом зв'язку Головного управління охорони МДБ, і на знов утворене формування була покладена відповідальність за організацію міського урядового зв'язку в Москві.

Наприкінці 1920-х років в умовах політики жорсткої централізації, що проводилася вищим партійно-державним керівництвом СРСР, дозріла найгостріша необхідність у вдосконаленні системи управління державою та його найважливішими інститутами. При цьому функцію телекомунікаційної основи управління повинна була реалізувати система відокремленого елітного спеціального зв'язку, яка б дозволяла забезпечити не тільки оперативність переговорів, але і конфіден-



№№ телеф.	Фамилии абонентов.	Прим.
049	Богданов каб.	
052	Бубнов кв.	
054	Бухарин кв.	
125	Брюханов каб.	
063	Бройдо „	
	В.	
060	Владимиров каб.	
111	Горбунов каб.	
137	Гонецкий „	

№№ телеф.	Фамилии абонентов.	Прим.
159	Гонецкий кв.	
006	Газета „Правда"	
	Д.	
007	Дзержинский каб.	
020	„ „	
032	„ кв.	
046	Довголевский каб.	
064	Долецкий „	
076	Данилов „	
	Е.	
013	Енукидзе каб.	

ційність передаваної по її каналах інформації.

Завдання створення подібної системи зв'язку з 1 грудня 1929 року було покладене на Оперативний відділ (далі - ОВ) Секретно-оперативного управління (СОУ) ОДПУ, у складі якого для цього було утворене 4-е відділення. Саме цей підрозділ, крім забезпечння усіма видами зв'язку підрозділів ОДПУ та контролю телефонної мережі, прийняв на себе відповідальність за організацію і створення мережі міжміського високочастотного (далі - ВЧ) телефонного урядового зв'язку. Начальником відділення до 7 червня 1936 року був Іван Юрійович Лоренс. НКВС також не залишилось осторонь цього завдання, де у 1928 році за розпорядженням Сталіна була створена група секретного зв'язку.

Зв'язок називався ВЧ, тому що по проводах передавався струм високої частоти, модифікований звуковим сигналом від мембрани мікрофону телефонного апарату. Такий сигнал, як і сигнал радіозв'язку, не сприймався людським вухом без відповідної обробки, тому сприяв конфіденційності переговорів і не піддавався простому перехопленню, оскільки звичайним телефонним апаратом підслухати було неможливо.

До середини 1930-х років у якості пристроїв ВЧ ущільнення на каналах урядового міжміського зв'язку використовувалася, в основному, апаратура імпортного виробництва (головним чином, «Телефункен»), і лише в окремих випадках - дослідні зразки аналогічної вітчизняної апаратури. Важливо підкреслити, що в кінці 1920-х - першій половині 1930-х років застосування принципу ВЧ телефонування (перенесення розмовного частотного спектру у ВЧ область) вважалося гарантом забезпечення конфіденційності телефонних переговорів. Тому організація урядового зв'язку по каналах низької частоти (далі - НЧ) допускалася лише у виняткових випадках.

Цей чинник зумовив необхідність упровадження на мережі міжміського урядового зв'язку вітчизняної апаратури високої частоти (далі - ВЧ). Завдання організації виробництва подібної апаратури тривалий час значно випереджала економічні можливості країни. Річ у тому, що перші досліди багатоканального телефонування в СРСР проводилися ще у 1921 році колективом інженерів радіовідділу та радіолабораторії московського заводу «*Электросвязь*» під керівництвом В.М.Лебедєва.

У тому ж році по кабельній лінії була здійснена одночасна передача 3-х телефонних розмов. У 1923 році учений П.В.Шмаков закінчив досліди з одночасної передачі 2-х телефонних переговорів на ВЧ і одного - на НЧ по кабельній лінії протяжністю 10 кілометрів. А у 1925 році на ленінградській науково-випробувальній станції під керівництвом П.Азбукіна була вперше розроблена та виготовлена апаратура ВЧ телефонування для мідних ланцюгів.

Перший зразок вітчизняної одноканальної апаратури ущільнення був встановлений у 1926 році на лінії Ленінград - Бологоє. А у 1930 році були побудовані

перші лінії міжміського ВЧ зв'язку Москва - Ленінград та Москва - Харків (столиця України) через Тулу, Орел і Курськ.

Наказом ОДПУ № 308/183 від 10 червня 1931 року була введена (з 1 червня) нова структура ОДПУ, згідно з якою 4-е відділення ОВ СОУ стало 5-м відділенням ОВ ОДПУ. На нього було покладено завдання щодо забезпечення державних високопосадовців секретним телефонним ВЧ зв'язком. З того часу 1 червня в СРСР було прийнято вважати офіційним днем народження урядового міжміського зв'язку.

10 липня 1934 року ОДПУ увійшло до складу НКВС як ГУДБ, а його регіональні органи увійшли до складу регіональних управлінь НКВС. ОВ ОДПУ був реорганізований в ОВ ГУДБ. У тому же році була введена в дію станція урядового зв'язку в Києві. З 25 грудня 1936 року ОВ став 2-м відділом ГУДБ, у складі якого відділення урядового ВЧ зв'язку (далі - ВУЗ) стало 3-м відділенням.

Починаючи з червня 1936 року до керівництва ВУЗ прийшли люди, обізнані з теорією та практикою організації зв'язку. Начальником відділення був призначений Іван Якович Воробйов, який до цього очолював відділення зв'язку АГУ НКВС. Помічником начальника відділення був призначений Ігор Васильович Вінецький, який у 1928-1936 роках працював на посаді інженера для доручень при заступнику наркома зв'язку та одночасно співробітника ОВ. Старшим техніком-інженером був призначений Михайло Ілліч Ільїнський, молодий фахівець, який вже мав наукові роботи в сфері електрозв'язку.

Споруджені наприкінці 1920-х і на початку 1930-х років ВЧ лінії урядового зв'язку були надзвичайно витратні в експлуатації. Якщо на етапі впровадження цікавих радіоінженерних напрацювань усе було добре, то при їхній експлуатації проявлялися недоліки. Так, більше 300 абонентів «кремлівської» системи урядового зв'язку обслуговувалися по всій країні відразу 80 станціями, а для ущільнення сигналу на лініях використовувалася вітчизняна апаратура. Щоб уникнути неполадок, в Англії для ВУЗ був закуплений спеціальний комутатор фірми «Стандарт». Завдяки йому

Первая отечественная установка ВЧ-телефонирования. С мая 1926г. работала на линии железной дороги Ленинград - Бологое.

користувачі «кремльовки» могли зв'язуватися один з одним в автоматичному режимі (так званий «негайний» зв'язок), або робити попередні замовлення через телефоністку. Крім того, якщо ВЧ-лінія була вільна, по ній можна було передавати й урядові телеграми.

Недостатня розвиненість радіотехнічної промисловості та нечисленність кваліфікованих кадрів були серйозними перешкодами на шляху організації розробки та серійного виробництва вітчизняної апаратури ВЧ телефонування і телеграфування, зокрема для урядового зв'язку. Лише завдяки зусиллям інженерно-технічного складу у 1934 році на заводі «*Красная Заря*» в Ленінграді (нині – Санкт-Петербург), директором якого був з 1933 року М.В.Ясвойн, була закінчена розробка й почалося крупносерійне виготовлення 3-канальної апаратури ВЧ телефонування СМТ-34 (система багатоканального телефонування 1934-го року). Вона працювала в діапазоні 10,4 - 38,4 кГц та забезпечувала задовільну якість зв'язку на відстані до 2000 кілометрів.

Оснащення центральної та периферійних ВЧ станцій цим типом апаратури ущільнення повітряних ланцюгів дозволило до кінця 1930-х років практично виключити використання на мережі міжміського урядового зв'язку подібної апаратури іноземного виробництва. У 1936 році при будівництві повітряних магістралей зв'язку №№ 557-558 Харків - Сімферополь було створено станцію ВЧ-зв'язку в Запоріжжі. Наказом по Управлінню НКВС УРСР по Запорізькій області № 224 від 03.07.1939р. «про зміни в штатах УНКВС» до штату 2-го спецвідділення (ВЧ зв'язок) додатково було введено 4 посади. Тоді ж на телефонній станції, що ослуговувалася штатом із 4-х осіб, було встановлено комутатор «ЦБ» ємністю на 200 абонентів.

У той же час було відкрито станцію ВЧ зв'язку у Севастополі та організовано урядовий ВЧ-зв'язок на території Криму при будівництві магістральної лінії Москва-Севастополь через Харків і Запоріжжя. До 1936 року ВЧ-зв'язок був встановлений з 12 адміністративними центрами СРСР, зокрема із Смоленськом і Мінськом (1932), Горьким (нині – Нижній Новгород) і Ростовом (1933), Києвом (1934), Ярославлем, Тбілісі і Севастополем (1936). А до 1937 року в мережу ВЧ зв'язку були включені 10 урядових дач Чорноморського узбережжя.

До того ж збільшення кількості периферійних станцій та числа абонентів урядового зв'язку, що ними обслуговувалися, потребувало налагодження виробництва АТС. Тому ще у 1937 році на заводі «*Красная Заря*» під керівництвом і за безпосередньою участю

Ільїнського була розроблена перша міжміська АТС для ВЧ-зв'язку на 5 абонентів і 10 каналів «МА-5» та її зменшений варіант на 3 абоненти «МА-3». У 1938 році ця апаратура, що дозволяла здійснювати автоматичне з'єднання абонентів, пройшла державні іспити, а з початку 1939 року поступила в серійне виробництво. А для станцій урядового зв'язку у тому же році була розроблена спеціальна установка - стояк буферного електроживлення, що забезпечував роботу ВЧ-станцій у польових умовах і при виході з ладу джерел електроживлення загального користування.

Таким чином, протягом всього трьох років (1934-1937) був здійснений істотний стрибок у галузі розвитку вітчизняних засобів електрозв'язку, що дозволив створити передумови для впровадження на мережі урядового зв'язку каналоформуючої (ВЧ телефонування і телеграфування) та комутаційної апаратури, що відповідала б вимогам часу.

Розвиток мережі міжміського урядового зв'язку стимулювався ще і тією обставиною, що у 1930-і роки в СРСР було розгорнуто активне будівництво магістральних постійних повітряних ліній зв'язку середньої і великої протяжності. Необхідність їх введення в експлуатацію диктувалася збільшеними вимогами до системи управління в ході індустріалізації, а також зміцненням обороноздатності держави. У кожному окремому випадку керівництвом НКВС, як правило, виносилося клопотання про передачу наркомату виділених ВЧ каналів для організації урядового міжміського зв'язку.

З 7 серпня 1937 року ВУЗ як 8-е відділення увійшло до складу 12-го відділу (оперативної техніки) ГУДБ, який був утворений наказом НКВС № 00464. На укомплектовування цього відділу були виділені штати та особовий склад 5-го, 6-го, 7-го, 8-го і 9-го відділень 2-го відділу ГУДБ, 5-го відділення 9-го відділу ГУДБ і спецгрупи 3-го відділу ГУДБ.

З 23 вересня 1937 року ВУЗ було перейменоване у 3-е відділення 12-го відділу. З 9 червня 1938 року наказом НКВС № 00378 відділ був перейменований у 2-й спецвідділ, а ВУЗ у його складі став 3-м відділенням. Його начальником став лейтенант держбезпеки Воробйов, а його помічником - лейтенант держбезпеки Ільїнський.

Спецвідділ здійснював так звану мікрофонну та телефонну роботу, проводив перлюстрацію, обслуговував урядові органи урядовим ВЧ-зв'язком, виготовляв необхідні в оперативній роботі відділів різного роду документи, вів перехоплення радіопередач закордонних станцій, виявляв нелегальні станції на території СРСР, проводив секретні виїмки. Окрім обслуговування оперативних відділів НКВС технічними засобами спостереження, 2-й відділ ГУДБ займався і проведенням науково-дослідних і експериментальних робіт у цій сфері.

Важливої віхою в розвитку урядового міжміського зв'язку як усієї радянської країни, так і України зокрема, став 1938 рік, і перш за все тому, що протягом цього року (вперше з початку розвитку ВЧ-зв'язку) Урядом СРСР було прийнято 3 поста-

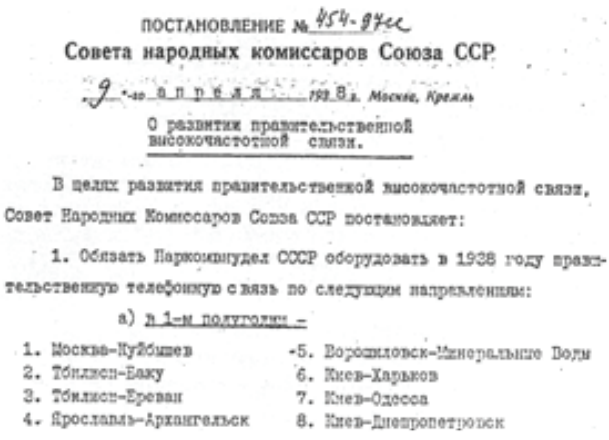
нови з однаковою назвою «Про розвиток урядового ВЧ зв'язку». Перша постанова № 53/ко від 5 січня 1938 року було націлена винятково на зміцнення матеріально-технічної бази урядового зв'язку, зокрема, у ній передбачалася розробка й постачання міжміських АТС для НКЗ України. Інші постанови № 454-97сс від 9 квітня і № 1240-300сс від 17 листопаду 1938 року передбачали розширення мережі урядового міжміського зв'язку та налагодження роботи станцій ВЧ телефонного зв'язку на таких напрямках, як Київ-Харків, Київ-Одеса і Київ-Дніпропетровськ.

Організація нових ВЧ-станцій і встановлення нових апаратів ВЧ-зв'язку проводилися тільки з санкції наркома внутрішніх справ або його першого заступника. Включення ж нових міст у мережу ВЧ-зв'язку та оснащення її спеціальною технікою здійснювалося відповідно до рішень РНК СРСР.

Розширення мережі урядового міжміського зв'язку набувало, таким чином, все більш планомірного характеру. По урядових каналах, що вперше відкривалися, забезпечувалися такі види зв'язку:

- автоматичне з'єднання абонентів «кожного з кожним» (так званий негайний зв'язок);
- з'єднання абонентів за допомогою телефоністок за попереднім замовленням (якщо лінія на момент замовлення зайнята);
- передача телеграм по ВЧ каналу за допомогою тонального телеграфування з букводрукувальним апаратом (якщо лінія не зайнята телефонною розмовою).

Будівництво і монтаж нових станцій і цілих напрямків ВЧ-зв'язку здійснювалося, як правило, на підставі затверджених НКВС проектів і технічних завдань. Так, наприклад, в пояснювальній записці до «Проекту організації урядового ВЧ-зв'язку Москва-Хабаровськ (вересень-жовтень 1938 року)» наголошувалося: «Урядовий ВЧ-зв'язок повинен забезпечити чітке, оперативне і в той же час високоякісне обслуговування Уряду СРСР і керівництва НКВС телефонним зв'язком», а сам проект включав відомості необхідного устаткування, майна і матеріалів, перелік виконуваних підрядчиками робіт, а також креслення кабелірування і розміщення апаратури в приміщеннях ВЧ- станцій (всього на магістралі обладнува-



ПОСТАНОВЛЕНИЕ № 454-97сс
Совета народных комиссаров Союза ССР
9-го апреля 1938 г. Москва, Кремль
О развитии правительственной высокочастотной связи.

В целях развития правительственной высокочастотной связи, Совет Народных Комиссаров Союза ССР постановляет:

1. Обязать Наркомпочтель СССР оборудовать в 1938 году правительственную телефонную связь по следующим направлениям:

а) в 1-м полугодии –

1. Москва-Куйбышев
2. Тбилиси-Баку
3. Тбилиси-Ереван
4. Ярославль-Архангельск
5. Ворошиловск-Минеральные Воды
6. Киев-Харьков
7. Киев-Одесса
8. Киев-Днепропетровск

лося 8 станцій і більше 20 пунктів трансляцій).

Темпи введення в дію нових периферійних станцій ВЧ зв'язку були достатньо високими. Часто відомчі плани НКВС по розвитку мережі міжміського ВЧ-зв'язку значно випереджали урядові завдання. Так, у 1938 році було відкрито ВЧ-станцію у Вінниці, яка забезпечувала роботу 2-х напрямків зв'язку, один з яких – на Київ. До 1939 року ВЧ-зв'язком було охоплено такі українські міста, як Чернігів, Одеса, Дніпропетровськ, Полтава, Донецьк і Луганськ. Вже на початку 1939 року у країні функціонувало 58 ВЧ-станцій і 16 пунктів (1 резервний) трансляцій, а кількість абонентів досягла 290.

Протягом 1939 року кількість ВЧ станцій була доведена до 78, а пунктів трансляцій – до 28 (8 резервних). Кількість абонентів за рік збільшилося майже в півтора разу і досягло 430. У 1939 році були відкриті ВЧ станції в 24 містах країни: столицях союзних і автономних республік (2), центрах країв і областей (16), а також районних центрах і містах обласного підпорядкування (6), причому відкриття 4 крупних ВЧ-станцій (Іркутськ, Новосибірськ, Чита, Хабаровськ) було обумовлене введенням в експлуатацію магістралі Москва-Хабаровськ, що дозволило включити в сферу дії міжміського ВЧ зв'язку обширні регіони Забайкалля і Далекого Сходу.

Кожна з кінцевих і проміжних ВЧ станцій здійснювала експлуатацію не тільки своєї ділянки магістралі або напрямку урядовому зв'язку, але й абонентської мережі (сукупність ліній, прокладених до місць розташування конкретних абонентів, тобто, в даному випадку, до телефонних і телеграфних ВЧ апаратів).

При цьому абонентські пункти знаходилися деколи на значній відстані від приміщень станцій і навіть населених пунктів, в яких станції розміщувалися. Наприклад, до кінця 1938 року севастопольська ВЧ-станція обслуговувала 7 віддалених абонентських пунктів; сочинська – 3; мурманська, вінницька, ярославська – 1 тощо. Цей факт увів в обіг такий термін, як «вузол урядового зв'язку».

Оскільки окремі вузли обслуговували абонентські пункти на об'єктах, що ретельно охоронялися НКВС (наприклад, 10 урядових дач Чорноморського узбережжя), їх експлуатація була пов'язана з труднощами міжвідомчого

характеру. Із спогадів Петра Миколайовича Вороніна, що працював у 1940-1941 роках інженером ВУЗ: «На Кавказі і в Криму було декілька державних дач, на кожній з яких – своя станція урядового зв'язку. Станції були заздалегідь змонтовані, так що періодичне їх включення не викликало особливих труднощів. Але не завжди все йшло гладко».

Загальне керівництво експлуатацією та розвитком урядового зв'язку з 1938 року здійснювали:

- у центрі – начальник 2-го спеціального відділу НКВС і його заступник через начальника відділення урядового зв'язку;
- на периферії – начальники 2-х спеціальних відділів і відділень НКВС союзних республік, управлінь (УНКВС) країв і областей через начальників відділень (груп) урядового зв'язку.

Узгодження дій різних структурних підрозділів НКВС деколи здійснювалося на нарадах представників і керівників цих підрозділів. Одна з таких нарад, проведена 5 червня 1938 року, переслідувала мету упорядкувати процес функціонування Кавказького (сочинського) і Кримського (симферопольського) вузлів урядового зв'язку. Як випливає з протоколу наради, підписаного керівниками підрозділів зв'язку 1-го (охорона) і 12-го (оперативної техніки) відділів ГУДБ НКВС, був встановлений певний порядок обслуговування станційних і лінійних об'єктів ВЧ зв'язку. Згідно з ним, лінійні споруди (лінії зв'язку до ВЧ станцій) обслуговувалися відповідними підрозділами ГУПО або НКЗ (під контролем 12-го відділу ГУДБ), станційні споруди (ВЧ-станцій) – підрозділами 12-го відділу ГУДБ, а абонентські установки (телефонні апарати і працююче разом з ними устаткування) – підрозділами зв'язку 1-го відділу ГУДБ.

Така складна схема обслуговування абонентів пояснювалася тим, що до середини 1930 років засоби урядового та службового зв'язку в Москві, крім ВУЗ, обслуговувалися ще трьома підрозділами наркомату. У 1934 році був утворений відділ зв'язку АГУ НКВС, до завдань якого входило обслуговування спеціальним зв'язком оперативних підрозділів НКВС у Москві.

З 1935 року обслуговуванням телефонних станцій міського урядового зв'язку, кабельної мережі, абонентських установок в межах Москви і Московської області займався відділ технічного зв'язку УКМК. Одночасно існувало відділення зв'язку 1-го відділу, або відділу охорони ГУДБ НКВС, що обслуговувало урядовий зв'язок в кабінетах, на квартирах і дачах членів Політбюро ЦК ВКП(б) поза Кремлем.

«Станційне й кабельне господарство знаходиться в обслуговуванні декількох відділів, – писав заступник наркома внутрішніх справ В.М.Меркулов у доповідній записці наркому Л.П.Берії про підсумки перевірки московської телефонної урядової мережі у січні-лютому 1939 року, – внаслідок чого на цій ділянці роботи велика плутанина. Зважаючи на безсистемну організацію має місце розпилювання технічних сил, нераціональне використання матеріальних засобів і виробничих

можливостей». Аналогічна ситуація складалася і при обслуговуванні абонентів периферійних станцій.

Меркулов мав рацію, оскільки на вказаний момент тільки в Москві під егідою різних підрозділів НКВС функціонувало декілька станцій спеціального телефонного зв'язку:

- Станція Політбюро;
- Урядова АТС Кремля (так звана «вертушка»);
- Центральна станція міжміського ВЧ-зв'язку;
- станція 1-го відділу ГУДБ НКВС;
- станції Центрального і Московського комітетів ВКП(б);
- станція відділу зв'язку АГУ НКВС.

Лінійно-кабельне господарство московської урядової телефонної мережі також ділилося на ділянки, що знаходилися у веденні різних організацій, що істотно утрудняло вирішення завдань конфіденційності і якості зв'язку.

Оптимальним вирішенням виниклої міжвідомчої проблеми могло стати утворення на основі всіх перерахованих підрозділів спеціального зв'язку єдиного відділу урядового зв'язку з введенням його до складу ГУДБ НКВС. Проект наказу НКВС про подібну реорганізацію був підготовлений у січні 1939 року.

Запропонована структура відділу включала управління (начальник відділу, 3 заступники, політичний відділ і секретаріат) і 10 відділень (зв'язку охорони, зв'язку Кремля, міжміського зв'язку, радіозв'язку, нових розробок і лабораторій, будівництва і експлуатації, телефонного зв'язку НКВС, технічного постачання і майстерень, роботи з агентурою, кадрове).

Однак проект, що переслідував мету реконструкції як системи урядового, так і відомчого електрозв'язку СРСР, не був підтриманий вищим керівництвом НКВС, хоча надалі, вже після початку Великої Вітчизняної війни, саме він склав ідейну основу реорганізації системи урядового міжміського зв'язку в умовах військового часу. Можливо, у зв'язку з тим, що зусилля щодо реалізації цього проекту начальника ВУЗ лейтенанта держбезпеки Воробйова виявилися марними, він перейшов на посаду начальника іншого відділення 2-го спецвідділу. Разом з тим, з 1 травня 1939 року ВУЗ у складі 2-го спецвідділу НКВС стало називатися «відділенням урядового «ВЧ» зв'язку», а його начальником став старший лейтенант держбезпеки Ільїнський.

У жовтні 1939 року була завершена операція із захоплення Червоною Армією території Західної України, після чого розпочалася організація стаціонарної мережі ВЧ-зв'язку. Для цього у Львівському управлінні НКВС при 2-му спецвідділі була уведена посада начальника району ВЧ-зв'язку Західної України. Район складався з ВЧ-станцій у Львові, Тернополі, Станіславі (нині – Івано-Франківськ), Рівному, Луцьку та Дрогобичі, які організаційно входили до складу 2-х спецвідділів обласних управлінь НКВС. Самі ВЧ-станції обслуговувалися старшим техніком, трьома

техніками та телефоністками. Тривалий час вирішувалося питання про адміністративну посаду начальника ВЧ-станції, тому що старший технік був лише технічним виконавцем й адміністративних питань не вирішував.

На нараді в Москві було прийняте рішення про те, щоб начальника ВЧ-станції називати «оперуповноваженим», який матиме право вирішення питань забезпечення конспірації ВЧ-зв'язку на телефонних станціях Наркомату зв'язку та оперативних питань. Він мав на зв'язку декількох інформаторів серед співробітників Наркомату зв'язку, які мали відношення до каналів, що використовувались в інтересах ВЧ-зв'язку. А у Львові замість начальника району ВЧ-зв'язку була введена посада начальника відділення. Така структура існувала аж до початку Великої Вітчизняної війни.

Наприкінці 1939 року кількість ВЧ-станцій досягла 78, трансляційних пунктів – 28, абонентів урядового зв'язку – 430. За період 1939-1940 років були відкриті ВЧ-станції в Рівному, Луцьку, Тернополі, Станіславі та Дрогобичі.

Таким чином, на даному етапі забезпечення секретності урядового зв'язку досягалося за рахунок розробки і впровадження нової апаратури засекречування переговорів і активної реалізації цілеспрямованих оперативних заходів. Поєднання матеріально-технічного і оперативного забезпечення секретності інформації, що передавалася по каналах і лініях урядового зв'язку, стало принциповим положенням і отримало подальший розвиток у всі подальші роки.

До кінця 1930-х років система урядового міжміського зв'язку все більше набувала рис загальнодержавної. Її абонентами стали сотні керівних працівників партійних, радянських і господарських органів у центрі і на місцях. В той же час, знаходячись у веденні НКВС, система ВЧ-зв'язку продовжувала функціонувати і як система відомчого (оперативного) зв'язку наркомату, причому зростання кількості абонентів з числа керівного складу органів внутрішніх справ і державної безпеки в 1937-1940 роках значно випереджало аналогічні показники по інших категоріях абонентів.

Збільшення кількості абонентів урядового зв'язку, а також обсягів обігу інформації при порівняно невеликій канальній ємності часто призводило до тривалого очікування абонентами з'єднань, що позначалося на якості їх обслуговування. З метою вирішення цієї проблеми був підписаний наказ НКВС № 0042 від 16 січня 1940 року «Про покращення урядового ВЧ-зв'язку», згідно з яким вводився пароль «*Молния*» для обслуговування абонентів вищої категорії, а на 28 основних лініях урядового зв'язку необхідно було встановити додаткову засекречуючу апаратуру. У наказі також містилася вимога щодо застосування простих шифраторів на всіх наявних лініях зв'язку.

До липня 1940 року з наявних 103 ліній зв'язку 50 були обладнані апаратурою засекречування телефонних переговорів, а станом на 1 квітня 1941 року шифратори були встановлені на 66 лініях зв'язку з наявних 134, що свідчило про невиконання наказу № 0042. Повне впровадження спецапаратури гальмувалося обме-

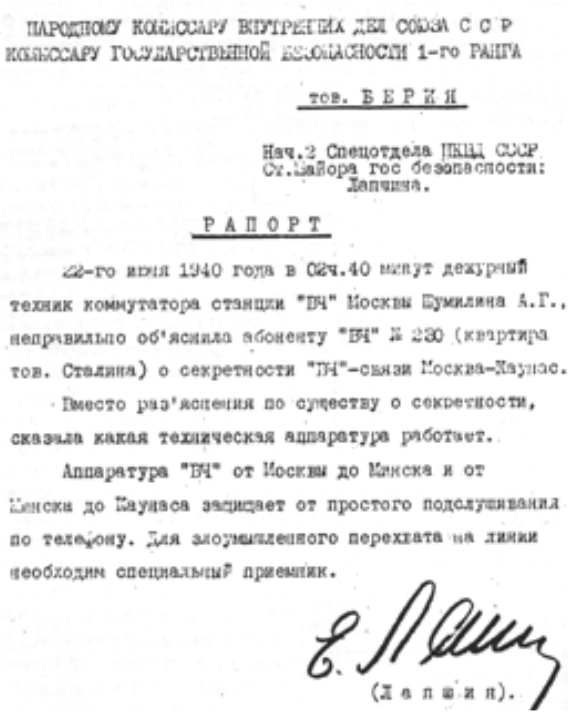
женими виробничими можливостями заводів, що її випускали, а також їх недостатнім фінансуванням.

Як свідчить «Список абонентів урядового (ВЧ) телефонного зв'язку», виданий у березні 1940 року, 9 з 40 (тобто 22,5 %) наявних у списку московських абонентів складали керівники НКВС і його основних структурних підрозділів. На периферії ситуація була ще сприятливішою для органів і підрозділів НКВС.

Так, з 286 перерахованих у списку прізвищ і посад 149 (більше 52 %) мають пряме відношення до структурних підрозділів НКВС (керівний склад республіканських, крайових, обласних і міських органів, командування з'єднаннями і підрозділами прикордонної і внутрішньої охорони, керівництво особливими відділами військових округів і флотів, директори особливих будівництв тощо). Більш того, для багатьох периферійних ВЧ-станцій керівний склад місцевих органів НКВС складав левову частку загальної кількості абонентів.

Так, наприклад, з п'яти абонентів єреванської ВЧ-станції три належали до керівництва структур НКВС (нарком внутрішніх справ Вірменії і його заступник, а також начальник прикордонних військ республіки); у Іваново, Курську, Кам'янець-Подільському, Дніпропетровську, Дрогобичі і деяких інших містах двома з трьох абонентів були начальник УНКВС і його заступник; у Гродно, Кисловодську, Новоросійську, Туапсе і Ялті абонентами ВЧ станції були виключно співробітники обласних управлінь і міських відділів НКВС тощо.

Приведена статистика свідчить про те, що за рахунок загальнодержавної мережі ВЧ-зв'язку НКВС активно нарощував відомчу мережу оперативного управління своїми місцевими органами, і цей факт, разом з іншими, також пояснює ініціативні дії наркомату в області організаційного і



НАРОДНОМУ КОМИССАРУ ВНУТРЕННИХ ДЕЛ СОЮЗА С С Р
КОМИССАРУ ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ 1-го РАНГА

тов. Б Е Р И Я

Нач.2 Спецотдела НКВД СССР
Ст.Майора гос безопасности:
Лапчина.

Р А П О Р Т

22-го июня 1940 года в 02ч.40 минут дежурный техник коммутатора станции "ВЧ" Москвы Бумилина А.Г., неправильно об'яснила абоненту "ВЧ" № 230 (квартира тов. Сталина) о секретности "ВЧ"-связи Москва-Каунас.

Вместо раз'яснения по существу о секретности, сказала какая техническая аппаратура работает.

Аппаратура "ВЧ" от Москвы до Минска и от Минска до Каунаса защищает от простого подслушивания по телефону. Для злоумышленного перехвата на линии необходим специальный приемник.

(Л а п ш и н).

матеріально-технічного вдосконалення системи урядового міжміського зв'язку.

Разом з тим, перші події Другої світової війни і пов'язана з ними активізація партійно-державного курсу на зміцнення обороноздатності зумовили тенденцію розширення мережі урядового міжміського зв'язку за рахунок командування вищих об'єднань і стратегічних об'єктів РСЧА, а також керівництва підприємств оборонної промисловості.

Так, в другій половині 1940 року за ініціативою наркома авіаційної промисловості А.І.Шахуріна співробітниками 2-го спецвідділу НКВС була проведена низка організаційно-технічних заходів щодо встановлення телефонних апаратів ВЧ-зв'язку на авіаційних заводах. Восени 1940 року абонентами Кремлівської урядової АТС стали директори 6 московських авіазаводів і Центрального авіаційного державного інституту в підмосковному селищі Раменське. Апарати урядового зв'язку були також встановлені та включені у відповідні міські ВЧ-станції на заводах № 153 (Новосибірськ), № 292 (Саратов), № 380 (Ленінград), імені Молотова (Горький) і № 125 (Іркутськ). Для того, щоб встановити ВЧ-апарат директору заводу № 18 (Вороніж), довелося прокладати спеціальний кабель від заводу до міської телефонної станції.

Але найсерйозніші проблеми виникли при організації ВЧ-зв'язку із заводами Наркомату авіапромисловості, що були розташовані в Уфі, Казані, Таганрозі і Комсомольську, оскільки з цими населеними пунктами урядовий зв'язок взагалі був відсутній. Незважаючи на те, що клопотання про організацію ВЧ-зв'язку з Уфою було ініційоване партійним керівництвом Башкирії ще в лютому 1940 році, реалізувати його вдалося тільки весною 1941 року, що дозволило здійснити безпосередній телефонний зв'язок центру з трьома авіамоторними заводами.

Монтаж устаткування ВЧ станції в Казані був завершений до червня 1941 року. Що ж до лінії ВЧ-зв'язку Ростов-Таганрог, то вона була здана в експлуатацію 14 травня 1941 року, і першими абонентами нової станції стали саме керівники об'єктів оборонної промисловості – заводу № 31 Наркомату авіапромисловості і заводу № 65 Наркомату боєприпасів.

Згідно з Постановою РНК СРСР № 2408-107сс від 25 листопада 1940 року «Про включення в урядовий зв'язок ВЧ-об'єктів Військово-Повітряних Сил Червоної Армії» абонентами став керівной склад ВПС РСЧА.

Восени та взимку 1940 року НКВС виконав особисту вказівку Й.Сталіна про організацію урядового зв'язку з установами і промисловими об'єктами Наркомату озброєння. Був встановлений ВЧ апарат наркому Б.Ваннікову, а також організований ВЧ-зв'язок із заводами наркомату № 2 (Килимов) № 66 (Тула) і № 74 (Іжевськ). При цьому в ході організації ВЧ зв'язку з Килимом (прийнятий в експлуатацію 20 грудня 1940 року) був створений прецедент: директор заводу № 2 став єдиним абонентом нового пункту, тоді як начальник міськвідділу НКВС (традиційно пріоритетний абонент ВЧ для населеного пункту районного масштабу) ще тривалий час був

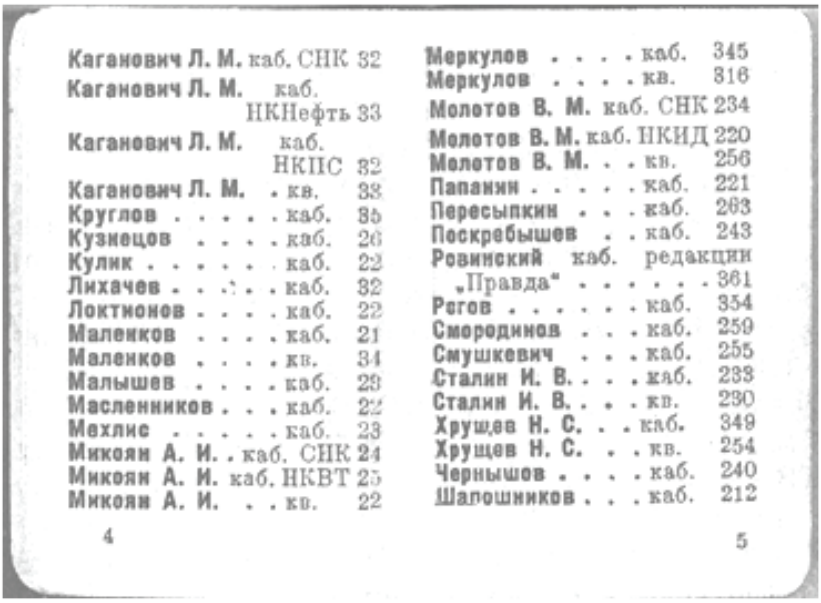
вимушений користуватися ВЧ зв'язком безпосередньо з Івановської ВЧ-станції.

Значно складніше було реалізувати рішення РНК СРСР і ЦК ВКП(б) про встановлення телефонних ВЧ-апаратів директорам підприємств Наркомату боєприпасів, прийняте в кінці 1940 року. У затвердженому списку, крім кабінету наркома, містився перелік 23-х заводів, розкиданих по всій території країни, – від Ленінграда до Молотова. Тому пункти, в яких належало організувати ВЧ-зв'язок, були розділені на дві групи:

- міста, де вже були ВЧ-станції (всього 14 – Москва, Ленінград, Тула, Куйбишев, Ростов-на-Дону, Новосибірськ, Молотов тощо), і в яких апарати директорам заводів могли бути встановлені до 21 січня 1941 року;
- населені пункти, в яких організація необхідних ВЧ-зв'язків була пов'язана з будівництвом нових ВЧ-станцій (всього 10 – Казань, Златоуст, Нижній Тагіл, Пенза, Кемерово тощо).

За розрахунками співробітників центрального апарату урядового зв'язку устаткування станцій ВЧ-зв'язку, що вперше відкривалися, могло бути здійснене в лютому-березні 1941 року за умови додаткового фінансування НКВС СРСР (1,5 млн. крб.), збільшення штатів НКВС на 70 одиниць інженерно-технічного персоналу, передачі Наркоматом зв'язку ВЧ каналів на всіх необхідних напрямках, а також виділення Держпланом СРСР додаткових фондів за рахунок Наркомату боєприпасів або резерву на користь виробництва необхідних матеріалів і апаратури.

Ці умови лягли в основу Постанови РНК СРСР № 303-144сс від 14 лютого



Каганович Л. М.	каб. СНК 32	**Меркулов**	каб. 345
Каганович Л. М.	каб. НКНефть 33	**Меркулов**	кв. 316
Каганович Л. М.	каб. НКПС 32	**Молотов В. М.**	каб. СНК 234
Каганович Л. М.	кв. 33	**Молотов В. М.**	каб. НКИД 220
Круглов	каб. 35	**Молотов В. М.**	кв. 256
Кузнецов	каб. 26	**Папанин**	каб. 221
Кулик	каб. 22	**Пересыпкин**	каб. 263
Лихачев	каб. 32	**Поскребышев**	каб. 243
Локтионов	каб. 22	**Ровинский**	каб. редакции „Правда" 361
Маленков	каб. 21	**Рогов**	каб. 354
Маленков	кв. 34	**Смородинов**	каб. 259
Малышев	каб. 29	**Смушкевич**	каб. 255
Масленников	каб. 22	**Сталин И. В.**	каб. 233
Мехлис	каб. 23	**Сталин И. В.**	кв. 230
Микоян А. И.	каб. СНК 24	**Хрущев Н. С.**	каб. 349
Микоян А. И.	каб. НКВТ 25	**Хрущев Н. С.**	кв. 254
Микоян А. И.	кв. 22	**Чернышов**	каб. 240
		Шапошников	каб. 212
4		5	

1941 року «Про включення в урядовий ВЧ-зв'язок заводів Наркомату боєприпасів у 1941 році». Крім того, РНК зобов'язав: Наркомат електропромисловості – виготовити і відвантажити для НКВС необхідні матеріали і устаткування; НКЗ – підготувати в своїй учбовій мережі і направити до НКВС для обслуговування об'єктів ВЧ-зв'язку 10 інженерів і 50 техніків у 1941 році та 50 техніків у 1942 році. Відповідно до Постанови, Наркомат зв'язку виділив НКВС 10 міжміських телефонних каналів для включення об'єктів Наркомату боєприпасів і ще 9 – для резервування основних напрямків урядовому зв'язку.

Ще до ухвалення Постанови РНК завдання більш ніж на 50 % було виконано. Станом на 26 січня 1941 року ВЧ зв'язок був встановлений з 14 об'єктами Наркомату боєприпасів. У «Довідці про стан урядового ВЧ-зв'язку на 04.03.1941р.», підготовленою М.І.Ільїнським, наголошувалося: «За рішенням РНК СРСР в даний час будується ВЧ-зв'язок з 10 об'єктами Наркомату боєприпасів». Однак цей процес був пов'язаний з певними труднощами, що випливало з відомості про загальну кількість абонентів, датованої 17 травня 1941 року, відповідно до якої до вказаної дати по Наркомату боєприпасів обслуговувалися все ті ж 14 абонентів. Інші об'єкти включалися в мережу урядового зв'язку по мірі надходження апаратури і виділення необхідних ВЧ-каналів.

Висновок про особливе відношення керівництва країни і НКВС до забезпечення об'єктів оборонної промисловості ВЧ-зв'язком випливав також з рішень, що приймалися за заявками інших промислових наркоматів. Так, в листі заступнику наркома середнього машинобудування від 22 травня 1941 року заступник наркома внутрішніх справ С.М.Круглов писав: «Внаслідок перевантаженості ВЧ-зв'язку урядовими переговорами включити вказані вами заводи не представляється можливим». Аналогічна відповідь дещо раніше була надана й наркому загального машинобудування.

Одним із найважливіших завдань керівництва НКВС у той час було також включення в мережу урядового міжміського зв'язку адміністративних центрів територій, що «добровільно» приєднувались до СРСР за результатом «пакту Рібентропа-Молотова». Цей процес почався взимку 1939 року, по мірі утворення Молдавської РСР і нових областей у Західній Україні і Західній Білорусії. Характерно, що з 24-х ВЧ-станцій, введених у дію протягом 1939 року, більше 40 % були в найкоротші терміни обладнані саме в нових адміністративних центрах Західної Білорусії (Брест-Літовськ, Белосток, Барановичі, Гродно, Пінськ) і Західної України (Луцьк, Львів, Рівне, Станіслав, Тернопіль).

Дещо пізніше, у 1940 році, в мережу ВЧ зв'язку були включені міста Кишинів (столиця Молдавської РСР), Ліда (одне з міст Гродненської області Білоруської РСР) і Чернівці, а в першій половині 1941 року – Ізмаїл (обидва останні – адміністративні центри нових областей Української РСР).

Після завершення радянсько-фінляндської війни (листопад 1939 – березень 1940) подібна проблема виникла з адміністративними і стратегічно важливими

центрами, розташованими на територіях, які відійшли до Карело-фінської РСР за мирним договором з Фінляндією від 12 березня 1940 року. «Для забезпечення нормального і безперебійного ВЧ-зв'язку столиці КФРСР м.Петрозаводська з новими містами, – відзначав у листі керівництву НКВС нарком внутрішніх справ республіки Баскаків, – необхідно у м.Сортавала відкрити ВЧ пункт».

Крім ВЧ станції в м.Сортавала, що дозволила організувати обхідний ВЧ-канал Мурманськ-Петрозаводськ-Ленінград, у 1940 році також обладнані станції в містах Виборг і Кексгольм, які мали велике оборонне і господарське значення, оскільки Виборг, будучи крупним залізничним вузлом і морським портом, був важливим стратегічним пунктом на північно-західному напрямі, а в Кексгольмі розташовувалися частини прикордонних військ і деякі підприємства паперової промисловості.

Заходи щодо організації урядового міжміського зв'язку проводилися і в Прибалтиці, причому ще до входження Латвії, Естонії і Литви до складу СРСР на правах союзних республік. Відомо, що пункти ВЧ-зв'язку були відкриті на міжміських станціях міст Рига, Таллінн і Каунас (через Вільно) 20 червня 1940 року. Для забезпечення роботи нових ліній і пунктів відряджалися технічні працівники урядового зв'язку: до Каунасу, Риги і Таллінна – по 3, у Вільно – 2.

Крім того, з метою запобігання несанкціонованих підключень до лінії на міжміській станції в Ризі було встановлено чергування трьох зв'язківців – червоноармійців РСЧА. Надалі, після створення Латвійської, Естонської і Литовської РСР (серпень 1940 року) та організації в їх столицях відповідних структур внутрішніх справ і держ-

НАРОДНЫЙ КОМИССАР
ОБОРОНЫ СОЮЗА ССР

марта 1941 г.
№ 30182.

/ СЕКРЕТНО
экз. № 1
157

НАРОДНОМУ КОМИССАРУ ВНУТРЕННИХ ДЕЛ СССР
товарищу Б Е Р И Я

Взято на контроль
Секретариатом НКВД СССР

Прошу Ваших указаний об установке телефонов высокой частоты /ВЧ/ в кабинетах - Зам.Начальника Генерального Штаба Красной Армии Генерал-лейтенанта тов.СОКОЛОВСКОГО и Начальника Управления Оборонительного Строительства Главного Инженерного Управления Красной Армии Генерал-майора инженерных войск тов. КОТЛЯР.

МАРШАЛ СОВЕТСКОГО СОЮЗА
(С.БУДЕННЫЙ)

безпеки, прибалтійські станції ВЧ-зв'язку почали експлуатуватися постійним штатом 2-го спецвідділу НКВС, а обслуговування абонентів здійснювалося на підставі наказу НКВС № 001103 від 3 вересня 1940 року «Про включення абонентів урядового ВЧ-зв'язку у знов відкритих станціях ВЧ у містах Ризі, Таллінні, Каунасі».

На початку 1941 року у державі розпочалася чергова реорганізація органів внутрішніх справ і державноїх безпеки. Так, Указом ПВР СРСР від 3 лютого 1941 року зі складу НКВС був виділений НКДБ. Тому з 26 лютого ВУЗ стало «відділенням урядового «ВЧ» зв'язку» 4 відділу (оперативної техніки) НКДБ. Однак вже 26 березня спільним наказом НКВС/НКДБ № 00332/0066 ВУЗ було передано до складу Особливого технічного бюро (далі - ОТБ) при наркомі внутрішніх справ. Таким чином, структурна належність урядового зв'язку до НКВС була відновлена, що свідчило про високий авторитет цього зв'язку серед вищого партійного та радянського керівництва.

А історія появи ОТБ розпочалася ще 29 вересня 1938 року, коли наказом НКВС № 00641 був організований Відділ особливих конструкторських бюро НКВС. А 21 жовтня відповідно до наказу НКВС № 00698 цей підрозділ став 4-м спецвідділом НКВС. 10 січня 1939 року наказом НКВС № 0021 він був перетворений в ОТБ з метою використання ув'язнених, які мають спеціальні технічні знання. Його беззмінним керівником з 14 листопаду 1939 року по 8 квітня 1947 року був Валентин Олександрович Кравченко.

Станом на квітень 1941 року штат ВУЗ разом з Московською ВЧ-станцією складав 60 одиниць, а периферійних підрозділів – 863. Причому за рахунок введення в штат інженерно-технічного складу (з 1940 року) кількість посад інженерів, старших техніків була доведена в центрі до 43-х (71,7 % від загального штату), а на периферії – до 720 (83,4 %). Ці кількісні показники були досягнуті, незважаючи на проведене у квітні скорочення апарату НКВС, в ході якого в підрозділах ВЧ-зв'язку на периферії було скорочено 181 штатну одиницю, а в Москві – 8.

Станом на 5 травня 1941 року в СРСР функціонувало 116 ВЧ станцій і 39 трансляційних пунктів (зокрема 9 резервних). Кількість абонентів урядового зв'язку в СРСР досягла 733, з яких 184 – вище партійне та державне керівнийтво, 157 – НКВС, 188 – НКДБ, 128 – Наркомат оборони. В Україні станом на 1 квітня 1941 року було 103 абоненти урядового зв'язку.

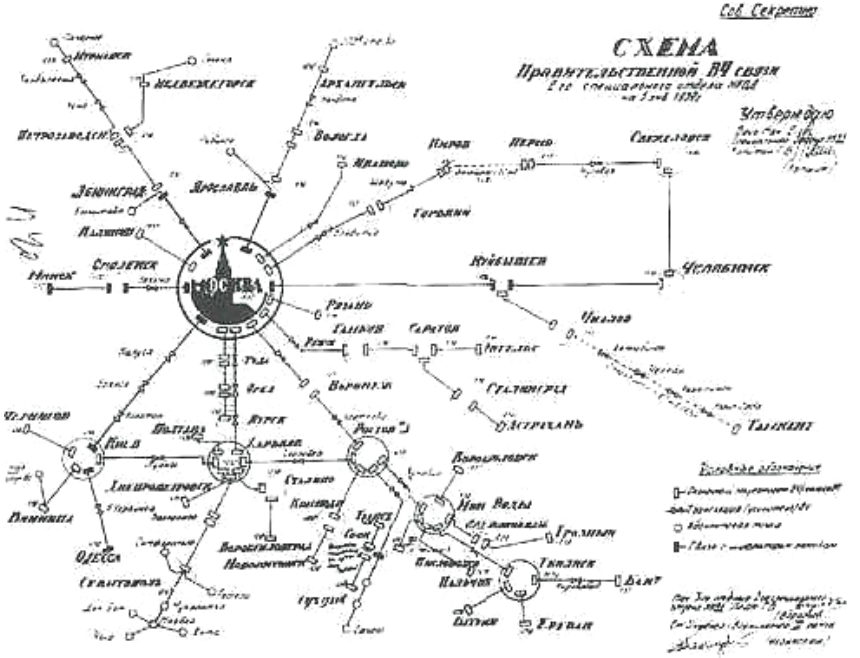
По суті, урядовий зв'язок НКВС перетворився на загальнодержавну мережу спеціального телефонного зв'язку, що географічно охоплювала всю територію СРСР і обслуговував керівництво партії, уряд, а також центральні апарати і периферійні об'єкти низки народних комісаріатів (внутрішніх справ, державної безпеки, оборони, військово-морського флоту, боєприпасів, озброєнь, авіаційної промисловості).

Тим часом продовжувалося вдосконалення організаційно-штатної структури підрозділів урядового зв'язку. Так, 6 травня 1941 року розпорядженням РНК СРСР № 5-рс було затверджене «Положення про порядок експлуатації урядового ВЧ

зв'язку НКВС СРСР», а трохи пізніше – «Положення про урядовий ВЧ зв'язок СРСР», у якому засекречений ВЧ-зв'язок був віднесений до категорії урядового зв'язку.

В «Положенні» жорстко регламентувався порядок обслуговування ВЧ зв'язком: включення нових абонентів здійснювалося виключно за рішенням РНК СРСР, а користування апаратами ВЧ дозволялося тільки особам, яким апарат був персонально встановлений, або їх безпосереднім заступникам. У ньому визначалися також основні принципи взаємодії відомств, відповідальних за експлуатацію станційних і лінійних споруд урядового міжміського зв'язку: ВЧ-зв'язок НКВС працював по телефонних лініях Наркомату зв'язку, покриття витрат якого на обслуговування цих ліній здійснювалося за рахунок спеціальних асигнувань. Передбачалося також, що при необхідності для організації ВЧ зв'язку могли бути використані телефонні лінії НКПС, НКО, НКВМФ й інших наркоматів СРСР.

Проте найбільш значущим був перший пункт «Положення», який свідчив: «Урядовий високочастотний (ВЧ) зв'язок НКВС СРСР здійснює прямі міжміські телефонні переговори ЦК ВКП(б), уряду СРСР і керівництва окремих наркоматів з центрами союзних республік і найголовнішими пунктами Союзу». Це було офіційне визнання статусу міжміського ВЧ-зв'язку як мережі спеціального електрозв'язку вищої партійної і державної еліти СРСР.



Ось як писав про значимість урядового зв'язку у своїх спогадах М.Карпов: «Значення цьому зв'язку надавалося виключно серйозне, кількість апаратів була дуже обмеженою, і ніхто не знав, навіть серед співробітників НКВС, про існування ВЧ-зв'язку. Коли начальник Управління НКВС Дукельський виходив з кабінету, то телефонний ВЧ-апарат він зачиняв у письмовий стіл. Так було й в інших абонентів».

5.3. Перша апаратура засекречування

Сама технологія ВЧ-зв'язку без застосування апаратури засекречування могла захистити тільки від прямого прослуховування. А ось якщо до лінії ВЧ-зв'язку підключити найпростіший детекторний приймач, то розмову можна було відновити в первозданному вигляді та здійснювати прослуховування. Проблема була в тому, що в інтересах урядового зв'язку використовувались лінії та канали, як правило, НКЗ, працівники якого, маючи необхідну технічну підготовленість та службовий доступ до цих ліній і каналів, могли здійснити прослуховування.

Вперше про уразливість ВЧ-зв'язку написав у своєму рапорті від 8 серпня 1936 року старший технік-інженер Ільїнський на ім'я начальника ВУЗ Воробйова. Основними джерелами погроз були агентура іноземних спецслужб серед обслуговуючого персоналу та використання різних портативних і простих в обслуговуванні технічних засобів.

У документі, що був написаний у лютому 1937 року, була фраза про те, що «розмови можуть підслухуватися (і слухаються) нашими працівниками ВЧ, а їм також цілком довіряти не можна». У першому пункті «Акту комісії про перевірку технічного стану Центральної станції урядового ВЧ-зв'язку» також зазначалося: «Існуючий стан ВЧ-зв'язку не гарантує таємність урядових зв'язків».

У 1938 році начальник відділення урядового ВЧ-зв'язку Воробйов в одному з рапортів зазначив, що «спецзв'язок НКЗ, яким користуються абоненти Кремля, не забезпечує ніякої таємності розмов, тому що цей зв'язок надається Кремлю у відомі години і розмова членів уряду проходить через ту ж апаратуру НКЗ, що обслуговується технічним складом, який обслуговує й комерційні розмови». Тому в терміновому порядку довелося прокласти спеціальний кабель, що з'єднав станцію ВЧ-зв'язку з АТС Кремля.

Таким чином, з розвитком мережі урядового міжміського зв'язку все більш актуальною ставала проблема створення власної спеціальної апаратури (згідно з термінологією того часу – оперативної техніки) для забезпечення автоматичного засекречування мовного сигналу.

Історія створення такої апаратури розпочалася ще на початку XX століття. Так, у 1900 році Паульсеном була запропонована «розбивка» мовного сигналу на сегменти та передача їх у зворотньому напрямку (тимчасова інверсія). У 1918 році датський інженер Тігерстедт запропонував «розбивати» мову на тимчасові сегменти і пере-

ставляти їх у часі (тимчасові перестановки). У 1920 році російський вчений Михайло Бонч-Брує́вич удосконалив тимчасову перестановку, увівши кадрову структуру перетворень (кожні «N» сегментів переставлялися по-своєму). У 1922 році англієць Хоу-Гольд запропонував застосовувати синхронну зміну несучої частоти передавача та настроювання приймача (для засекречування радіотелефонного зв'язку).

Початком утворення радянської апаратури засекречування став 1930-й рік, коли у НКПіТ почав роботу Володимир Олександрович Котельников. У 1931 році у цьому наркоматі під його керівництвом була створена науково-дослідна група у кількості 5-10 осіб, що розпочала розробку телефонної апаратури засекречування для магістральної короткохвильової (далі - КХ) лінії радіозв'язку Москва-Хабаровськ.

Оскільки повідомлення, передані лінією радіозв'язку, легко могли бути перехоплені іноземною розвідкою, Котельников у 1939 році запропонував створити шифратор для засекречування мовних сигналів. Ця пропозиція мала важливе державне значення, тому для його реалізації в Центральному науково-дослідному інституті зв'язку (далі - ЦНДІЗ) НКПіТ була організована спеціальна лабораторія.

Для підвищення стійкості засекречування мови Котельников запропонував нову систему, засновану на квазівипадкових (відомих тільки одержувачу повідомлення) перестановках тимчасових відрізків мовного сигналу, переданого телефонним каналом. Прийнятий сигнал піддавався зворотній операції, у результаті чого відновлювався вихідний порядок проходження тимчасових відрізків мовного сигналу, і він ставав розбірливим.

В результаті у 1939 році лабораторією Котельникова була створена унікальна багатоканальна телефонно-телеграфна апаратура радіозв'язку, що вперше використовувала одну бічну смугу частот, та відповідна апаратура телефонного засекречування. Ця апаратура була встановлена на Жовтневому передавальному центрі в Москві та введена в дослідну експлуатацію на лінії радіозв'язку Москва-Хабаровськ. Ця магістраль з'явилася найбільшим досягненням вітчизняної і світової радіотехніки того часу.

Оскільки потреба в апаратурі засекречування телефонних розмов була дуже велика (про стан робіт неодноразово доповідалося наркомом внутрішніх справ керівництву держави), органи держбезпеки вважали можливим одночасно звернутися до закордонних фірм-виробників подібної апаратури. На той час вітчизняним фахівцям уже були відомі наявні іноземні аналоги апаратури секретної телефонії, що проектувалася у СРСР.

Так, американська установка з однократним перевертанням частот використовувалася в Московському радіотелефонному центрі, а шифратор фірми «Сіменс» був у 1936 році випробуваний на магістралі Москва-Ленінград. Однак була необхідна повна та достовірна інформація щодо закордонних шифраторів: розглядалася можливість розміщення замовлень на розробку нової апаратури або

придбання готової продукції.

20 березня 1937 року «Технопромімпорт» одержав від НКВС «Замовлення на закупівлю за рубежем апаратури секретної телефонії». Через «Технопромімпорт» і Наркомат зовнішньої торгівлі на початку 1937 року було запитано більш десятка європейських фірм, що робили апаратуру надтонального телефонування, у тому числі «Сіменс» і «Лоренц» (Німеччина), «Бел Телефон» і «Аутоматик Електрик» (Бельгія), «Стандарт Телефон енд Кеблз» (Великобританія), «Хаслер» (Швейцарія), а також «Еріксон» (Швеція). До запитів, як правило, додавалися технічні вимоги до апаратури: забезпечити захист від розшифрування за допомогою радіоприймача з додатковими простими пристроями.

Проте більшість фірм відповіли на запит прямою відмовою. Деякі зажадали за розробку шифраторів дуже високу ціну (у межах 40-45 тисяч доларів – у той час це була досить велика сума). Серед деяких прийнятних пропозицій заслуговувала уваги тільки відповідь англійської фірми «Стандарт Телефон енд Кеблз», чиї шифратори могли бути використані як додаткове устаткування на каналі радіозв'язку Москва-Хабаровськ.

Тому актуальною була проблема створення власної (в рамках ОВ ГУДБ НКВС) науково-технічної бази, яка дозволила б в найкоротші терміни вирішити завдання оснащення ВЧ станцій апаратурою засекречування (згідно з термінологією того часу – оперативною технікою). У 1936 році у складі 13-го відділення Оперативного відділу вже функціонувала радіолабораторія, яка займалася розробкою спеціальної радіо-, телеграфної й телефонної апаратури урядового зв'язку. Подібна лабораторія була також створена при оперативному відділі Управління держбезпеки НКВС по Ленінградській області.

У той період у сфері секретної телефонії працювали ще 6 організацій: ЦНДІЗ НКПіТ, НДІЗ і телемеханіки НКВМФ, НДІ РСЧА НКО, НДІ-20 Наркомату електропромисловості (далі - НКЕП), а також комбінат імені Комінтерну і завод «*Красная Заря*». Однак чисельність цих підрозділів тоді була невелика: 5-10 осіб. Найбільше активно працювали та створили зразки апаратури засекречування ЦНДІЗ НКПіТ і завод «*Красная Заря*».

Навесні 1936 року після того, як співробітники ВУЗ ознайомилися з наявними матеріалами щодо апаратури засекречування в СРСР і за кордоном, був зроблений висновок про необхідність і можливість проектування та зборки двох напівкомплектів апаратури, подібної до апаратури надтонального телефонування системи «Сіменс» зразка 1932 року.

Такі напівкомплекти були виготовлені до середини червня 1936 року лабораторією ВУЗ і випробувані на зв'язку між різними пунктами Москви. Однак у ході іспитів поряд з явними достоїнствами устаткування були виявлені істотні недоліки технічного характеру (перекручування мови, прослуховування робочих частот,

відсутність сигналізації, неможливість контролю роботи і перевірки режиму ламп тощо).

Головна ж проблема полягала в тому, що лабораторія-виготовлювач могла робити таку апаратуру тільки у вигляді макетів. Був потрібний принципово новий підхід до вирішення проблеми, оскільки на той час стало очевидно, що ВЧ апаратура (СМТ-34 тощо) не забезпечувала таємності переговорів через такі причини:

- розмови легко прослуховувались на міжміських станціях НКЗ при наявності спеціальної вимірювальної або ВЧ-апаратури;
- існувала можливість прихованого підключення на будь-якому лінійному контрольному пункті НКЗ або безпосередньо до лінії та контролю всіх переговорів за допомогою нескладної апаратури (наприклад, довгохвильового радіоприймача);
- була висока ймовірність прийому розмов на радіоприймач з антен, розташованих поблизу міжміських ліній, по яких організовувалися канали ВЧ-зв'язку;
- були можливі переходи розмов, що велися по лініях НКВС, на лінії НКЗ (взаємні переходи при незначних ушкодженнях кіл, асиметрії і замінах).

Прийнявши до уваги той факт, що декілька організацій інших наркоматів (оборони, зв'язку, важкої промисловості) уже протягом 3-4 років займалися питаннями секретної телефонії, керівництво відділення урядового зв'язку ГУДБ НКВС до кінця літа 1936 року дійшло висновку про необхідність термінового замовлення на розробку та виготовлення за визначеними технічними умовами пристроїв, що засекречували би телефонні розмови. Найважливішими з умов були можливість сполучення з наявною ВЧ-апаратурою та урахування специфіки експлуатації станцій урядового зв'язку.

У ті часи єдиним методом забезпечення достатнього маскування мови при прямому прослуховуванні лінійної передачі були такі методи перетворення мовного сигналу:

1. Інверсія всього спектра мови (апарат одержав назву інвертора). При цьому найнижчі частоти мови ставали високими, а високі – навпаки. Всі інші частоти переміщалися щодо центра смуги спектра. На початку першого періоду цей спосіб мав широке застосування у нас і німців. Німецькі фахівці любовно називали його «наш маленький інвертор». Цей дуже простий прилад забезпечував маскування розмови в лінії, але супротивник міг, побудувавши аналогічний прилад, відновити «відкриту» мову, підключившись до каналу зв'язку.

2. Розбивка частотного спектра на ряд смуг і перестановка їх між собою, застосовуючи незалежну інверсію в окремих полюсах спектра. Якщо перетворення були не статичними, а змінювалися у часі та зміни керувалися шифратором, то така передача вимагала дешифрування.

3. Тимчасові перетворення мовного сигналу: тимчасові перестановки окре-

мих відрізків мови на заданому інтервалі часу, зрушення окремих частотних смуг, зміна швидкості відтворення мови.

4. Накладання перешкоди поза смугою мови з перестановкою частотних смуг.

5. «Хитання» несучої частоти передавача - «воблінг» (англ. *wobbling* - коливання).

Одним з перших претендентів на отримання замовлення стала лабораторія відділу радіопередаючих пристроїв комбінату імені Комінтерну (Ленінград). Фахівці лабораторії у період з 1933 по 1936 роки розробили 4 типи апаратури:

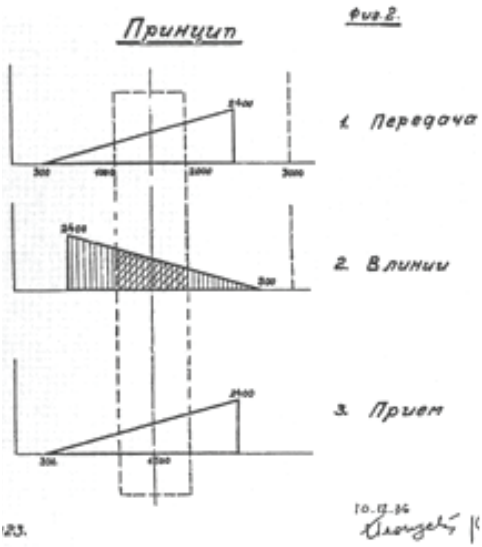
1) установка з однократним перекиданням розмовних частот і «воблінгом»;

2) малогабаритна переносна шифрувальна установка, що працювала за принципом однократної інверсії;

3) «*СЭТ-2*» – складна система шифрування з розподілом розмовної смуги частот на 3 канали і «перемішуванням» смуг за довільним законом з довільною (у відомих межах) швидкістю;

4) СУ-1 – установка з «дробленням» розмовного спектра на дві частини та перекиданням нижчого каналу з інверсією двох смуг розмовних частот з довільною швидкістю.

Незважаючи на те, що проекти комбінату імені Комінтерну відкрили шлях вітчизняним дослідженням у цій сфері, їхнє використання було визнано недоцільним, головним чином через відсутність на комбінаті виробничої бази для виготовлення станційної телефонної апаратури. Тому центром розробки та виробництва вітчизняної апаратури засекречування був обраний завод «*Красная Заря*», де передбачалося створити спеціальну лабораторію. Там повинні були спроектувати та до середини 1937 року виготовити перші зразки «секретки», тобто апаратури секретної телефонії. Одночасно з цим, інші заводи наркомату важкої промисловості були зобов'язані за кілька місяців забезпечити випуск необхідних деталей (зокрема, спеціальних купроксів).



У лабораторії планувалося створити:

- абонентську кінцеву шифрувальну установку;
- стаціонарну установку 1-ї і

2-ї черги для станцій ВЧ зв'язку;

- стаціонарну і переносну апаратуру засекречування телефонних розмов по радіотелефонних лініях зв'язках;
- спеціальну апаратуру переносного типу для розсекречування перехоплених розмов ймовірного супротивника.

Абонентська установка призначалася для встановлення замість звичайного телефонного апарата в абонента, а у тексті технічних умов для стаціонарної «секретки» відзначалося: «пристрій засекречування повинний працювати спільно з апаратурою ВЧ-телефонування типу СМТ-34, цілком бути пристосований до умов її експлуатації та підключатися як додатковий пристрій на протилежних станціях до напівкомплектів ВЧ».

Аналогічними проблемами секретної телефонії займалася також Дослідна радіолабораторія Управління НКВС по Ленінградській області, що мала власну науково-виробничу базу. Роботи в обох лабораторіях були розгорнуті вже узимку 1936 року та вже до травня 1937 року, коли керівництвом НКВС були підготовлені офіційні замовлення та розпорядження, у радіолабораторії ленінградського Управління НКВС абонентська установка знаходилася в стадії конструювання лабораторного макета, а в лабораторії зв'язку заводу «*Красная Заря*» був зібраний макет стаціонарного шифратора для одного кінця лінії. На заводі планували завершити розробку інвертора та виготовити 2-4 комплекти устаткування не пізніше 1 липня 1937 року.

У доповідній записці від 5 грудня 1936 року начальник ОВ УДБ управління НКВС по Ленінградській області Михайло Альохін підкреслював: «Для створення рішучого повороту в техніці необхідна організація в Москві і Ленінграді груп, що працюють виключно по спостереженню за науково-технічною діяльністю в галузях, що цікавлять нас. Без відповідальних тільки за цю справу людей, без використання всіх досягнень техніки, що проходять зараз повз нас, без залучення до цієї справи молодих талановитих сил повороту в бік прогресу не домогтися».

З 14 липня 1937 року на лінії ВЧ зв'язку Москва-Ленінград розпочалися іспити двох кінцевих напівкомплектів переносної установки засекречування, створеної ленінградським Управлінням НКВС. Кількома днями раніше були завершені та на тій же лінії випробувані макети стаціонарної «секретки» заводу «*Красная Заря*», що одержала найменування «*ЕС-2*» (за прізвищами інженерів заводської лабораторії зв'язку Костянтина Петровича Єгорова та Георгія Васильовича Старіцина). Установка «*ЕС-2*» являла собою інвертор, що не захищав від спеціального перехоплення, але забезпечував неможливість підслуховування:

- у ході технічного контролю апаратури ВЧ телефонування;
- за допомогою аналогічної ВЧ апаратури міжміських станцій НКЗ;
- безпосередньо з лінії за допомогою радіоприймача без додавання демодулятора і генератора.

Шифратор «*ЕС-2*» при роздільному читанні тексту забезпечував розбірливість всього 20-30% слів, цифри при цьому розпізнавалися повністю. Незважаючи на те, що зміст тексту уловити практично не вдавалося, апарат пройшов додаткові іспити (разом з переносним шифратором лабораторії ленінградського Управління НКВС) на лінії Москва-Сочі. У ході іспитів, що відбулися у період з 4 по 14 серпня 1937 року, шифратор зарекомендував себе, в цілому, позитивно. Більш того, з'ясувалося, що експлуатація «секреток» на лінії ВЧ-зв'язку вимагала високої якості проводових каналів зв'язку (гарна амплітудно-частотна характеристика, відсутність перешкод і шумів тощо), що потребувало обов'язкове врахування цих параметрів на всіх наступних етапах розвитку мережі міжміського урядового зв'язку.

У вересні 1937 року, коли завод «*Красная Заря*» подав на затвердження другий зразок установки «*ЕС-2*», було прийняте рішення ввести її в постійну експлуатацію на лінії Москва-Ленінград. Постановою РНК СРСР «Про розвиток урядового ВЧ-зв'язку» № 53/до від 05.01.38р. НКЗ пропонувалося до 1 травня 1938 року забезпечити НКВС 12 напівкомплектами стояків типу «*ЕС-2*». Так був покладений початок серійному виробництву першого покоління радянської апаратури автоматичного засекречування телефонних переговорів.

У цей період також приймалися заходи, направлені на розробку засекречуючих пристроїв для радіотелефонних каналів. Така апаратура під індексом «*ЕИС-3*» (Єгоров-Ільїнський-Старіцин) була розроблена і підготовлена до серійного виробництва лабораторією заводу «*Красная Заря*» у 1937 році.

Протягом наступних 3-х років завод «*Красная Заря*» забезпечив виготовлення цілої серії апаратури простого засекречування «*ЕС-2*» (*ЕС-2М, МЕС, МЕС-2, МЕС-2А, МЕС-2АЖ* тощо). Цими установками у 1938 році було обладнано 9 міжміських урядових ліній зв'язку, а на 1 квітня 1941 року – 66 ліній із наявних 134.

За два роки (1938-1940) завод «*Красная Заря*» випустив 262 апарати для урядового телефонного зв'язку «*ЕС*». Даний пристрій гарантував «закриття» телефонних переговорів на відстані до 2 тисяч кілометрів. Треба сказати, що пристрій «*ЕС*» успішно використовувався для організації ВЧ-зв'язку практично впродовж всієї Вітчизняної війни. Принаймні, відомостей про перехоплення й дешифрування «закритих» переговорів наших воєначальників немає.

У другій половині 1938 року на заводі була завершена розробка та проведені іспити апаратури складного засекречування С-1, яка забезпечувала вже неможливість підслуховування за допомогою простих пристроїв та техніки, що була на станціях НКЗ. Разом з тим, від спеціального підслуховування апаратура С-1 захищала неповністю, при цьому частково погіршувала якість розмови.

Експлуатація секретної телефонії привела до ідеї створення комплексного пристрою, який би поєднував в собі функції як каналоутворення, так і засекречування. В результаті був створений шифратор ПЖ-8М, що працював у комплексі з

3-канальною апаратурою ВЧ телефонування СМТ-34 і забезпечував засекречування за простою схемою.

На користь масового випуску спецапаратури виникла необхідність створення спеціального заводу. У доповідній записці наркому внутрішніх справ Л.П.Берії про заходи з підвищення якості урядового телефонного зв'язку від 5 лютого 1939 року підкреслювалося: «Вважаючи, що засекречуюча апаратура повинна широко застосовуватися по всьому Союзу, поставити питання перед ЦК ВКП(б) і РНК СРСР про необхідність створення спеціального заводу при Наркоматі зв'язку з відповідними лабораторіями для виробництва всіх видів засекречуючої і спеціальної телефонної, телеграфної, радіоапаратури і сигналізації».

Питання про створення подібного заводу ставилося не тільки НКВС, але й Генштабом РСЧА ще в червні 1938 року, оскільки ні армія, ні флот не мали на озброєнні приладів, що гарантують секретність телефонно-телеграфних передач. Однак ще тривалий час завод «*Красная Заря*» (директор заводу з грудня 1937 року М.В.Мельніков) залишався основним постачальником апаратури засекречування.

У 1939 році Котельникову була доручена важливе державне завдання - створення шифратора для засекречування мовних сигналів з підвищеною стійкістю до дешифрування, замовником якої виступав ВУЗ. Для цього в ЦНДІЗ була організована лабораторія під керівництвом Котельникова із засекречування телефонної інформації. В основному, лабораторія була укомплектована інженерами, що тільки закінчили інститут зв'язку або завершали навчання на етапі дипломного проекту, який захищали за тематикою своєї нової роботи.

Крім Котельникова в роботах із секретної телефонії брали участь Мінц, Єгоров, Віторський. Учені намагалися забезпечити конфіденційність передачі інформації за допомогою створеної ними унікальної багатоканальної апаратури радіозв'язку, яка вперше використовувала одну бічну смугу частот. У 1939 році вона була встановлена на магістралі Москва – Хабаровськ.

Ідею шифру, який не дешифрується, Котельников сформулював незадовго до війни: «Я чув, що всякі шифри розсекречуються. Вирішив розібратися, чи можливо зробити шифр, який абсолютно не дешифрується. Ну, і розібрався. Довів, що можливо. Але для цього шифр повинен бути випадковим і використовуватися тільки один раз».

Із спогадів Котельникова: «Використання одноразового ключа корисне і для засекречування в телефонії як проводовій, так і радіо. Тільки там все набагато складніше, та у разі аналогової передачі спектру мови, не перетворюючи його в цифрову, отримати абсолютно стійке засекречування неможливо. Можна отримати високий ступінь стійкості, але не абсолютний. При мозаїчному шифруванні спектру, навіть, якщо застосовується одноразовий ключ, система залишається вразливою, оскільки кожен «шматочок», сам по собі, виявляється незашифро-

ваним. Тому-то важливо зробити інтервали та по можливості менше, але при цьому втрачається якість передаваної мови».

Свій закритий звіт «Основні положення автоматичної шифровки», в якому було вперше представлене суворе обгрунтування того, що системи шифрування з одноразовими ключами абсолютно стійкі, Котельников здав за три дні до початку вітчизняної війни. Ця робота, на жаль, маловідома, оскільки так і не вийшла у відкритому друці. Через 5 років Клод Шеннон виклав підходи до побудови стійких систем шифрування в своїй секретній доповіді, датованій 1 вересня 1946 року. У відкритому друці вона з'явилася у 1949 році.

Під керівництвом Котельникова був розроблений перший телефонний шифратор «мозаїчного типу», що поєднував у собі частотні перетворення мовного сигналу з перестановками його відрізків за часом. Перетворення, що ним реалізовувалися, були динамічними, тобто періодично змінювалися за законом розподілу випадкових величин, і тому їх розкриття представляло дуже серйозне завдання навіть для кваліфікованих фахівців. Була запропонована система, заснована на квазівипадкових (відомих тільки одержувачеві) перестановках тимчасових (100 мілісекунд) відрізків і двох частотних смуг з інверсією мовного сигналу. Управління частотними і тимчасовими перестановками на передачі і прийомі здійснювалося шифратором, що генерував 5 біт гамми 10 разів в секунду.

Із спогадів Котельникова: «Спочатку ми просто «перевертали спектр» (інвертували), але швидко зрозуміли, що це легко розгадати. Тоді почали розбивати мову на деякі «відрізки» за частотою з інверсією спектру та їх «переплутувати»... «переплутували» не просто так, як доведеться, а певним чином, за допомогою шифратора... Був у нас «барабан», наповнений маленькими кульками, який крутився, і з нього висипалися кульки на спеціальний пристрій з штирькамі і щілинами так, що потім через ці щілини кульки випадковим чином потрапляли на дві рухомі телеграфні стрічки, які були накладені одна на одну через «копірку». В результаті виходив на обох стрічках однаковий малюнок - «доріжки» з випадково розташованих плямочок.

Потім по цих мітках стрічки перфорувалися. Одна стрічка залишалася на «передавальному кінці», а другу ми акуратненько скручували і упаковували в пластмасову коробочку, яку запаювали, щоб ніхто не підглянув. Цю процедуру повторювали кілька разів. Таким чином отримували два однакові набори шифрів. Ми їх нумерували, і один з наборів відправляли на «пункт прийому». А туди, під час сеансу зв'язку таємно повідомляли номер шифру, і таким чином на тому кінці знали, яку з коробочок треба розпаковувати, щоб використовувати захований там шифр».

Котельниковим був розроблений перший в СРСР смуговий «вокодер» (англ. *voice coder* - голосовий шифратор) з виділенням основного тону мові. Робота була

доведена до діючого макету, який був випробуваний і показав можливість використання цього принципу для стиснення мовного сигналу. В ході цієї роботи Котельниковим був також запропонований і випробуваний принцип тестування артикуляції систем передачі мові. На базі цього вокодера Котельниковим були задумані принципи засекречування мовного сигналу.

Із спогадів Котельникова: «Для того, щоб було важче розшифрувати передавану мову, було важливо зробити «відрізки», на які ми її розбивали, якомога коротше. А це проблема тому, що тоді погіршується якість передаваної мови. Я почав думати, як би передавати мову не всю повністю, а якось стиснути її спектр. Почав розглядати спектр звуків, щоб зрозуміти, які частоти «*определяющие*»...

В цей час попалося на очі посилання на статтю Хомера Дадлі, опубліковану в жовтні 1940 року, де мовилося, що він зробив перетворювач мови - «вокодер». Кинувся дивитися, а виявилось, що там нічого конкретного не написано. Але все одно, це було дуже корисно: ідея у нього та ж, значить, ми на правильному шляху. Загалом, ми почали робити свій «вокодер». І перед самою війною у нас вже працював його дослідний зразок. Правда, поки він ще «говорив» погано, «тремтячим голосом».

Тільки в 1940 році у лабораторії Котельникова розпочалися роботи з виготовлення зразків найбільш складного за тих часів апарата телефонного засекречування «Соболь-П», у якому використовувалися тимчасові та частотні перестановки, а у якості шифратора використовувалася телеграфна стрічка з випадково нанесеними отворами. У той же час лабораторія заводу «*Красная Заря*», в основному, випускала інвертори.

Завдяки вжитим заходам у лабораторії Котельникова приблизно за три місяці після початку війни були виготовлені та випробувані лабораторні макети окремих основних вузлів апаратури «Соболь-П». Це були вузол частотних перестановок з інверсією спектра, вузол тимчасових перестановок, вузол шифратора на базі трансмітера та 5-рядкової перфорованої телеграфної стрічки (перфострічки), макет генератора, що створював гаму керування перестановками частотних смуг і тимчасових відрізків.

Крім того, в процесі «подолання труднощів» з'явилися і немало інших винаходів, але Котельников і його колеги їх не публікували і не патентували, по-перше, унаслідок секретності розробок, а, по-друге, на це у вчених просто «не було часу».

З якими труднощами довелося мати справу конструкторам у ході розробки, покажемо на прикладі вузла тимчасових перестановок. Він складався з двох основних об'єктів: прилад уповільнення мовного сигналу на 100 і 200 мілісекунд і схема переключення уповільнених сигналів, що здійснювала перестановку стомілісекундних відрізків мови. Тоді розглядалися 4 варіанти приладу уповільнення мовних сигналів:

1. Швидкість поширення звуку в повітрі складає 330 м/сек. Якщо взяти гумовий шланг довжиною 33 метри, подати на вхід його мовний сигнал (від динаміка), а на виході поставити мікрофон з підсилювачем, то одержимо сповільнювач на 100 мілісекунд. Досвід показав, що такий пристрій мав досить велике загасання на високих частотах, а якщо врахувати громіздкість пристрою, такий варіант виявився явно невідповідним.

2. Вдалося отримати шведську вузьку та порівняно тонку сталеву стрічку для магнітного запису. Для забезпечення малогабаритності приладу її натягували на барабан, намагаючись забезпечити досить гладкий стик. Однак при знятті мовних сигналів адаптером при проходженні стику виникав «щиглик», що значно заважав веденню переговорів. Спроби накласти на обід барабана кілька витків стрічки та здійснити запис по центру багатовиткової «навивки», також не дали позитивного результату, тому що адаптер, проходячи по стику двох витків, створював заважаючий шум.

3. Третя спроба зводилася до того, щоб «щиглик» повторювався якоможна менше. Для цього бралася довга петля, що проходила через багато роликів. У скільки разів збільшувалася довжина петлі, у стільки ж разів скорочувалося число «щигликів». Однак через громіздкість спорудження та великий шум під час руху сталевої стрічки цей варіант не пройшов.

4. Була використана звичайна циркулярна пилка, а її площина була добре відшліфована (для безпеки обслуговуючого персоналу зубці сточувалися). Запис здійснювався на площині диска. Адаптер відтворював запис, але якість мови при відтворенні була незадовільною.

Таким чином, і 4-й варіант виявився неприйнятним. В результаті було прийняте рішення щодо використання більш якісної для магнітного запису сталі та здійснення запису не на площині диска, а на його ободі.

Необхідний метал був знайдений на московському заводі «*Серп и Молот*», на якому створювалися експериментальні зразки сталі «*ЭХ-3А*» і «*ЭХ-6А*». Завод надав необхідну кількість сталі листової прокатки. Так, протягом декількох місяців була вирішена проблема створення вузла магнітного запису, іспити якого показали можливість його використання в майбутній апаратурі засекречування.

Наведений приклад досить чітко показує, на якому рівні комплектуючої техніки СРСР знаходився того часу. Забігаючи наперед відзначимо, що на другому році існування Марфинської лабораторії був утворений магнітний запис, що використовував диск із немагнітного матеріалу, обід якого мав тонке нікель-кобальтове покриття.

Оцінюючи в загальному вигляді результати робіт з секретної телефонії, можна сказати, що за цей період був створений фундамент для подальшого більш швидкого просування вперед у цій галузі техніки. Конкретизуємо цей загальний висновок, визначивши окремі його положення.

1. Важливе значення мало вже саме формулювання завдання щодо засекречування мовної інформації в практичній площині. Це послужило поштовхом до створення перших колективів розробників.

2. Була зібрана та узагальнена у вигляді довідок, оглядів, дипломних проектів студентів інформація щодо принципів засекречування телефонних переговорів.

3. Десятирічній період був багатий винаходами в сфері методів засекречування телефонних переговорів.

4. Було створено кілька лабораторних зразків, що дозволили експериментально перевірити можливість реалізації запропонованих ідей і провести їхні іспити на реальних каналах зв'язку.

5. Заводами були виготовлені перші невеликі партії найпростішої апаратури (яка за сучасною класифікацією відноситься до маскуючого класу).

6. Була створена служба експлуатації та накопичено перший досвід.

7. Були створені перші невеликі колективи розробників техніки засекречування, що стали основою для формування більш могутніх організацій.

Тим часом держава як могла захищала свої телефонні лінії урядового зв'язку. 16 січня 1940 року був виданий наказ НКВС № 0042 «Про покращення ВЧ-зв'язку», що передбачав подальший його розвиток та встановлення апаратури засекречування на таких лініях зв'язку України, як Харків-Донецьк, Харків-Запоріжжя, Харків-Дніпропетровськ, Київ-Вінниця і Київ-Чернігів.

До липня 1940 року з наявних 103 ліній ВЧ зв'язку 50 було обладнано апаратурою шифрування, а до квітня 1941 року шифратори було встановлено на 66 лініях із 134 наявних. Причому апарати складного засекречування С-1 були встановлені тільки на магістралях Москва-Ленінград і Москва-Хабаровськ. У абонентів вищої категорії, таких як члени Політбюро, була встановлена апаратура абонентського засекречування.

Згідно з Постановою РНК СРСР № 2408-107сс від 25 листопада 1940 року «Про включення в урядовий зв'язок ВЧ-об'єктів ВПС ЧА» апаратура засекречування встановлювалася на всіх таких лініях. Відповідно до Постанови завод «*Красная Заря*» був зобов'язаний розробити і виготовити до 1 січня 1941 року 10 зразків, а протягом лютого випустити ще 150 комплектів панелі ПЖ-8, яка виконувала функції простого шифратора і підключалася безпосередньо до апаратури ВЧ телефонування СМТ-34.

Разом з тим, говорити про успіхи в сфері розробки шифраторів не доводилося. Так, у листі заступника керівника НКВС В.Меркулова заступнику керівника НКЗ К.Сергейчуку, датованому 14 квітня 1940 року, констатувалося, що «розроблена за замовленням НКВС заводом «*Красная Заря*» апаратура для засекречування телефонних розмов має слабку стійкість і не має коду».

На початку 1940-х років розпочали використовувати апаратуру, що працюва-

ла за алгоритмом мозаїчного шифрування. Ці шифросистеми можна було розкрити, використовуючи аналізатор мовного сигналу – спектрометр. Хоча для цього було потрібно складне устаткування та фахівці. У квітні 1941 року була підготовлена «Довідка про стан урядового ВЧ-зв'язку», яка показала неготовність системи урядового зв'язку до роботи в особливих умовах. Зокрема, у документі перераховувалися усі відомі способи перехоплення інформації.

5.4. «Радянське вухо» і «Великий терор»

З червня 1936 року нарком шляхів сполучення Лазар Каганович разом з новим наркомом внутрішніх справ Миколою Єжовим зайнявся розслідуванням обставин діяльності колишнього наркому внутрішніх справ Генріха Ягоди і можливого встановлення несанкціонованої техніки прослуховування на урядових лініях зв'язку. Через деякий час вони виявили численні порушення, які допускав Ягода. Він несанкціоновано прослуховував розмови багатьох членів уряду, у тому числі і самого Сталіна.

У березні 1937 року заарештували Ягоду, який у в'язниці розповів, що дав вказівку начальнику оперативного відділу ГУДБ НКВС Карлу Паукеру (з 1936 року – начальник 1 відділу ГУДБ) прослуховувати всі телефонні розмови Сталіна, у тому числі й ті, що велися по ВЧ-зв'язку. З цією метою він неодноразово посилав Паукера до Німеччини для придбання спеціальної апаратури для дистанційного прослуховування. Її виявили в його робочому кабінеті та в одній конспіративній квартирі НКВС, яку використовував тільки Ягода.

Для підтвердження цього приведемо витяг з такого документу, як *«Протокол допроса № 5 Ягоды Генриха Григорьевича от 13 мая 1937 года» (ЦА ФСБ. Ф. Н-13614. Т. 2. Л. 117-145):*

«***Вопрос.*** *На допросе 26 апреля вы показали, что Волович наряду с другими заданиями, которые он выполнял в плане заговора, организовал для вас возможность прослушивания правительственных разговоров по телефонам «ВЧ». Когда, как и в каких целях вы прослушивали правительственные разговоры?*

Ответ. *Раньше чем ответить на этот конкретный вопрос, разрешите мне остановиться на общем состоянии, в котором я лично находился в продолжение многих лет моей заговорщической и предательской деятельности. Я всегда чувствовал к себе подозрительное отношение, недоверие, в особенности со стороны Сталина. Я знал, что Ворошилов прямо ненавидит меня. Такое же отношение было со стороны Молотова и Кагановича. Особенно меня тревожил интерес к работе Наркомата внутренних дел со стороны Николая Ивановича Ежова, который начал проявляться еще во время чистки партии в 1933 году, переросший в конце 1934 года в контроль, настойчивое влезание им в дела НКВД, вопреки препятствиям, которые мы (участники заговора) чинили*

ему; все это не предвещало ничего хорошего. Это я ясно понимал, отдавая себе во всем отчет, и все это еще больше усиливало тревогу за себя, за свою судьбу. Отсюда целый ряд мероприятий страховочного порядка, в том числе и мысль о необходимости подслушивания правительственных переговоров...

***Вопрос.** Вы показываете, что подслушивание правительственных разговоров являлось составной частью всей вашей системы мероприятий «страховочного порядка». Как оно было организовано?*

***Ответ.** Аппарат для прослушивания был по моему распоряжению куплен в Германии в 1933 году и тогда же был установлен у меня в кабинете инженером Винецким, работником Оперода. Распоряжение о покупке этого аппарата я дал Паукеру и Воловичу. Мысль о необходимости подслушивания правительственных разговоров возникла у меня в связи с разворотом моей заговорщической деятельности внутри НКВД. Меня, естественно, тревожила мысль, не прорвется ли где-нибудь нить заговора, не станет ли это известно в кругах правительства и ЦК. Особенно мне понадобилось подслушивание в дни после убийства С.М.Кирова, когда Ежов находился в Ленинграде. Но так как дежурить у подслушивающего аппарата в ожидании разговоров между Ежовым и Сталиным у меня не было никакой физической возможности, я предложил Воловичу организовать подслушивание переговоров Ленинград – Москва на станции «ВЧ» в помещении Оперода.*

***Вопрос.** Волович подслушивал разговоры между тов.Ежовым и тов. Сталиным?*

***Ответ.** Да, прослушивал и регулярно мне докладывал.*

***Вопрос.** А после событий, связанных с убийством тов.Кирова, продолжалось подслушивание?*

***Ответ.** Только тогда, когда Сталин выезжал в отпуск. Я помню, в частности, что в сентябре 1936 года Волович подслушивал разговор между Сталиным, находившимся в Сочи, и Ежовым. Волович мне доложил об этом разговоре, сообщил, что Сталин вызывает Ежова к себе в Сочи.*

***Вопрос.** Вы поручили Воловичу, немецкому шпиону, подслушивание правительственных разговоров не только потому, что эти разговоры интересовали вас, но и потому, что это требовала немецкая разведка. Вы признаете это?*

***Ответ.** Я давал задание Воловичу подслушивания правительственных разговоров только по мотивам, о которых я говорил выше. Но несомненно, что Волович передал содержание этих переговоров и в германскую разведку...*

Записано с моих слов верно, мною прочитано. Г.Ягода

Допросили:

Нач. отд. 4 отдела ГУГБ капитан государств. без. Коган

Опер.уполн. 4 отдела ГУГБ лейтенант государств. без. Лернер».

Під час допитів Ягоди слідчі з'ясували, що він навмисно гальмував створення систем криптозахисту зв'язку, оскільки це заважало йому контролювати відомства

і людей. З документів, направлених Ягоді керівниками технічних відділів НКВС, виявилося, що вже у 1935 році технічні фахівці визначили, що ВЧ-зв'язок легко прослуховувався, і по ньому не можна було вести секретні переговори.

На допитах Ягода пояснив, що він спеціально гальмував створення апаратури для захисту ліній зв'язку, оскільки не уявляв, як їх можна контролювати. Він вважав, що йому і в першу чергу Сталіну були потрібні такі канали отримання інформації, щоб можна було контролювати всіх.

Цією роботою керував начальник Оперативного відділу ГУДБ НКВС К.Паукер, який відповідав за всю систему урядової охорони. Його заступник Захар Волович, який займався урядовим зв'язком, через резервну станцію в будівлі НКВС на Луб'янці мав можливість прослуховувати всі переговори по внутрішньому «кремлівському» зв'язку та по ВЧ. «Кремлівський» телефонний зв'язок, а з 1935 року і ВЧ-зв'язок знаходилися у складі 13-го відділення Оперативного відділу, яке також називалося відділенням урядового зв'язку (далі – ВУЗ). Його працівники повинні були забезпечувати захист інформації, що проходив по цих лініях зв'язку, але попутно вони самі передавали її Воловичу, який докладав про все важливе безпосередньо Ягоді.

За інформацією радянського дипломата-перебіжчика Г.З.Беседовського, у Спецвідділі Бокія створювалася та застосовувалася техніка для прослуховування розмов, але не по телефонних лініях, як це робив ВУЗ у відділі Паукера, а у приміщеннях службових кабінетів, квартир і дач «відповідальних» працівників.

Фахівці НКВС створювали численні системи прослуховування, за допомогою яких збирали компрометуючий матеріал на всіх, хто цікавив Ягоду. Для цього в Німеччині закуповували величезну кількість систем для прослуховування. З початку 1920-х років по 1937 рік НКВС встановив декілька сотень тисяч мікрофонів у робочих кабінетах керівників різного рангу. Мікрофони встановлювали і в будинках, де вони проживали.

Відомий «Будинок уряду» у Москві, де жили багато наркомів і їх заступників, був буквально весь «нашпигований» мікрофонами. А у готелі «Москва», в якому зазвичай розміщувалися важливі гості і делегати з'їздів партій і конференцій, був розміщений цілий підрозділ НКВС, що здійснював цілодобове прослуховування кожного зітхання в будь-якому приміщенні цієї величезної будівлі. За цей період було використано більше 20 тисяч кілометрів дротів для підключення мікрофонів. Завдяки Ягоді система управління прослуховуванням стала фактично другою системою зв'язку в СРСР.

Для її організації виробничих потужностей СРСР було недостатньо. Розпочалися крупні закупівлі спецтехніки за кордоном. Зазвичай вони оформлялися у вигляді заявок від наркомату зв'язку (далі – НКЗ) СРСР. З 1924 року відповідальним за закупівлі був Захар Волович, який згодом став заступником начальника Закордонного відділу (далі – ЗВ) НКВС. Він також входив до складу керівництва наркомату зв'язку.

Звичайно, для організації прослуховування потрібна була реєструюча апаратура – магнітофони, а їх в СРСР не виготовляли. Кількість магнітофонів, що замовлялась наркоматом зв'язку у німецьких фірм, спочатку налічувалася тисячами штук, а потім – десятками тисяч.

Ягода створив, як він виразився під час допитів, систему пірамід прослуховування, величезне «радянське вухо», яке чуло будь-яке, навіть слабке, «шепотіння» невдоволення. А оскільки це «радянське вухо» було, в основному, створене на німецькому устаткуванні, то виникло не менше «німецьке вухо», яке, в свою чергу, уважно прослуховувало «радянське вухо».

Звичайно, такий всеосяжний контроль вимагав значних людських ресурсів. НКВС мудро вирішив використовувати співробітників НКЗ як позаштатних співробітників НКВС. У статистичних звітах, опублікованих у той час, повідомлялося про різке збільшення чисельності НКЗ. Преса пояснювала це турботою уряду про радянських людей, яким необхідний сучасний зв'язок у будь-який час.

Грандіозне будівництво «радянського вуха» не обійшлося без чуйного керівництва партії. Під час будівництва московського метро вірний Сталіну Каганович невсипущо контролював створення підземних контролюючих центрів, які могли функціонувати при будь-яких бомбардуваннях, оскільки під землею знаходилися основні кабелі і розподільники зв'язку.

Коли після арешту Ягоди Сталіну показали приміщення, де зберігалися записи телефонних розмови сотень тисяч радянських громадян, він був приголомшений розмахом робіт Ягоди. Ягода був новатором застосування найостанніших досягнень техніки. Хоча у нього була незавершена середня освіта, він любив похизуватися своїми технічними знаннями перед вченими світилами. На його вимогу

ЗВ НКВС надавав йому необхідну для нього технічну інформацію про останні світові новинки спецтехніки, а часто й самі новинки, якщо вдавалося десь їх вкрасти. У архівах Ягоди можна було знайти практично всі відомості про багатьох радянських людей, аж до чуток і інтимних подробиць. На допиті Ягода сказав: «Я знав все в СРСР, або майже все. Я навчив всіх і все підслуховувати та бачити».

Точні дані про «імперію прослушки» Ягоди отримати ніхто не зміг. Особливо про технічні особливості побудови своєї «імперії прослушки» і про те, у кого конкретно за кордоном купували спецтехніку. В допомогу для розгляду справи Ягоди був залучений Яків Серебрянський (Бергман), який був найближчим помічником розвідника Сергія Шпігельгласа, що брав участь в закупівлях спецтехніки. Серебрянський виявив у записаних телефонних розмовах інтимні переговори Єжова та Паукера, які підтверджували, що вони знаходилися у гомосексуальному зв'язку, і доповів про це Сталіну. Єжов на допиті детально розповів про це і про інших своїх партнерів.

Цікавий факт: відповідно до діючого в ті часи законодавства СРСР Єжова повинні були засудити також і за гомосексуалізм. Проте Сталін дав вказівку не розглядати ці вчинки Єжова. Мабуть, не хотів поширювати інформацію про гомосексуальні зв'язки у керівництві країни. Вірогідніше, не хотів, щоб його теж запідозрили в причетності до таких чоловічих «забав», оскільки за півтора роки «Великого терору» Єжов більше 1100 разів бував у Сталіна, тобто по два-три рази на день. А іноді Сталін вночі підвозив наркома на його дачу.

Вождь, знову наляканий темою гомосексуалізму та вірогідністю того, що можуть розкритися його інтимні розмови по телефону, підслухані командою Ягоди, наказав розстріляти всіх, хто був причетний до розслідування справи про прослуховування телефонних розмов, і в першу чергу Єжова, а потім Серебрянського і Шпігельгласа та багатьох технічних працівників. Тим паче, що в документах Єжова при обшуку виявили матеріали, які могли скомпрометувати Сталіна тим, що підтверджували його зв'язки з царськими жандармами. Сталін всіма доступними способами рятував свою репутацію незважаючи на будь-які жертви та відданість його соратників!

За його вказівкою велика частина матеріалів з архівів Ягоди була знищена. Технічне обслуговування «радянського вуха» фактично припинилося, оскільки багато інженерів, що займалися цим, було розстріляно або арештовано.

Так почалося грандіозне «чищення»: знищували всіх, хто знав хоча б що-небудь про цей проект, а також людей, які відповідали за урядовий та засекречений зв'язок у СРСР. Найближчі соратники Сталіна, Каганович, Ворошилов, Будьонний, налякані такою своєрідною формою технічної змови, в різкій формі зажадали розслідувати діяльність співробітників всіх організацій, які займалися питаннями зв'язку, її захисту та контролю.

16 лютого 1937 року був здійснений перший арешт – помічника начальника 6 відділення 2 відділу ГУДБ Ігоря Васильовича Вінецького. 53-річний Вінецький, випус-

кник одного з німецьких престижних інститутів, інженер, зв'язківець технолог широкого профілю, знавець трьох іноземних мов, був оголошений шпигуном за підозрою, що перебуваючи за кордоном, він отримував цінні подарунки, купував не ту технічну апаратуру, дарма витрачав державні гроші, невірно встановлював техніку, не захищав членів уряду від «прослушки».

Ось як про це пише 22 березня 1937 року Єжов у своїй доповідній записці Сталіну *(АП РФ Ф.3, Оп.58. Д.250. л.116а-116б):*

«НКВС № 56360. Направляю 4 протоколи допиту арештованого працівника Оперативного відділу ГУДБ інженера Вінецького Ігоря Васильовича.

Вінецький працював у НКВС з 1928 року і відав секретною телефонною технікою, у тому числі і станцією високої частоти «ВЧ».

В період 1928-1933 р.р. він неодноразово виїжджав за кордон з метою закупівлі телефонного устаткування, необхідного для секретної роботи НКВС.

У 1929 році, знаходячись у Берліні, Вінецький був завербований німецькою військовою розвідкою, за завданнями якої виконував різні доручення розвідувального характеру.

Вінецький систематично підслуховував по «ВЧ» розмови керівників партії та уряду, передаючи їх зміст німецькій військовій розвідці через її агентів – представників фірми «Сіменс» Шварца, Бергмана і Ерузаліма-Вельтера.

Звертає на себе увагу свідчення Вінецького про те, що за спеціальним завданням Ягоди, він купив за кордоном особливий апарат для підслуховування ліній «ВЧ», який був встановлений у кабінеті Ягоди. Цей апарат був знятий за декілька днів до мого вступу на посаду Наркома Внутрішніх Справ.

На неодноразові мої запити Воловичу з цього приводу, він мене обдурював, запевняючи, що у Ягоди був тільки звичайний апарат для підслуховування розмов по загальній міській телефонній мережі.

Вінецький користувався особливою довірою і заступництвом Воловича, якому систематично привозив дорогі закордонні речі, купуючи їх на свої гроші та на гроші, отримувані ним від німецької розвідки за шпигунські відомості.

Волович арештований.

Резолюція Сталіна: Слідчий не знає справи, він майже пасивний при допиті. Справа дуже серйозна, а слідчий відноситься до справи, як до звичайної».

Попсували нерви і Михайлу Ільїнському, згадали, скільки технічних висновків по ВЧ-зв'язку він зробив разом з Вінецьким. Але «криміналу» не виявили, не заарештували та навіть підвищили за посадою.

16 травня 1937 року був арештований начальник 9 відділу (колишній Спецвідділ при ВНК-ДПУ) ГУДБ НКВС Гліб Бокій. Цього дня його викликав до себе нарком внутрішніх справ Микола Єжов. Він зажадав від нього компрометуючі матеріали на деяких членів ЦК і високопоставлених комуністів, які Бокій збирав з 1921 року

за особистим розпорядженням Леніна (так звана «Чорна книга»). При цьому Єжов продемонстрував Бокію, що це не його власна ініціатива, а «наказ товариша Сталіна». Бокій на це розлютився: «А що мені Сталін?! Мене Ленін на це місце поставив!»

Після сказаних слів Бокій додому вже не повернувся. Уже на перших двох допитах 17 і 18 травня Гліб Іванович «покаявся» слідчим у своїх гріхах. Повідомив про організовану у 1925 році разом із вченим-містиком Барченко масонську ложу «Єдине трудове братерство». В результаті всі її члени були заарештовані та розстріляні.

Єжов особисто перевіряв біографії співробітників спецвідділу Бокія. Виявилось, що багато співробітників його відділу були у минулому дворянами та навіть князями, що ще більше посилило гнів Сталіна. В результаті практично був розгромлений спецвідділ Бокія: близько 70 % співробітників його відділу було репресовано.

На наступний ранок після арешту Бокія на своїй московській квартирі на Ленінградському шосе був заарештований його колега і конкурент Олександр Формайстер, нині майже забутий засновник більшості методів негласного вилучення інформації, що застосовували в СРСР.

Перлюстрацією, виїмкою та обробкою дипломатичної пошти іноземних держав, оперативним обслуговуванням іноземних дипломатичних місій і представництв займалося 1-е відділення контррозвідувального відділу ОДПУ. Формайстер залучив до цієї роботи старих фахівців царського Охоронного відділення з організації так званих «чорних кабінетів». Він у короткий термін навчив своїх співробітників методам таємного фізичного проникнення, розтину сховищ дипломатичної пошти, підробки пломб і друку, підмішування дурманних препаратів дипломатичним кур'єрам, а трохи пізніше почав використовувати техніку прослуховування.

Він першим створив з цією метою технічну лабораторію, а потім і пересувний вагон-лабораторію, який причіплювали до потягів з міжнародними вагонами для дипломатів. У результаті всі іноземні посольства, консульства, а також представництва приватних осіб були «нашпиговані» підслуховуючою апаратурою та агентурним апаратом. Завдяки Формайстеру через декілька років дипломатична таємниця в СРСР просто перестала існувати. Разом з тим, це не допомогло йому уникнути арешту та розстрілу.

Репресії сильно вдарили по криптослужбах НКВС і РУ РСЧА на чолі з їх керівниками, що привело до зупинки розробки перспективної спеціальної апаратури засекречування та систем перехоплення. Арешти боляче вдарили по кращих розробниках і виробниках шифрувальної техніки в СРСР. Розстріляли практично всіх начальників відділів РУ РСЧА і їх заступників. У 1937 році криптослужби в НКВС і РУ РСЧА були фактично знищені також, як і радіорозвідка. Виробництво нових видів шифрувальної техніки припинилося.

На репресованих співробітників часто «списувалися» організаційно-технічні недоробки, допущені при будівництві та обладнанні об'єктів урядового зв'язку. «Те-

лефонна станція Політбюро привезена з Німеччини і змонтована під керівництвом надалі викритого «шпигуна» Вінецького, – наголошувалося у доповідній записці В.Меркулова на ім'я Л.Берії від 5 лютого 1939 року, – Кремлівська АТС також привезена з Німеччини, технічно зношена. Телефонний зв'язок ВЧ також спочатку змонтовувався з імпортної апаратури під керівництвом того ж Вінецького».

За архівними даними відомо, що були арештовані та розстріляні у такій послідовності:

† Ігор Васильович Вінецький – помічник начальника 6 відділення (урядового зв'язку) 2 відділу ГУДБ – 16 лютого та 14 серпня 1937 року;

† Захар Ілліч Волович – заступник начальника оперативного відділу ГУДБ – 22 березня та 14 серпня 1937 року;

† Іван Юрійович Лоренс – начальник 6 відділення 2 відділу ГУДБ – 23 квітня та 14 серпня 1937 року;

† Гліб Іванович Бокій – начальник 9 відділу ГУДБ (колишній Спецвідділ) – 16 травня та 15 листопада 1937 року;

† Євген Євгенович Гоппіус – начальник хімічної лабораторії 9 відділу ГУДБ – 4 червня та 30 грудня 1937 року;

† Федір Іванович Ейхманс – заступник начальника 9 відділу ГУДБ, начальник 3 відділення цього відділу – 22 липня 1937 року та 3 вересня 1938 року;

† Едуард Янович Озолін – начальник секретно-шифрувального відділення РУ РСЧА – 29 листопада 1937 року та 25 квітня 1938 року;

† Олександр Петрович Лозовський – начальник 10 відділу (спеціальної техніки) РУ РСЧА – 2 грудня 1937 року та 22 серпня 1938 року;

† Яків Аронович Файвуш – начальник 6 відділу (радіорозвідки) РУ РСЧА – 16 грудня 1937 року та 27 квітня 1938 року;

† Вольдемар Янович Закіс – колишній (до 1930 року) начальник шифрувальної частини РУ РСЧА – у 1937 році та у жовтні 1938 року;

† Карл Густавович Тракман – військовий цензор 8 відділу (до 1936 року – помічник начальника 5 відділу) РУ РСЧА – 10 січня та 11 травня 1938 року (помер у в'язниці);

† Олександр Георгійович Гусєв – начальник 4 відділення 9 відділу ГУДБ – 29 січня та 22 квітня 1938 року;

† Володимир Дмитрович Цибізов – помічник начальника 9 відділу ГУДБ, начальник 8 відділу ГШ РСЧА – 29 січня та 9 травня 1938 року;

† Антон Дмитрович Чурган – начальник технічного відділення 9 відділу ГУДБ – 29 квітня та 28 серпня 1938 року;

† Михайло Сергійович Альохин – начальник відділу оперативної техніки НКВС – у вересні 1938 року та лютому 1939 року;

† Ісаак Ілліч Шапіро – начальник 9 відділу ГУДБ (з 05.07.1937 по 28.03.1938) –

11 листопада 1938 року та 4 лютого 1940 року;

✝ Семен Борисович Жуковський – колишній начальник 12 відділу (оперативної техніки) ГУДБ – 23 жовтня 1938 року та 24 січня 1940 року.

Пощастило лише Борису Володимировичу Звонарьову – заступнику начальника 7 (дешифрувального) відділу РУ РСЧА, який був арештований 13 вересня 1938 року, але не розстріляний та навіть реабілітований 28 лютого 1941 року.

Нові кадри, які прийшли на заміну репресованих фахівців, мали дуже слабку технічну підготовку та не могли розібратися у всіх тонкощах побудованої системи. Тим паче, що фахівці, які обслуговували цю систему прослуховування, проходили технічне навчання у німецьких фірмах, і це було найважливішою підставою для звинувачення їх у шпигунстві. Тільки через два роки, у 1939 році, начальник охорони Сталіна Микола Власик пригадав про численні системи прослуховування, встановлені Вінецьким, який був інспектором зв'язку НКВС і НКЗ та контролював працездатність систем прослуховування, встановлених за вказівкою Ягоди.

У своєму рапорті від 8 грудня 1939 року на ім'я комісара державної безпеки 1-го рангу Л.Берії він повідомив, що телефонний зв'язок по АТС ВЧ дає можливість підслуховувати телефонні розмови:

«Телефонний зв'язок для осіб, що охороняються, здійснений по прямих спеціальних кабелях, що йдуть від об'єктів охорони до тефонних станцій у Кремлі. Виняток становлять об'єкт Архангельське, Мешеріно, Горі-6, де телефонний зв'язок до виходу з міста здійснений по прямих кабелях і далі по повітряних лініях. Телефонний зв'язок з народними комісаріатами для осіб, що охороняються, також здійснений по прямих кабелях.

Зв'язок по міських телефонних апаратах здійснений через кроси міських телефонних станцій.

До 1937 року будівництвом і експлуатацією телефонного зв'язку для осіб, що охороняються, керував шпигун Вінецький, під безпосереднім керівництвом і участю якого були побудовані і введені в експлуатацію наступні споруди:

1. Спеціальна телефонна станція АТС у Кремлі.

2. Прямий спеціальний кабель 27х4 по Можайському напрямку.

3. Прямі спеціальні кабелі між телефонною станцією у Кремлі та народними комісаріатами.

4. Прямі телефонні кабелі до міських телефонних станцій НК зв'язку.

5. Побудована і введена в експлуатацію телефонний зв'язок по АТС ВЧ.

Всі ці споруди, побудовані і введені в експлуатацію шпигуном Вінецьким, викликають певні думки щодо гарантії секретності розмов, підключення, а, отже, і прослуховування розмов, а також не виключена можливість сторонніх відпаювань у цих кабелях... Телефонний зв'язок АТС ВЧ знаходиться в такому ж стані. Тому з упевненістю можна сказати, що телефонний зв'язок по АТС ВЧ за своїми

технічними даними, тобто наявність повітряних ліній і проміжних станцій, дає пряму можливість підслуховувати розмови...»

Звичайно, М.Власик не був технічним фахівцем і ці дані отримав у в'язниці від колишніх технічних фахівців НКВС, яких «посадили» за участь у шпигунстві. Якщо урядовий зв'язок можна було прослуховувати, що казати про звичайний зв'язок!

Цікава ситуація складалася у СРСР того часу з технічним захистом урядового зв'язку. Після численних репресій СРСР залишився без сучасних високошвидкісних систем шифрування та ефективних систем радіоперехоплення. Для шифрування інформації застосовували, в основному, ручні документи кодування. Швидкість шифрування інформації за їх допомогою була надзвичайно низькою.

Шифрування наказу або розпорядження, обсяг якого займав півтори друкарські сторінки, займало приблизно 4-5 годин. Відповідно, стільки ж часу витрачалося на дешифрування. Під час шифрування або передачі тексту по телеграфних каналах зв'язку часто допускалися помилки, а це відбувалося практично завжди через громіздкість та незручність використання шифроблокнотів і неякісних каналів зв'язку. Це також збільшувало час на шифрування і дешифрування інформації. На шифрування-дешифрування півтора сторінок тексту наказу йшло близько 10-12 годин. Якщо шифрограму передавали голосом по звичайному телефону, її обробляли приблизно стільки ж часу, а при погіршенні чутності шифрування було взагалі неможливе.

Зашифровані дані можна було передавати як по телеграфних лініях зв'язку, так і кодом Морзе по радіолініях зв'язку. Це дуже влаштовувало керівника НКО К.Ворошилова. Керівництво озброєних сил СРСР ще з громадянської війни звикло передавати накази по телеграфу.

Що залишалося робити Сталіну з «імперією прослушки», побудованою Ягодою? Він вже не міг спокійно говорити по телефону, побоюючись, що його можуть прослуховувати невиявлені вороги. Тому Сталін дав вказівку начальнику ГУДБ НКВС М.Фриновському про закупівлю німецької шифрувальної техніки. Він більше побоювався свого ближнього оточення, ніж «далеких» німців. У крайньому випадку можна було уздовж всієї лінії зв'язку поставити солдатів НКВС, які б спостерігали, що її ніхто не прослуховує.

22 червня 1937 року Фриновський направив запит народному комісару зовнішньої торгівлі Розенгольцу про виготовлення шифрувальної техніки за кордоном. Пізніше, у 1939 році, це розцінили як співпрацю з німецькою розвідкою. 6 квітня 1939 року Розенгольца заарештували, а у 1940 році розстріляли. Також розправилися і з Фриновським. Він був арештований того ж дня, 6 квітня 1939 року, і розстріляний у 1940 році. Всі, хто брав участь у закупівлі та встановленні німецької шифрувальної техніки, були розстріляні. Сталін умів ліквідовувати небажаних свідків своїх контактів із німцями.

Щоб не афішувати використання німецької шифрувальної техніки, її купували

у Німеччині, привозили у СРСР, знімали етикетки виробника, та видавали за техніку радянського виробництва. Так німецькі шифратори опинилися на радянських урядових лініях зв'язку.

23 серпня 1939 року вночі рейхсміністр Іоахим фон Ріббентроп прилетів до Москви на літаку фюрера «Кондор Імельман III». Його делегація складалася з 30 осіб. Троє з цієї делегації були з НДІ Герінга та привезли телефонний «скремблер» (англ. *scrambler* - шифратор) і шифрувальний апарат «Енігма».

Перша зустріч Ріббентропа із Сталіном відбулася в три години ночі. Результати переговорів не влаштували Ріббентропа, і він виїхав до свого посольства. В цей час фахівці Герінга разом із співробітниками ВУЗ 2-го спецвідділу НКВС на чолі з Ільїнським і Воробйовим почали встановлювати телефонно-телеграфний зв'язок Москва-Берлін. До 21-00 цього ж дня зв'язок був встановлений. У 22-00 Ріббентроп приїхав у Кремль і запропонував Сталіну самому з'ясувати всі незрозумілі питання безпосередньо з Гітлером. Близько години Сталін розмовляв з Гітлером по «скремблеру» фірми «Сіменс». Його працездатність заздалегідь випробували на лініях зв'язку Москва-Ленінград з 1937 по 1938 роки.

Потім всі, хто брав участь в організації підготовки зв'язку між Гітлером і Сталіним, таємничим чином зникли у в'язницях або були не менш загадковим чином убиті. Так трапилося з першим начальником ВУЗ Ільїнським, який 13 жовтня 1941 року був застрелений із пістолета в потилицю в будівлі Центрального телеграфу заступником наркома зв'язку Г.Омельченком.

Він одразу був заарештований, але Сталін наказав «зам'яти» цю справу, і ска-

зав Берії: «На фронт не пускати, наручники зняти, генералів втрачати у військовий час небезпечно». Через рік Омельченко був підвищений у званні та закінчив свою службу у 1953 році у званні генерал-лейтенанта. У 1947 році арештований був і Воробйов, але його виновність доведена не була, і у 1952 році він був звільнений.

Репресії 1937 року негативно вплинули також на виробництво шифрувальної техніки в СРСР. Особливо це торкнулося провідного виробника шифрувальної техніки – заводу «*Красная Заря*» в Ленінграді. Багато перспективних розробок шифрувальної техніки залишалися на рівні дослідних зразків. Перспективна апаратура М-100/101 була випущена дуже маленькою серією та призначалася для шифрування інформації, що передавалася по телеграфних лініях зв'язку між штабами військових округів і флотів.

Труднощі були і з випуском апаратури шифрування С-1 для засекречування телефонних розмов по звичайних телефонних лініях. Щоправда, ступінь захисту у неї був дуже низький, тому вона, в основному, захищала від стандартних схем прослуховування, які співробітники НКЗ мали на своїх станціях. Була розроблена апаратура шифрування для телеграфного зв'язку С-380М. Її стійкість теж була слабка. Вона, в основному, використовувалася для захисту від можливого прослуховування співробітниками НКЗ. Сталін не забув, що керівниками НКЗ багато років були його вороги Риков і Ягода.

До 1941 року на заводі «*Красная Заря*» тільки почали освоювати виробництво невеликої серії шифрувальної техніки для «закриття» розмов по польових телефонних раціях, що використовувалася в РСЧА. Розробкою шифрувальної апаратури для «закриття» радіоканалів фактично ніхто не займався. Отже на початку війни радянські танки не були оснащені взагалі ніякою апаратурою шифрування. Були тільки макети типу «*ЕИС-3*», однак для їх завершення було потрібно багато часу.

Сталін боровся з «радянським вухом», створеним Ягодою, як тільки міг. Йому було не до захисту від зовнішнього ворога. Зв'язок своєї могутньої армії, розвідки, уряду і ЦК він теж не дуже хотів захищати, побоюючись змов. В результаті на початок Великої Вітчизняної війни в СРСР не була розроблена та впроваджена на лініях зв'язку РСЧА, НКВС, ЦК і інших оборонних відомств апаратура засекречування гарантованої стійкості від прослуховування! Більше того, з відкриттям ВЧ-лінії зв'язку Москва-Берлін, яка проходила через Брест, німецька розвідка отримала можливість прослуховувати всі розмови радянського уряду та наркомату оборони.

5.5. Урядовий зв’язок у Вітчизняній війні

Ось як згадує початок Великої Вітчизняної війни ветеран урядового зв’язку М.Карпов:

«У ніч із 21 на 22 червня 1941 року особовий склад львівського відділення виконував роботи щодо переобладнання ВЧ-станції в будинку Управління НКВС... При-

близно о 2-ій годині ночі як ніколи піднялося навантаження на комутаторі, стали надходити тривожні дзвінки зі Станіслава, Дрогобича, інших міст. З Перемишля надійшло донесення про те, що після сильного шуму машин і танків по наших прикордонних районах був відкритий артилерійський вогонь. Тієї ж години в Тернополі з'явились абоненти: командуючий Київським військовим округом генерал Кирпонос, начальник штабу генерал Тупіков, член військової ради Хрущов, начальник особливого відділу Селіванський та начальник оперативного управління полковник Баграмян.

Після деякого затишшя львівська ВЧ-станція прийняла таке небувале навантаження, що на комутаторі одна людина не змогла впоратися, довелося на допомогу надіслати ще одного техніка. Розпочалися безперервні дзвінки командуючому 6-ою армією, командуючому прикордонним округом генералу Хоменку, до обкому, Управління НКВС, до Києва, Москви.

На світанку німці почали бомбити львівський аеродром та місто. Одна бомба впала у дворі поштамту, перед входом у напівпідвал, де був обладнаний ЛАЗ, і не вибухнула. Між станцією «ВЧ» та міжміською телефонною станцією після бомбардування був порушений зв'язок, МТС не відповідала. Я був змушений бігти до МТС. Виявилося, що міжміська телефонна станція не відповідала тому, що співробітники кинули свої робочі місця й розбіглися, хто у підвал, а хто додому. У місті після бомбардування було тихо, пустельно, на вулицях ходили самі військові, проходили колони техніки, танків було дуже мало.

Звичайно, ми були налякані ситуацією, що склалася. Я доповів начальнику спецвідділу П.Копилову (загинув у Куп'янську), який прийняв рішення відправити всіх жінок у тил. Чоловіки... залишилися обслуговувати ВЧ-станцію. Абоненти виїхали на запасні пункти управління за містом, а ми залишилися у Львові. Незважаючи на нальоти ворожої авіації, робота відділення увійшла в нормальний ритм, ми якось втратили почуття страху.

На другий день війни активізували свої дії бойові групи ОУН, на вулицях розпочалася стрілянина. Була пошкоджена повітряна лінія на Тернопіль, у районі парку. Ми виїхали усувати пошкодження, але два кулемети з костьолу не давали цього зробити. Лише за допомогою танку, який надіслав начальник прикордонних військ, вдалося придушити вогневу точку та поновити зв'язок.

Бої ставали все більш жорстокими. Оунівці обстрілювали подвір'я Управління НКВС, стріляли по окремих військових, по частинах на вулицях. У деяких районах Львова ще до приходу німців зав'язалися вуличні бої. На 3-ій чи 4-ий день запеклі бої з участю великої кількості танків з обох сторін розгорнулися між Львовом і Луцьком.

Нашому відділенню керівництво НКВС поставило завдання забезпечити ВЧ-зв'язок Південно-Західному фронту після залишення Львова. Відповідальним за організацію зв'язку був призначений я. Але я не тільки не уявляв, яка це відпо-

відальність, але й не знав, як цей зв'язок буде здійснюватися, якими засобами, силами. Не уявляли цього й наші вищі інстанції. Про майно «НЗ» ми не мали ніякого уявлення, його ніде не було. Як організувати зв'язок, чим і з ким – це теж було невідомо. Я знав лише, що після здачі Львова треба їхати до Тернополя й обслуговувати місцеву ВЧ-станцію. Штаб фронту вже був сформований.

На п'ятий день війни німці далеко обійшли Львів. Начальник Управління НКВС капітан держбезпеки Михайлов повідомив, що Управління підлягає евакуації. Заступник Наркому Сєров наказав начальнику прикордонного округу генералу Хоменку виділити нам для охорони два взводи прикордонників з кулеметами на двох військових вантажівках. Скориставшись військовим станом, ми зуміли мобілізувати ще дві цивільні машини з водіями – поляками Кінересом та Данеком. Ці поляки дійшли з нами до Воронежа, а потім вступили до Війська польського.

На п'ятий день війни ми залишили Львів, забравши з собою апаратуру НВЧТ та шифрувальні приставки. Решту апаратури побили, закоротили джерела живлення, підпалили таємну документацію та виїхали до Тернополя. Але штаб Південно-Західного фронту був уже в Житомирі. Не затримуючись, через Вінницю ми виїхали до Житомира, але штабу фронту там вже не було. У Києві отримали вказівку виїхати до Броварів, де й перебував штаб фронту. Позивний нашої ВЧ-станції був «*Пурга*».

На околиці Броварів ми організували ВЧ-станцію з апаратури, що привезли зі Львова. Частину техніки дав Київ, а комутатор Р-20 дав начальник зв'язку фронту генерал Добикін. Упродовж війни комутатори були найбільш слабким місцем ВЧ-зв'язку. Відразу з'явилося багато труднощів. Ніхто нас не хотів брати на продовольче, речове, фінансове забезпечення через відсутність атестатів.

Абоненти не мали уявлення про правила та вимоги, що висувалися до урядового зв'язку. Не знаючи специфіки роботи, командування фронтом вважало, що ми повинні виконувати всі їхні вказівки щодо включення абонентів, та що ми підпорядковуємося начальнику зв'язку фронту. Командуючий фронтом Кирпонос був дуже здивований, коли я не виконав його наказ – включити на комутатор ВЧ-станції командуючого артилерією, тилу та деяких інших абонентів.

Він був дуже обурений, що якийсь молодший лейтенант держбезпеки не виконує наказу командуючого, і дуже сварив за це начальника зв'язку фронту. І коли мені довелося в особистій бесіді пояснити наші права, обов'язки та вимоги до абонентів ВЧ-зв'язку, що пред'являються НКВС, він, отримавши роз'яснення з цього приводу з Генерального Штабу, почав ставитися до нас дуже добре. Це були перші кроки в організації урядового ВЧ-зв'язку на Південно-Західному фронті».

З початком Великої Вітчизняної війни різко зросла роль урядового зв'язку для забезпечення безперебійним зв'язком в умовах найтяжкого воєнного часу Ставки Верховного Головнокомандувача (далі - СВГК) і ще 735 абонентів вищого ешелону влади і командування Армії і Флоту, наркоматів і відомств. З метою забезпечен-

ня живучості та безпеки Центральної станції ВЧ-зв'язку вона була перенесена до захищеного місця – на платформу станції московського метро «Кіровська» (нині - «*Чистые пруды*»).

20 липня 1941 року на базі ОТБ НКВС, до якого входило ВУЗ, і 4-го відділу НКДБ був організований 4-й спецвідділ НКВС (ОТБ і ВЧ-зв'язок). Його начальником став майор держбезпеки Кравченко, а його помічником і начальником 8-го відділення (ВЧ зв'язок) - капітан держбезпеки Ільїнський. Основними завданнями спецвідділу було, крім забезпечення абонентів урядовим зв'язком, використання ув'язнених фахівців для виконання науково-дослідних і проектних робіт з розробки, зокрема, нових засобів радіозв'язку, оперативної техніки та апаратури засекречування.

2 жовтня того ж року відбулася одна з найважливіших подій в історії урядового зв'язку країни. Наказом НКВС № 001430 відділення урядового ВЧ зв'язку виділялося з 4-го спецвідділу в самостійну структуру в рамках наркомату Відділ урядового зв'язку (далі - ВУЗ) НКВС, на який була покладена відповідальність за зв'язок СВГК з командуванням усіх діючих фронтів і армій, а також із союзними, республіканськими та обласними центрами тилових регіонів країни, забезпечення вузлів ВЧ-зв'язку та схоронність спецапаратури, підбір, підготовку й розміщення кадрів фахівців урядового зв'язку в центрі й на місцях, у тилу й на фронті.

Начальником ВУЗ НКВС був призначений капітан держбезпеки Ільїнський. Після його трагічної загибелі 15 жовтня 1941 року до виконання обов'язків начальника ВУЗ приступив капітан держбезпеки Воробйов. Початковий штат ВУЗ становив усього 62 одиниці та складався з таких підрозділів:

- 1 відділення - експлуатація зв'язку;
- 2 відділення - розвиток і будівництво ВЧ зв'язку;
- 3 відділення - радіозв'язок;
- 4 відділення - лінійна експлуатація;
- 5 відділення - кадри;
- 6 відділення - матеріально-технічне постачання;
- спецлабораторія.

З урахуванням настійної потреби в організації стійкого засекреченого польового телефонного ВЧ зв'язку в ланці Ставка-фронт-армія в серпні 1941 року були засновані посади Уповноважених з урядового зв'язку при штабах фронтів, а наприкінці листопада – початку грудня стали створюватися ВУЗ фронтів, що передбачали введення в дію ВЧ станцій у штабах оперативних з'єднанъ. До початку 1942 року були сформовані ВУЗ на 10 діючих фронтах, при яких були створені фронтові ВЧ станції, а на найбілъш важливих напрямках – перші ВЧ станції в штабах армій. Загальний штат фронтових ВУЗ становив 500 співробітників.

Гостро постало питання про ВЧ зв'язок з Ленінградським фронтом і містом, коли

наприкінці 1941 року Ленінград був блокований німцями. Наркомати зв'язку та оборони прийняли рішення в екстреному порядку прокласти кабельну лінію зв'язку єдино можливим напрямком – дном Ладозького озера. Робота велася вже під обстрілом супротивника. У результаті був організований проводовий зв'язок з Ленінградом через Вологду на Тихвін, далі – кабелем до Всеволожької, потім по повітряній лінії до Ленінграда. Ставка всю війну мала з Ленінградом стійкий ВЧ зв'язок.

Головним нормативним актом для першого періоду війни, що регламентував діяльність органів управління службами урядового зв'язку Ставки ВГК із фронтами й арміями, була «Інструкція з обслуговування урядового ВЧ-зв'язку НКВС» від 3 січня 1941 року. Наступна «Інструкція про роботу урядового зв'язку у військовий період» від 2 жовтня 1942 року вже містила спеціальний розділ щодо організації засекреченого зв'язку в оперативно-стратегічній ланці військового управління.

Начальник фронтового ВУЗ (він же - начальник урядового зв'язку НКВС фронту) був зобов'язаний у повсякденній роботі з керівництва фронтовими станціями та лінійними спорудами тісно взаємодіяти з наркомами внутрішніх справ республік і начальниками управлінь НКВС областей, на території яких розташовувалися станції та проходили магістральні лінії зв'язку. Весь особовий склад станцій і лінійних споруд фронтового напряму в оперативно-технічному відношенні підпорядковувався начальнику фронтового ВУЗС, він же у свою чергу підпорядковувався безпосередньо ВУЗ НКВС, виконуючи тільки його вказівки, розпорядження та накази.

Керівництво роботою стаціонарних і пересувних ВЧ станцій, організованих при штабі фронту, здійснював начальник фронтової станції, який призначався на посаду наказом НКВС і підпорядковувався безпосередньо начальнику урядового зв'язку фронту. Начальник пересувної ВЧ станції призначався наказом НКВС і, підпорядковуючись безпосередньо начальнику фронтової станції, був одночасно ад'ютантом з

урядового зв'язку при командувачі фронтом (призначення на суміжну посаду здійснювалося особливою вказівкою ГШ РСЧА).

В цілях надання ДКО негайного ВЧ зв'язку з штабами фронтів при ВУЗ НКВС функціонував спеціальний комутатор, куди включалися прямі ВЧ канали від штабів фронтів з кінцевими пристроями засекречування, абоненти за особливо затвердженим ДКО списком, а також з'єднувальні лінії від центральної станції ВЧ зв'язку.

Для технічного спостереження за роботою прямих ВЧ каналів, обладнаних апаратурою засекречування, а також для надання абонентам вищої категорії негайного ВЧ зв'язку на спецкомутаторі було введено чергування кваліфікованих інженерів ВУЗ НКВС. Всі вказівки чергових, що стосувалися настроювання ВЧ каналів фронтових напрямів, повинні були виконуватися технічним персоналом периферійних станцій беззастережно та негайно.

Організація фронтових мереж урядового зв'язку ускладнювалася тим, що на початку війни ОТБ НКВС не мав в своєму розпорядженні портативної польової апаратури для створення пересувних станцій, необхідних для роботи на фронтах і в арміях. Для організації ВЧ каналів використовувалися прийняті у той час на міжміській мережі НКЗ системи ущільнення СМТ-34 і ТВЧ-34. Це була суто стаціонарна апаратура. Стояки висотою 2,5 метра важили більше 400 кілограм. На автомашині стояк можна було перевозити, тільки поклавши на бік. Ніякої тряски апаратура не витримувала. Найчастіше після перевезення доводилося цілодобово відновлювати монтаж.

Не було також пристосованих до польових умов комутаторів, акумуляторів, блокстанцій та іншого устаткування. Усе треба було створювати заново. Виходячи з цього, необхідно було в найкоротші терміни організувати розробку та серійне виробництво комплексу польової апаратури ВЧ зв'язку. Тим паче, що, мінімальна потреба в апаратурі зв'язку для підрозділів ВУЗ тільки на 3-й квартал 1941 року складала близько 200 півкомплектів.

Єдиною базою для виробництва апаратури далекого зв'язку в той час був цех на ленінградському заводі «*Красная Заря*». Але до кінця 1941 року Ленінград виявився у блокаді. Завчасно були вжиті екстрені заходи щодо евакуації цього цеху до Уфи, де був створений завод № 697 з виробництва апаратури далекого зв'язку та науково-дослідний інститут. Після введення облогового положення в Москві всі лабораторії, що займалися секретною телефонією, також були евакуйовані з наданням співробітникам «броні» від мобілізації до армії. Евакуація до Уфи відбулася наприкінці жовтня 1941 року. Значна частина документації та листування, а також лабораторних макетів були знищені.

Зусиллями керівництва НКВС восени 1941 року в Державному союзному виробничо-експериментальному інституті «*ГСПЭИ № 56*» НКЕП (Уфа) був зібраний великий колектив фахівців, зокрема групи Єгорова та Старіцина, які були переве-

дені до Уфи з ленінградського заводу «*Красная Заря*», а також лабораторія ЦНДІЗ Котельникова, передана в розпорядження НКЕП з НКЗ. Інститут очолив Єгоров, а у 1943 році його змінив Котельников. З боку ВУЗ НКВС діяльність «*ГСПЭИ № 56*» координував інженер Олександр Спиридонович Колядов. Інститут зайнявся розробкою та підготовкою до серійного виробництва цілого ряду нових типів апаратури зв'язку в портативному виконанні.

Завдяки напруженій роботі колективів, очолених освіченими фахівцями Плешаковим і Востоковим, вже у 1942 році була створена 3-канальна польова апаратура СМТ-42 «Сойка», а потім СМТ-44 (польовий варіант апаратури СМТ-34: висота - 60 см, маса - 50 кг). Вона була зручна для швидкого розгортання й згортання ВЧ станцій, витримувала тряску під час перевезення. Була також розроблена портативна апаратура ВЧ телефонування НВЧТ-42 «*Сокол*», що передбачала використання двох варіантів: організацію по одному ланцюгу 2-х незасекречених розмов або 1-ї розмови з засекречуванням апаратурою складної схеми з кодуванням.

Перелік апаратури засекречування у перший період війни був також істотно доповнений. Вже 4 липня 1941 року лабораторією 4-го відділу Управління НКДБ по Ленінградській області був виготовлений зразок переносної малогабаритної (маса близько 20 кг) каналообразуючої апаратури зі вбудованим шифратором, який був успішно випробуваний на лініях Москва-Ленінград і Москва-Рязань.

Керівництвом ОТБ НКВС був підготовлений проект ухвали ДКО про виготовлення 50 комплектів подібної апаратури на заводі «*Красная Заря*», проте евакуація основних потужностей заводу на схід перешкодила реалізації цих планів. До першого періоду війни відносилася розробка комутатору малої ємності К-2/5 і портативної маскуючої апаратура СИ-15 «*Синица*», яка застосовувалася для засекречування каналів, утворених за допомогою будь-якого типу каналообразуючої апаратури. Її аналог - САУ-16 «*Снегирь*», виконаний у вигляді валізи, використовувався в основному при виїздах командувачів фронтами та представників СВГК до пунктів, які не мали ВЧ станції.

Одна з найважливіших проблем технічного характеру була пов'язана з утворенням апаратури засекречування для радіоканалів. Відомо, що зважаючи на труднощі із забезпеченням безперебійного проводового зв'язку з фронтами ВУЗ НКВС з кінця 1941 року провів низку заходів щодо організації радіотелефонного зв'язку в ланці Ставка-фронт: штабу кожного діючого фронту була додана автомобільна радіостанція, яка використовувалася для службового зв'язку при пошкодженнях на проводових лініях.

Тому на перший план висувалося завдання розробки спеціального пристрою, який міг би забезпечити конфіденційність телефонних переговорів по радіоканалах. Розпочаті в лабораторії ЦНДІЗ Котельникова до війни роботи щодо створення апаратури телефонного засекречування успішно продовжилися в уфімському

«*ГСПЭИ № 56*». В інституті Котельников з 16 лютого 1942 року керував спецгрупою № 2, а з 11 листопада того ж року - лабораторією. Зокрема, під його керівництвом був розроблений високоякісний шумовий генератор, покладений в основу шифроутворення.

У 1941 році Котельниковим були сформульовані технічні принципи, на яких повинна була ґрунтуватися стійка система засекречування сигналів. Така система повинна була бути цифровою, а перетворення аналогового сигналу в цифрову форму повинно було ґрунтуватися на теоремі відліків Котельникова. Однак подібна апаратура була розроблена тільки в післявоєнні роки.

Лабораторія Котельникова інтенсивно працювала над апаратурою «Соболь-П», що дозволяла вести по радіоканалах цілком таємні переговори і не боятися радіоперехоплення. Виробництво розробленої апаратури було налагоджене в блокадному Ленінграді на заводі № 209 також при безпосередній участі Котельникова. В ході цих робіт йому довелося вирішити багато наукових, технічних і організаційних проблем. Перші її зразки були зроблені за участю фахівців ВУЗ НКВС у «*ГСПЭИ № 56*» і випробувані на зв'язку Москва-Тбілісі.

Спеціально створеною комісією було встановлено, що апаратура «Соболь-П» дозволяла вести по радіоканалах цілком таємні переговори. Проте впровадження радіотелефонного урядового зв'язку на фронтах затримувалося у зв'язку з невисоким рівнем мовної розбірливості. Тем не менше перші її зразки одержали бойове хрещення вже в 1942 році, коли Москві було важко зв'язатися з Закавказзям у зв'язку з боями в Сталінграді. Можна уявити, які труднощі треба було подолати, щоб за рік виготовити та встановити складнішу апаратуру на бойовий зв'язок.

Наприкінці 1942 року була організована також лабораторія з розробки секретної телефонії при КБ заводу № 209 НК судової промисловості в Ленінграді. Загальна чисельність лабораторії складала 25-30 осіб. Маючи потужну виробничу базу, лабораторія розробляла механічні вузли шифраторів, а пізніше апаратуру засекречування в цілому.

27 грудня 1942 року були здійснені кадрові перестановки в керівництві ВУЗ НКВС, в результаті яких начальником відділу був призначений майор держбезпеки Михайло Олександрович Андреєв, а майор держбезпеки Воробйов переведений на посаду його заступника. А причиною цього стала нарада у Верховного Головнокомандувача, що відбулася в самий розпал Сталінградської битви. На нараді вирішувалася доля урядового зв'язку: бути їй самостійним відомством в рамках НКВС або влитися в структуру ГУЗЧА, чого активно добивався його начальник генерал Пересипкін.

Самостійність ВУЗ тоді вдалося відстояти, але сам Воробйов був за посадою понижений. За свідченням Петра Миколайовича Вороніна, який тоді вже був заступником начальника ВУЗ, Сталін не схвалив пониження Воробйова, але Берія, вірний власним принципам «кадрової політики», на своєму рішенні все ж таки наполіг.

На початку 1943 року було налагоджено виробництво вдосконаленої серії апаратів «Соболь-П». Складні механічні вузли унікальних шифраторів, розроблених у лабораторії Котельникова, виготовлялися на одному з ленінградських заводів. Готові апарати терміново відправляли на фронт. Як згадували ветерани вітчизняної війни, застосування шифраторів Котельникова в ході вирішальних боїв на Курській дузі в значній мірі визначило успішний результат битви. Вони забезпечували систему кодування мови для закритого радіозв'язку, який практично не піддавався «зламу».

В результаті 23 березня 1943 року РНК СРСР була прийнята Ухвала «Про присудження Сталінських премій за видатні винаходи за 1942 рік». Першу ступінь з винагородою у 150 тисяч карбованців за розробку нової апаратури зв'язку отримали начальник лабораторії «*ГСПЭИ № 56*» Котельников Володимир Олександрович, інженери «*ГСПЭИ № 56*» Єгоров Костянтин Петрович і Старіцин Георгій Васильович, начальник лабораторії ЦНДІЗ Цукублін Анатолій Іонович, інженери лабораторії ЦНДІЗ Борисов Дмитро Акимович і Солдатіхін Юрій Анатольевіч.

У лабораторії Котельникова в Уфі працював тоді ще молодим фахівцем учений і винахідник Лев Олександрович Коробков, який очолював протягом багатьох років відділ кінцевого спеціального устаткування. Пізніше колективом фахівців, що очолював Коробков, був розроблений цілий комплекс апаратури засекречування для багатоканальних систем радіозв'язку. Ці системи були широко упроваджені на лініях зв'язку СРСР і продовжують працювати на російських лініях зв'язку.

Пропрацювавши трохи більше року в Уфі, лабораторія Котельникова була розпорядженням ДКО передана до ВУЗ НКВС та у квітні-травні 1943 року перебазувалася назад у Москву. Розроблена під керівництвом Котельникова під час вітчизняної війни апаратура телефонного засекречування широко використовувалася в діючій армії. Вона застосовувалася також для зв'язку з Москвою радянської делегації під час прийняття капітуляції Німеччини в травні 1945 року.

У серпні 1943 року лабораторія «*ГСПЭИ № 56*» була передана до лабораторії спеціальної техніки 4-го спецвідділу (ОТБ) НКВС, завданнями якого було використання ув'язнених фахівців для виконання науково-дослідних і проектних робіт з розробки, зокрема, нових засобів радіозв'язку, оперативної техніки та апаратури засекречування. Керував лабораторією спецтехніки ув'язнений вчений Олександр Львович Мінц, який у 1932 році винайшов систему радіотелефонного зв'язку з широко-імпульсною модуляцією. А багатоканальна система зв'язку з амплітудно-імпульсною модуляцією була винайдена у 1935 році С.Кокуріним.

Приблизно з початку 1943 року у Москві розпочали активно працювати лабораторії, організовані в НКВС, де провідне місце займали колишні співробітники

лабораторії Котельникова. Розроблялося декілька типів апаратів секретної телефонії і, що дуже важливо, почалися серйозні роботи з дешифрування лінійної передачі. Ці підрозділи пізніше стали експертами з оцінки стійкості апаратури засекречування, що розроблялася в інших організаціях СРСР.

Зусиллями провідних наукових і інженерно-технічних кадрів країни в «*ГСПЭИ № 56*» НКЕП до кінця 1944 року практично завершилася розробка апаратури засекречування складної схеми із застосуванням кодування «Сова», яка призначалася для закриття ВЧ каналів, утворених апаратурою НВЧТ-42. Перші зразки іншого типу апаратури засекречування такого ж класу «Нева» були виготовлені та встановлені на дослідній лінії зв'язку Москва-Ленінград літом 1944 року.

Апаратуру «Нева», серійне виробництво якої було організоване на заводі № 209, передбачалося використовувати на всій мережі урядового зв'язку, оскільки вона сполучалася зі всіма типами каналообразуючої апаратури ВЧ зв'язку. До третього періоду війни відносилася і розробка складного пристрою засекречування «Волга-С», якому готували велике майбутнє на стаціонарній мережі урядового зв'язку.

Тим часом з'явилися фронтові рухомі станції ВЧ зв'язку, які були змонтовані у спеціальних автобусах та оснащені апаратами ВЧ телефонування, маскування, комутатором і акумуляторами для живлення апаратури. Урядовий зв'язок одержав закінчений комплекс засобів зв'язку в польовому виконанні, що давав можливість оперативно вирішувати питання організації ВЧ зв'язку на фронтах у бойових умовах.

12 квітня 1946 року наказом МВС № 524 генерал-майор Андреєв був звільнений з посади начальника ВУЗ і призначений колишній його заступник полковник держбезпеки Воробйов. Заступником Воробйова став полковник держбезпеки Воронін. Станом на 1 квітня 1945 року ВУЗ нараховував за штатом 296 одиниць, а в наявності - 263 особи. Воробйов вважав, що ВУЗ у великому боргу перед країною в частині забезпечення безпеки зв'язку

Вочевидь, його стараннями лабораторія Котельникова в середині 1946 року «повернулася» до складу ВУЗ із 4-го спецвідділу МВС, де вона функціонувала до моменту її передачі до Марфинської лабораторії. Протягом приблизно 5 років лабораторію реорганізовували та передавали між відомствами 6 разів, що, природно, порушувало нормальний ритм її роботи.

В цілому, за роки війни і перші післявоєнні роки 7 наукових організацій всього здійснили 22 розробки апаратури засекречування. Частина розробок була здійснена спільно двома лабораторіями різних відомств. Половина розробок була зі статичним варіантом перетворення – інверсією. З 22 розробок 16 були використані на лініях, а 6 розробок були завершені на рівні лабораторних зразків, але за різними причинами не дійшли до серійного виробництва.

З 22 апаратів 10 були маскуючими (проста інверсія спектра), а інші мали шиф-

ратор. Найскладніша апаратура була розроблена в лабораторії В.Котельникова. Найбільша кількість розробок була виконана лабораторією заводу «Красная Заря» (в основному, це інвертори з різною модифікацією).

В роки війни була створена промислова база для випуску техніки засекречування телефонних переговорів. Приведемо такі дані про випуск цієї техніки на промислових підприємствах у період 1941-1947 років:

1. Дослідне виробництво «*ГСПЭИ-56*» в Уфі. Виготовлено 70 апаратів засекречування типу інвертора.

2. Завод № 697 НК промислового зв'язку в Уфі. Виготовлено 1898 апаратів засекречування, в основному типу інвертора. Однак у ряді апаратів, у тому числі дослідних зразках апарата «Соболь-П», використовувався шифратор для зміни способу перетворення мови.

3. Завод № 209 НК судової промисловості у блокадному Ленінграді. Починаючи з 1942 року, завод випустив 56 апаратів засекречування, в основному, з шифруючими пристроями із складною механікою.

Всього 3 підприємства за роки війни і перші післявоєнні роки випустили, в цілому, 2024 апарати секретної телефонії, що використовувалися на лініях урядового зв'язку. Таким чином, у роки війни СРСР був отриманий перший досвід щодо виготовлення великих серій апаратури промисловістю.

Досвід масового застосування апаратури засекречування в період війни і перших післявоєнних років зіграв велику роль у визначенні організаційних принципів побудови служби експлуатації, у придбанні визначених технічних навичок по забезпеченню роботи цієї техніки на проводових і радіоканалах зв'язку, а також у визначенні впливу характеристик каналів зв'язку на якість передачі інформації.

У наступних розробках апаратів телефонного засекречування остання обставина допомогла сформулювати, з одного боку, вимоги до каналів зв'язку, а з іншого – вибрати таку систему перетворення мови, що була менш чутлива до впливу параметрів каналу зв'язку на якість відновленої на прийомі мови. Приведемо декілька прикладів використання апаратури засекречування у той період.

1. Для зв'язку СВГК з фронтами по каналах КХ радіозв'язку використовувалася апаратура «Соболь-П», а по проводових – «Сова», «Нева» тощо. Вперше апаратура «Соболь-П» працювала наприкінці 1942 року на КХ радіозв'язку Москва-Тбілісі, заміняючи порушений німцями проводовий зв'язок Москви зі штабом Закавказького фронту.

Цей радіозв'язок був припинений тільки після того, коли була побудована нова лінія проводового зв'язку довжиною 1315 км, що проходила по узбережжю Каспійського моря.

2. Апаратура «Нева» працювала на дротових лініях зв'язку Москви з 1-м Білоруським і 2-м Білоруським фронтами.

3. Техніка засекречування використовувалася під час проведення Тегеранської, Ялтинської і Потсдамської конференцій глав 3-х держав.

4. Апарати «Соболь-П» і «Нева» тривалий час працювали на зв'язках Москви з Гельсінкі, Парижем і Віднем у період проведення переговорів з питань міждержавних мирних договорів після закінчення Другої світової війни.

5. Апаратура засекречування використовувалася для зв'язку зі штабами груп Радянських військ за кордоном.

6. Тисячі інверторів і десятки апаратів засекречування з шифраторами працювали на внутрішніх лініях зв'язку СРСР.

27 січня 1946 року результатом вищезазначеної роботи стала Ухвала РНК СРСР «Про присудження Сталінських премій за видатні винаходи за 1943-44 роки». Першу ступінь з винагородою у 150 тисяч карбованців отримали за утворення нової апаратури звязку інженери спеціальної лабораторії Котельников Володимир Олександрович, Нейман Йосиф Семенович, Горелов Дмитро Петрович, Трахтман Авраам Менделевич, Найдьонов Микола Миколайович; за розробку схем могутніх радіомовних станцій інженер-полковник професор Мінц Олександр Львович.

Підведемо деякі підсумки цього періоду в розвитку секретної телефонії. Якщо перший період (1930-і роки) був періодом пошуку основних напрямків у роботі, підготовки кадрів розроблювачів, визначення і формулювання перших завдань щодо розробки окремих зразків і дрібних серій апаратури, то на другому періоді (1940-і роки) були пройдені всі стадії «життя» техніки засекречування (розробка, освоєння в промисловості й експлуатація).

Відзначимо головне в досягнутих результатах.

1. Можна стверджувати, що в СРСР одержав право на подальший розвиток новий напрямок у науці і техніці – секретна телефонія. Багато державних діячів і воєначальників, що широко використовували урядовий зв'язок, зрозуміли роль секретної телефонії в забезпеченні безпеки держави, і велику роль у цьому зіграв досвід війни.

2. Як вже говорилося, приблизно за 6 років було здійснено 22 розробки техніки засекречування, 16 з яких було виготовлено промисловістю серійно. Усього промисловість виготовила більш 2000 апаратів.

3. Склалася система експлуатації техніки засекречування, у тому числі в бойових умовах.

4. Разом з тим, досвід роботи з технікою засекречування поставив перед її розробниками нові, ще більш важкі завдання, про що буде сказано нижче.

5.6. Війська урядового зв'язку

За ствердженням Ю.Толмачова, начальника Управління урядового зв'язку з

1973 по 1985 роки, на початку Великої вітчизняної війни мережі зв'язку СРСР і засоби зв'язку ЧА значно відставали від систем зв'язку фашистської Німеччини, США й інших розвинених капіталістичних країн. На стаціонарній мережі країни телекомунікації базувалися в основному на постійних повітряних лініях зв'язку і 3-канальній ламповій апаратурі ущільнення СМТ-34.

Тільки між Москвою і Ленінградом працювала 24-канальна апаратура зв'язку «*L-2*» американського виробництва, але й вона через нестабільність лінійних характеристик використовувалася у 12-канальному режимі. Телефонний зв'язок забезпечувався в 1-канальному режимі симплексними апаратами СМ-35 і дуплексними апаратами Бодо. Кращими з міських АТС були громіздкі станції машинної системи швецького виробництва.

Не набагато кращі були справи й у військах зв'язку Червоної Армії. Розроблених на автомобільній базі рухомих засобів зв'язку фактично не було. Винятком були тільки автомобільні радіостанції дивізійного армійської і фронтової ланок «*РСБ-Ф*», «*РАФ*» і «*РАТ*» потужністю від 50 до 1000 Вт. Через нестабільність випромінювання приймальна частина станцій вимагала налаштування в ході роботи. Решта елементів вузлів зв'язку поспішно обладнувалася в кузовах автомобілів з використанням цивільного типу комутаторів ручного обслуговування і телеграфної апаратури СТ-35 і Бодо.

Лінійне устаткування було представлене жердяними лініями з мідним дротом 2,2 мм і кателями з бавовняним обплетенням «*ПТФ-7*» (телефонними) і «*ГПТ-19*» (телеграфними). У дивізійній ланці використовувалися переносні малопотужні радіостанції «*РБМ*» і «*РБМ-5*», в основному, в телеграфному слуховому режимі.

Звідси і серйозні недоліки, і перебої в організації зв'язку на першому етапі війни.

Так, у Акті про передачу справ Наркомату Оборони від Ворошилова Тимошенко у 1940 році в п.7 було записано: «Війська зв'язку в даний час на своєму озброєнні мають багато застарілих типів телеграфно-телефонних апаратів і радіозасобів. Впровадження нових засобів радіотехніки проходить украй поволі і у недостатніх розмірах. Війська погано забезпечені майже по всіх видах майна зв'язку. Великим недоліком військ зв'язку є відсутність швидкодіючих і засекречуючих приладів».

Жуков, тоді командувач Київського Особливого Військового Округу, на грудневій нараді 1940 року підкреслював: «Для повного використання найбільш сучасного засобу зв'язку - радіо - необхідно навести порядок в засекречуванні. Існуюче положення в цьому питанні призводить до того, що цей чудовий засіб зв'язку використовується мало і неохоче».

В той же час техніка зв'язку німецько-фашистської армії значно відрізнялася в кращий бік від аналогічної радянської. Парк радіостанцій тактичної ланки був представлений сімейством «*TORN-VB*» з жорсткою параметричною стабілізацією, комутаторами польового типу, 4-жильним пупінізованим кабелем «*FK-4*» з гумовою оболонковою і герметичними муфтами, радіорелейними 8-канальними станціями «*Muchail*», надійними таксофонними апаратами «*FF-33*» тощо.

Істотну допомогу надало постачання американської польової техніки, що розпочалося у 1942 році, за «ленд-лізом». Особливо це відносилося до парку автомобільних радіостанцій з кварцовою стабілізацією «*SCG-299*» і «*CSR-399*», змонтованих на автошасі «Шевроле» і «Студебеккер», УКХ-радіостанцій «*SCR-284*», парку телефонних апаратів «*EE-8A*» і зарядних агрегатів на базі двигунів «*Visconsin*». З'явились також польові майстерні зв'язку на автошасі.

Помітний перелом в кількісному і якісному відношенні в оснащенні засобами зв'язку радянських військ наступив завдяки зусиллям керівництва військ зв'язку тільки у 1943 році. Були розроблені і надійшли у війська польові комутатори «*ПК-40*», польовий варіант телеграфної дуплексної апаратури «*2БДА-43*», ретранслятори телеграфних сигналів, надійні телефонні апарати «*ТАИ-43*», модернізований парк радіостанцій тактичної ланки «*РБ-М*».

У перші 2 роки війни для організації засекреченого зв'язку з військовими штабами підрозділи урядового зв'язку використовували повітряні лінії наркоматів зв'язку та оборони. Основним засобом зв'язку Ставки ВГК був телеграфний зв'язок. ВУЗ НКВС забезпечував організацію урядового зв'язку та роботу станційних служб. Лінії зв'язку обслуговували співробітники НКЗ та ГУЗЧА.

Питання забезпечення урядового зв'язку Ставки ВГК з діючими фронтами і арміями все частіше ставали предметом обговорення на найвищому рівні. Так, восени 1942 року, в розпал Сталінградської битви, у Верховного Головнокоманду-

вача відбулася нарада, на яку були запрошені нарком внутрішніх справ Берія, начальник ГУЗЧА НКО Пересипкин і начальник ВУЗ НКВС Воробйов. Пригадавши події 1918-19 років, коли командування Південного фронту мало постійний зв'язок з Леніном, Сталін виразив крайнє незадоволення відсутністю стійкого телефонного зв'язку із Сталінградом.

Берія і Воробйов пояснили таку ситуацію відомчою роз'єднаністю з питань будівництва й експлуатації ліній зв'язку та привели як головний аргумент той факт, що підрозділи НКО і НКЗ не завжди рахують будівельно-відновлювальні роботи на лініях урядового зв'язку своїм головним завданням. Пересипкин, зі свого боку, вніс пропозицію про передачу всієї інфраструктури польового урядового зв'язку до складу ГУЗ ЧА. Проте Сталін ухвалив протилежне рішення, доручивши Берії підготувати пропозиції по зосередженню всіх без виключення структур урядового зв'язку у складі НКВС. Такі пропозиції були підготовлені та привели у січні 1943 року до повної реорганізації лінійної служби ВЧ-зв'язку СВГК, що стало відправною точкою появи військ урядового зв'язку.

У зв'язку з проведенням широкомасштабних бойових дій на власній території розпочалася реорганізація системи урядового зв'язку, характерною рисою якої став її розподіл на стаціонарну та польову. Основним правовим актом, який визначив стратегію реорганізації, стала Постанова Державного Комітету Оборони (далі - ДКО) «Про незадовільне забезпечення ГУЗЧА НКО якісними дротами для урядового ВЧ-зв'язку СВГК зі штатами фронтів і армій» № 2804сс від 30 січня 1943 року. З метою організації безперебійної дії цього зв'язку ДКО звільнив ГУЗЧА від робіт з обеспечення її лінійної служби та поклав будівництво, відновлення, експлуатацію та охорону всіх магістральних ліній, які використовувались для засекреченого телефонного зв'язку у ланці Ставка-фронт-армія, на НКВС.

Виходячи з цього, згідно наказу НКВС № 00204 від 31 січня 1943 року «Про будівництво, відновлення й охорону ліній і дротів урядового ВЧ-зв'язку» було створене Управління зв'язку Головного Управління Внутрішніх військ (далі - УЗ ГУВВ) НКВС. УЗ ГУВВ мало у своєму складі 3 відділи: ліній урядового зв'язку, зв'язку внутрішніх військ і постачання. Цим наказом був встановлений термін завершення

формування нових частин внутрішніх військ НКВС і прийому ліній урядового ВЧ зв'язку - 15 лютого. Ним же були затверджені «Положення про обслуговування урядового ВЧ зв'язку НКВС СРСР» і «Положення про Управління зв'язку внутрішніх військ НКВС СРСР».

Згідно Положення про Управління на нього були покладені такі завдання:

1. Організація та здійснення робіт щодо будівництва, відновлення, утримання та охорони дротів урядового зв'язку від СГВК до штабів фрогтів і армій.

2. Керівництво спеціальною службою окремих полків, окремих будівельних і експлуатаційних батальонів з будівництва та експлуатації дротів урядового ВЧ-зв'язку через начальників зв'язку управлінь військ НКВС з охорони тилів фронтів.

3. Постачання будівельних і експлуатаційних рот матеріалами, інструментом і майном зв'язку.

4. Розробка міркувань з організації, укомплектування рядовим складом і молодшими командирами та підбір начальницького складу для частин, обслуговуючих дроти урядового зв'язку.

На виконання наказу УЗ ГУВВ прийняло від НКО 135 окремих рот зв'язку, з яких до 15 лютого 1943 року було сформовано 17 окремих частин урядового зв'язку (5 окремих полків й 12 окремих батальйонів). Очолив Управління генерал-майор військ зв'язку Павло Федорович Угловський, який до цього був начальником зв'язку прикордонних військ, а керівник лінійної служби ВУЗ Костянтин Олександров став його заступником.

Спільний наказ НКО/НКВС № 0118/053 від 11 лютого 1943 року передбачав передачу у розпорядження НКВС сформованих НКО частин зв'язку та основних магістральних ліній з дротами для урядового зв'язку СВГК зі штабами фронтів і армій. Наказом зобов'язував привести у справний у технічному відношенні стан всі лінії та дроти, що використовувались для урядового зв'язку. Встановлювався також порядок і терміни проведення цих робіт, а також відповідальні за це відомства та посадові особи.

26 травня 1943 року наказом НКВС № 00895 «Про переформування ГУВВ НКВС СРСР» було створене Управління військ урядового зв'язку (далі - УВУЗ) НКВС. Для військ урядового зв'язку це означало вихід зі складу внутрішніх військ і безпосереднє підпорядкування керівництву НКВС. Начальником УВУЗ був затверджений Угловський.

10 червня 1943 року згідно наказу НКВС № 00970 УВУЗ прийняло у своє підпорядкування 17 окремих полків і батальйонів зв'язку загальною чисельністю 31 475 одиниць. Наказом № 00970 було також затверджене «Положення про роботу ВУЗ і УВУЗ НКВС щодо забезпечення безперебійного та якісного урядового зв'язку СГВК зі штабами фронтів і армій та їх взаємовідносинах у цих питаннях».

З цього моменту організація та забезпечення оперативної, захищеної й без-

СХЕМА
организации частей правительственной связи НКВД

перебійної роботи урядового ВЧ-зв'язку СВГК, Генштабу, ЦК ВКП(б), РНК СРСР із командуванням фронтів і армій, органами влади на місцях, найважливішими оборонними об'єктами й підприємствами промисловості, органами державної безпеки й внутрішніх справ повністю були покладені на ВУЗ і УВУЗ НКВС, які курирував заступник наркома внутрішніх справ комісар держбезпеки 2 рангу І.Сєров.

Здається трохи дивним рішення про створення в НКВС двох підрозділів, що відповідали за урядовий зв'язок, - ВУЗ і УВУЗ. Однак це диктувалося специфікою роботи органів держбезпеки: були оперативні підрозділи та війська, що виконували специфічні військові завдання за вказівкою оперативних органів. В НКВС існували оперативний орган - ВУЗ, що займався питаннями організації зв'язку, її розвитком, технічним оснащенням, станційною службою, питаннями збереження секретності, - та війська, які будували лінії зв'язку, забезпечували їхню безперебійну дію та надійну охорону, припиняли можливі диверсії. ВУЗ і УВУЗ всю війну працювали в тісному контакті, і яких-небудь непорозумінь у їхніх взаєминах не було. Разом вони були здатні комплексно виконувати завдання з організації та забезпечення зв'язку в складних умовах бойової обстановки.

Так, урядовий зв'язок організовувався по вісях і напрямках. Вісьову лінію тягли до штабу фронту. Як правило, намагалися будувати дві вісьові лінії по різних трасах, до армій прокладався напрямок - одна лінія зв'язку. На ній підвішувалися два ланцюги: один ущільнювався ВЧ апаратурою, а інший - службовий - призначався для зв'язку з постами обслуговування. На армійських напрямках при будівництві ліній зв'язку фахівці урядового зв'язку часто працювали разом із зв'язківцями НКО.

Тягли одну лінію, що використовували для ущільнення, а «середню точку» передавали армійським зв'язківцям для телеграфного зв'язку за системою Бодо. ВЧ-зв'язок організовувався на основному командному пункті (КП), запасному (ЗКП) і передовому пунктах (ПКП). При виїзді командуючого фронтом у війська його супроводжував офіцер урядового зв'язку із засекречуючою апаратурою зв'язку (ЗАЗ). ВЧ-зв'язок організовувався в місці знаходження командуючого з урахуванням наявних армійських ліній зв'язку або ліній НКЗ.

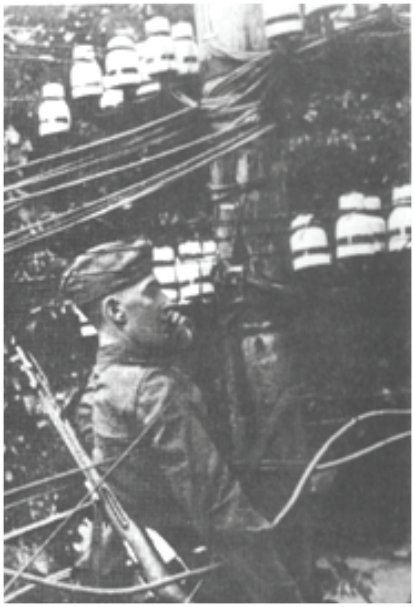
При проведенні наступальних операцій 1943-45 років ВЧ зв'язок був основним засобом управління у ланці Ставка-фронт-армія. Особливо цінили переваги використання ВЧ зв'язку в ланці управління фронт-армія відповідні командуючі. Так, ВЧ зв'язок дозволяв вести секретні та цілком секретні переговори тоді, коли ГУЗЧА надавало незасекречений радіо- та телеграфний зв'язок.

Бойове хрещення війська урядового зв'язку одержали в битві на Орловсько-Курській дузі, де одночасно діяли п'ять фронтів і було розгорнуто кілька десятків ВЧ станцій. Зв'язківці успішно впоралися з поставленими завданнями, забезпечивши безперервний зв'язок Ставки з усіма фронтами, арміями й двома представниками Ставки - Жуковим і Василевським, які мали свої ВЧ станції.

Великі труднощі виникли при організації урядового зв'язку на Тегеранській конференції трьох союзних держав. Дротового зв'язку у мирний час у Радянського Союзу з Тегераном не було, тому треба було його організовувати. Завдання ускладнювалося тим, що Сталіну як Верховному Головнокомандуючому зв'язок потрібний був не тільки з Москвою, але й з усіма фронтами й арміями. Єдина лінія, яку можна було використати, – це повітряна лінія зв'язку Ашгабат – Кзил-Арават – Астара – Баку, що була прокладена берегом Каспійського моря. За домовленістю з Іраном ця лінія була побудована Наркоматом зв'язку як обхідна для зв'язку із Закавказзям, оскільки німці проривалися до Кавказу та могли перерізати лінії, що йшли на Баку, Закавказький фронт, Грузію, Вірменію.

Потрібно було знайти вихід з Тегерана на цю обхідну лінію. Іранські лінії зв'язку, що були на цьому напрямку, перебували в жалюгідному стані: ішли по рисових полях та були недоступні для обслуговування. Стовпи покосилися, ізолятори на багатьох стовпах були відсутні, дроти висіли на гаках або були просто прибиті до стовпів. Більш-менш збереглася так звана індо-європейська лінія зв'язку, що йшла через Іран. Її й вирішили використати. У свій час вона була побудована англійцями на металевих стовпах для зв'язку Лондона з Індією. Лінія за прямим призначенням не використовувалася та перебувала у веденні іранських зв'язківців.

Було ухвалене рішення щодо розміщення радянської делегації та ВЧ-станції в будинку посольства СРСР. До посольства була заведена зазначена лінія зв'язку, а в населених пунктах Сарі й Астара зробили переприйомні пункти. Тепер з Тегерана було забезпечено два виходи – на Баку через Астару й на Ашгабат – Ташкент через Кзил – Арават (Туркменістан). Таким чином, хоча й з великими труднощами, вдалося забезпечити стійкий ВЧ-зв'язок на увесь час роботи Тегеранської конференції.



2 січня 1944 року наказом НКВС № 3 був визначений День військ урядового зв'язку - 15 лютого. У тому ж році начальником ВУЗ НКВС УРСР було призначено полковника О.Гриба, який до кінця війни командував ВУЗ НКВС 1-го Українського фронту.

В Україні станом на 11 січня 1944 року діяли у:

- 1-му Українському фронті – 3

окремий полк урядового зв'язку (далі – ОПУЗ) у складі 12 окремих батальйонів урядового зв'язку (далі – обуз), 7 лінійних (далі – олрз) і 6 кабельно-жердинних рот зв'язку (далі – кжрз);

- 2-му Українському фронті – 16 ОПУЗ у складі 7 обуз, 9 олрз і 6 кжрз;
- 3-му Українському фронті – 4 ОПУЗ у складі 4 обуз, 6 олрз і 1 кжрз;
- 4-му Українському фронті – 5 ОПУЗ у складі 7 обуз, 10 олрз і 3 кжрз;
- Окремій приморській армії – 15 обуз у складі 6 олрз.

У Харкові було розміщено 7 ОПУЗ у складі 9 олрз, а у Києві – 14 ОПУЗ у складі 2 олрз. Під час боїв під Харковом у 1943 році для поновлення пошкоджених ліній ВЧ-зв'язку активно використовувалася окрема мотострілецька бригада особливого призначення (ОМСБОП) НКВС.

21 липня 1944 року Державний Комітет Оборони постановою № 6232сс «Про забезпечення урядового ВЧ-зв'язку НКВС СРСР» дозволив НКВС збільшити чисельність військ урядового зв'язку на 10 600 одиниць і штатну чисельність ВУЗ – на 500 одиниць. На кожному фронті був один окремий полк урядового зв'язку чисельністю від 1,5 до 4,8 тисячі одиниць, а за кожною армією був закріплений окремий батальйон урядового зв'язку. Тільки для охорони та обслуговування ліній ВЧ-зв'язку від Москви до штабів фронтів нараховувалася 81 окрема рота урядового зв'язку.

З 4 по 11 лютого 1945 року 14 окремих рот військ урядового зв'язку забезпечували надійний урядовий зв'язок під час проведення Ялтинської конференції голів урядів 3-х союзних держава: Й.Сталіна, Ф.Рузвельта та У.Черчилля в Криму. Силами військ були прокладені й охоронялися магістральні лінії зв'язку між Сімферополем, Севастополем і об'єктами на Південному узбережжі Криму. Незважаючи на сильні урагани й ожеледь, був організований безперебійний зв'язок з Москвою, з усіма фронтами, тилом, а також з усіма членами і радниками всіх делегацій на конференції.

7 травня 1945 року в передмісті Берліна - Карлхорсті - військами урядового зв'язку була прокладена лінія зв'язку до будинку, де відбулося підписання Акту про безастережну капітуляцію Німеччини. Складні завдання довелося вирішувати військам й у ході операцій з розгрому мілітаристської Японії. Через хребти Хінгану та степи Монголії до Пхеньяну, Порт-Артуру й Дальнього були протягнені лінії урядового зв'язку. ВЧ-зв'язок, незважаючи на величезні відстані, був надійним, тому його висока якість неодноразово відзначалася в наказах Верховного Головнокомандуючого.

У травні 1945 року довжина ліній, що обслуговувалася військами ВЧ-зв'язку, становила 32944 кілометри, а в серпні 1945 року під час бойових дій проти Японії досягла 36854 кілометри.

10 жовтня 1945 року після закінчення Другої світової війни наказом НКВС СРСР № 001185 від «Про розформування частин військ урядового зв'язку» відповідно до Постанови РНК СРСР № 2417-643 від 21 вересня 1945 року «Про скорочення чисель-

ності військ НКВС» були розформовані окремі частини та підрозділи військ урядового ВЧ-зв'язку, окремі бригади переформовані у полки, а окремі батальйони – у роти.

Усього за роки війни військами урядового зв'язку у взаємодії зі зв'язківцями Червоної Армії і Наркомату зв'язку, найчастіше в бойовій обстановці, було побудовано та відновлено 66 500 кілометрів повітряних ліній, підвішено та відновлено 363 200 кілометрів мідних і сталевих дротів, побудовано 33 800 кілометрів тичинових ліній.

Широко відомі позитивні відгуки про урядовий зв'язок воєначальників І.Баграмяна, П.Батова, О.Василевського, Г.Жукова, І.Конєва, І.Пересипкіна, К.Рокоссовського, Б.Шапошнікова. У своїх спогадах вони так озивалися про ВЧ-зв'язок:

- маршал І.Баграмян: «Без ВЧ-зв'язку не починалося і не проводилося жодної значної військової дії. ВЧ-зв'язком забезпечувались не лише штаби, але й командування безпосередньо на передових лініях, на дозорних пунктах, плацдармах. У Вітчизняній війні ВЧ-зв'язок зіграв виняткову роль як засіб управління військами і сприяв виконанню бойових операцій»;
- маршал О.Василевський: «Перебуваючи на посаді начальника Генерального штабу, я ні на хвилину не міг обійтися без ВЧ-зв'язку, який, завдяки високій свідомості, самовідданості та майстерності воїнів-зв'язківців, найкращим чином забезпечував оперативне управління діючими фронтами та арміями»;
- маршал І.Конєв: «Треба взагалі сказати, що цей зв'язок ВЧ, як кажуть, нам був Богом посланий. Він так виручав нас, був настільки стійким у найскладніших умовах,

Б О Е В А Я Х А Р А К Т Е Р И С Т И К А

На Отдел Правительственной ВЧ связи за период действия 2-го Украинского и Забайкальского фронтов.

В период действия войск 2-го Украинского и Забайкальского фронтов отдел Правительственной ВЧ связи в условиях проведения сложнейших боевых операций как Ясско-Кишиневская , Будапештская, Гронская, Венская, Пражская (2-й Украинский фронт) и Мунь-чжурская (Забайкальский фронт самоотверженно работая всем коллективом связистов частей связи ВЧ, успешно справлялся с поставленными перед ним задачами по обеспечению ВЧ связи с ГШКА и штабами армий, входящими в состав фронта.

Во весь период действия войск 2-го Украинского и Забайкальского фронтов ВЧ связь от штаба фронта к штабам соединений подавалась своевременно и работала бесперебойно, предоставляя возможность командованию фронтам вести непосредственные телефонные переговоры с командующими армий и, облегчая тем самым общее управление войсками.

Возглавлявший отдел Правительственной ВЧ связи, весь период действия обеих фронтов, полковник КАРПОВ со своими задачами вполне справился.

Части связи ВЧ как и сам полковник КАРПОВ за обеспечение бесперебойной ВЧ связи, 2-го Украинского и Забайкальского фронтов с ГШКА и со штабами армий, неоднократно отмечались приказами Главнокомандующего товарища СТАЛИНА и награждались Правительственными наградами.

КОМАНДУЮЩИЙ ВОЙСКАМИ
ЗАБАЙКАЛЬСКО-АМУРСКОГО ВО
МАРШАЛ СОВЕТСКОГО СОЮЗА
/МАЛИНОВСКИЙ/

ЧЛЕН ВОЕННОГО СОВЕТА
ЗАБАЙКАЛЬСКО-АМУРСКОГО ВО
ГЕНЕРАЛ-ЛЕЙТЕНАНТ:-
/ТЕВЧЕНКОВ/

НАЧАЛЬНИК ШТАБА ЗАВО
ГЕНЕРАЛ-ЛЕЙТЕНАНТ:- /ТРОЦЕНКО/

що треба віддати належне нашій техніці й нашим зв'язківцям, що спеціально забезпечували цей зв'язок ВЧ й у будь-якій обстановці буквально по п'ятах супроводжували при пересуванні усіх, кому було визначено користуватися цим зв'язком»;

- маршал К.Рокоссовський: «Спеціальний ВЧ-зв'язок завжди своєчасно і точно забезпечував командуванню військ фронту надійно діючу систему зв'язку з командуючими та штабами армій і до всіх інших оперативних напрямків. Все це, безумовно, дуже позитивно відобразилось на надійності керування командуючим військами фронту». У травні 1945 року на нараді у Кремлі при обговоренні підсумків війни він заявив: «Використання засобів урядового зв'язку в роки війни здійснило революцію в керуванні військами».

Всього за час війни силами Відділу й військ урядового зв'язку було знову побудовано й відновлено 257 ВЧ-станцій і підсилювальних пунктів: з них відновлено на території СРСР – 73, знову організовано в тилу і прифронтовій смузі – 64, сформовано фронтових і армійських ВЧ-станцій – 120.

За героїзм, мужність і військову доблесть, виявлені в роки Великої Вітчизняної війни, більше двадцяти тисяч військовослужбовців цих військ були визнані гідними високих нагород СРСР. Орденами були нагороджені 12 окремих бригад і полків, 36 окремих батальйонів, 10 окремих рот, а бойові прапори семи з'єднань і частин були прикрашені стрічками двох орденів. За зразкове виконання завдань командування в боях з німецько-фашистськими загарбниками і японськими мілітаристами двадцять одна частина отримала почесне звання.

З військових частин, дислокованих в Україні, у бойових діях під час Великої Вітчизняної війни брали участь:

- 4-ий окремий «Одеський» орденів Олександра Невського й Червоної Зірки полк урядового зв'язку;
- 23-ій Гвардійський окремий ордена Червоної Зірки полк урядового зв'язку;
- 30-ий окремий ордена Олександра Невського полк урядового зв'язку;
- 31-ий окремий ордена Червоної Зірки полк урядового зв'язку.

Протягом 1945-1946 років перед військами урядового зв'язку та ВУЗ НКВС було поставлене завдання щодо забезпечення урядовим зв'язком командування груп радянських військ, що дислокувалися на території Східної Німеччини, Угорщини, Австрії, Польщі, Чехословаччини, Румунії, Монголії. Крім того, було відремонтовано 1965 кілометрів ліній, замінено 77000 тисяч кілометрів дротів робочих і службових зв'язків та укріплено більше 36 тисяч підпор ліній зв'язку.

На початку 1943 року у зв'язку з наближенням радянських військ до кордонів СРСР з НКВС був виділений НКДБ. У листопаді 1944 року військами 4-го Українського фронту під командуванням генерала армії Івана Єфимовича Петрова було звільнено від угорсько-фашистських військ Закарпаття, що входило до складу Австро-Угорської держави. Відразу ж після звільнення регіону розпочи-

нали свою роботу органи внутрішніх справ і державної безпеки спершу у вигляді оперативних груп, а потім і у вигляді новоорганізованих управлінь НКВС і НКДБ.

Так, 8 лютого 1946 року наказом НКВС № 0099 було організовано Управління НКВС Закарпатської області з дислокацією в місті Ужгороді (на підставі Указу ПВР СРСР від 22 січня про утворення Закарпатської області у складі УРСР). А 8 березня наказом НКВС № 00189 були затверджені штати нового управління, у складі якого було створено 2-е (шифрувально-дешифрувальне) спецвідділення .

У той же час було організовано і Управління НКДБ Закарпатської області та Закарпатський округ Управління прикордонних військ (далі - УПВ) НКВС також з дислокацією в місті Ужгороді. Навесні 1946 року наркомати були перейменовані в міністерства, НКВС став МВС, а НКДБ став МДБ.

26 серпня 1947 року наказом МВС/МДБ № 00877/00458 УВУЗ (разом з ВУЗ) МВС було передано до МДБ. А 17 жовтня 1949 року спільним наказом МВС/МДБ № 00968/00334 прикордонні війська також були передані до МДБ.

18 жовтня 1951 року наказом МДБ СРСР № 00764 частини військ урядового зв'язку на території СРСР були реорганізовані в частини урядового ВЧ-зв'язку Внутрішньої охорони МДБ, при цьому окремі полки, батальйони та роти урядового зв'язку були переформовані в окремі загони, дивізіони та команди урядового ВЧ-зв'язку внутрішньої охорони МДБ. До складу МДБ СРСР на території країни входили: 4 окремі загони, 7 окремих дивізіонів і 11 окремих команд урядового ВЧ-зв'язку, а за кордоном: 4 окремі полки і 18 окремих рот військ урядового зв'язку.

14 березня 1952 року наказом МДБ № 00182 УВУЗ МДБ було реорганізовано в Управління частин урядового ВЧ-зв'язку Головного управління внутрішньої охорони (далі - ГУВО) МДБ. У березні 1953 року в складі об'єднаного МВС СРСР був утворений Відділ частин ВЧ зв'язку ГУВО МВС. Штатна чисельність військ урядового зв'язку в 1954 році складала 8021 одиницю.

25 вересня 1954 року після утворення КДБ при РМ СРСР розпорядженням РМ СРСР № 10709рс Відділ військ урядового ВЧ зв'язку ГУВО МВС з підпорядкованими йому частинами був переданий до складу КДБ із присвоєнням йому умовного найменування «в/ч 9737».

26 жовтня 1954 року наказом КДБ № 00708 окремі полки урядового ВЧ-зв'язку Внутрішніх військ МВС і окремі дивізіони урядового ВЧ-зв'язку внутрішньої охорони МВС були перейменовані в окремі полки й окремі батальйони військ урядового ВЧ-зв'язку та у грудні того ж року передані з МВС до КДБ. У 1955 році на війська урядового зв'язку було покладене завдання щодо забезпечення зв'язком командування Об'єднаних збройних сил країн-учасниць Варшавського договору під час проведених навчань і спецзаходів.

Восени 1956 року під час угорських «антирадянських» подій три роти урядового зв'язку, які були сформовані у 1-й окремий батальйон урядового зв'язку КДБ на базі

311-го окремого полку урядового зв'язку КДБ, що дислокувався у м.Винники Львівської області, взяли участь у забезпеченні урядовим зв'язком військ на території Угорщини. Особовий склад виконував завдання щодо спорудження та охорони постійних ліній урядового зв'язку. До речі, втрати Радянської Армії в ході боїв угорської операції «Вихор» за офіційними даними, склали 669 осіб убитими, 51 зниклими без вісті, 1540 - пораненими, а також 18 танків і САУ (загиблих членів екіпажів - 111).

13 березня 1956 року через те, що кількісний склад військ урядового зв'язку не відповідав мобілізаційним планам розгортання частин у воєнний час, Постановою РМ СРСР № 333-210сс їхня чисельність була збільшена на 13 тисяч одиниць і до 1958 року була доведена до 21846 одиниць, що дозволило мати 13 окремих полків і 11 окремих батальйонів урядового зв'язку.

1 вересня 1957 року відповідно до наказу КДБ при СМ СРСР в м.Кодима Одеської області розпочалося формування 21-го окремого батальйону військ урядового зв'язку. Частина формувалася на базі радіорелейної роти старшого лейтенанта І.Пашина, переданої з 23-го Гвардійського ордена Червоної зірки полку урядового зв'язку. У листопаді 1960 року роту включили до складу 35-го ОПУЗ (м.Одеса).

23 червня 1959 року Відділ військ урядового зв'язку разом з Відділом «С» увійшли в єдиний ВУЗ КДБ при РМ СРСР. 17 серпня 1959 року наказом начальника військ урядового зв'язку № 0137 окремі полки, батальйони та роти військ урядового ВЧ-зв'язку стали іменуватися окремими полками, окремими батальйонами та окремими ротами військ урядового зв'язку КДБ.

9 липня 1959 року був затверджений новий штат ВУЗ, у складі якого був утво-

рений Штаб військ урядового зв'язку, що у різні періоди часу очолювали:

1. Александров Костянтин Олексійович (липень 1959 – квітень 1961).
2. Колесніков В.М.
3. Брусніцин Микола Олександрович.
4. Орєхов С.Г.
5. Бєда Анатолій Григорович.
6. Самохін Р.В.
7. Іванов О.В.

У зв'язку з проведенням СРСР політики роззброєння у січні 1960 року був прийнятий закон «Про нове значне скорочення Збройних сил СРСР», відповідно до якого істотно скорочувалися і війська урядового зв'язку. 5 лютого 1960 року відповідно до Постанови ЦК КПРС і РМ СРСР їхня чисельність була скорочена на 4168 одиниць. 16 березня 1960 року наказом КДБ № 00109 була встановлена чисельність окремих полків урядового зв'язку на території СРСР у кількості 15.

15 жовтня 1960 року Постановою РМ СРСР № 1102-455 була передбачена організація урядового зв'язку до командирів бригад ракетних військ, командирів дивізій протиповітряної оборони, командирів дивізій і бригад ракетних підводних човнів включно, для чого протягом 1961-1965 років було побудовано 50 нових ВЧ-станцій.

У 1960 році частини військ урядового зв'язку, що дислокувалися за кордоном, були об'єднані з відповідними відділами урядового зв'язку під загальним командуванням, а також створені відділи урядового зв'язку при групах радянських військ. За кордоном для забезпечення зв'язку з групами військ дислокувалася така кількість частин і підрозділів військ урядового зв'язку: Східна Німеччина – 3 батальйони, 2 вузли, Польща – 4 батальйони, 1 вузол, Угорщина – 1 вузол, 6 рот, Монголія – 1 батальйон.

Рішення про відновлення чисельності військ було прийнято тільки у 1961 році. Заново були розгорнуті 15 окремих полків і 11 окремих батальйонів урядового зв'язку. В Україні частини військ урядового зв'язку були розгорнуті в містах Київ, Миргород, Рівне, Сарни, Мирополь, Львів й Одеса. Трохи пізніше вузлові батальйони були сформовані в Кодимі й Сколе, а лінійні полки доукомплектовані вузловими підрозділами.

5 лютого 1962 року відповідно до Постанови РМ СРСР № 130-61 «Про створення системи польового урядового зв'язку» було додатково розгорнуто комплекти частин урядового зв'язку для військових округів і напрямків.

У 1964 році за ініціативою керівництва КДБ при РМ СРСР було прийнято Постанову ЦК КПРС і РМ СРСР «Про посилення протидії іноземним радіо- та радіотехнічним розвідкам». Зокрема, було вирішено збільшити можливості ВЧ зв'язку перспективою його якісної модернізації. Так було розпочато роботи з проектування апаратури автоматичного контролю стану зв'язку.

У той період було здійснено розробку та забезпечено виробництво комплек-

су рухомих майстерень для тактичної й оперативної ланок військ, розроблено систему засекреченого зв'язку «Інтер'єр», що дотепер діє в Міністерстві оборони Росії. Були задіяні заводи для виготовлення апаратури засекречування, спочатку тимчасової стійкості, а потім і гарантованої стійкості, що принципово змінило якісні можливості системи військового зв'язку.

У 1967-1968 роках були проведені роботи із впровадження на польовій мережі урядового зв'язку апаратури засекречування тимчасової стійкості «Корал» і гарантованої стійкості «Лагуна».

З метою підготовки офіцерських кадрів для системи урядового зв'язку 27 вересня 1965 року у Багратіоновську Калінінградської області було створено Військово-технічне училище КДБ при СМ СРСР із 3-річним терміном навчання. У 1971 році ВТУ КДБ при РМ СРСР було передислоковано в Орел і перетворено в Орловське вище військове командне училище зв'язку з 4-річним терміном навчання.

З 1968 року розпочалася підготовка інженерних кадрів для військ урядового зв'язку на базі кафедри «Автоматичного засекречування зв'язку» Київського вищого військового інженерного училища зв'язку (далі – КВВІУЗ). У 1972 році у КВВІУЗ відбувся перший випуск офіцерів-інженерів з експлуатації та ремонту засобів криптографічного захисту урядового зв'язку.

Крім того, офіцерів для військ та територіальних підрозділів урядового зв'язку готували у Бабушкінському прикордонному училищі. Також для підготовки офіцерів урядового зв'язку в Академії зв'язку в Ленінграді (нині - Санкт-Петербург) та Військовій школі у Свердловську (нині - Єкатеринбург) відкрито Групу урядового зв'язку.

Влітку 1968 року під час Чехословацьких «антирадянських» подій засекречений зв'язок забезпечували Відділ урядового зв'язку по Южній Групі Військ (в/ч 23705), 26-й окремий тропосферний батальйон урядового зв'язку КДБ (в/ч 21438) і 305-й окремий станційний батальйон урядового зв'язку КДБ (в/ч 34047) (з ЮГВ).

Втрати радянських військ в ході чехословацької операції «Дунай» склали 96 осіб загиблими і помершими, а також 87 пораненими і травмованими.

У 1969 році за наслідками Чехословацьких «антирадянських» подій військами урядового зв'язку було розпочато, а в 1972 році закінчено будівництво лінії тропосферного зв'язку у напрямку на відділи урядового зв'язку при групах радянських військ за кордоном (Угорщина – Чехословаччина – Польща – Німеччина).

Станція урядового зв'язку в м. Мукачево, що на території Закарпатської області, знаходиться поруч із кордоном, стала пунктом переходу дротових каналів зв'язку з Москви на тропосферні канали зв'язку на закордонній території, що забезпечували війська урядового зв'язку. Окремий тропосферний транзитний пункт № 41 (ОТП-41), де була змонтована радіостанція Р-410, був побудований у селищі Лавки Мукачівського району.

Розвивається тим часом нормативна база з питань організації та безпеки урядового зв'язку. Розробляються та розсилаються у всі підрозділи такі документи:

- у 1974 році - «Інструкція з організації та забезпечення безпеки засекреченого зв'язку ЗС СРСР»;
- у 1980 році - «Основні спеціальні вимоги з розміщення та монтажу устаткування стаціонарних станцій телеграфного засекреченого зв'язку» (ОСТ-ТЛГ);
- у 1983 році - «Настанова з організації урядового зв'язку в операціях ЗС СРСР»;
- у 1984 році - «Керівництво з безпеки зв'язку в РА і ВМФ» (РБС-84).

Військові частини урядового зв'язку, дислоковані в Україні, забезпечували керівництво Збройних Сил СРСР урядовим зв'язком при проведенні військових навчань «Дніпро», «Волга-71», «Захід-72», «Карпати-72», «Захід-73», «Дніпро-77», навчань держав-учасниць Варшавського договору на території Болгарії, Угорщини, Румунії «Щит-82», «Союз-84», «Граніт-85».

Вони брали участь у великомасштабних стратегічних навчаннях зі зв'язку

«Волна-87», під час яких на території Росії, України, Білорусі, республік Прибалтики, а також Польщі, НДР, Чехословаччини та Угорщини було реально побудовано польову систему урядового зв'язку, розраховану на особливий період. Під час навчань найбільш важливі канали урядового зв'язку стаціонарних тропосферних і радіорелейних оіній зв'язку резервувалися через повітряний ретранслятор, розташований на борту літака АН-26.

Після приходу до влади Михайла Горбачова у період з 1989 по 1992 роки було здійснено виведення всіх груп радянських військ за кордоном, у тому числі й частин урядового зв'язку з Чехословаччини, Угорщини, Монголії, Польщі і Східної Німеччини. Лінія та пункти тропосферного зв'язку були демонтовані.

Цікаву інформацію про організацію та обладнання засекречених видів зв'язку російських військ у Чечні можна отримати з найденої в Інтернеті доповіді начальника штабу Північно-Кавказького військового округу «Дії з'єднань, частин і підрозділів Сухопутних військ при проведенні спеціальної операції з роззброєння незаконних збройних формувань на території Чеченської Республіки 1994-1996р.».

Так, для керування з'єднаннями та частинами об'єднаного угруповання військ засекречений телефонний зв'язок був організований по напрямках і в радіомережах. Засекречений телеграфний зв'язок був організований тільки по напрямках з пунктів керування угруповань військ, окремих з'єднань і частин.

Для забезпечення засекреченого зв'язку по каналах, утворених різними засобами зв'язку, використовувалася апаратура гарантованої стійкості Т-230-03, Т-230-

1А, Т-240С(Д), Т-206-3М1, Т-208, однак для забезпечення засекреченого телефонного зв'язку по радіоканалах командно-штабних машин частин і підрозділів у передових порядках використовувалася апаратура засекречування тимчасової стійкості Т-219М «Ельбрус».

Впродовж своєї історії війська урядового зв'язку під впливом зовнішніх обставин та зростанням обсягу завдань постійно реорганізовувалися та, рухаючись від НКВС до КДБ, змінювали свою структуру та назву:

Дата утв.	*Найменування підрозділу*
10.06.1943	Управління військ урядового зв'язку НКВС СРСР
12.04.1946	Управління військ урядового зв'язку МВС СРСР
26.08.1947	Управління військ урядового зв'язку МДБ СРСР
19.05.1951	Управління «ВЧ» зв'язку ГУВО МДБ СРСР
29.03.1954	Відділ частин «ВЧ» зв'язку ГУВКО МДБ СРСР
27.09.1954	Відділ військ урядового «ВЧ» зв'язку КДБ при РМ СРСР (в/ч 9737)
23.06.1959	Війська урядового зв'язку ВУЗ КДБ при РМ СРСР
13.03.1969	Війська урядового зв'язку Управління урядового зв'язку КДБ при РМ СРСР (КДБ СРСР з 05.07.1978)

5.7. Секрети Марфінської «шарашки»

Післявоєнне протистояння СРСР і США поставили декілька серйозних проблем для подальшого розвитку секретної телефонії. Для розуміння цих проблем розглянемо особливості передачі та прийому мови. При розмові один з одним без використання каналу зв'язку ми сприймаємо мову як звукові коливання з обмеженим спектром частот приблизно від 50 до 15 тисяч Герц. З метою економії витрат на засоби електрозв'язку смуга частот стандартного каналу зв'язку обмежується приблизно до 3 кГц (300 - 3400 Гц). При цьому забезпечується досить висока розбірливість мови та розпізнавання голосу кореспондента за його індивідуальними ознаками.

У 1946 році в США була опублікована стаття в журналі «Акустичне Суспільство» (англ. *The Acoustical Society*) з описом аналізатору спектра мови. Цей аналізатор давав зображення спектра мови по трьох координатах: горизонтальній вісі (час), вертикальній вісі (частота), а енергія в окремих смугах спектра визначалася ступенем почорніння паперового носія. В американському приладі «Саунд Спектрографі» запис здійснювався на фотопапір. Приблизно через 2 роки аналогічні прилади були виготовлені й у нас із записом на електрохімічний та термічний папір шляхом пропалювання.

На фотопапері вся площа спектрограми розбивалася на маленькі прямокутники розміром ***F***x***t***, де ***F*** – ширина смуги, на які розбивався весь спектр мови, а ***t*** – мінімальна тривалість відрізка передачі при розбивці її за часом.

Вважаю за доцільне дати опис мозаїчної системи засекречування, приведеної в книзі Льва Зиновійовича Копелєва «*Утоли мои печали*» (1981). Таке визначення він вклав у вуста начальника Марфінської лабораторії (жаргонна назва - шарашка) Антона Михайловича Васильєва, висловлене групі ув'язнених: «В останні роки застосовуються складні системи так званої «мозаїчної» шифрації. В роки війни ними вже користувалися і наші союзники, і наші супротивники, і ми. Звукові сигнали розділяються частотними фільтрами на три або чотири смуги і за допомогою магнітного звукозаписного диска дробляться за часом. На короткі частки – від 100 до 150 мілісекунд. Шифратор перемішує ці відрізки. І по дроту йде отаке кришиво з вересків і шумів. А на прийомі передачу декодують і відновлюють первісну мову...».

Що ж собою являла «мозаїчна» система шифрування. Вузол шифратора, що здійснював частотні перетворення, переставляв прямокутники з боками ***F*** і ***t*** за частотою, у деяких випадках інвертуючи спектр частот, а вузол тимчасових перестановок переставляв їх за часом. Так, в основному, з «плавної» спектрограми мови з'являлася «мозаїчна» картинка. В результаті необхідно було вирішувати питання щодо відновлення за лінійною передачею нормальної мови з природним вихідним положенням її відрізків.

До 1944 року це здавалося неможливим – спектрографа не було. Єдиним ме-

тодом оцінки стійкості був метод прослуховування лінійної засекреченої передачі, де прослухувалися двозначні числа, окремі слова і фрази. Апарати засекречування з шифратором забезпечували необхідну стійкість проти такого дешифрування.

Спектрограф при значеннях ***F*** у сотні Герців і ***t*** у 60-100 мілісекунд із глибиною тимчасових перестановок у 200 мілісекунд дозволяв за час, обумовлений складністю перетворень, що здійснювались шифратором, відновити вихідну картину спектрограми, тобто дешифрувати передачу.

В СРСР група дешифрування під керівництвом співробітника 5-го Управління (шифрувально-дешифрувального) НКДБ (з 1946 року – 6-го Управління МДБ) Андрея Петровича Петерсона була створена через 4-5 років після початку розробок складних «мозаїчних» систем. Перші результати група стала видавати в середині 1944 року. Використовуючи багатошлейфний осцилограф (як прообраз американського «Саунд Спектрографа») група почала «розкривати» апарати засекречування один за одним. Підсумковим документом був звіт групи, затверджений 28 грудня 1945 року. Приведемо три головних положення цього звіту:

1. Всі апарати «мозаїчного» типу були дешифровані.

2. Не можна було збільшити стійкість за рахунок зменшення ***F*** і ***t***, тому що різко погіршувалася якість відновленої мови.

3. Запропоновано було шукати вирішення завдання створення стійкої апаратури двома шляхами – удосконалення розробленої у 6-му Управлінні «мозаїчної» апаратури «РТС», а також використання *вокодера* як мовноперетворюючого приладу.

Після написання звіту з початку 1946 року експертна дешифрувальна група «бомбардувала» власне керівництво, обґрунтовуючи необхідність вживання термінових заходів для того, щоб уникнути витоку інформації, переданої по каналах зв'язку.

Крім того, ще у вересні 1944 року начальник УВУЗ НКВС (МВС з 1946 року) генерал-майор П.Угловський підготував «Доповідну записку заступнику народного комісара внутрішніх справ НКВС І.Сєрову». У ній він указав на недосконалість апаратури засекречування та високу ймовірність підключення до магістралей зв'язку технічної розвідки супротивника.

Нарешті, орієнтовно в квітні-травні 1946 року керівництвом МДБ була проведена нарада з обговорення гострої ситуації, що склалася в секретній телефонії. У нараді брали участь представники ВУЗ МВС і 6-го Управління (шифрувально-дешифрувального) МДБ, у тому числі дешифрувальники. Учасник цієї наради А.Петерсон розповідав, що багато виступаючих (не тільки представники ВУЗ) висловлювали думку про те, що всі дешифрувальні результати є плодом теоретизування, що все це треба показати на практиці – одержати засекречену передачу з каналу зв'язку та за нею встановити передану інформацію. Дешифрувальників дуже критикували.

Нарада вирішила провести ці іспити та за їх результатами підготувати практичні заходи щодо проведення подальших робіт у сфері секретної телефонії. Матеріал для дешифрування повинен бути підготовлений ВУЗ і переданий 6-му Управлінню по телефонній лінії. При підготовці зашифрованої передачі фахівці ВУЗ пішли на хитрість – в один з апаратів засекречування, виготовлений заводом, у систему засекречування були внесені деякі зміни. Засекречений текст був переданий кабельною лінією зв'язку з ВУЗ до 6-го Управління.

Перед дешифрувальниками було два завдання:

- визначити принципи засекречування;
- здійснити дешифрування засекреченої передачі та надати дешифрований текст.

Дешифрувальники швидко встановили систему перетворення мови, після чого дешифрували мовну передачу тривалістю в 24 хвилини. «Замовнику» – ВУЗ був надісланий надрукований на машинці відкритий текст. При порівнянні цього тексту з оригіналом, що зберігався в міністра МВС Круглова, вони виявилися ідентичними.

У планах робіт лабораторії Котельникова передбачалася робота над двома перспективними темами: розробка вокодера, що забезпечував створення одного з варіантів апаратури засекречування з гарантією забезпечення безпеки зв'язку, а також проведення робіт з дешифрування «мозаїчних» систем. Лабораторія чисельно зросла з 45 до 57 осіб за короткий час. Створювалися плани розширення складу лабораторії спочатку до 200, а потім до 325 осіб. Було підібране приміщення поблизу від МЗС з орієнтованою площею близько 2500 м^2.

Однак у другій половині 1947 року відбулися події, що привели до зовсім іншої організації робіт з розробки апаратури гарантованого засекречування телефонних переговорів.

Десь у середині 1947 року роботу ВУЗ МВС обстежувала могутня комісія, що складалася з кількох робочих груп. В одній з таких груп брав участь А.Петерсон. Ця робоча група обстежувала стан абонентських ліній, у тому числі кабельних шаф у м.Клині. Висновок цієї групи щодо забезпечення безпеки зв'язку був негативним. Вочевидь, і загальний висновок комісії, з огляду на основну якість «мозаїчної» апаратури, був негативним.

Під час роботи комісії відбувся також візит міністра держбезпеки СРСР Абакумова до центрального вузла зв'язку, де розміщалася лабораторія ВУЗ. Після цього візиту були звільнені два техніки лінійно-апаратного залу (далі - ЛАЗ). Серед співробітників лабораторії існувала версія, що на питання міністра про те, чи можна прослухати переговори абонентів, було розказано та показано, як це можна зробити, що й послужило причиною звільнення.

Керівництво МВС і МДБ, що було детально інформоване про стан справ, мабуть, розуміло не тільки важливість, але і складність проблеми, що виникла в

секретній телефонії. Тому були зроблені спроби залучити до цих робіт видатних вчених країни. Керівництво міністерства розмовляло з Котельниковим і Мінцем, пропонуючи очолити цю роботу, обіцяло максимальну допомогу в організації, забезпеченні і проведенні робіт, але переговори не привели до позитивних результатів. У ході перемовин Котельников і Мінц заявили, що малими силами проблеми секретної телефонії не вирішити – треба створювати дуже могутню організацію.

В інтересах ВУЗ була переглянута вся тематика робіт лабораторії з секретної телефонії. Керівником лабораторії був призначений Олександр Спиридонович Колядов, а його заступником Дмитро Акимович Борисов. У лабораторії працювало 45 осіб при наявності 8 груп. До кінця 1947 року склад лабораторії збільшився до 57 осіб. Серед 8 груп – дві групи загального призначення (конструкторська і група зі створення фільтрів і моткових виробів), 2 групи з модернізації діючої апаратури та 3 групи з перспективної тематики.

Була утворена група № 1, перед якою було поставлене задання щодо дешифрування існуючих апаратів засекречування та тих, що тільки розроблялися. Розробники апаратури засекречування розуміли, що без знання слабких боків цієї техніки не можна створити апаратуру високого класу.

Робота групи № 1 йшла, в основному, трьома напрямками:

1. Оцінка можливості використання звукового спектрографа з метою дешифрування. У ході роботи в звіті «Нові методи дешифрування» було показано, що створена в СРСР апаратура засекречування, у тому числі й розроблена в 6-му Управлінні МДБ апаратура «РТС», може бути дешифрована.

2. Розробка двох типів спектрографів із записом спектрограми на електрохімічному папері. Один – 19-канальний (фільтри зі смугою 300 Гц), у якому запис здійснювався би одночасно з передачею. Другий – у якому би аналіз здійснювався 45-герцовим фільтром шляхом багаторазового прокручування відрізка передачі в декілька секунд. Виготовлення цих приладів було закінчено в 1948 році у Марфінській лабораторії.

3. Спроба дешифрувати передачу одного з більш простих апаратів засекречування не візуальним аналізом, а спеціально створеним автоматом, що здійснював би аналіз лінійної передачі в ході розмови. Обґрунтування було простим: якщо людина може зробити це, аналізуючи спектрограму, то чому процес не можна механізувати.

Улітку 1947 року групі № 1 (Калачов, Бобров) вдалося створити прилад, що автоматично аналізував засекречену передачу та дешифровував вслід за нею розмову без лабораторної обробки. Це був перший прилад автоматичного дешифрування.

Якщо вважати створення апаратури гарантованої стійкості однією з найважливіших завдань держави, то треба було зібрати разом більшість фахівців, що працювали у сфері секретної телефонії та призначити керівником лабораторії видатного

вченого або досить досвідченого фахівця з молоді.

Приблизно такий порядок створення лабораторії планувався і в ВУЗ. Взагалі варто помітити, що начальник ВУЗ Воробйов розумів, у якому становищі щодо забезпечення безпеки зв'язку знаходився відділ, і тому намагався зробити все, що було в його силах, для створення в рамках відділу могутньої науково-технічної організації, хоча відділ мав експлуатаційний профіль.

26 серпня 1947 року спільним наказом МВС/МДБ № 00877/00458 ВУЗ МВС був переданий до МДБ. Тепер завдання створення науково-технічної організації для розробки апаратури гарантованого засекречування телефонних переговорів стало завданням МДБ. Разом з тим, у той період Воробйов потрапив під слідство за одним з «огульних» процесів кінця 1940-х років, був знятий з посади та заарештований.

У тому ж році Відділом зв'язку Головного Управління охорони МДБ, на який була покладена відповідальність за міський урядовий зв'язок у Москві, була створена система автомобільного дуплексного радіозв'язку «Інтеграл-Градієнт» і система радіорухомого зв'язку «Красная площадь» (для забезпечення радіозв'язком заходів на Червоній площі й в інших місцях).

У середині другої половини 1947 року рішенням МДБ була утворена робоча група з підготовки проекту постанови Ради Міністрів СРСР щодо розробки апаратури засекречування телефонних переговорів. До складу робочої групи увійшли: Селіванський - заступник міністра, Желєзов - начальник відділу оперативної техніки (далі - ВОТ) і Воронін - заступник начальника ВУЗ.

Група повинна була підготувати доповідну записку та проект постанови ЦК ВКП(б) і РМ СРСР із зазначеного питання. У цих документах було необхідно визначити:

- основне завдання створюваного колективу;
- відомство, що буде відповідати за виконання цього завдання;
- комплектування кадрами;
- терміни розробки;
- матеріально-технічне забезпечення, у тому числі місце розміщення нової лабораторії.

У надісланих до високих інстанцій матеріалах пропонувалося утворити у складі МДБ спеціальну лабораторію для розробки апаратури засекречування телефонних переговорів для урядового зв'язку з абсолютною стійкістю. Комплектування кадрами передбачалося співробітниками ВОТ і лабораторії ВУЗ, а також фахівцями на договірних засадах. На жаль, з технікою засекречування телефонних переговорів досить добре були знайомі тільки фахівці лабораторії ВУЗ.

Із 43 осіб лабораторії ВУЗ, переданих до ВОТ, 14 пройшли школу Котельникова, з них 7 осіб працювали в його лабораторії в ЦНДІЗ НКЗ. Інші співробітники лабораторії ВУЗ мали 5-7-літній досвід розробки або експлуатації апаратури за-

секречування телефонних переговорів. Співробітники лабораторії ВУЗ у подальшому увійшли в основне ядро фахівців Марфинської лабораторії. Співробітникам ВОТ і новим фахівцям у ході розробки нової апаратури засекречування доводилося проходити курс навчання та знайомства з даною технікою.

Воронін, який 25 липня 1949 року був призначений начальником ВУЗ МДБ, висвітлюючи працю робочої групи, відзначив, що в ході підготовки матеріалів до інстанцій керівництву МДБ було запропоновано використати репресованого Воробйова у спецлабораторії як помічника майбутнього начальника Марфінської лабораторії Васильєва.

Праця робочої групи завершилася восени 1947 року. 21 січня 1948 року вийшла постанова Ради міністрів СРСР, а 19 лютого 1948 року Міністр МДБ СРСР видав наказ щодо організації у ВОТ спецлабораторії з розробки апаратури засекречування для ВЧ зв'язку, розмістивши її в селищі Марфіно. Ці рішення передбачали використання праці ув'язнених, серед яких навряд чи були фахівці, знайомі з технікою засекречування. Працівникам Марфінської лабораторії треба було вирішити складніші проблеми науки й техніки, які за своєю складністю були проблемами світового рівня.

Нова лабораторія повинна була пійти шляхом шифрування мовних сигналів, використовуючи послідовність дискретних сигналів гами шифру (метод телеграфного шифрування). Щоб реалізувати це рішення, треба було працювати над 4-ма складнішими проблемами:

1. Дискретизація безперервного мовного сигналу в послідовність двійкових імпульсів. Складність проблеми полягала в тому, що необхідно було забезпечити високу якість мови на прийомі (гарну розбірливість і природність звучання) при мінімальній швидкості передачі по каналу зв'язку.

2. Збільшення швидкості передачі двійкових сигналів по каналу зв'язку в 3-4 рази. Постановка таких робіт визначалася тим, що в той час телеграфні канали зв'язку забезпечували максимальну швидкість передачі 1200-1800 біт/сек, а дискретизація мови могла викликати двояку послідовність з істотно більшою швидкістю.

3. Розробка високошвидкісного шифратора, який би працював на швидкостях у багато десятків разів більше швидкості телеграфного шифратора.

4. Утворення нового напрямку в криптології – криптоаналізу та забезпечення стійкості високошвидкісного шифратора.

Ці 4 фундаментальні проблеми лабораторія повинна була вирішити у надстислі терміни. Наказ міністра про утворення лабораторії був підписаний 19 лютого 1948 року, а термін готовності лабораторних зразків апаратури був встановлений 1 травня 1949 року. Якщо врахувати, що лабораторія ВУЗ могла прибути в ще невідремонтоване приміщення тільки 31 березня 1948 року, то на вирішення фундаментальних проблем залишалося тільки 13 місяців.

5 лютого 1948 року відбулося приймання від МВС об'єкта «Марфіно», який

став спецв'язницею № 16 МДБ або «об'єктом № 8». Об'єкт був розташований на окраїні Москви у будинку колишньої духовної семінарії та був з'єднаний з центром автобусом № 37, що проїжджав біля об'єкта 1-2 рази в годину. Раніше будинок належав духовній семінарії, потім у ньому розміщалася дитяча колонія МВС. Стан об'єкта був жахливим. Ще більш жахливим був внутрішній стан приміщень: у коридорах не було ні підлоги, ні стель. Ситуація нагадувала зиму 1941 року, коли евакуйована на схід із західних районів СРСР промисловість починала роботу «з коліс».

Керівництво міністерства, відділу та лабораторії задіяли найактивніші прийоми з прискорення ремонтних робіт:

- 4 березня був погоджений та затверджений договір з Держпромбудом щодо ремонтних робіт;
- 17 березня була прийнята постанова РМ СРСР щодо постачання будматеріалів.
- 20 березня був введений в експлуатацію перший поверх для розміщення підрозділів лабораторії;
- 30 березня перебазовувалася на об'єкт лабораторія ВУЗ.

Однак у будинку були відсутні головні сходи, велика частина кімнат не відремонтована. Тільки в червні 1948 року лабораторний корпус був відремонтований остаточно. Перед переїздом у Марфіно співробітників ВУЗ попередили, що доведеться працювати разом з ув'язненими, і проінструктували, як треба будувати взаємини з ними.

Життя ув'язнених Марфінської лабораторії протягом доби можна було розділити на дві половини: від вечора до ранку – в'язниця з усім, що пов'язане з приниженням гідності людини, і з ранку до пізнього вечора – важка, напружена робота, але для багатьох цікава. Перша частина була описана Солженіциним у книзі «У колі першому», а друга – Калачовим у книзі «У колі третьому».

До кінця 1948 року в Марфінській лабораторії працювало 490 осіб, з них було 280 ув'язнених. Серед ув'язнених були люди різного фаху та рівня знань. Солженіцин спочатку аж до вересня 1948 року працював у групі № 3, до складу якої входили В.Владіміров (керівник групи), доктор технічних наук В.Тимофеєв і А.Парфіянович.

Перед групою № 3 було поставлене глобальне завдання – теоретична розробка основ проектування систем телефонного шифрування. У щомісячних оглядах роботи груп Марфінської лабораторії робота групи № 3 оцінювалася негативно. Негативна оцінка була дана і роботі самого Солженіцина, оскільки він не виявив бажання працювати в групі. Тому група була розформована, її працівники Владіміров і Тимофеєв увійшли до складу групи № 2, а Солженіцин і Парфіянович – до складу акустичної лабораторії, науковим керівником якої був Трахтман.

В акустичній лабораторії Солженіцин пропрацював приблизно до середини 1950 року, займаючись організацією артикуляційних іспитів. Як він сам написав у книзі «У колі першому», у середині 1950 року він був етапований до таборів за відмову працювати над криптологічними проблемами.

У квітні-грудні 1948 року начальник Марфінської лабораторії Васильєв видав 92 розпорядження, що визначали діяльність лабораторії. З них 8 про недбайливе ставлення до роботи окремих ув'язнених. Найбільш характерні недоліки – це заняття сторонніми справами замість роботи та «халатне» відношення до роботи: писання листів, приховане прослуховування радіопередач саморобним приймачем, бійка між ув'язненими, незібраність і неуважність, а в результаті – зламані окремі деталі та прилади, матеріальні збитки. Покарання за провини були такими: бійка – карцер, за недбалість і заняття сторонніми справами – догана. Слід зазначити, що і штатний склад також отримував дисциплінарні стягнення.

Отже, групи Марфінської лабораторії тимчасово розмістилися в основному корпусі, зайнявши його частину. В іншій частині основного корпуса ще йшли ремонтно-оздоблювальні роботи. Основними завданнями 2-го кварталу 1948 року, які треба було вирішувати одночасно і якомога швидше, були:

- завершення ремонтно-оздоблювальних робіт у основному корпусі та визначення перспектив розвитку лабораторії на найближчі роки;
- вибір основних наукових напрямків і визначення перших планів роботи зі створення лабораторних зразків апаратури;
- визначення і реалізація структури Марфінської лабораторії для вирішення основного завдання.

Для прискорення проведення ремонтно-оздоблювальних робіт було створено 7 ремонтних бригад, і в червні 1948 року ці роботи були закінчені. Після цього групи лабораторії зайняли всю робочу площу будинку, що сприяло переходу до нормальної дослідницької роботи. Одночасно з завершенням будівельних робіт було здійснено перспективне проектування розвитку лабораторного містечка протягом

1948-51 років. При створенні проекту розвитку лабораторії враховувалося забезпечення надійності постачання електроенергією, опаленням, істотне розширення виробничих площ, будівництво житла.

Лабораторія повинна була виконати два основні завдання. По-перше, необхідно було створити апаратуру з високою стійкістю засекречування, здатну працювати по стандартному телефонному каналу зв'язку та забезпечувати прийнятну для абонентів урядового зв'язку якість мови. По-друге, необхідно було створити апаратуру засекречування телефонних переговорів для дециметрової широкосмугової радіолінії, що була отримана за «репараціями» з Німеччини.

Друге завдання могло бути вирішене при використанні імпульсно-кодової модуляції (далі - ІКМ) і стійкого швидкодіючого шифратора, який треба було розробити. Перше завдання можна було вирішити шляхом використання у якості мовноперетворюючого приладу *вокодера* або кліпованої мови.

20 травня 1948 року Васильєв доповідав на спеціальній комісії Вченої Ради МДБ ці пропозиції. Комісія затвердила пропозиції лабораторії: групи № 1 і № 7 розробляють апаратуру на базі вокодера, група № 6 – на базі кліпованої мови і група № 5 – апаратуру засекречування для широкосмугової дециметрової радіолінії з перетворенням мови за допомогою ІКМ.

Відповідно до рішення комісії Вченої Ради та обраних напрямків роботи була створена структура Марфінської лабораторії та визначені завдання її підрозділів. До кінця червня 1948 року вперше був складений орієнтовний план роботи всіх підрозділів лабораторії. Оскільки групи та лабораторії в червні ще тільки розгортали свої дослідження, план визначав завдання підрозділів з орієнтуванням на готовність до іспитів стійкості засекречування апаратів М-801, М-803, М-804, М-805 у травні 1949 року.

З огляду на складність розв'язуваних завдань та відведені стислі терміни щодо розробки апаратури вибір оптимальної структури Марфінської лабораторії здобував найважливіше значення. Крім 7 груп, що брали участь у розробці апаратури засекречування, до складу лабораторії входили ще 5 спеціалізованих лабораторій. Необхідність створення деяких з них визначалася тим, що в 1948 році важко було розраховувати на одержання деяких приладів і комплектуючих виробів від інших організацій.

Таке передбачення керівництва ВОТ і Марфінської лабораторії виявилися цілком виправданим – вакуумна та хімічна лабораторії зробили великий внесок у розробку апаратури та випуск її серії, розробивши ряд комплектуючих виробів. У структуру лабораторії входила досить могутня виробнича база, здатна забезпечити розробку і випуск малих серій апаратури.

З 1 червня 1948 року згідно з розпорядженням начальника відділу Желєзова у лабораторії було створено 3 сектори: особливий, загальний та виробничий.

Особливий сектор складався з 7 тематичних науково-дослідних груп і по-

ста контролю та допуску до сектора за особливими пропусками.

Група № 1. Керівник – Волошенко. Завдання групи – розробка апаратури засекречування на базі *вокодера*, що забезпечив би прийнятну якість мови, причому найбільших труднощів треба було здолати при виборі методів аналізу та синтезу спектра мови. Що стосується розробки швидкодіючого шифратора, то всі групи були в однаковому стані. Створивши прийнятний шифратор для одного варіанта апаратури, можна було автоматично вирішити завдання для всіх інших. У складі групи було 10 фахівців.

Група № 2. Керівник – Калачов. У роботі групи брали активну участь і надали значну допомогу відряджені співробітники МДБ Петерсон і Салтиков. На початку роботи групи в ній були тільки штатні співробітники, однак восени 1948 року її склад був поповнений ув'язненими. Центральним завданням групи № 2 був вибір методу шифрування мови та вирішення проблем синтезу й аналізу стійкості шифраторів. До завдань групи входило проведення статистичного аналізу послідовностей мовних сигналів для різних варіантів мовноперетворюючих пристроїв за замовленням 6-го Управління МДБ.

Іншими словами, група № 2 була криптологічним центром Марфінської лабораторії. Крім криптологічних завдань група повинна також була завершити інженерні роботи з утворення двох апаратів аналізу спектра мови з записом спектрограм на електрохімічний папір.

Для експертного аналізу в 6-му Управлінні МДБ необхідно було розробити генератор гами шифру на базі лічильника Гейгера, що використовував розпад радію. Чисельний склад групи за роки її роботи змінювався з 20 до 35 чоловік. У групі було три бригади: інженерна, криптологічна та статистична.

Група № 3. Керівник – Владиміров. Протягом декількох місяців завдання групи – розробка основ проектування систем телефонного засекречування – не було вирішено. Тому у жовтні 1948 року група була розформована.

Група № 4. Керівник – Нейман. Тематика групи була досить різноманітною. По-перше, група завершила роботу з модернізації парку старої техніки для нестатків ВУЗ. Далі група випробувала варіанти компресії спектра мови методами Ксеплі і Габора, одержавши негативні результати. Далі група практично перевірила можливість компресії спектра в 2 і 4 рази шляхом розподілу частоти гармонік основного тону, однак результати знову були негативні.

Керівництво ВОТ і Марфінської лабораторії поставило перед групою № 4 завдання щодо розробки ще одного варіанта апаратури – 14-канального *вокодерного* варіанта (М-809). Апаратура була розроблена та забезпечувала достатню розбірливість, але за якістю «звучання» поступалася М-803. Тому розробка її була припинена.

В останні роки роботи лабораторії для внутрішньосоюзних зв'язків група № 4 розробила апаратуру тимчасової стійкості, яка була випущена промисловістю

великою серією. Крім зазначених різноманітних завдань група № 4 займалася ще розробкою апаратури для оперативних підрозділів МДБ.

Група № 5. Керівник – Ходаков, потім Назаров. Основним завданням була розробка апарата засекречування для широкосмугового каналу зв'язку. За технічною складністю проблема була більш простою, ніж в інших групах. Однак роботи за цим напрямком були припинені в 1949 році, а група була розформована. Вочевидь, була занадто мала потреба в такій апаратурі.

Група № 6. Керівник – Дементьєв. Основним завданням була розробка апаратури на базі кліпованої мови. Перші місяці в розпорядженнях і наказах начальника Марфінської лабораторії група вважалася кращою, однак пізніше у роботі виникли великі труднощі в забезпеченні високої якості мови.

Група № 7. Керівник – Васильєв, з початку 1949 року – кандидат технічних наук Кузнєцов. Станом на травень 1948 року система мовноперетворюючого пристрою була ще не обрана. Вважалося, що в результаті компресії спектра мови максимальна частота буде 900 Гц, а швидкість передачі інформації складе приблизно 6 Кбіт/сек. Ймовірно Васильєв розраховував на успіх компресії мови в групі № 4. Однак після невдачі група вирішила перейти на використання *вокодера.*

Загальний сектор складався з 7 підрозділів: 5 лабораторій і 2 бюро.

1. Акустична лабораторія (найбільш пов'язана з групами особливого сектора, що розробляли апаратуру засекречування). У квітні – червні керівники лабораторії змінювалися. З липня 1948 року керівником лабораторії став Воробйов, а науковим керівником – Трахтман.

Завданням лабораторії було вивчення звукового та складового змісту мови, її спектрального складу, розробка методів оцінки якості мови, у тому числі наукового обґрунтування проведення артикуляцій та складання артикуляційних таблиць, що відбивали характерні риси російської мови. На лабораторію покладалися також обов'язки з організації та проведення артикуляційних іспитів зразків апаратури.

2. Фільтрова лабораторія. Завданням лабораторії був розрахунок, виготовлення та настроювання фільтрів, трансформаторів і інших моткових виробів. Керівник – Вольфтруб. У червні 1948 року мала чисельність лабораторії гальмувала роботу всього колективу Марфінської лабораторії. Після збільшення чисельності лабораторії її робота істотно покращилася.

3. Вимірювальна лабораторія. Керівник – Єршов. Завдання лабораторії – постачання груп вимірювальними приладами і проведення контролю над їхньою якістю.

4. Конструкторське бюро (КБ). Керівник – Горєлов. Завданням бюро було конструювання окремих панелей та апаратури в цілому. Особливі труднощі в роботі КБ виникли при конструюванні дискових машин для шифраторів. Наприкінці діяльності Марфинської лабораторії КБ домоглося істотних успіхів у цьому напрямку.

5. Інформаційне бюро і бібліотека. Завідувачка – Станішевська. Завданням

було забезпечення всіх співробітників (і штатних, і ув'язнених) необхідною інформацією зі свого книжкового та журнального фонду, а також з бібліотек, у тому числі з Ленінської бібліотеки.

6. Вакуумна лабораторія. Керівник – кандидат технічних наук Бучинський. Завданням бюро було забезпечення груп, які розробляли апаратуру засекречування, радіоелектронними приладами, що не випускала вітчизняна радіопромисловість. Монтаж лабораторії був розпочатий у травні 1948 року на площі 200 кв. метрів. А з жовтня 1948 року групи №№ 1, 6 і 7 одержували нові електронні прилади для проведення досліджень, а також випуску серії апаратури. За роки роботи лабораторії було випущено десятки різних виробів. Відзначимо декілька з них:

- електронно-променеві трубки для першого варіанта шифратора з комплектом у 256 світловодів, що забезпечували «зняття» знаків гами шифру, зафіксованих на кадрі кіноплівки у вигляді затемнених і світлих крапок;
- фотоелементи різної конструкції;
- реалізація схеми ІКМ за допомогою електронно-променевої трубки;
- створення двопроменевих осцилографічних трубок, що дозволяли вести спостереження одночасно двох процесів. Трубки були використані для випуску серії контрольно-іспитового пристрою (далі - КІП), призначеного для проведення щоденної профілактики розробленої апаратури, а також у ході розробок у лабораторії;
- виготовлення спільно з хімічною лабораторією лічильників Гейгера, що працювали у схемі генератора шифруючих імпульсів. Лабораторія надала неоціненну допомогу групам особливого сектора.

7. Хімічна лабораторія. У перші місяці керував лабораторією професор Сухотський. Заступником начальника лабораторії була призначена Комова, а пізніше вона стала начальником лабораторії. Як і вакуумна, лабораторія здійснювала роботу за дуже багатьма напрямками. Назвемо тільки деякі з них:

- розробка люмінофорних покрить для осцилографічних трубок;
- спільне з вакуумною лабораторією виготовлення лічильника Гейгера;
- розробка та нанесення на ободі диска нікель-кобальтового покриття для магнітного запису;
- розробка германієвих діодів і транзисторів;
- розробка конденсаторів для фільтрової лабораторії;
- участь у розробці та створенні елементів пам'яті з магнітним пермалоєвим сердечником.

Виробничий сектор складався з 4 груп.

1. Токарно-фрезерна група.
2. Слюсарно-складальна група (включаючи пресування та зварювання).
3. Обробно-гальванічна група.

4. Столярна група.

Завдання кожної групи визначалися назвою. Спочатку роботою виробничого сектора та його підрозділів керували Саприкін, Мильніков і Фролов. До 1949 року виробничий сектор розміщався в цокольному поверсі головного будинку Марфінської лабораторії. У першій половині 1949 року було закінчене будівництво одноповерхового та двоповерхового будинків, куди було переміщено основне устаткування виробничого сектора, який пізніше став іменувати експериментальними майстернями.

Такою була первісна структура Марфінської лабораторії секретної телефонії, у подальшому ця структура трохи змінювалася в залежності від результатів роботи основних груп і лабораторій.

Розпорядженням у грудні 1948 року були визначені підпорядкованість лабораторних підрозділів та плани робіт групи № 1 і акустичної лабораторії. Всі роботи з аналізу та синтезу мови, тобто розробки вокодера, було запропоновано зосередити в спеціальній групі з безпосереднім її підпорядкуванням Трахтману.

У червні 1948 року до терміну пред'явлення зразків апаратури залишалося тільки 10 місяців. Це змушувало начальника лабораторії Васильєва приділяти велику увагу організації робіт, твердому плануванню та посиленому контролю за виконанням планів підрозділів. Відзначимо, що за 9 місяців 1948 року було видано 92 розпорядження начальника лабораторії з усіх питань організації і діяльності лабораторії. В наступні роки число розпоряджень доходило до 190.

Відзначимо стисло деякі організаційні заходи.

1. Визначення структури всіх 18 підрозділів лабораторії, що входили у 3 сектори.

2. Визначення порядку планування робіт та звітності щодо виконання плану.

3. Щомісячні та щоквартальні огляди ходу робіт в окремих підрозділах.

4. Створення науково-технічної ради при начальнику лабораторії, на засіданнях якої обговорювались:

а) досягнення науки і техніки за профілем лабораторії;

б) підсумки роботи груп;

в) ескізні та технічні проекти апаратури;

г) наукові праці співробітників лабораторії.

5. Найбільша кількість розпоряджень (38) відносилася до вирішення кадрових питань – призначення на керівництво роботою або підрозділом, переміщення штатного складу та ув'язнених з одного підрозділу до іншого, дисциплінарні стягнення за провини та заохочення за якісну роботу тощо.

Становить інтерес кількісний склад фахівців Марфінської лабораторії (без урахування виробництва) станом на 27 квітня 1949 року.

Номер групи, назва лабораторії	Прізвище начальника	Кількість штатних співробітників	Кількість ув'язнених фахівців	Усього
Особливий сектор				
Група № 1	Волошенко	10	11	21
Група № 2	Калачов	9	10	19
Група № 4	Нейман	7	3	10
Група № 5	Назаров	4	8	12
Група № 6	Воробйов	8	13	21
Група № 7	Кузнєцов	7	13	20
Усього		45	58	103
Загальний сектор				
Акустична	Трахтман	10	10	20
Вимірювальна	Єршов	2	3	5
Конструкторська	Горелов	13	7	20
Фільтрова	Вольфтруб	6	9	15
Хімічна	Комова	4	8	12
Вакуумна	Бучинський	7	10	17
Усього		42	47	89

Таким чином, у складі лабораторії (без виробничого сектора) до кінця квітня 1949 року працювало 192 особи, з яких 45% були штатні співробітники та 55% – ув'язнені фахівці.

5.8. Розробка стійких шифраторів

Розглянемо завдання, які вирішували кожна з груп №№ 1, 6, 7, що розробляли апарат засекречування у цілому. Кожна з цих груп повинна була розробити проект апарата з високою стійкістю засекречування, а в результаті вибору найкращого варіанту всі наявні сили та засоби необхідно було об'єднати для виготовлення лабораторного зразка.

Розроблені проекти повинні були містити рішення для всіх трьох основних блоків апаратури: мовноперетворюючого шифруючого пристрою, пристрою з системою синхронізації та модему для передачі інформації стандартним телефонним каналом зв'язку. Взаємодія мовноперетворюючого пристрою та шифратору повинна була визначатися обраною системою засекречування.

Група № 1 працювала над варіантом із використанням *вокодера*. У випадку успіху забезпечувалася максимальна компресія спектра мови в порівнянні з усіма іншими варіантами, що практично забезпечувало просте вирішення проблеми створення модему та шифратора, а також підвищення якості мови. Основні труднощі з'явилися при вирішенні завдання з підвищення якості відновленої мовної

інформації, тому що на початку роботи якість не відповідала вимогам ВУЗ.

Група № 6 працювала над варіантом з використанням кліпованої мови. Нова система перетворення мови – граничне обмеження амплітуд (кліпування) – була вперше опублікована через 10 років після публікацій про *вокодер* у період організації Марфінської лабораторії.

Група № 7 працювала над багатоканальною системою передачі засекречених сигналів каналом зв'язку на відміну від одноканальних варіантів груп №№ 1 і 6. У початковий період у цій групі не була визначена система перетворення мови: сподівалися використати результати роботи інших груп (№№ 1, 6, 4).

У довідці для заступника міністра державної безпеки Селівановського за підписами Желєзова та Васильєва було зазначено, що план на 1949 рік передбачав три етапи:

1) розробка макетів, складання технічного проекту в термін до 15 жовтня;

2) готовність виробничого зразка та всієї технічної документації у термін до 15 жовтня;

3) виготовлення головної серії апаратури у термін до 31 грудня.

У довідці було також зазначено, що роботи велися за 4 темами (М-801, М-803, М-804, М-805), і внесене клопотання затвердити наданий план. Відзначимо, що пропонувався перший відступ від директивного терміну, установленого Постановою Уряду: надати дослідні зразки (а не макети та техпроекти) до здачі 1 травня.

Безсумнівною заслугою Васильєва було те, що він мав достатню інформацію про хід робіт у всіх підрозділах Марфінської лабораторії, роблячи щомісячні огляди про хід робіт у групах, аналізуючи їхні досягнення та недоліки, даючи рекомендації щодо поліпшення роботи. Впродовж другої половини 1948 року та першого кварталу 1949 року було складено 6 місячних оглядів роботи груп.

Групи № 1 і № 2, в основному, одержували позитивні оцінки, при чому група № 1 заслужила подяку за якісну роботу. Групи № 4 і № 6 у різні місяці мали і позитивні, і негативні оцінки. Робота груп №№ 3, 5, 7 зазнавала різкої критики, тому до кінця 1948 року була розформована група № 3, навесні 1949 року – група № 5, а до кінця 1949 року – група № 7. Фахівці цих груп були переведені в інші групи.

У групах №№ 1, 6, 7 на початку розглянутого періоду здійснювалася розробка систем перетворення мови в дискретну послідовність, придатну для шифрування методом, подібним до шифрування телеграфних сигналів. При проведенні цих робіт зверталася особлива увага на якість відновленої мови та максимальне зниження швидкості передачі двійкових сигналів мовної інформації. Одночасно велися роботи з підвищення пропускної здатності каналу зв'язку в 2-3 рази та робилися спроби щодо спрощення апаратури, відходячи від методів телеграфного шифрування.

Відповідно до своєї кваліфікації група № 2 могла вирішувати проблеми криптології тільки «інженерними» методами. Після того, як вона поступово змінювала свій профіль на вирішення чисто криптологічних завдань, інженерний склад групи поступово переходив на роботу в розробляючі групи, займаючи там ведуче положення. Восени 1948 року у групу № 2 прийшло підкріплення: з 6-го Управління МДБ – Петерсон, що працював у 1940-41 роках у лабораторії Котельникова, а з іншого підрозділу МДБ – Салтиков.

Васильєв приділяв роботі групи № 2 велику увагу, вона була предметом його особливих турбот. На початку 1949 року було видане розпорядження щодо реорганізації роботи декількох груп, у тому числі № 2, з розширенням фронту досліджень. У групі були створені 3 бригади:

- аналітична бригада для проведення аналізу стійкості запропонованих способів шифрування «інженерними» методами та розробки апаратури для забезпечення проведення статистичних досліджень;
- криптологічна бригада для вибору криптосхем шифраторів і аналізу їхньої стійкості, а також формулювання вимог щодо їхнього конструювання;
- статистична бригада для підготовки матеріалів щодо статистичної структури мови та вихідних послідовностей шифраторів.

Начальнику групи № 2 Калачову доводилося більше займатися справами першої і другої бригад. Роботу статистичної бригади вміло та технологічно організував її начальник Баруткин. У напружені моменти до роботи зі статистики цифрових послідовностей залучалися всі співробітники групи № 2. Рекордсменом був працівник Тейван, який виконував за 10-годинний робочий день до 40 тисяч двійкових операцій, за що був відзначений декількома подяками.

Приведемо короткий опис спільної роботи групи № 2 із трьома розробляючими групами особливого сектора. Ця спільна робота одночасно була «битвою» за високу стійкість засекречування, прийнятну якість мови та зниження вимог до пропускної

здатності каналу зв'язку. Кожна з груп «воювала» за свої параметри, але з максимальним врахуванням інтересів іншої сторони. Робота йшла в «човниковому» режимі, та до весни 1949 року система засекречування і шифратор придбали «товарний» вигляд.

Дуже коротко у хронологічному порядку викладемо деякі матеріали з аналізу трьох варіантів системи засекречування з використанням кліпованої мови.

Варіант № 1 до групи № 2 надійшов 24 листопада 1948 року. Висновок щодо цього варіанту був підписаний Петерсоном і Калачовим 25 грудня та затверджений начальником лабораторії Васильєвим 28 грудня. Запропонована система була практично дешифрована, тому були надані рекомендації щодо її зміни.

Варіант № 2 був наданий до групи № 2 розробниками Бриксіним, Ізмайловим і Воробйовим 2 лютого 1949 року. У негативному висновку, підписаному Калачовим і Салтиковим, був запропонований новий метод дешифрування, заснований на дуже повільній зміні періоду основного тону мови. До аналізу другого варіанта залучався Копелєв, що оцінив можливість визначення спектра мови на ділянках голосних звуків і 2-3-варіантного визначення звуку мови.

Варіант № 3 був направлений на експертизу до 6-го Управління МДБ 17 червня 1949 року. У ньому мова гранично обмежувалася та квантувалася частотою 4500 Гц. У такий спосіб перехід через «нуль» міг здійснюватися для мови тільки в точках, рознесених одна від одної на відстань за часом у 1/4500 сек. Цією ж частотою квантувалися й знаки гами, а зашифрування здійснювалося аперіодичною гамою шифратора за принципом «знак на знак» шляхом додавання за «модулем 2».

Спільна робота з групою № 7 складалася з великими труднощями. Причина полягала в тому, що групою не була чітко визначена система перетворення мови, як це зробили групи №№ 1 і 6. Автори розробки назвали свою систему засекречування лічильно-імпульсною, і зміст її полягав у тому, що мова перетворювалася у цифрову форму за допомогою ІКМ (8 рівнів) з наступним застосуванням шифрів перестановки на глибину в 24 знаки. Для кожного циклу перестановки необхідно було не менше 70 знаків гами шифру.

Події розвивалися в такій послідовності. Група № 2 запросила дані 20.11.48 р., а одержала їх 27.11.48 р. Оскільки в даних були виявлені помилки, то 29.11.48 р. був зроблений повторний запит. Васильєв наказав видати дані 30.11.48 р. Попереднє вивчення матеріалів змусило сформулювати 04.12.48 р. ще 4 питання, на які була отримана відповідь 07.12.48 р. Після цього через два тижні був зроблений докладний аналіз на 25 машинописних аркушах, який був затверджений Васильєвим.

За результатами аналізу були зроблені висновки про те, що дана система шифрування не підходить для інтервалів часу в 200 мсек і необхідно переходити на шифрування «знак на знак». 10.02.49 р. роботи щодо лічильно-імпульсної системи були припинені, та група № 7 обрала у якості мовного тракту *вокодер*.

Розпорядженням начальника лабораторії Васильєва від 08.01.49 р. була здій-

снена реорганізація групи № 1 і акустичної групи. З того часу розробкою *вокодера* для груп № 1 і № 7 стала займатися акустична лабораторія, технічним керівником якої був Трахтман.

Перший варіант системи засекречування був наданий до групи № 2 у листопаді 1948 року, а негативний висновок на нього був складений 18.12.48 р. Другий і третій варіант надійшли до групи № 2 відповідно у березні й травні 1949 року. У цих останніх варіантах система шифрування будувалася за принципом «біт на біт», стійкість якої була доведена у червні 1941 року В.Котельниковим, а пізніше Шенноном. Це означало, що на один знак відкритої інформації накладався випадковий рівноймовірний знак гами шифру.

Таким чином, у групі № 2 за стислий термін у 8 місяців невелика група криптологів Марфінської лабораторії проаналізувала та довела до обґрунтованих висновків 9 варіантів систем шифру. Паралельно з цим була розпочата розробка шифраторів, що виробляли гаму шифру.

13 січня 1949 року начальником групи № 2 Калачовим була складена службова записка (попередньо погоджена з Васильєвим), у якій говорилося, що Марфінська лабораторія розробила систему шифрування імпульсів мови, але розробка шифраторів для таких систем могла бути зроблена тільки криптологічними методами. У записці було звернуто увагу на те, що лабораторія не має фахівців з криптології, та викладене клопотання про запрошення на тимчасову роботу криптологів з 6-го Управління МДБ, які працювали у сфері конструювання та оцінки стійкості шифраторів.

Приблизно через місяць – 12 березня 1949 року міністру держбезпеки Абакумову надійшов рапорт від начальника відділу. Приведемо кінцівку рапорту: «... робота криптографів є вирішальною, прошу перевести в лабораторію ВОТ до закінчення розробки криптографів 6 Управління МДБ СРСР – фахівців Верченко і Тюрина, а також продовжити термін перебування відрядженого до лабораторії фахівця Петерсона». Міністр наклав резолюцію: «Тов. Шевельов. Подзвоніть мені. Абакумов». Незабаром у Марфінській лабораторії з'явилося не двоє запрошених, а троє: Верченко, Тюрин і Дайчик.

22 березня 1949 року Васильєв зібрав організаційну нараду представників лабораторії та 6-го Управління МДБ, пояснив завдання, його труднощі та організував у подальшому під своїм головуванням «особливу нараду» з проблем криптографії швидкодіючих шифраторів.

На цій нараді 6 основних криптологічних працівників були розподілені по 3-х розробляючих групах. Здавалося, що успішно був даний старт роботі, але... подальші події з детективним відтінком затримали початок активної роботи ще на 3 тижні. Справа була в тому, що група відряджених співробітників 6-го Управління МДБ доповіла своєму керівництву про те, що їх бентежить факт задіяння у розробці шифраторів нового типу великої групи ув'язнених, яким стануть відомі останні відомості з теорії шифрування та дешифрування, а також пристроїв розроблених систем.

Оскільки від керівництва 6-го Управління МДБ не було чітких вказівок відряджeним співробітникам, вони звернулися 15 квітня 1949 року до заступника міністра держбезпеки Селівановського. На доповідній записці була накладена така резолюція заступника міністра: «Т.Желєзову. Треба створити такі умови роботи, щоб арештовані не могли знати всієї системи шифрування». Желєзов направив цей документ зі своєю резолюцією Васильєву лише через три місяці (11.07.49р.): «Товаришу Васильєву, до виконання».

Васильєв написав свою резолюцію (16.08.49р.): «Тов. Калачову. Прошу надати точний перелік працюючих з/к із вказівкою, хто з них до якої частини роботи допущений, які терміни ув'язнення, які наші перспективи по відношенню до цих людей. Це надамо до санкції в міністерство».

Список щодо групи № 2 (5 осіб у криптологічній бригаді і 6 – у статистичній) був наданий керівництву та з відомостями інших груп наприкінці серпня направлений до міністерства. Надалі вказівки щодо обережності ознайомлення ув'язнених з матеріалами, особливо щодо аналізу шифраторів, виконувалися, але не можна сказати, що це давало повну гарантію нерозповсюдження секретних даних.

Марфінська лабораторія не мала права гаяти час, тому Желєзов виявив дивну оперативність, звернувшись з відповідним рапортом (наступного дня після 15.04.49р.) на ім'я міністра. Рапорт був складений у досить «різких тонах». У рапорті вказувалося, що відряджені співробітники вважають, що їхня участь у роботі лабораторії приведе до розголошення таємниць 6-го Управління серед співробітників ВОТ і ув'язнених. Що відряджені співробітники будуть працювати тільки після письмового дозволу керівництва МДБ, оскільки посилання на відповідний пункт Постанови Уряду з організації лабораторії щодо використання праці ув'язнених відряджених не задовільняють. До рапорту була прикладена виписка з Постанови Уряду та доповідна записка на ім'я Селівановського.

При такій «тональності» рапорту можна було передбачити реакцію міністра. Чорним олівцем розмашисто була накладена така його резолюція: «Примусити працювати. В.Абакумов». Ознайомлені під розписку «відмовники», одержавши цю вказівку, приступили до активної роботи в лабораторії.

Після проведення спільної наради із співробітниками 6-го Управління з обговоренням питань про те, що таке гарантована стійкість, Васильєв швидко зрозумів, що ця фундаментальна проблема додасть турбот не менше, якщо не більше, ніж проблема забезпечення компресії та якості мови.

Незабаром після зазначеної наради він написав 3-сторінковий лист на ім'я Селівановського, оцінюючи ситуацію, що склалася. У листі було відзначено, що центральним питанням безпеки зв'язку була гарантія, доказовість стійкості системи шифрування та самого шифратора. Створені на той час телеграфні шифратори для телефонного засекречування були непридатні як за швидкістю, так і надій-

ністю роботи. Далі мовилося, що Марфінська лабораторія повинна створити нову школу теоретичних і практичних основ проектування швидкодіючих шифраторів. Для цього було запропоновано:

1. Організувати в Марфінській лабораторії дослідну лабораторію з теоретичної розробки всіх питань стійкості телефонних шифраторів за спеціальним планом.

2. Об'єднати для цієї роботи відповідних працівників ВОТ і 6-го Управління МДБ, для чого здійснити всі заходи щодо поповнення складу математиків і інженерів з використанням ув'язнених на великі терміни.

Після цього через якийсь час у 6-му Управлінні під керівництвом Верченко була створена група фахівців з 29 осіб для аналізу шифраторів, розроблених у лабораторії. Причому первинний аналіз проводився в лабораторії, а експертизу здійснювало 6-е Управління. Таким чином вирішилося організаційне питання, що було поставлене Васильєвим.

«Особлива нарада» лабораторії працювала з 22 березня по 9 червня 1949 року. Матеріали, що характеризували її роботу, були викладені в 10 протоколах на 44 сторінках. Перші 5 найбільш важливих за змістом протоколів підписувалися всіма учасниками наради. На обговорення робіт запрошувалися провідні спеціалісти, у тому числі зі складу ув'язнених (на 5 засіданнях були присутні 13 осіб).

На першій нараді 22 березня 1949 року розглядалося питання про основний зміст роботи фахівців 6-го Управління. Були присутні і виступили всі 7 постійних учасників наради. Був схвалений розподіл працівників по розроблюючих групах з метою спільного вирішення загальнодержавного складнішого завдання:

- 🗝 група № 1 (М-801) – Тюрин, Владимиров;
- 🗝 група № 6 (М-803) – Верченко, Петерсон;
- 🗝 група № 7 (М-804) – Калачов, Дайчик.

Для навчання була сформована група з 15 осіб (з них 5-6 ув'язнених) за списком, затвердженим керівництвом міністерства.

Для лабораторії, однак, залишалося незрозумілим головне питання: як сформулювати кількісні та якісні вимоги до основного параметра апаратури – її стійкості. Цього не міг зробити ні замовник, ні розробник, ні навіть 6-е Управління МДБ.

Ще в 1941 році Котельниковим було доведено, що можна створити математично недешифровану систему засекречування, якщо кожен знак повідомлення буде засекречуватися рівноймовірно обраним знаком шифру, або як тоді говорили – шифруванням «знак на знак».

До квітня 1949 року були визначені три варіанти системи засекречування. При цьому сама низькошвидкісна мала швидкість близько 2 Кбіт/сек. Щоб реалізувати таку математично недешифровану систему потрібно було готувати заздалегідь для кожної розмови тривалістю 15 хвилин паперову телеграфну 5-розрядну стрічку, що містила $1{,}8 \times 10^6$ знаків шифру або близько 1 кілометр такої стрічки.

Практично використовувати таку систему було нереально. Тому постало питання щодо створення так званих програмних шифраторів, коли до шифратора вводився ключ у кілька сотень біт, на основі якого шляхом складних перетворень за програмою, обумовленою криптологічною схемою, вироблялася істотно більша кількість знаків шифру, що забезпечувала засекречування інформації.

Після 3-тижневої перерви 13 квітня 1949 року нарада відновила свою роботу для обговорення 3-х кардинальних питань, сформульованих начальником лабораторії Васильєвим.

Приведемо в стислому вигляді основний зміст цих питань:

1) чи є впевненість у тому, що системи шифраторів, засновані на розмноженні знаків ключа, що вводяться в них, у сукупності з заходами для зниження статистичних ознак відкритої інформації, забезпечать абсолютно стійке шифрування телефонних переговорів;

2) якщо на перше питання не можна відповісти позитивно, то в яких формулюваннях може бути встановлений ступінь гарантованої стійкості;

3) що може бути запропоноване для того, щоб можна було відповісти позитивно на перше питання.

13 квітня відбулася «довга», важка і змістовна нарада, яка однак не дала чітких відповідей на кожне з трьох питань, але примусила усіх узятися енергійніше за практичне вирішення завдань щодо 3-х розробок Марфінської лабораторії. Нарада прийняла рішення про перехід до практичної оцінки розроблюваних систем М-801, М-803 і М-804.

У протоколах нарад за квітень-травень 1949 року були зафіксовані дані про розгляд запропонованих криптосхем і технічних рішень щодо 3-х варіантів шифраторів (М-801, М-803, М-804) і прийняті відповідні рішення. Були розглянуті доповіді щодо методів шифрування та критеріїв оцінки стійкості.

У липні 1949 року «особлива нарада» закінчила свою роботу. Вона яскраво висвітила стан радянської криптології того часу і тим самим допомогла чітко сформулювати завдання на найближчі роки та успішно вирішити їх у подальшому.

Вирішуючи проблему синтезу швидкодіючого шифратора, здавалося найпростіше задіяти наявні телеграфні шифратори, що вже тривалий час знаходилися в експлуатації. Найбільш широко використовувалися в той час стрічкові шифратори з зовнішнім носієм шифру та дискові машини, в яких були послідовно включені диски, вхідні-вихідні контакти кожного з яких мали різну комутацію після кожного кроку обертання дисків.

Як уже відзначалося вище, для вокодерного варіанту (2 кбіт/сек) витрата стрічки для забезпечення навіть 15 хвилин розмови складала б близько 1 кілометр, а для цілодобової роботи – у сто разів більше. Та й техніка кінця 1940-х років не могла забезпечити «зняття» знаків, нанесених на стрічку, зі швидкістю сотні

кроків у секунду. Тому використання стрічкового шифратора відпадало.

У випадку використання дискової машини з 32 контактами необхідно було б робити 2000/32 = 62,5 кроку в секунду, що не забезпечувало надійної роботи системи та приводило б до швидкого зносу контактів і частих збоїв. Таким чином, для створення швидкодіючого шифратора треба було знайти нові рішення з використанням нових елементів, здатних працювати надійно на високих швидкостях.

У наданих на експертизу до 6-го Управління МДБ 3-х варіантах шифраторів були використані 2 методи побудови схем шифраторів. У 2-х варіантах як основний вузол використовувалася дискова машина, що працювала на експлуатаційно-надійних швидкостях та видавала в кожен такт групу двійкових символів, що розмножувалися далі електронною схемою. У 3-му варіанті шифратор мав ключовий пристрій, що використовував 5-розрядну паперову стрічку.

Замість механічних пристроїв зйому знаків зі стрічки використовувався фототрансмітер, що працював на швидкості близько 2000 біт/сек. Потім знаки, що знімалися з фототрансмітера, розмножувалися в електронному пристрої до необхідного співвідношення «біт гами шифратора на біт інформації, що шифрується». При цьому витрата стрічки, що фіксувала знаки ключа, різко скорочувалася.

Першим успіхом лабораторії було надання на експертизу до 6-го Управління 3-х варіантів системи засекреченого зв'язку з описом пристроїв мовного перетворення, системи передачі інформації каналом зв'язку та шифратора. Важливо при цьому помітити, що спільно співробітниками лабораторії та 6-го Управління було забезпечене попереднє обґрунтування гарантованої стійкості всіх 3-х варіантів.

Якщо протягом 1948 року (починаючи з квітня) основна увага колективу приділялася розробленню методів компресії мови та вибору системи шифрування, а також проблемі передачі інформації каналом зв'язку, то протягом першої половини 1949 року більша увага стала приділятися розробленню швидкодіючого шифратора з подоланням великих труднощів у вирішенні проблеми синтезу шифратора та оцінки його стійкості математичними методами.

Головним успіхом лабораторії у 1949 році було завершення на рівні ескізного проекту розробки 3-х варіантів апаратури секретної телефонії для роботи по стандартному телефонному каналу та надання експертній організації необхідних матеріалів для аналізу стійкості засекречування. Однак докладних комплексних іспитів апаратів, у цілому, ще не проводилося, хоча 3 основні вузли апаратів (перетворення мови, шифратор і модем) були виготовлені та пройшли іспити.

Найголовнішою проблемою, як і раніше, було істотне підвищення якості мови, відновленої на прийомному кінці тракту зв'язку, а найголовніше, «природність» її звучання. Приведемо витяг з доповіді Васильєва від 21 грудня 1949 року «Розробка системи Урядового зв'язку». У доповіді було висунуто дві пропозиції:

🗝 для якнайшвидшого впровадження таємного зв'язку необхідно виготовлення невеликої серії апаратури, допускаючи при цьому деяке зниження якості зв'язку;

🗝 радикальне покращення якості мови може бути досягнуто у разі подвоєння смуги частот каналу зв'язку.

У цих пропозиціях проявилася втрата надії на покращення якості мови при роботі по стандартному каналу апаратури М-803 з використанням кліпованої мови. Крім цієї центральної проблеми треба було вирішити завдання щодо двох інших вузлів апаратури.

Щодо шифратора, то необхідно було істотно спростити його схему та складність реалізації. Схема шифратора містила дискову машину, «кіноустановку» з розгортанням ключа шифратора, фіксованого на кіноплівці, складне електронне устаткування. При цьому необхідно відзначити ненадійну роботу контактів у дискових машинах.

У криптологів чітко визначилися два напрямки роботи: вирішення проблем синтезу та аналізу електронних схем вихідних вузлів шифратора. Якщо за першим напрямком міг використовуватися досвід 6-го Управління, то за другим напрямком довелося починати фактично з «нульової» оцінки.

Третя проблема була пов'язана з розробкою пристроїв передачі «високошвидкісної» інформації стандартним телефонним каналом зв'язку. У ході іспитів цих пристроїв на каналі зв'язку виявилася нестійкість роботи окремих вузлів, що призвела до зриву передачі.

Якщо можна було сподіватися на подолання труднощів 2-ї та 3-ї проблеми, то з доповіді Васильєва випливало, що з кліпованої мови треба було переходити на *вокодер*, вирішуючи при цьому важке завдання щодо покращення природності його «звучання».

Отже, незважаючи на напружену роботу колективу лабораторії, до початку червня комплексні іспити трьох зразків апаратури М-801, М-803 і М-804 не були завершені. Апарати з використанням вокодера і кліпованої мови завзято не хотіли «говорити по-людськи», тобто якість відновленої мови не відповідала вимогам ВУЗ. Складова артикуляція мови в пункті прийому для системи М-803 складала 31,2 % замість необхідних 60 %. Слід зазначити, що в той час ви-

користовувалися більш складні артикуляційні таблиці, ніж ті, що використовуються в даний час. Однак необхідність підвищення артикуляції, що характеризувала розбірливість мови, залишалася актуальною.

Виходячи з вищезазначеного, начальнику відділу 2 липня 1949 року довелося коригувати план на 1949 рік. Термін завершення іспитів дослідних зразків М-803 і М-804 відклали на 1 вересня, а М-801 – на 15 вересня.

У серпні 1949 року Васильєв зробив важкий вибір. Незважаючи на низьку артикуляцію для остаточного відпрацьовування зразка апаратури він обрав систему М-803. В другій половині серпня було видано декілька розпоряджень щодо організації спеціальних груп і бригад для налагодження окремих вузлів, комплектуванню та іспитів дослідних зразків.

Поряд з підготовкою до проведення дослідної експлуатації зразків апаратури на лінії зв'язку була проведена реорганізація структури особливого сектора. Крім розформування груп № 3 і № 5, була розформована група № 7, основний склад її був переданий до групи № 4. Група № 4 почала розробку 4-го варіанта апарата засекречування М-809 і повинна була згідно з наказом Васильєва від 29.08.49р. зробити його до 15 листопада 1949 року.

Два з половиною місяця – термін явно нереальний, однак це був резервний варіант. У цей напружений період роботи лабораторії вийшла Постанова Уряду про створення Державної комісії з приймання дослідних зразків апаратури засекречування для урядового зв'язку від 15 жовтня 1949 року.

Вихід Постанови Уряду підштовхнув керівництво лабораторії прискорити реорганізацію структури лабораторії з метою концентрації сил на головних напрямках. На початку листопада були припинені роботи щодо системи М-801 (*вокодер* був знятий з виробництва у групах № 1 і № 7). Склад групи № 1 був переданий до групи № 4 для розробки шифратора резервної системи М-809.

Наприкінці 1949 року з груп особливого сектора залишилося тільки три – № 2, № 4 і № 6. У середині листопада 1949 року було створено 2 групи по 8 фахівців у кожній для проведення дослідної експлуатації зразків апаратури, встановленої в Києві і Москві.

Група № 2 підготувала для дослідної експлуатації ключову документацію та інструкцію з обслуговування шифратора, доповнену спеціальним інструктажем обслуговуючого персоналу. Ця інструкція стала прототипом правил користування апаратурою засекречування на лініях зв'язку.

Колектив розробників працював напружено, на рівні фізіологічних можливостей людини. Рік роботи в такому режимі повинен був зараховуватися за 3-5 років. За наказом був установлений 12-годинний робочий день з 9 ранку до 9 вечора, а за окремими розпорядженнями – з 9 до 23 годин. Часто за наказом вводився «казармений стан», і працівники всю ніч проводили на об'єкті у «спальному» корпу-

сі. На сон залишалося лише 5-6 годин. Переважна більшість штатних і ув'язнених працівників з розумінням приймали такий режим роботи, тому що в тій ситуації іншого виходу, напевно, не було.

Спільна робота Марфінської лабораторії з експертною групою криптологів 6-го Управління здійснювалася через групу № 2. Для проведення робіт з експертизи в 6-му Управлінні була створена спеціальна група в складі 29 осіб. Керівником групи був кандидат фізико-математичних наук Іван Якович Верченко, а група складалася з 4 кандидатів наук і 9 осіб, що мали вищу математичну або технічну освіту. Група працювала з липня 1949 року по січень 1950 року.

Працюючи разом з експертною групою, лабораторія ставила перед собою три завдання:

- одержати позитивний висновок щодо стійкості апаратури;
- одержати дозвіл на лінійні іспити на каналах зв'язку;
- спробувати домогтися спрощення складного шифратора.

Усе це з розуміння та доброзичливо було сприйняте керівником експертної групи. Потрібно відзначити, що у зв'язку з припиненням розробки систем М-801 і М-804, робота експертної групи стала менш трудомісткою, однак варто сказати, що в нормальних умовах на аналіз схеми шифратора, побудованого на нових принципах, потрібен був час до одного року, незалежно від того, скільки осіб було зайнято роботою з аналізу.

Експертна група працювала напружено, і 31 серпня 1949 року був отриманий позитивний висновок щодо стійкості шифратора та дозвіл на проведення лінійних іспитів. Уже на цьому етапі удалося внести деякі спрощення в схему шифратора М-803.

По-перше, час використання одного кадру шифру кіноплівки в «кіноустановці» вдалося збільшити приблизно в 1000 разів, що дозволило різко зменшити добовий обсяг ключової інформації та понизити швидкість роботи «стороннього тіла» у шифраторі – «кіноустановки». Зазначимо, що в 1950 році вона була виключена зовсім. По-друге, приблизно в 50 разів була зменшена довжина накопичувача на виході шифратора з 1800 до 30-40 біт, що дозволило реалізувати його методами радіоелектроніки.

5 листопада 1949 року до експертної групи були відправлені матеріали щодо резервної системи М-809 із шифратором Ш-47. Позитивний висновок щодо стійкості шифратора Ш-47 був підготовлений за 2 місяці. У ході аналізу експертами було запропоновано кілька змін, що були прийняті Марфінською лабораторією. На відміну від трьох перших варіантів, шифратор Ш-47 не мав дискової машини та був побудований на релейно-контактних схемах.

Система М-809 виникла як резервний варіант, що підстраховував три основні розробки. Головні конструктори Нейман і Нанос довели розробку до лабораторних

зразків, по яких можна було розмовляти, хоча мова «звучала» своєрідно – «музично». У 1950 році, коли один з варіантів раніше розроблених систем був прийнятий Державною комісією, роботи щодо системи М-809 були припинені.

Іспит апаратури М-803 на лінії зв'язку Москва-Київ продовжувався більше місяця. За цей час удалося перевірити працездатність усіх трьох блоків апаратури: мовноперетворюючого пристрою, шифратора та модема. Підсумки іспитів були такими:

1. Лабораторія наблизилася до вирішення всіх сформульованих вище проблем і створення для ВЧ-зв'язку телефонної апаратури засекречування високої стійкості. Була доведена працездатність основних блоків апаратури, що додало більше впевненості щодо успіху проведеної розробки.

2. Були виявлені такі недопрацювання в окремих вузлах апаратури:

- апаратура забезпечувала проведення переговорів, однак мова була зашумлена, розбірливість складів – 30%, у той час як канал зв'язку забезпечував 70%, – необхідно було знайти способи підвищення розбірливості і зменшення зашумлення;
- у шифраторі необхідно усунути пропадання контакту в дисковій машині, що викликало неприємні відчуття в пункті прийому;
- у модемі було виявлене перекидання фази в системі з фазовою модуляцією, що приводило до зриву передачі, тому необхідно було підвищити стійкість фази на прийомі;
- визначені труднощі виникали у зв'язку з наявністю на кінцевих пунктах зв'язку одного шифратора, що працював на прийом і на передачу, – необхідно було перейти на використання двох шифраторів.

Проведені експерименти виявили, що низька розбірливість та велика зашумленість кліпованої мови в апаратурі М-803 пов'язані як із широким спектром мови (200-3400 Гц), що піддавалася обмеженню (кліпуванню), так і з низькою частотою дискретизації кліпованої мови (відношення частоти дискретизації, рівної 4,5 кГц, до верхньої частоти спектра мови 3,4 кГц складало всього 1,32). Значне підвищення частоти дискретизації (до 7-8 кГц) у той час було неможливе через відсутність пристроїв, за допомогою яких така швидкість могла бути передана по дротовому каналу зв'язку.

У Києві в проведенні лінійних іспитів брав участь працівник 6-го Управління Петерсон. Наприкінці грудня в нього з'явилася нова оригінальна ідея створення мовного тракту. Приїхавши в Москву, він зустрівся з Васильєвим і розповів, яким чином можна було б істотно поліпшити якість мови. Начальник Марфинської лабораторії швидко створив групу з найкваліфікованіших розробників, що повинна була за 2-3 місяці створити новий мовноперетворюючий пристрій.

Як вихід з цього становища Петерсоном було запропоновано використання в якості мовноперетворюючого пристрою модифікованого 8-канального *вокодера*, додавши до нього розширений до смуги 200-600 Гц перший канал. У цьому

каналі для утворення спектра замість основного тону використовувалася кліпована мова, яка передавалася з малими перекручуваннями. Одержання такої кліпованої мови досягалося як за рахунок використання вузької смуги кліпування (200-600 Гц), так і за рахунок високої частоти її дискретизації – 2250 Гц (при цьому відношення частоти дискретизації до верхньої частоти мови дорівнювало 3,75).

Спектр інших 7 каналів *вокодера* (канали 2-8) утворювався за рахунок перетворення кліпованої мови. У результаті вийшов мовноперетворюючий пристрій, у якому натуральність мови забезпечувалася за рахунок передачі з порівняно невеликими перекручуваннями смуги 200-600 Гц, а розбірливість, в основному, за рахунок передачі вокодером смуги 600-3400 Гц. Цей мовноперетворюючий пристрій надалі одержав назву «напіввокодер». Забігаючи наперед, скажемо, що реалізація цієї ідеї була надалі схвалена Державною комісією.

15 жовтня 1949 року була створена Державна комісія з приймання апаратури, але в той час не було завершено налагодження М-803 та резервний варіант М-809.

Пропозиція щодо створення нового варіанту (напіввокодера) вимагала для своєї реалізації мінімум 2-3 місяці. Навіть у разі успішного налагодження напіввокодера готовність апаратури була б із запізненням на півроку. Треба було заново створити всі схеми мовного тракту, сконструювати та виготовити всі панелі, а також налагодити всі схеми та систему в цілому. А іншими словами, виготовити нову апаратуру.

У лабораторії створився складний, нервозний стан. «Дамоклів меч» висів не тільки над головами керівництва відділу та лабораторії, але й над провідними розробниками. Розплата могла бути досить суворою. У такому стані працювали і дні, і ночі. Головним завданням була реалізація нового варіанту та усунення недоліків, виявлених у ході лінійних іспитів. Кропітка робота полягала в узгодженні режимів роботи вузлів у місцях стиків та уповільнень сигналів в окремих вузлах.

Особливо важким становище склалося в лабораторії наприкінці лютого – початку березня 1950 року. Міністр нещадно критикував керівництво відділу та лабораторії за багаторазові зриви знову встановлених термінів. А тим часом налагодження нової апаратури було завершено: покращена якість звучання, а артикуляція складів збільшилася з 31% до 51,1% (у 1,64 разу).

Державна технічна комісія, призначена Постановою Ради Міністрів СРСР, почала свою роботу 1 квітня 1950 року з запізненням на 5,5 місяця. У комісію входили фахівці досить високої кваліфікації. Головою комісії був професор І.Г.Кляцкін. Комісія працювала з 1 по 17 квітня, а результати її роботи були викладені в акті, протоколах іспитів і висновків.

Комісії були надані два напівкомплекти апаратури М-803, кожний з яких містив у собі чотири стандартні стояки та «стіл» шифратора. Була також надана технічна документація на апаратуру та результати лабораторних іспитів. Ознайомившись з матеріалами та визначивши найбільш слабкі місця апаратури, комісія призначила серію до-

даткових іспитів, а також повторних випробувань, проведених раніше лабораторією.

За 17 днів роботи комісії було проведено безліч іспитів щодо експлуатаційної надійності, стійкості роботи в різних умовах, визначення якості мови. В результаті комісія дала задовільну оцінку якості відновленої мови (артикуляція складала 51,8 %) та рахувала цю якість придатною для експлуатації. Разом з тим, комісія рекомендувала продовжити роботу з поліпшення якості мови, домагаючись більшої природності її звучання. Крім того, у ході проведення іспитів комісія встановила достатню експлуатаційну надійність апаратури М-803.

Приведемо витяг з підсумкового висновку комісії:

- лабораторні зразки апаратури засекречування для урядового ВЧ зв'язку були вирішенням складнішого науково-дослідного завдання щодо гарантованого засекречування телефонних переговорів;
- була потрібна велика науково-дослідна робота (далі - НДР) для вишукування нових способів перетворення мови. Вперше в СРСР МДБ виконало таку НДР і створило зовсім новий спосіб ВЧ-зв'язку з телеграфним шифруванням мови;
- перетворення телефонної передачі в телеграфну забезпечило досягнення гарантованої стійкості шифрування мови.

Комісія дійшла висновку, що були всі підстави для виготовлення головних виробничих зразків і запуску у виробництво дослідної серії з метою проведення детальних іспитів і нормальної експлуатації на лініях ВЧ-зв'язку. При виготовленні апаратури необхідно було врахувати всі пропозиції Державної Технічної комісії.

Робота Комісії та її результати були найважливішою подією в житті Марфінської

лабораторії та суворим іспитом щодо оцінки її діяльності. Якщо врахувати складність і фундаментальність розв'язуваних проблем, оцінка комісії була досить високою. Після цього розпочалася робота з усунення недоліків в апаратурі: тих, які відзначила комісія, і тих, які знали тільки розробники.

У цей час керівництво лабораторії, ВОТ і МДБ займалося підготовкою проекту Постанови Ради Міністрів з урахуванням рекомендацій комісії та потреб ВУЗ в апаратурі засекречування. Працівники на рівні керівників груп до цієї роботи не залучалися. Вочевидь, робота була нелегкою, тому що між її початком і датою виходу Постанови Уряду пройшло 3,5 місяця.

Постанова РМ СРСР вийшла 29 липня 1950 року, та в ній можна було виділити 3 частини: констатація роботи комісії, заохочення штатних і ув'язнених співробітників, а також зобов'язання, що накладалися на Марфінську лабораторію з випуску малих серій апаратури. Рада Міністрів високо оцінила досягнення колективу. 10 ув'язнених фахівців достроково були звільнені за значний внесок у розробку зразків апаратури та сумлінну працю протягом 2,5 року в лабораторії. Після свого звільнення вони працювали вільнонайманими співробітниками лабораторії.

Керівник розробки Васильєв був визнаний гідним вченого ступеня доктора технічних наук без захисту дисертації. 5 учасників роботи отримали вчені ступені кандидатів технічних наук: начальник ВОТ Желєзов, співробітник 6-го Управління Петерсон, керівники груп Волошенко і Калачов, старший інженер групи № 4 Нанос.

Крім двох зазначених заохочень штатного складу та ув'язнених, наказом по МДБ працівникам була видана грошова винагорода. Був нагороджений весь провідний штатний склад та працівники на рівні 10 тисяч карбованців, інші по кілька тисяч карбованців. Був нагороджений також керівник експертної групи Верченко (15 тисяч карбованців) і співробітники його групи. Достроково звільнені працівники одержали від 5 до 15 тисяч карбованців. Премії від 100 до 1000 карбованців одержали близько 300 ув'язнених.

Крім щедрих нагород, Постанова Ради Міністрів визначила для Марфінської лабораторії складніше завдання щодо виготовлення у 1951 році 22 напівкомплектів апаратури М-803 і необхідної кількості ретрансляторів. У 1952 році треба було випустити 32 напівкомплекти апаратури та велику кількість ретрансляторів. Якщо врахувати, що кожен напівкомплект складався з 4-х стояків великих габаритів, то у 1951 році треба було випустити більш 100 стояків (враховуючи і ретранслятори). Це було під силу лише великому заводу, тому треба було терміново створювати могутню виробничу базу та у той же час покращити якість мови.

У зв'язку з вищевказаним потрібно було розібратися з тим, чим були зайняті окремі лабораторні підрозділи. Як уже відзначалося вище, у зв'язку з недостатністю сил у лабораторії роботи щодо апаратури М-809 у групі № 4 у 1950 році були припинені, а вся група № 4 була націлена на розробку апаратури тимчасової стійкості

М-503, що виключала можливість прямого прослуховування розмови в лінії.

У другій половині 1950 року з первісної структури лабораторії збереглися тільки дві групи: № 2 і № 4. З інших груп формувалися тимчасові та постійні колективи, що були потрібні у той час для вирішення завдань з доробки головного серійного зразка апаратури М-803, а також для підготовки до випуску серії відповідно до Постанови Уряду.

Досвід роботи у 1948-49 роках довів, що розроблена апаратура типу М-803 буде складнішим комплексом електронно-вакуумних і точних механічних приладів, що вимагали при виготовленні складніших технологій. У той час вже стало зрозуміло, що треба створювати нову галузь промисловості, засвоювати нові тонкі технології та для забезпечення успішної експлуатації апаратури виготовляти спеціальні контрольно-вимірювальні прилади, необхідні при проведенні профілактичних робіт.

Тому ще в квітні 1949 року у довідці лабораторії «Про хід робіт із засекречування Урядового ВЧ-зв'язку» начальником лабораторії Васильєвим було запропоновано утворити при Марфінській лабораторії виробничу базу для виготовлення протягом 1950-1952 років апаратури для засекречування 100 ліній зв'язку.

А після рішень Державної технічної комісії та Постанови Уряду в липні 1950 року завдання з розробки головних зразків серії та виготовлення серійної апаратури в 1951-52 роках стало головним для лабораторії. Відзначимо, що виготовлення головних зразків апаратури ускладнювалося пропозиціями комісії щодо необхідності покращення якості мови та деяких інших характеристик апаратури.

5.9. Утворення науково-промислової бази

10 жовтня 1949 року на базі радіолабораторій ЦНДІЗ був утворений НДІ-100 (з липня 1966 року - НДІ радіо), де вчений Коробков, талановитий учень і колега Котельникова, продовжував займатися вирішенням проблем секретного радіозв'язку. В інституті були розроблені методи засекречування інформації, що передавалася по багатоканальних радіорелейних лініях (далі - РРЛ) зв'язку. Ці методи розвивали ідеї Котельникова та були засновані на випадковій перестановці відліків певного тимчасового відрізання групового сигналу багатоканальної телефонії, що передається по РРЛ зв'язку.

Коробков володів широкою ерудицією та займався не тільки проблемами телефонного засекречування. Йому належать десятки винаходів в області зв'язку. Зокрема, він у 1948 році один з перших у світі запропонував дельта (імпульсно-різницеву) модуляцію - спосіб перетворення аналогового сигналу в цифрову форму, який сьогодні широко застосовується в цифрових системах зв'язку. Багато років ним було спрямовано на інженерну реалізацію цього фундаментального винаходу. Оскільки дельта-модуляція є одним з методів аналого-цифрового перетворення, отриманий цифровий сигнал легко поєднується з вимогами щодо захисту інформації від раді-

оперехоплення.

У серпні 1951 року відбулася реорганізація підрозділів Марфінського об'єкта, яка стала відправною точкою утворення науково-технічної бази для виготовлення апаратури засекречування. Експериментальні майстерні лабораторії здобули статус незалежного підрозділу - відділу точної механіки (далі - ВТМ) - і були підпорядковані безпосередньо керівництву відділу. На об'єкті два самостійні підрозділи підпорядковувалися начальнику об'єкта кандидату технічних наук Наумову. Начальником ВТМ був призначений Коробан. Для виготовлення серії апаратури був залучений завод у підмосковному Теплому Стані.

Найбільш складною для виконання була рекомендація Державної комісії щодо покращення якості мови: підвищення натуральності її звучання. Перша пропозиція надійшла незабаром після закінчення роботи комісії та зводилася до збільшення точності положення фази фронту мовного сигналу. Автором цієї пропозиції був ув'язнений Файнберг. У другій половині 1950 року з'явилися 2 нові ідеї щодо вирішення головної проблеми: варіант Васильєва, названий як М-803-М, і варіант Волошенко, названий як М-803-5.

Васильєв вважав, що недоліки якості мови в системі М-803 варто пояснити тим, що в її передачі була відсутня хоча б мінімальна ділянка спектра природної мови. Для усунення цього недоліку було запропоновано збільшити кількість біт для передачі першого каналу з 2,25 кбіт/сек приблизно до 3,6-4 кбіт/сек і зменшити кількість біт для передачі формантних каналів: замість 8 формантних каналів використовувати тільки 3, виділені за допомогою «плаваючих» фільтрів.

У системі М-803-5 Волошенко запропонував покращити якість звучання за рахунок значного покращення системи виділення та використання основного тону. До літа 1951 року були налагоджені макети 3-х варіантів системи мовного тракту: М-803-3 із введенням кодування фронту імпульсу в 1-му каналі, а також нові системи М-803-М і М-803-5. Для порівняння варіантів була призначена спільна комісія ВУЗ і ВОТ з вибору мовного тракту для першої серії апаратури М-803. Комісія вирішила порівняти варіанти М-803-М і М-803-5, а потім кращий з них – зі зразком М-803-3.

Для цього на пульт слухача анонімно підводилися виходи двох апаратів засекречування та для орієнтування вихід відкритого каналу зв'язку. Прослухавши передачу в трьох положеннях, слухач визначав кращий (оцінка «2») і гірший апарат (оцінка «0»). Якщо на думку слухача обидва апарати «звучали» приблизно однаково, то обом давалася оцінка «1».

Загальна оцінка якості мови кожного апарата визначалася як сума оцінок усіх слухачів, що брали участь в іспиті. Робота комісії проходила з 25 жовтня по 3 листопада 1951 року. Акт комісії був затверджений заступником міністра Держбезпеки СРСР Савченко 22 листопада 1951 року.

При першому порівнянні М-803-М і М-803-5 при роботі в дуплексному режимі як диктори та слухачі використовувалися члени комісії. Крім того, для іспитів як диктори були притягнуті три жінки лабораторії. В другому іспиті залучалася більша кількість дикторів (31 особа з лабораторії, що не проходила дикторську підготовку) і 24 слухачі (8 членів комісії і 16 співробітників ВУЗ). За підсумками цих двох іспитів комісія віддала перевагу варіанту М-803-5, який потім порівнювався із зразком М-803-3.

2 листопада 1951 року комісія провела обговорення доповідей Васильєва і Волошенко, висновків опонентів Файнберга і Ізмайлова та з урахуванням результатів порівняльних іспитів висловилася на користь системи М-803-5.

Дискусія була «гарячою» та її опис в акті комісії зайняв 12 сторінок. Основними мотивами для вибору мовного тракту М-803-5 для серії апаратури були дві обставини: по-перше, абонентами Урядового ВЧ-зв'язку переважною більшістю були чоловіки, а апаратура М-803-5 передавала ці голоси істотно краще двох інших варіантів, і по-друге, ця апаратура мала помітно меншу чутливість до недоліків абонентських ліній.

Відзначимо, що й після 50 років проблема якості мови для аналогових телефонних каналів, як і раніше, була основною та завжди існувала у планах робіт наукових організацій СРСР і за кордоном.

У 1950 році стало зрозуміло, що розроблена апаратура засекречування була досить складною, і розраховувати на істотне спрощення в найближчому майбутньому не доводилося. Створений головний зразок серії апаратури М-803 складався з 3-х стояків основних вузлів висотою 2,5 метра та стояка живлення. Приведемо деякі дані щодо стояка шифратора: кількість розривних контактів 5152, з них рухомих – 2080, кількість електронних ламп – 213, кількість електромагнітних реле – 145, кількість магнітних елементів пам'яті – 700.

У цей період теорії надійності як наукової дисципліни ще не було створено. Однак розробники усвідомлювали те, що треба здійснювати спеціальні заходи щодо забезпечення безвідмовної роботи зв'язку. Вкажемо основні заходи для підвищення надійності. По-перше, створення служби суворого вхідного контролю всіх радіоелементів. В експлуатаційній документації передбачалося проведення щоденної 2-годинної профілактики апаратури. Для проведення профілактичних робіт був створений спеціальний контрольно-вимірювальний прилад (далі - КВП).

По-друге, основним вузлом в апаратурі, що зменшував надійність роботи, була дискова машина. Проблема вирішувалася двома шляхами: підбір металу для контактних пар, їхня конструкція, змащення та зменшення кількості контактів шляхом вибору кращих криптологічних рішень.

До кінця діяльності Марфінської лабораторії була створена дискова машина зі стартостопним рухом дисків зі швидкістю 2 кроки в секунду. Остаточне її до-

опрацювання було завершене в перші роки створеного науково-дослідного інституту. Працювали дискові машини досить надійно та знаходилися в експлуатації тривалий час, поки їм на зміну не прийшли «електронні» шифратори.

У 1950 році було утворене ГУСС при ЦК ВКП(б), на яке було покладене завдання з проведення експертних робіт та видачі дозволів на проведення іспитів і експлуатацію апаратури засекречування. Розробка апаратури секретної телефонії, як і раніше, залишалася за Марфінською лабораторією. У такому порядку йшла розробка телефонної апаратури засекречування у 1950-51 роках.

У складі ГУСС був утворений науково-дослідний інститут № 1 (далі – НДІ-1), у якому Марфінську лабораторію курирувала група Верченка. «Положення про НДІ-1» було введене в дію ухвалою Секретаріату ЦК ВКП(б) від 9 червня 1950 року та наказом начальника ГУСС від 1 липня 1950 року. Цим положенням у складі НДІ-1 передбачалися: вчена рада, аспірантура, спеціальна науково-технічна бібліотека. У завдання НДІ-1 також входила організація науково-технічного інформування та видання наукових робіт і навчальних посібників.

Влітку 1951 року у лабораторії йшла напружена робота щодо налагодження та іспитів трьох зразків системи М-803. Події, що відбувалися в лабораторії влітку і восени цього року, свідчили про те, що в найближчому майбутньому було варто очікувати змін в організації її роботи. У середині червня спеціальним письмовим розпорядженням начальника відділу Желєзова криптографічна група № 2 була переміщена на самий верхній поверх надбудови основного будинку лабораторії, подалі від інших підрозділів.

У вересні відбувалася реорганізація групи № 2: ув'язнені, що працювали, в основному, в статистичній бригаді, були переведені в інші підрозділи, а група була поповнена п'ятьма штатними працівниками, яких було треба терміново навчити основам криптології. Восени 1951 року відбулася зміна керівника Марфінського об'єкта: замість Васильєва був призначений І.І.Наумов.

Робота з підготовки до реорганізації лабораторії завершилася виходом Постанови Ради Міністрів СРСР від 12 січня 1952 року «Про розробку апаратури для засекречування телефонних переговорів». Відповідно до цієї постанови в ГУСС на базі переданих з ВОТ МДБ Марфінської лабораторії та ВТМ, а також 3-й і 5-й лабораторій ГУСС був створений науково-дослідний інститут № 2 (далі – НДІ-2). Начальником інституту був призначений І.І.Наумов. Чисельність НДІ-2 у момент його створення складала 374 особи, а штат був визначений у 700 одиниць. При створенні НДІ-2 було обговорено, що протягом року зі складу його працівників будуть виведені всі ув'язнені.

Так завершила свою діяльність Марфінська лабораторія, що проіснувала близько 4-х років. Відразу після виходу постанови щодо утворення НДІ-2 в ГУСС розпорядженням Уряду була створена комісія щодо вивчення результатів діяльності ла-

бораторії у складі: Псурцев (голова), Алексеєнко, Пересипкін, Савченко, Белишев, Котельников, Какуін, Верченко і Шевельов.

В акті комісії, представленому в бюро Президії Ради Міністрів СРСР від 15 лютого 1952 року, відзначалася погана якість відновленої мови в системі М-803-3. Прослухавши зразки апаратури М-803-5, комісія визнала апаратуру М-803-5 прийнятною для використання на закордонних лініях ВЧ-зв'язку та рекомендувала провести іспити дослідних зразків. Щодо апаратури тимчасової стійкості М-503 комісія визнала її придатною для використання на внутрішніх лініях зв'язку.

Акт урядової комісії можна вважати підведенням підсумків діяльності Марфінської лабораторії за 4 роки. Прийнята Урядовою комісією як серійні зразки апаратура М-803-5 і М-503 була дороблена та виготовлена в НДІ-2. Цей інститут також одержав умовне найменування «*почтовый ящик № 37*», що було запозичено з номера автобусного маршруту, який закінчувався біля його території.

Колишній начальник ВУЗ Воробйов, в'язень Марфінської «шарашки», після її ліквідації у лютому 1952 року був звільнений та «пішов» працювати цивільним старшим інженером ВОТ МДБ (5-го спецвідділу МВС з 25.04.1953). Після утворення КДБ з 28 квітня 1954 року став начальником планово-економічного відділення ЦНТБ опертехніки (ЦНДІ спецтехніки з 17.08.1955) 5-го спецвідділу КДБ. 4 травня 1971 року Воробйов був нагороджений Орденом Жовтневої революції, а у 1972 році помер від тяжкої хвороби.

У 1953 році після смерті Сталіна відбулася чергова реорганізація: ГУСС було розформовано, його основні підрозділи передані назад в органи МДБ, а НДІ-2 – у промислове міністерство: спочатку в Міністерство електропромисловості й електростанцій, а потім у Міністерство промисловості засобів зв'язку (далі - МПЗЗ).

У лютому-березні 1954 року начальник НДІ-2 Наумов призначив інститутську комісію з визначення готовності магістралі Москва-Берлін, обладнаної апаратурою М-803-5 і М-803-Т (ретранслятор), до спільних лінійних іспитів із замовником. Упродовж 2-х місяців роботи на лінії зв'язку комісія встановила достатню стійкість роботи апаратури, після чого рекомендувала надати апаратуру на спільні іспити з замовником. Акт інститутської комісії був затверджений 3 квітня 1954 року.

У період з 15 квітня по 26 травня 1954 року працювала спільна комісія ВУЗ і НДІ-2 з проведення лінійних іспитів апаратури М-803-5 і М-803-Т на лінії зв'язку Москва-Берлін. Комісія оцінила якість мови прийнятною для проведення дослідної експлуатації магістралі Москва-Берлін. Акт комісії був затверджений начальником ВУЗ Вороніним і начальником 3-го Головного Управління МПЗЗ Лобовим у червні 1954 року.

Після проведення працівниками ВУЗ дослідної експлуатації була виготовлена партія апаратури М-803-5, М-803-Т (головний конструктор Кабатов), якою були оснащені важливі закордонні магістралі: Москва-Берлін і Москва-Пекін. Тракт

зв'язку Берлін-Москва-Пекін був у той час найбільш довгою у світі магістраллю засекреченої проводової лінії зв'язку. Це був початок міжнародного урядового зв'язку. За виготовлення серії апаратури М-803-5 і М-803-Т група співробітників НДІ-2 була відзначена урядовими нагородами, зокрема, головний конструктор Кабатов був нагороджений орденом Леніна.

Крім НДІ-1 і НДІ-2, у 1950-і роки в країні були створені та почали функціонувати також і промислові науково-дослідні та проектні організації, зокрема, особливе конструкторське бюро (далі - ОКБ) при заводі «*САМ*» (рос. *Счётные Аналитические Машины*) у Пензі та ОКБ при заводі «*КЭМЗ*» (рос. *Калужский электромеханический завод*) у Калузі. Вони включилися в процес розробки та забезпечення промислового випуску апаратури криптографічного захисту телефонних переговорів і телеграфної інформації та визначили початок процесу активного використання й розвитку науково-виробничого потенціалу промисловості на користь оснащення структур держави технікою захисту інформації.

Не дивлячись на прийняті заходи, все ще мала місце невідповідність між потребами замовників в особі Міністерства Оборони, КДБ і інших відомств, і можливостями промисловості, що визначило актуальність створення додаткових НДІ і заводів, що розширили би ресурси в області розробки та промислового виготовлення нового виду техніки захисту інформації спеціального призначення.

Враховуючи це, наказом Держкомітету з радіоелектроніки при РМ СРСР від 18 січня 1958 року № 34 для вказаних цілей був утворений у Пензі НДІ-3 (Пензенський науково-дослідний електротехнічний інститут, ПНДЕІ), а Ухвалою ЦК КПРС і РМ СРСР від 1 серпня 1961 року № 963290 був створений серійний профільний завод «*Электроприбор*». Директором НДІ-3 (ПНДЕІ) був призначений Іван Іванович Чернєцов, а головним інженером - Михайло Григорович Демков, які для організації свого інститута відібрали 10 фахівців з НДІ-2. Серед запрошених був Володимир Іванович Смислов, якому була запропонована посада начальника конструкторського відділу.

Підприємство розвивалося швидкими темпами, та у зв'язку з виробничою необхідністю вже через 5 років в конструкторському відділі працювало більше 100 фахівців. Паралельно створювалися загальні технічні підрозділи: відділ стандартизації (керівник - Калерія Михайлівна Лещенко), відділ науково-технічної інформації (Гаврило Степанович Билін), відділ технічної документації (Лідія Перфіловна Бурніна), відділ вимірювальних приладів (Вячеслав Миколайович Мукін).

У зв'язку з необхідністю впровадження мікросхем в розроблену спецапаратуру, фахівці ПНДЕІ неодноразово відвідували НДІ точної технології (далі - НДІТТ) і завод «Ангстрем» у Зеленограді. Поїздки здійснювалися, як правило, спільно

з провідними фахівцями НДІ-2, зокрема: з Йосипом Семеновичем Нейманом і Абрамом Марковичем Наносом. За роки своєї роботи ПНДЕІ вніс значний внесок у вирішення комплексних проблем криптографічного захисту інформації, розвиток техніки шифрування інформації та її передачі в мережах і системах засекреченого зв'язку. В даний час Відкрите акціонерне товариство «ПНДЕІ» є одним з найбільших підприємств в Росії, розробляючих шифротехніку .

У вересні 1959 року калузький завод пірометричних приладів був переорієнтований на виробництво спеціальної апаратури зв'язку та почав називатися «*Калугаприбор*». З 1960 року завод почав виробляти апаратуру засекречування для потреб урядового зв'язку. У 1983 році за успіхи у виробництві нової спеціальної техніки зв'язку завод був нагороджений орденом Трудового Червоного Прапора. До теперішнього часу підприємство спеціалізується на виробництві апаратури зв'язку, що забезпечує обробку оперативної інформації, як в стаціонарних, так і в рухомих об'єктах інформаційних мереж.

Наприкінці 1950-х – на початку 1960-х років у проектуванні систем засекречування завдяки Клоду Шеннону настав час технічного становлення математичної криптографії. Інтерес до розгляду таких систем як кінцевих автоматів привів до того, що стали успішно розвиватися багато розділів математики, які передбачили досить швидке просування інформаційних технологій.

Так, отриманий теоретиками результат, що в будь-якому кінцевому автоматі можна виділити автономну частину, яка відігравала роль внутрішніх «годинників» або підсистеми синхронізації для нього, дозволив інакше розглянути структуру систем засекречування. Тепер можна було періодичну синхронізуючу послідовність використовувати як шифруючу після спеціального перетворення, а здійснюючи її кодування, домагатися високонадійної роботи в зашумлених каналах зв'язку. Важливим кроком в розвитку процесу шифрування інформації стало розуміння, що його можна було будувати, як накладення шуму, тобто він мав випадковий характер.

У 1960-х роках настав новий етап у світовому шифраторобудуванні. Аналіз і синтез шифраторів нового покоління супроводжувався глибокими теоретичними дослідженнями в зовсім новій галузі криптології. Були визначені основні принципи побудови їхніх криптосхем і досліджені їхні типові вузли і блоки, розроблені основні методи математичного розрахунку

У дослідженнях були отримані важливі наукові і практичні результати, що дозволили обґрунтувати високі спеціальні якості вітчизняних шифрів і знайти підходи до дешифрування деяких іноземних шифраторів. Одночасно ці результати склали істотний внесок у розвиток теоретичної криптології.

Поряд із математизацією та комп'ютеризацією вітчизняної криптології особливо важливу роль зіграв розвиток фізико-технічного напрямку. Дослідження в

цій галузі дозволили на основі синтезу математичних і інженерних ідей із криптологією вирішити ланку важких криптологічних завдань.

В галузі теоретичної криптології в той період великий цикл математичних робіт в інтересах криптології був виконаний у зв'язку з дослідженнями характеристик булевих функцій і відображень кінцевої безлічі. В даний час цей напрямок досліджень одержав значний розвиток і йому присвячена велика кількість відкритої літератури. Для оцінки якості гам та вирішення інших завдань були розроблені нові статистичні критерії.

Говорячи про зв'язки між криптологією та сучасною математикою, варто підкреслити, що ці зв'язки двобічні: у даний час не тільки криптологія використовує готові математичні результати для своїх цілей, але все частіше завдання, що виникають у криптології, стають джерелом розвитку ряду галузей математики.

Значною мірою дослідженнями математиків-криптологів був розвинутий напрямок, що одержав назву ймовірнісної комбінаторики. Вона містить у собі дослідження випадкових розміщень часток в осередках, випадкових підстановок і відображень з обмеженнями, загальних методів перерахування комбінаторних конфігурацій та багато чого іншого. Для вирішення цих завдань використовувався глибокий апарат граничних теорем теорії імовірностей, теорії функцій комплексного змінного, методи виробляючих і характеристичних функцій.

Методи теорії чисел, кінцевих полів і кілець широко використовувалися для вирішення завдань з дискретного логарифмування та завдань з факторизації цілих чисел. До речі, завдання з дискретного логарифмування в кінцевих полях виникло в криптографічній службі наприкінці 1950-х років і першу нетривіальну оцінку складності її рішення одержав О.Гельфонд на початку 1960-х років задовго до відомих відкритих публікацій.

В ті роки у НДІ-2 розширювалися роботи зі створення шифраторів для різних видів зв'язку, наприклад, фототелеграфного або телефонного між рухомими об'єктами. Розвивавалися методологія аналізу та стійкості в залежності від відмовостійкості її компонентів. Велися активні теоретичні й експериментальні роботи з кількісних оцінок стійкості, що вивели співробітників інституту на поняття алгоритмічної складності.

Спроби засекречування багатоканальної роботи апаратури починалися ще наприкінці 1940-х років, а перші мережні моделі надійних систем з'явилися вже на початку 1960-х років. Для цього були досліджені класи псевдоциклічних кодів, добре вивчені структурні елементи шифраторів: різні класи функцій алгебри логіки, лінійні регістри зрушення та нелінійні перетворювачі у вигляді багатоканальних ліній затримки, що генерували детерміновані й випадкові послідовності. Були отримані ефективні оцінки для складності алгоритмів вирішення систем лінійних рівнянь над кінцевим полем. Одержали розвиток статистичні методи аналізу вихідної послідовності шифратора, що дозволяли знижувати стійкість системи засекречування. До

криптоаналізу увійшла методологія визначення довжини експерименту над кінцевим автоматом, що дозволяв розібратися з його структурою – коли автомат переставав бути «чорною шухлядою» для особи, що проводила криптоаналіз.

У той же період інтенсивно проводилася розробка високопродуктивної обчислювальної техніки. Групою інженерів-винахідників і криптографів була розроблена спеціалізована ЕОМ, що мала продуктивність 10^6 операцій у секунду. Відзначимо, що в той час при створенні перших радянських електронних цифрових машин загального призначення «*БЭСМ*» і «*Стрела*» була досягнута швидкодія 10^4 операцій у секунду.

Важливим у розумінні систем засекречування в ті роки стала роль електромагнітних випромінювань від їхніх компонентів, що вдосконалювало не тільки криптоаналіз, але й впливало на самі системи засекречування, приводячи до розробки нових моделей. Системи засекречування передачі інформації усе більше віддалялися від організаційних систем, стаючи автоматизованими. У той час науково-практична робота розробників систем засекречування вже не обходилася без ЕОМ «*Раздан*», що головним чином використовувалися для вирішення завдань криптоаналізу компонентів систем. Створив інститут також і лабораторію, що стала займатися власною елементною базою.

Протягом багатьох років роботами в інституті керував криптограф Дмитро Всеволодович Скороходов. У 1959 році він після закінчення механічно-математичного факультету МДУ був направлений на роботу в НДІ, де проробив 46 років. Скороходов був у числі перших математиків-криптологів, що впроваджували математичні методи при аналізі й синтезі апаратури засекречування. Розроблені ним алгоритми були реалізовані в ряді апаратів і витримали випробування часом. Він був основоположником специфічного напрямку з синтезу алгоритмів для зразків нової техніки системи впізнання («свій-чужий») і Головним криптографом системи.

У 1966 році НДІ-2 був реорганізований та перейменований в НДІ автоматики (далі - НДІА). За всі роки колективом НДІА було створено кілька поколінь технічних засобів і систем шифрованого зв'язку. Це дозволило вирішити різноманітні завдання з засекреченого зв'язку, бойового і державного управління в СРСР. Очолювали інститут у різні роки Наумов (1952-53), Іванов (1954-68), Гаммов (1968-82), Алексеєв (1982-93), Ліхоманов (1993-99).

За час роботи 38 співробітників інституту стали лауреатами Ленінських і Державних премій, більше 400 фахівців нагороджено орденами і медалями. Великий внесок до створення нових зразків техніки внесли конструктори, технологи, працівники дослідного виробництва та інших підрозділів інституту: В.Єрмолаєв,

В.Пумінов, Ю.Іноземцев, А.Савельєв, М.Чекрижов, Г.Орешкін і багато інших. У 1978 році НДІА за досягнення в області науки і техніки був нагороджений орденом Леніна.

Сьогодні федеральне державне унітарне підприємство «НДІА», що працює під егідою Російської агенції з систем керування, знаходиться в числі провідних установ Росії з проблем інформаційної безпеки, розробки та виробництва технічних засобів і систем засекреченого зв'язку, систем автоматизованого керування спеціального призначення.

НДІА - головний виконавець робіт з однієї з найбільш значимих федеральних цільових програм, спрямованої на створення і розвиток інформаційно-телекомунікаційної системи спеціального призначення в інтересах державної влади. Апарати, комплекси засобів шифрованого зв'язку, захищені мережі й інформаційно-телекомунікаційні системи, розроблені і виготовлені співробітниками підприємства, встановлені у Московському Кремлі, Будинку Уряду, міністерствах, штабах і на передових позиціях військових підрозділів. Поруч із Президентом Росії постійно знаходиться один із виробів НДІА – відома усьому світу «ядерна валізка».

5.10. Урядовий зв'язок другої половини XX ст.

У 1951 році штат центрального апарата ВУЗ МДБ нараховував 371 співробітника. Територіальні органи урядового зв'язку становили 18 відділів, 111 відділень і 155 груп штатною чисельністю 2174 особи, за кордоном 5 відділів та 1 відділення урядового зв'язку штатною чисельністю 294 особи. До середини 1951 року на території СРСР і за кордоном функціонували 223 ВЧ станції (199 і 24 відповідно), що обслуговували 2904 абоненти (2465 і 439 відповідно). Також треба відмітити, що період 1950-х років був пов'язаний з «закриттям» каналів урядового зв'язку маскувальною спецапаратурою «*Синица*», яка здійснювала тільки інверсію частотного спектру мовних сигналів.

7 березня 1953 року МДБ увійшло до складу МВС СРСР, в результаті чого 25 квітня у складі МВС наказом № 00159 був утворений Відділ «С». Завданнями відділу, начальником якого став полковник Воронін, було забезпечення державних установ урядовим зв'язком і підрозділів МВС - оперативним радіозв'язком.

13 березня 1954 року був утворений КДБ при РМ СРСР, до складу якого з МВС був переведений Відділ «С», що займався урядовим зв'язком. Цей відділ, який знову очолив Воронін, складався з таких підрозділів:

- Центральний вузол урядового зв'язку (ЦВУЗ);
- Московський вузол урядового зв'язку (МВУЗ);
- 1 відділення (ВЧ станції територіальних органів);
- 2 відділення (ЛАЗ і міжміські АТС);
- 3 відділення (апаратура засекречування);

- 4 відділення (зонові станції урядового зв'язку);
- 5 відділення (АТС, ЕЖУ, кроси, годинофікація);
- 6 відділення (абонентські засоби);
- 7 відділення (радіозв'язок і звукопідсилення);
- 8-і відділення (лінійно-кабельні споруди).

Урядовим зв'язком України з грудня 1945 по березень 1953 року керував полковник В.Цилбов, який очолював Київський ВУЗ, а з травня 1953 по квітень 1971 року – полковник В.Барабанов. Підрозділи урядового зв'язку в обласних центрах України після війни розміщувалися, в основному, в тимчасових приміщеннях. ВЧ станції у Миколаєві, Херсоні, Львові, Ужгороді, Сумах, Харкові та деяких інших містах були змонтовані в будинках обласних управлінь МДБ, відновлених після війни, тому було терміново розгорнуто спорудження будівель, спеціально пристосованих до потреб зв'язківців.

Так, у 1950 році споруджено 2-поверховий будинок ВЧ станції у Полтаві, у 1957 році - у Житомирі, у 1960 році - у Донецьку. Об'єкти урядового зв'язку будувалися і в деяких великих промислових районних центрах: Кривому Розі, Маріуполі, Мелітополі, Краматорську, Керчі, Феодосії, Євпаторії тощо.

У 1954 році в СРСР була впроваджена 4-канальна система засекреченого радіоорухомого зв'язку «Ай-Петрі-Памір» та дальністю радіозв'язку без переприйому в 50-60 кілометрів. У ті ж роки був організований канал ВЧ-зв'язку Москва-Пекін, що було початком утворення урядового міжнародного зв'язку.

У жовтні 1955 року наказом Голови КДБ при РМ Казахської РСР у складі Кзил-Ордінського відділення урядового зв'язку була створена група з 5 осіб для будівництва та подальшої експлуатації ВЧ станції на території ракетного науково-дослідного і випробувального полігону (НДВП-5). Будівництво приміщення для станції урядового зв'язку на космодромі Байконур було завершено у грудні 1955 року, та протягом зими був проведений монтаж устаткування.

9 квітня 1956 року ВЧ станція з позивним «Маяк» була введена в дію. Першим абонентом на станції був включений начальник будівництва космодрому Г.М.Шубніков. Потім телефон ВЧ зв'язку був встановлений у начальника полігону генерал-лейтенанта О.І.Нестеренко. У цей же період були встановлені телефони в будиночку С.П.Корольова, в

кабінеті начальника монтажно-випробувального комплексу та бункері № 1. Вже у липні 1956 року колектив станції брав участь в забезпеченні пуску першої міжконтинентальної балістичної ракети, а у жовтні 1957 року - першого штучного супутника Землі.

Крім того, введення ВЧ станції в експлуатацію дозволило полігону вийти на обласну міжміську телефонну станцію, відкрити телеграфний зв'язок з Москвою. У червні 1957 року група була введена до складу Особливого відділу КДБ СРСР на космодромі. З 1960 року почалося будівництво і введення в експлуатацію ВЧ станцій на пристартових майданчиках: у 1962 році - на 43-му майданчику, у 1964 році - на 95-му майданчику, у 1968 році - на 113-му майданчику.

У 1961 році з організацією станцій на майданчиках космодрому група була перетворена у відділення. В ході функціонування космодрому Байконур станції урядового зв'язку неодноразово реорганізовувалися і переносилися в інші приміщення та будівлі, створювалися та вводилися в експлуатацію станції на інших ключових майданчиках космодрому. Відділення урядового зв'язку входило до складу Особливого відділу КДБ на космодромі до 1996 року.

Значну роль при розгортанні Угорських революційних подій 1956 року відіграли станції ВЧ-зв'язку в містах Ужгороді та Мукачеві Закарпатської області, яка була приєднана до УРСР у 1946 році. Зв'язком користувалися як місцеві органи, так і політичні діячі, розвідники, дипломати, військове командування.

На базі ВЧ-станції м.Мукачева діяв штаб управління мережею польового урядового зв'язку, розгорнутою 1-м батальоном урядового зв'язку КДБ, який був сформований на базі 311-го окремого полку урядового зв'язку КДБ, дислокованого у м.Винники Львівської області. Він забезпечив урядовим зв'язком війська на території Угорщини, а також виконував завдання щодо спорудження та охорони постійних ліній урядового зв'язку. ВЧ станції як в м.Ужгороді, так і в м.Мукачеві разом з традиційними функціями розпочали виконували роль пункту транзиту каналів, які з'єднували Москву з Будапештом, Віднем, Прагою.

У країнах соціалістичного табору також були організовані свої мережі

урядового зв'язку, для чого їм було передано станції й обладнання урядового зв'язку та апаратура засекречування, шифри для якої виготовлялися в СРСР і направлялися до місць призначення дипломатичною поштою.

Поступово зростала технічна оснащеність станцій ВЧ зв'язку. Так, канали утворювалися апаратурою ущільнення типу «*ОКС*» та «*В-3*», а також обладнувалися апаратурою виклику. Абонентські лінії з легкого польового кабелю замінювалися на багатопарні кабелі в металевій (броньованій) оболонці, які за відсутністю телефонної кабельної каналізації прокладалися безпосередньо в грунті.

23 червня 1959 року була випущена серія наказів КДБ відносно реорганізації підрозділів Центрального апарата, згідно з якими Відділ «С» був об'єднаний з Відділом військ урядового зв'язку в єдиний ВУЗ КДБ, а територіальні відділення «С» перетворені у відділення урядового зв'язку. Начальником ВУЗ був призначений генерал-майор інженерно-технічної служби Воронін.

У 1960-і роки в системі урядового зв'язку йшов інтенсивний процес підвищення рівня її технічної оснащеності і безпеки інформації. Велика увага приділялася автоматизації зв'язку на базі як вітчизняних, так і зарубіжних АТС. Основним напрямом підвищення безпеці інформації в цей період став переведення мережі з апаратури маскуючої дії на апаратуру засекречування тимчасової стійкості, а на окремих напрямах, що мали найбільш важливе значення, на апаратуру гарантованої стійкості. Це був дуже важливий етап розвитку секретної телефонії в державі – етап реального засекречування телефонних розмов.

В цей час для потреб системи урядового зв'язку використовувалися більш якісні кабельні канали, обладнані апаратурою ущільнення К-24, які «закривалися» апаратурою засекречування «Алмаз» (+100). На ВЧ-станціях монтувалася нова апаратура тонального набору та виклику типу «СТН». На абонентських кабелях та кабелях станційного монтажу урядового зв'язку впроваджувалися заходи з некриптографічного захисту інформації. Для забезпечення надійності електроживлення апаратури на ВЧ-станціях монтувалия дизель-генератори та акумуляторні батареї. Додатково встановлювалися абонентські установки на квартирах регіональних керівників.

У той час зі станції урядового зв'язку м.Києва до м.Ужгорода була передана та змонтована частина автоматичної міжміської декадно-крокової телефонної станції англійського виробництва «*Strowger*» на 10 каналів та 15 абонентів. Мережа урядового зв'язку була переведена в автоматичний режим роботи. Титм часом розширювалася та вдосконалювалася абонентська мережа. Прокладалися в телефонній кабельній каналізації більш сучасні кабелі в свинцевих оболонках, які ставилися під надлишковий повітряний тиск. На мережі вдосконалювалася система некриптографічного захисту інформації, впроваджувалися заходи щодо виключення можливості несанкціонованого доступу до ліній урядового зв'язку.

З урахуванням досвіду карибської кризи 1962 року, яка ледве не призвела до ядерної катастрофи, 31 серпня 1963 року була введена в дію «Гаряча лінія» прямого урядового телеграфного зв'язку Москва-Вашингтон. 20 червня сторони уклали Меморандум про взаєморозуміння, який передбачав організацію зв'язку за маршрутом Вашингтон - Лондон, - Копенгаген - Стокгольм - Хельсінкі - Москва. Для реалізації пунктів, встановлених в угоді, в дуже стислі терміни через Атлантику був протягнутий спеціальний кабель з використанням найдосконаліших ізолюючих матеріалів. Цьому аспекту приділили особливу увагу, тому як у той час під Атлантикою вже лежав кабель (ще з 1858 року!), але використовувати його було не можна - морська сіль роз'їла його ізоляцію.

Як резервний канал «Гарячої лінії» був передбачений двосторонній радіообмін Вашингтон - Москва з ретранслятором у Марокко. СРСР і США обмінялися устаткуванням: телетайпи американського виробництва були встановлені в Кремлі, а апарати восточногерманської збірки - у Вашингтоні. Цікаво, що радянська сторона приймала повідомлення безпосередньо у Кремлі, а американці встановили апарати в Пентагоні, куди повинен був дзвонити Президент. Не дивлячись на всю очевидну необхідність таких заходів, приводу використовувати цей канал міжурядового зв'язку за прямим призначенням у Хрущова та Кенеді так і не з'явилося.

Під час запуску систему лише випробували, обмінявшись парою на перший погляд позбавлених сенсу фраз. З Америки прийшло повідомлення, що містило всі букви англійського алфавіту та цифри: «Швидка коричнева лисиця перестрибнула через спину ледачого собаки 1234567890» (англ. *The quick brown fox jumps over the lazy dog 1234567890*). Наші фахівці на це дали симетричну відповідь. Проте надалі, ймовірно, саме «гаряча лінія» запобігла можливим небезпечним ускладненням радянсько-американських відносин і навіть військовим зіткненням. Пізніше подібні лінії були організовані зі столицями інших держав. Важливість таких «гарячих ліній» була неодноразово підтверджена, вони стали по суті інструментом оперативного вирішення гострих конфліктних ситуацій світового масштабу.

У 1963 році була розроблена та введена в дію система радіозв'язку на Червоній площі «Север» для зв'язку оперативного складу КДБ у ході заходів на Червоній площі та в інших місцях. В 1967 році вступила в дію дуплексна радіорухома

ультракороткохвильова (далі - УКХ) система незасекреченого урядового зв'язку «*Роса*», попередниця сучасного мобільного зв'язку. Вже через декілька років в автомобілях вищих осіб держави була вже встановлена апаратура засекречування тимчасової стійкості.

Чехословацькі події у 1968 році прискорили технічний розвиток урядового зв'язку в Закарпатській області. Апаратура засекречування «Алмаз» (+100) була замінена на апаратуру «Корал» (+200). В той бурхливий час у м.Ужгороді працювали посланці з м.Москви, дипломати, «кандидати в керівники» Компартії та Уряду соціалістичної Чехословаччини. На базі Мукачівської станції був розгорнутий штаб з організації зв'язку силами військ урядового зв'язку.

На кінець 1968 року в мережу автоматичного телефонного урядового зв'язку було включено 184 населені пункти, а з іншими об'єктами, обладнаними ВЧ-зв'язком, зв'язок був організований за замовленою системою, тобто через телефоністку.

13 березня 1969 року ВУЗ був реорганізований в Управління урядового зв'язку (далі – УУЗ), яке у різні періоди часу очолювали:

1. Воронін Петро Миколайович (1959 – жовтень 1973).
2. Толмачов Юрій Олександрович (жовтень 1973 – грудень 1985).
3. Бєда Анатолій Григорович (грудень 1985 – серпень 1991).

У 1969 році на основі служб Московського вузла урядового зв'язку ВУЗ був сформований 3-й відділ ВУЗ (Московський відділ урядового міського зв'язку), на який було покладено завдання організації й обслуговування стаціонарних й абонентсько-кабельних засобів міського урядового й службового зв'язку, систем звукопідсилення, перекладу мов, телебачення та годинофікації на урядових і спеціальних об'єктах у Москві.

Наприкінці 1960-х років керівництвом КДБ було прийнято рішення щодо розгортання системи засекреченого оперативного зв'язку КДБ. Справа в тому, що ВЧ-апарати були тільки у Голів КДБ республік та начальників обласних управлінь. Районні відділи та відділення користувалися місцевим відкритим зв'язком, що суттєво знижувало оперативність управління підрозділами і не гарантувало конфіденційності інформації.

За рішенням Колегії КДБ Управлінню урядового зв'язку було доручено організацію і будівництво системи оперативного зв'язку КДБ СРСР, КДБ республік, обласних управлінь із будівництвом каналів зв'язку у кожному районному відділі та відділенні. Для керівництва системою та експлуатації засобів зв'язку у Москві було створено Відділ оперативного зв'язку, а на місцях – відповідно відділення та групи. У цей час з мережі урядового зв'язку знімалася морально застаріла апаратура засекречування, у якої ще залишався ресурс. Саме її спочатку і встановили на каналах оперативного зв'язку.

Для забезпечення оперативного зв'язку КДБ на ВЧ-станціях була встановлена маскувальна спецапаратура «Байкал» (+30). В районних відділах обласних Управлінь КДБ особовим складом ВЧ-станцій монтувалися та вводилися в дію пункти засекреченого оперативного зв'язку з використанням маскувальної спецапаратури «Терек» (+30). Поступово протягом декількох років, оперативним зв'язком було забезпечено всі підрозділи КДБ.

Наприкінці 1970-х років маскувальна спецапаратура була замінена апаратурою засекречування тимчасової стійкості Т-217 «Ельбрус» і Т-219 «Яхта», яка була передана з Міністерства оборони, де використовувалась на рухомих польових вузлах засекреченого зв'язку. Апаратура Т-217 входила в систему засекречування оперативної ланки військового управління, а Т-219 - тактичної ланки. Апаратура складалася з 2-х основних елементів: пульта управління і блоку шифрування/дешифрування, в якому знаходилися

ПУ-1 – пульт управления 1

2 ключових комутатори (шифрування та дешифрування).

Апаратура являла собою аналоговий скремблер, принцип роботи якого полягав в тому, що при мовному обміні в режимі «*FSK*» передавалася синхронізуюча послідовність, розташована точно по середині спектру, а сам мовний спектр розбивався на дві частини (півканали), вище і нижче за цю послідовність. Все це розбивалося на нерівні тимчасові відрізки, в межах яких переставлялися місцями та інвертувалися ці два мовних півканалів. У 1980-х роках відомчі системи засекреченого зв'язку на базі тієї ж апаратури створювались у багатьох міністерствах і відомствах військово-промислового комплексу СРСР.

У 1970-і роки в розвитку та озброєнні підрозділів урядового зв'язку був здійснений якісний «стрибок». Для потреб системи урядового зв'язку використовувалися більш якісні кабельні канали, обладнані апаратурою ущільнення «*К-60*». Розпочалося впровадження в експлуатацію на мережах урядового зв'язку апаратури засекречування гарантованої стійкості, яка виготовлялась Калузьким заводом. Були створені нові комплекси апаратури для міського та міжміського зв'язку, авіаційні та залізничні вузли урядового зв'язку, що дозволяли забезпечувати керівництво країни якісним безперервним закритим зв'язком з будь-якого місця, у тому числі при пересуванні на транспортних засобах і перебуванні за межами країни.

У той же час на озброєння підрозділів урядового зв'язку надійшла станція КХ радіозв'язку Р-140Д (радіостанції Р-155П, Р-311, Р-105М) з винесеним пунктом її керування, яка виконувала свої функції до кінця минулого століття. Щорічно влітку проводилися навчальні польові сеанси КХ засекреченого радіозв'язку обласних підрозділів з Москвою з додатковим залученням військовозобов'язаного приписного складу.

На урядових мережах телефонного зв'язку був розпочатий перехід на вико-

ристання екранованих телефонних апаратів, які були розроблені за спеціальними вимогами та виготовлялися Пермським і Ризьким заводами. Називалися вони скорочено «*ТАЭ*» – телефонний апарат екранований, а потім «*СТА*» – спеціальний телефонний апарат. На озброєння станцій урядового зв'язку почали надходити нові автоматичні міжміські телефонні станції координатного типу (АМТСК), які виготовлялись на Ленінградському заводі «*Красная Заря*». У подальшому поступово з'явились квазіелектронні та електронні станції («Квант»).

У 1970-1972 роках за ініціативою керівництва УУЗ група вчених розробила концептуальну програму розвитку та вдосконалення урядового зв'язку на найближчі 10-15 років, затверджену у 1972 році ухвалою ЦК КПРС і Ради міністрів СРСР. Програма передбачала залучення провідних науково-дослідних і виробничих організацій країни до створення передової технічної бази системи управління СРСР і Збройними силами. Її виконання вирішило проблему забезпечення гарантованого захисту інформації в будь-яких умовах оперативної обстановки, чи то автомобіль, літак, бойові або захищені пункти управління. В ході реалізації програми були створені новітні системи фіксованого та супутникового рухомого радіозв'язку, апаратура гарантованого захисту секретної інформації.

У 1972 році була завершена розробка концептуальної системи розвитку урядового зв'язку «Кавказ», що включала в себе 12 взаємопов'язаних підсистем. Ця система була прийнята в експлуатацію державною комісією під головуванням академіка В.Котельникова. Реалізуючи цю систему, за допомогою промисловості, провідних вчених і колективів наукових інститутів удалося створити нові системи засекреченого зв'язку: міський засекречений зв'язок, у тому числі і міжміський

зв'язок з інопредставництвами та зв'язок із рухомими об'єктами.

Вже у 1973 році були створені мобільні вузли зв'язку для забезпечення урядовим зв'язком перших осіб держави при їхньому виїзді в іноземні держави. Успішна робота цієї системи була продемонстрована у тому ж році при візиті генерального секретаря ЦК КПРС Л.Брежнєва до США. У період з листопада 1973 року по лютий 1974 року для забезпечення зв'язку під час візиту Л.Брежнєва до США в складних умовах зимового Атлантичного океану, під час постійних штормів силою 9-10 балів, з борту теплохода «Космонавт Комаров» був налагоджений стійкий зв'язок із використанням систем «Карпати» з літаками, що перевозили урядову делегацію.

Територіальні підрозділи урядового зв'язку України як в організаційному і технічному плані, так і у плані професійної підготовки були одними з кращих у СРСР. У 1973 році у Києві, а потім і у всіх обласних центрах України була введена в експлуатацію система засекреченого радіорухомого зв'язку «Роса». Центральні станції системи були змонтовані у великих містах, а лінійні – уздовж головних автомагістралей України, чим був забезпечений надійний захищений телефонний зв'язок з рухомими об'єктами (автомобілями) з можливістю виходу на стаціонарну мережу.

З 1976 року система «Роса» була обладнана апаратурою засекречування гарантованої стійкості, що виключило можливість розшифрування радіотелефонних переговорів абонентів. Абонентам урядового зв'язку була надана можливість користуватися захищеним зв'язком не тільки в місцях постійного перебування, але й при пересуванні на транспортних засобах і місцях тимчасового перебування. Усього в експлуатацію було введено 28 радіоцентрів і близько 100 лінійних станцій системи «Роса».

У 1977 році всі підрозділи були забезпечені «Основними спеціальними вимогами з розміщення та монтажу устаткування стаціонарних станцій телефонного засекреченого зв'язку» (ОСТ-ТЛФ), виконання яких підвищило стан безпеки урядового зв'язку. 13 червня 1979 року спільною Постановою ЦК КПРС і РМ СРСР №

Р-142 на ГАЗ-66

558-183 було затверджене «Положення про урядовий зв'язок», відповідно до якого урядовий зв'язок містив у собі такі види зв'язку, як міжнародний, міжміський, міський, із рухомими об'єктами та польовий.

У той же період з військ урядового зв'язку на озброєння регіональних станцій для організації у разі надзвичайних ситуацій оперативного радіозв'язку поступила командно-штабна машина (далі - КШМ) «Р-125» , обладнана засобами КХ і УКХ зв'язку (радіостанції Р-105М, Р-111, Р-123, Р-130). У складі оперативно-слідчої групи (далі - ОСГ) обласного УКДБ КШМ забезпечувала відкритий зв'язок між усіма членами ОСГ та засекречений зв'язок з оперативним черговим УКДБ із застосуванням Т-219 «Яхта». У 1988 році КШМ Р-125 була замінена на більш сучасну Р-142.

У 1974 році ВУЗ КДБ при РМ УРСР був реорганізований в УУЗ КДБ, що у різні періоди часу очолювали:

1. Тарієлашвілі Тингіз Семенович (1971 – 1988).

2. Напрієнко Борис Миколайович (1988 – 1991).

ПРОПУСК
№ 003255
ВСЮДУ
НА ПРАВО ВЪЕЗДА
В ЗАКРЫТУЮ ЗОНУ

Матеріальна база підрозділів і рівень підготовки фахівців дозволяли на базі УУЗ КДБ УРСР неодноразово проводити державні випробування нової техніки та цілих систем, які пізніше були впроваджені в системі урядового зв'язку. Так, в 1984 році в Києві були проведені державні випробування системи урядового зв'язку «Кавказ» з використанням радянських ЕОМ.

Назву «Кавказ» отримала система спеціального радіотелефонного рухомого урядового зв'язку, яка призначалася для забезпечення захищеним зв'язком керівників силових структур, міністерств і відомств, керівників всіх гілок влади, включаючи вищих керівників держави. У складі системи планувалося не менше 7 підсистем різного призначення, що мали індекси від «Кавказ-1» до «Кавказ-7» та таке призначення:

- «Кавказ-1» - стаціонарна мережа зв'язку із службою спеціального комутатора, що забезпечує автоматичний міжміський телефонний і документальний зв'язок з можливістю виходу абонентів на польову мережу, мережі зв'язку з рухомими об'єктами та урядову міську АТС московської зони.
- «Кавказ-2» - польова мережа зв'язку, реалізована на мобільних засобах, і призначена для організації телефонного і документального зв'язку в ланці «Ставка-фронт-армія».
- «Кавказ-3» - мережі КХ і УКХ радіозв'язку і супутникового зв'язку з великими (літак, поїзд, корабель) і малими (автомобіль, вертоліт, катер) рухомими об'єктами.

🗝 «Кавказ-4» - мережа УКХ радіозв'язку з малими рухомими об'єктами в Москві і Московській зоні.

🗝 «Кавказ-5» - мережа автоматичного міського телефонного зв'язку в Московській зоні.

🗝 «Кавказ-6» - вузол зв'язку, що перевозиться, для забезпечення закритим і відкритим урядовим зв'язком вищих керівників при їх перебуванні в зарубіжних країнах, з комплексним використанням каналів проводового, КХ і супутникового зв'язку.

🗝 «Кавказ-7» - захищений канал телекодового постійно діючого зв'язку з метою негайного доведення інформації про ядерний напад до спецабонентів (керівника держави, міністра оборони, начальника Генштабу) незалежно від їх місцезнаходження та трансляції в систему централізованого бойового управління ухваленого рішення (санкції) на організацію у відповідь дій (застосування ракетно-ядерної зброї).

Однак у зв'язку зі швидким моральним старінням матеріальної бази цих електронних комплексів та «застійних» тенденцій того часу у розвитку СРСР система «Кавказ» так і не була впроваджена в експлуатацію на території країни.

Тоді ж в Україні було споруджено шість наземних пунктів РРЛ зв'язку системи «Татри» й «Карпати» з використанням апаратури Р-409 і П-303 для підтримки постійного зв'язку з урядовими літаками, які використовували апаратуру гарантованої стійкості «Лагуна». А з метою підтримки постійного зв'язку з урядовими потягами у гірських карпатських тунелях функціонувала система тунельного зв'язку системи «Бескід».

У 1980-х роках на станціях урядового зв'язку апаратура засекречування тимчасової стійкості замінювалася на апаратуру гарантованої стійкості «Дельфін» (+1000) і М-461 «Рубін». Крім того, стаціонарні підрозділи отримали рухомі вузли урядового зв'язку Д-13КМ «Дон» на базі ГАЗ-66, оснащені апаратурою засекречування гарантованої стійкості «Дельфін», що значно збільшило можливості щодо забезпечення урядовим зв'язком з місць надзвичайних подій та непідготовлених у відношенні зв'язку районів.

Історія урядового зв'язку була на-

сичена багатьма подіями, під час яких був накопичений досвід роботи в «гарячих точках» (Афганістан, Північний Кавказ), в надзвичайних ситуаціях техногенних катастроф, стихійних лих. Київськими фахівцями для забезпечення закритого телефонного зв'язку з непідготовлених районів при техногенних аваріях та інших надзвичайних ситуаціях був змонтований Рухомий радіотелефонний центр (далі – РРТЦ), що перевершував за своїми можливостями вузли зв'язку промислового виробництва.

Завдяки наявності РРТЦ під час аварії на 4-му енергоблоці Чорнобильської АЕС зв'язківцями УУЗ уже ранком 26 квітня 1986 року в інтересах державної комісії був організований засекречений телефонний зв'язок із м. Прип'ять на Київ і Москву. Тільки протягом першої доби після аварії екіпаж РРТЦ забезпечив більше 300 переговорів членів комісії. Усього в 1986-1987 роках у забезпеченні урядового зв'язку при ліквідації наслідків аварії на Чорнобильської АЕС взяли участь більше 200 співробітників Управління та військ урядового зв'язку КДБ УРСР.

У грудні 1988 року при сильному землетрусі у Вірменії урядовий зв'язок був відновлений з доставленням техніки та особового складу менше ніж за 13 годин. Тоді була підтверджена й висока оперативність інформування глави держави по урядовому зв'язку незалежно від місця його перебування: інформацію про землетрус Президент СРСР отримав негайно під час візиту в США, коли знаходився на паромній переправі біля Нью-Йорка.

Крім того, 1980-і роки були відзначені активними роботами з будівництва нових станцій урядового зв'язку в Україні у містах: Хмельницький, Рівне, Вінниця, Житомир, Ужгород, Львів, Тернопіль, Сімферополь, Донецьк, Одеса, Миколаїв, Севастополь, Чернігів, Суми, Чернівці, Кіровоград і Херсон.

26 червня 1990 року у складі урядового зв'язку була створена система зв'язку для Президента СРСР.

Як відомо, 19 серпня 1991 року була здійснена невдала спроба «державного перевороту» в СРСР. Ще 15-17 серпня за особистою вказівкою Голови КДБ Крючкова начальник УУЗ КДБ генерал-лейтенант Бєда організував подачу у 12-ий відділ КДБ ліній урядового зв'язку абонентів – керівників СРСР і Росії. 18 серпня о 16.30 заступник начальника УУЗ генерал-майор Глущенко віддав розпорядження начальнику 21-го відділу УУЗ Паруснікову вимкнути всі види зв'язку на дачі

Президента СРСР у Форосі (об'єкт «Зоря»). Одночасно з 18.00 18 серпня по 09.00 22 серпня Службою охорони КДБ був відключений зв'язок з підрозділами прикордонних військ, що несли охорону зовнішнього периметра дачі Президента СРСР.

Після завершення цих подій начальник УУЗ КДБ генерал-лейтенант Бєда був знятий з посади, а система урядового зв'язку реорганізована. Після цього СРСР «розвалився» на окремі незалежні держави, які вже самостійно стали створювати свої криптологічні служби та підрозділи спеціального зв'язку.

Впродовж усієї історії СРСР органи державної безпеки та внутрішніх справ під впливом зовнішніх обставин та зростанням обсягу завдань постійно реорганізовувалися, змінювали свою структуру та назву. Відповідно змінювалася структура та назва підрозділу урядового зв'язку:

Дата утв.	*Найменування підрозділу*
01.12.1929	4 відділення Оперативного відділу (ОВ) Секретно-оперативного управління (СОУ) ОДПУ при РНК СРСР
01.06.1931	5 відділення ОВ ОДПУ при РНК СРСР
10.07.1934	5 відділення ОВ ГУДБ НКВС СРСР
07.06.1936	13 відділення ОВ ГУДБ НКВС СРСР
25.12.1936	3 відділення 2 (оперативного) відділу ГУДБ НКВС СРСР
07.08.1937	8 відділення 12 відділу (оперативної техніки - ОТ) ГУДБ НКВС СРСР
09.06.1938	3 відділення 2 спецвідділу (ОТ) НКВС СРСР
01.05.1939	відділення урядового «ВЧ» зв'язку 2 спецвідділу (ОТ) НКВС СРСР
26.02.1941	відділення урядового «ВЧ» зв'язку 4 відділу (ОТ) НКДБ СРСР
29.04.1941	відділення урядового «ВЧ» зв'язку ОТБ НКВС СРСР
07.08.1941	8 відділення 4 спецвідділу (ОТБ і ВЧ-зв'язок) НКВС СРСР
02.10.1941	Відділ урядового «ВЧ» зв'язку НКВС СРСР
12.04.1946	Відділ урядового «ВЧ» зв'язку МВС СРСР
26.08.1947	Відділ урядового «ВЧ» зв'язку МДБ СРСР
14.03.1953	Відділ «С» МВС СРСР
08.04.1954	Відділ «С» КДБ при РМ СРСР
27.09.1954	Відділ урядового зв'язку КДБ при РМ СРСР
13.03.1969	Управління урядового зв'язку КДБ при РМ СРСР (КДБ СРСР з 05.07.1978)

Частина 6.

Історія стеганографії

Розповівши про криптографію, не можна не розказати ще про один вид таємного письма, яке називається стеганографія та походить від грецьких слів «*steganos*» – «покритий» й «*graphein*» – «писати».

Основна відмінність стеганографії від криптографії полягає в тому, щоб приховати не тільки саму інформацію, але ще й факт її наявності, замаскувавши таємні відомості в яку-небудь повсякденну нетаємну інформацію, факт передачі якої не викликає ніяких підозр (наприклад, звичайний лист дружині). Вона не заміняє криптографію, а доповнює її ще одним рівнем безпеки.

Уперше про стеганографію було згадано ще в 5-му столітті до н.е. у літописі Геродота. У ньому він розповідав про збройні сутички між Грецією та Персією у 5-му столітті до н.е., які розглядав як протиборство між волею й рабством, між незалежними грецькими державами та тиранічною Персією. Згідно з Геродотом саме мистецтво тайнопису врятувало Грецію від поневолення Ксерксом, «царем царів», деспотичним правителем Персії.

Відносини між Грецією й Персією значно загострилися незабаром після того, як Ксеркс почав будівництво міста Персеполь, нової столиці свого царства. Дани-

на й дарунки надходили із всіх кінців імперії й із сусідніх держав, за винятком Афін і Спарти. Вирішивши помститися за таку зухвалість, Ксеркс розпочав мобілізацію війська, заявивши: «Ми так розширимо перську імперію, щоб її кордоном служило небо, щоб сонце не змогло б побачити ні клаптика землі поза наших кордонів». Наступні 5 років він витратив на те, щоб таємно зібрати найбільшу в історії армію, і в 480 році до н.е. вже був готовий завдати раптового удару.

Однак нарощування військової сили Персії бачив Демарат, грек, що був вигнаний з батьківщини та жив у перському місті Сузи. Незважаючи на вигнання, він все ж таки залишався лояльним до Греції й тому вирішив попередити спартанців про план вторгнення Ксеркса. Проблема полягала лише в тому, як передати повідомлення, щоб його не змогли перехопити перські солдати. Геродот писав так:

«Оскільки небезпека виявлення послання була дуже велика, то залишався тільки єдино можливий спосіб, яким Демарат міг успішно передати своє послання. Він зіскріб віск із двох складених дощечок для листа, написав прямо на дереві, що збирається робити Ксеркс, а потім знову покрив воском дощечки з повідомленням. За зовнішнім виглядом дощечки здавалися чистими, без яких-небудь записів, тому вони не викликали підозри в перських солдатів. Коли гонець із посланням добрався до місця призначення, ніхто не міг і припустити про наявність послання, поки, як я думаю, дочка Клеомена [царя Лаконіки у 520-491 р.р. до н.е.], Горго, що була дружиною Леоніда 1 [царя Лаконіки у 491-480 р.р. до н.е.], не здогадалася й не сказала іншим, що якщо вони зчистять віск, то знайдуть записане під воском на дощечках послання. Так і зробили; після того як був зчищений віск, під ним виявилося послання, яке прочитали, а потім передали в інші грецькі міста».

Завдяки цьому попередженню беззахисні на той момент греки стали самі озброюватися. Доходи від належних державі срібних рудників, які до цього розподілялися серед громадян, були спрямовані на будівництво 200 військових кораблів.

В результаті Ксеркс втратив елемент раптовості, і 23 вересня 480 року до н.е., коли перський флот досяг Саламинської протоки неподалік від Афін, греки вже були напоготові. Хоча Ксеркс думав, що він піймав грецький флот у пастку, але насправді греки свідомо заманювали перські кораблі в протоку. Греки знали, що їхні невеликі судна, яких до того ж було в декілька разів менше, ніж у персів, у відкритому морі будуть знищені, але усередині протоки, завдяки маневреності, вони зможуть перемогти персів. Оскільки вітер змінив напрямок, то перський флот виявився усередині протоки й змушений був прийняти бій на грецьких умовах. Корабель перської цариці Артемісії був оточений з трьох боків, так що вона змогла вирватися назад у море, тільки протаранивши один зі своїх кораблів. Виникла паніка, велика кількість перських судів зіштовхувалася один з одним, і греки почали стрімку атаку. Протягом одного дня величезні сили персів були знищені.

Геродот також згадав ще про один випадок, коли приховання послання вияви-

лося достатнім, щоб безперешкодно його передати. Він розповів історію про Гістія, який хотів підштовхнути Арістагора з Мілета до повстання проти перського царя Дарія. Щоб послання не виявили вороги, Гістій поголив голову свого вісника, написав на шкірі текст послання, а потім почекав, поки волосся не виросло знову. Що ж, неспішний у той час хід історії дозволяв користуватися такими способами. Посланець, у якого не було нічого явно його компрометуючого, міг подорожувати, не турбуючись. Після прибуття на місце він поголив голову та «вручив» послання адресату.

Помітним внеском у стеганографію у 357 році до н.е. був запропонований «книжковий шифр» давньогрецького полководця Енея Тактики, описаний *ним* у «Трактаті про перенесення облоги» (лат. *Taktikon upomuhma peri tou pws crh poliorkoumenous antecein*). У розділі «Про таємні листи» Еней запропонував проколювати малопомітні дірки в книзі або в іншому документі над буквами (або під ними) таємного повідомлення. Цікаво відзначити, що в Першій світовій війні германські шпигуни використали аналогічний спосіб приховування секретних листів, замінивши дірки на крапки, що наносилися симпатичним чорнилом на букви газетного тексту.

Древні китайці використовували такий вид стеганографії: писали повідомлення на тонкій шовковій тканині, що потім згорталася у крихітну кульку та покривалася воском. Посланець ковтав цю воскову кульку та у своєму шлунку доставляв послання до визначеного місця, де природним шляхом воно вилучалось і передавалось адресату.

Те, що стеганографія змогла проіснувати настільки тривалий час, показує, що вона, безсумнівно, забезпечує певну таємність, але їй властивий один принциповий недолік. Якщо кур'єр буде обшуканий й у нього виявлять повідомлення, то відразу ж стане відомий і його зміст. Перехоплення повідомлення миттєво ставить під загрозу всю безпеку. Пильна варта може ретельно обшукувати всіх, хто перетинає кордон, зчищаючи з дощечок весь віск, нагріваючи чисті аркуші паперу, очищаючи зварені яйця від шкарлупи, голячи людям голови тощо, так що випадки виявлення повідомлення будуть неминучі.

STEGANOGRAPHIA
ARS PER OC.
CVLTAM SCRIPTV
RAM ANIMI SVI VO
LVNTATEM ABSENTIBVS
DARMSTADII

У 1499 році Йоган Тритемій (Трисемус), абат бенедиктинського монастиря Святого Мартіна в Шпанхеймі (Німеччина), приступив до написання серії томів під загальною назвою «Стеганографія» (лат. *Steganographia*). У перших розділах він писав про способи заміни голосна-приголо-

сна, про криптографічне використання «пустих» знаків і слів, що не мають сенсу. Але із-за єресі, що на думку христянських священиків містилася у творі, він більше століття залишався у вигляді рукопису. А після того, як у 1606 році книга все ж була надрукована, вона одразу була внесена до католицького Індексу заборонених книг.

MYSTERIUM
ARTIS
STEGANO-
GRAPHICÆ
NOVISSIMUM,
IN
Gratiam Collegii Curiosorum,
Modum
Omnes Epistolas, aliaque
Scripta incognita, Characteri-
bus furtivis exarata in omnibus Lin-
guis, præsertim Latinâ, Germanicâ, Gal-
licâ, Italicâ expediat solvendi,
pandens,
editum in lucem
ex Musæo
M. LUDOVICI HENRICI
HILLERI, Diaconi Esslin-
gensis.
ULMÆ,
Sumtibus Georgii Wilhelmi [illegible]
Typis Hæred. Christiani Balth. [illegible]

У 1682 році Генріх Хіллер написав книгу «Якнайглибша таємниця стеганографічних мистецтв» (лат. *Mysterium artis steganographicae novissimum*), у якій мав намір навчити читача не тільки тайнопису, але й розпізнавати такі мови, як латинська, німецька, італійська і французька, просто визначаючи статистичну частотність букв і дифтонгів (поєднання двох простих голосних).

У 1900 році у Женеві в друкарні «Союзу російських соціал-демократів» була видана брошура Володимира Акімова «Про шифри», де у другій главі «Як сховати шифр» були описані різні стеганографічні методи, якими користувалися революціонери-підпільники.

6.1. Невидимі чорнила

У деяких способах стеганографії використовували фізичні особливості носіїв інформації. Так, симпатичні, тобто невидимі, чорнила зникали незабаром після написання ними тексту або були невидимі з самого початку. Вони являли собою хімічні розчини, що ставали безбарвними після висихання, але видимими після обробки іншим хімікалієм (реагентом). Наприклад, якщо писати залізним купоросом, то текст є невидимим, поки його не оброблять розчином ціанату калію, після чого утвориться берлінська лазур – речовина, що має дуже гарний колір. Мистецтво виготовлення якісного чорнила для тайнопису полягає в тому, щоб знайти речовину, яка б реагувала з мінімальною кількістю хімікалій (найкраще лише з одним).

Невидиме чорнило було двох видів: органічні рідини та «симпатичні» хімікалії. Перші, до яких відносяться сеча, молоко, оцет і фруктові соки, стають зримими в результаті незначного нагрівання. Другі – в результаті обробки паперу спеціальним хімічним реактивом або освітлення променями певної частини спектра, зазвичай, ультрафіолетом.

Цей спосіб стеганографії одержав свій початок з незапам'ятних часів. Ще китайський імператор Цин Шихуанді (249-206 р.р. до н.е.) використовував для своїх таємних листів густий рисовий відвар (утримуючий крохмаль), що після висихання написаних ієрогліфів не залишав ніяких видимих слідів. Якщо такий лист злегка змочували слаб-

ким спиртовим розчином йоду (або відваром водоростей), то з'являлися сині написи.

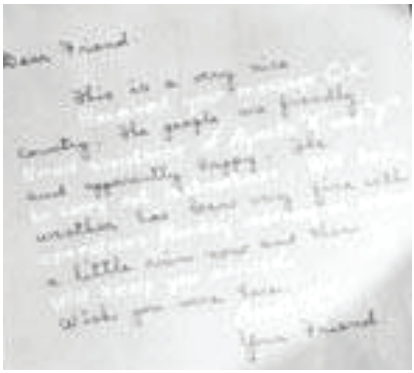
Ще в 1-му столітті н.е. Пліній-старший показав, як молочний сік деяких рослин використовується як такі чорнила. Після висихання напис, зроблений цим чорнилом, був не видний, але при несильному нагріванні ставав коричневий. Багато органічних рідин поводяться схожим чином: при нагріванні, через те, що в них утримується велика кількість вуглецю, вони темніють. І це відомо нинішнім шпигунам, які у випадку закінчення симпатичного чорнила використовують для цієї мети власну сечу.

Римський вчений Пліній Старший у своїй «Природній історії», написаній ним у 1-му столітті до н.е., розповідав, яким чином можна використовувати сік рослин із родини молочаїв як симпатичні чорнила. Римський поет Овідій, що жив також у той час, у книзі «Мистецтво кохання» рекомендував закоханим спосіб тайнопису молоком, що виявлявся посипанням паперу сажею. Після здування сажі на папері залишалися її дрібні частки, що прилипли до місць, де були букви, написані молоком.

Декілька видів симпатичного чорнила описав арабський криптолог Калкашанді. У XVI столітті італійський криптолог Джованні Порта присвятив питанню про невидиме листування окрему книгу «Магія природна». Він описав, як сховати послання усередині звареного вкруту яйця, спочатку виготовивши чорнило з однієї унції (28 г) квасців і пінти (0,5 л) оцту, а потім написавши послання цим чорнилом на шкарлупі. Розчин проникав крізь пори шкарлупи й залишав повідомлення на поверхні щільного яєчного білка, яке можна було прочитати, тільки розбивши яйце й очистивши шкарлупу.

Назва «симпатичне чорнило» була введена наприкінці XVII століття хіміком Лемортом з Лейдена. Він дав це ім'я водному розчину «свинцевого цукру». Так називалася оцтовосвинцева сіль (оцтовокислий свинець $Pb(CH_3COO)_2$), що у ті часи в значних кількостях вживалася у фарбуванні та ситцедрукуванні. Чорнило виявлялося нагріванням або ж обробкою сірководнем.

Російський цар Петро I займався не тільки складанням шифрів, але й приділяв належну увагу застосуванню симпатичного чорнила. Так, у квітні 1714 року цар написав послу Росії у Швеції І.Трубецькому: *«Посылаю к вам три скляницы для тайнова писма: чем перво писат под А. которая войдет в бумагу и ничево знат не будет; потом под В. – теми чернилы потом писат, что хочешь явъново; а третье под С. – то, когда от нас получишь писма, оною помазат, то чернилы сойдут, а первое выступит».*



У XVIII столітті керівник Колегії іноземних справ Росії М.Панін рекоменду-

вав в особливих випадках використовувати симпатичні чорнила для запису шифрованого тексту між рядками видимого тексту та відправляти ці листи спеціальним кур'єром, а не поштою. В одному з листів до Берліна Панін писав: *«Не имея под рукой симпатических чернил, к помощи которых я обычно прибегаю, сегодня при написании прилагаемого письма я использовал лимонный сок. Следовательно, при обработке не следует опускать его в азотную кислоту, а надо подогреть».*

У 1797 році дружина майбутнього російського імператора Олександра I велика княгиня Єлізавета Олексіївна у листуванні зі своєю матір'ю використовувала молоко і радила рідним: «Замість того, щоб тримати лист над вогнем, можна так само посипати його вугільним порошком; це робить видимим написане й у такий спосіб можна писати по обидва боки».

Симпатичне чорнило наприкінці XVIII століття одержало широке поширення й у Північній Америці. Його використовували у своєму листуванні брати Калпери, один із яких був агентом американців у Лондоні. Це унікальне чорнило поставляв їм лікар з Лондона сер Джеймс Джей – брат першого головного американського судді Джона Джея. Це стало першим в історії США випадком широкомасштабного застосування симпатичного чорнила. Джеймс Джей через багато років розповів історію з чорнилом в одному зі своїх листів, де описав утворений ним спосіб складання невидимого чорнила для зв'язку зі своїм братом Джоном у Нью-Йорку. Зокрема, він відзначав, що *«цією рідиною постачали також генерала Вашингтона, і в мене є його лист із визнанням її великої користі та з проханнями про подальші посилки...»*

У липні 1779 року генерал Вашингтон, що віддавав належне захисту зв'язку, в одному зі своїх листів писав: «Усе біле чорнило, яке я мав... відправлене полковником Уебом у скляночці № 1. Рідина в скляночці № 2 є доповненням, що робить першу рідину видимою при змочуванні нею паперу м'якою щіткою після того, як перша висохне... Я прошу ні за яких обставин ніколи не говорити про одержання вами таких рідин від мене або будь-кого іншого». Цей тайнопис дозволяв американцям успішно переборювати англійську цензуру.

Англійці також широко використовували тайнопис. Зокрема, у їхніх агентурних посланнях застосовувалася галодубильна кислота, що є сірчанокислим залізом (цей рецепт був запозичений з книги Джованні Порта «Магія природна»).

У XIX та на початку XX століття в Росії стеганографію активно використовували різні підпільні революційні організації, що були опозиційними до влади, такі як «Земля і Воля», «Народна воля», РСДРП, БУНД (єврейська підпільна організація), есери, анархісти тощо. Дуже широко хімічне листування застосовували «народники» 1870-х років. У матеріалах їхніх судових процесів було на цей рахунок чимало даних.

Так, Микола Тєплов листувався з петербурзьким кружком «артилеристів» розчином солі. Мається на увазі звичайний водний розчин повареної солі, сліди якого виявлялися простим нагріванням. Інші листувались лимонним розчином, сліди

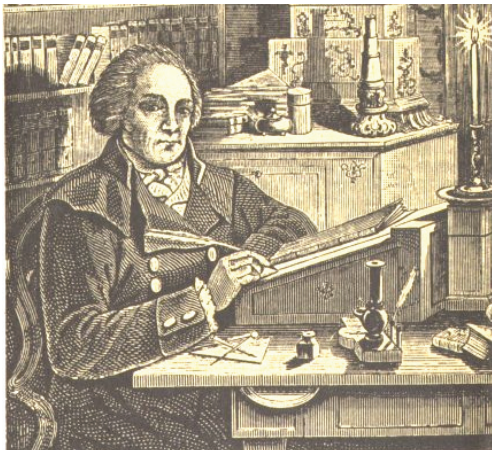
якого також виявлялися простим нагріванням. Микола Виташевський згадував, що для листування він користувався молоком: «Якщо пописаний молоком папірець злегка потерти попелом спаленого паперу, то написане проступає».

Усі ці прості рецепти «хімії» (сіль, лимон, молоко) виявлялися нагріванням і були, зазвичай, малонадійні. Створення в 1876 році такої сугубо конспіративної організації, як «Земля і Воля», а потім і «Народна Воля», зажадали від конспіраторів розробки іншого, більш стійкого хімічного чорнила. Так, у жовтні 1880 року жандарми при арешті у Києві керівників «Южноруського робочого союзу» знайшли листи, між рядками яких за допомогою хлористого заліза були виявлені шифри.

У 1884 році при розгромі київських народовольців була вилучена склянка з півторахлористим залізом, а також були виявлені листи, на яких, як сказано в поліцейських протоколах, «між рядками видніються смуги від розчину півторахлористого заліза». Тому з того часу усі листи ув'язнених у царських в'язницях стали перевірятися розчином півторавідсоткового хлористого заліза на предмет виявлення в них хімічного тексту. А у якості хімічного чорнила служив розчин жовтої кров'яної солі, а іншими словами – залізисто-синьородистого калію.

Писали революціонери свої послання не тільки в листах, але і між рядків книг, журналів і навіть газет. Так, Яків Стефанович у листуванні з Левом Дейчем використовував номери газети «Московські новини», де хімією наносив свої криптограми. Наприкінці кожного подібного листа ставилося слово «кінець» для позначення повного закінчення хімічного тексту. Це слово було присутнє в більшості стеганографічних листів, що зуміли скопіювати жандарми.

Володимир Ленін, коли знаходився у в'язниці, писав листи молоком на сторінках книг. Найбільш концентровано про це розповіла Ганна Ульянова-Єлізарова: «Це, мабуть, найцікавіші сторінки з його тюремного життя... Звичайно, ніяких хімічних реактивів у в'язниці одержати було не можна. Але Володимир Ілліч згадав, як розповідав мені одну дитячу гру, показану матір'ю: писати молоком, щоб виявляти потім на свічці або лампі. Молоко він одержував у в'язниці щодня... І ось він став писати ним між рядків пожертвованої для цього книги... Таким чином, шифровані листи крапками були замінені цим, більш швидким способом. У



листі крапками Ілліч повідомляв, що на певній сторінці є хімічний лист, який треба нагріти на лампі. Унаслідок труднощів прогрівання у в'язниці цим способом користувався більше він, ніж ми. Надія Костянтинівна указує, утім, що можна було виявляти листа опусканням у гарячий чай і що в такий спосіб вони листувалися молоком або лимоном... Взагалі Ілліч, завжди прагнув до уточнення всякої роботи, до економії сил, ввів особливий значок, що визначав сторінку шифрованого листа, щоб не ритися і не розшукувати в книгах. Перший час треба було шукати цей значок на сторінці сім. Це був тоненький олівцевий штрих, і перемножування числа рядків з числом букв на останньому рядку, де він знаходився, давало сторінку: так, якщо була відзначена 7-а буква, 7-ий рядок, ми розкривали 49-у сторінку, з якої і починався лист... Цей спосіб позначення, – сторінки час від часу мінялися, – зберігався в нас постійно».

У 1900 році був надрукований 58-ий том енциклопедії «Брокгауза й Ефрона», у якому була приведено п'ятнадцять різноманітних рецептів симпатичного чорнила. У тому ж році була надрукована брошура Володимира Акимова «Про шифри», у другому розділі якої він описав декілька способів хімічного листування:

«1. Усі кислоти при нагріванні обвуглюють ті місця, що нею покриті. Тому часто пишуть слабким розчином соляної або сірчаної кислоти (1-2% розчином), соком лимона, цибулі і, навіть, сечею. Кислоти, однак, залишають легкий слід і можуть самопроявитися згодом. Це залежить від міцності розчину і від якості паперу. Тому розчин кислоти потрібно готувати якомога більш слабкий (досвідченим шляхом), а папір брати кращих сортів, але не глянсовий!

Після нанесення хімічного тексту паперу потрібно дати можливість просохнути, а потім ретельно вичистити м'якою білою гумкою.

Соки лимона і цибулі не завжди бувають однакової густоти, а перо утримує дрібні волокна клітковини, що при висиханні стають видні на папері. Отже – це не кращий спосіб. Перо варто брати м'яке, з довгим розчіпом і вузькою повільно загостреною нижньою частиною. Кращий спосіб хімічного листування – писати азотно-свинцевою сіллю (*PbNO3*). Сіль варто розчинити у воді. Коли подальший додаток солі перестане розчинятися, ми одержимо насичений розчин. Його варто злити і розчинити в 4-5 разів, інакше він додасть глянець паперу. Папір потім варто також вичищати гумкою.

2. Більш надійне хімічне чорнило, що виявляється при обробці написаного визначеним хімічним складом. Найвідоміший спосіб – писати синьородистою окалиною, розчиненою у малій дозі води. Виявляється «хімія» півторахлористим залізом. Окалина – речови-

на дуже отруйна. У нечистому вигляді її можна добути в будь-якій слюсарні, де вона за назвою жовтої окалини застосовується при лудінні. А півторахлористим залізом жандарми перевіряють у в'язницях усі листи».

Мабуть, після ознайомлення з цими друкованими працями російські соціал-демократи одразу змінили своє хімічне чорнило. Саме на початку XX століття дружиною Леніна Надією Крупською нестійке природне «чорнило» було замінено на водний розчин оцтовокислого свинцю. За листами, написаними нею у ті роки, можна скласти цілу інструкцію з правил хімічного листування:

1. «Не пишіть лимоном, можна читати не виявляючи: виявляються самі».

2. «Для листів у книгах вживайте оцтовокислий свинець, але зробіть попередньо дослід... Можна так само писати... листа хімією й у звичайних листах між рядків, треба брати тільки товстий англійський папір, це найкращий спосіб стосунків».

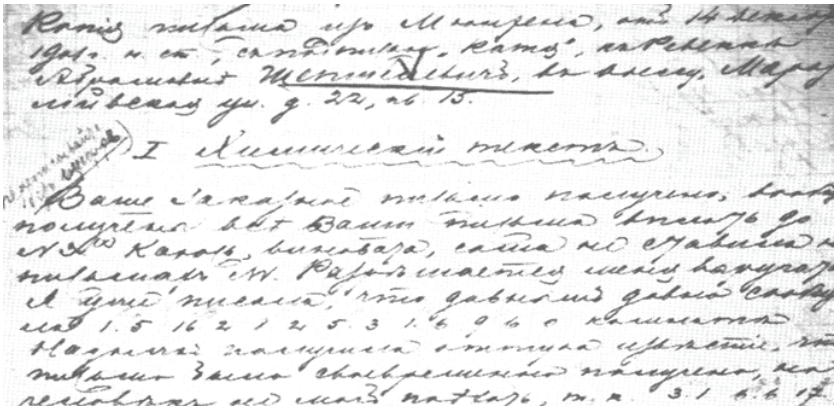
3. «В усіх... газетах і журналах папір ні до чорта не придатний».

4. «Треба писати зовсім чистим пером і зовсім не натискати, а то видно. Я писала вам про оцтовокислий свинець».

5. «Хімія ваша нікуди не придатна, ...можна було прочитати не гріючи. Перевірте свою хімію, усе ясно видно було блідо жовтим кольором, мабуть, розчин довго стояв».

Узагалі свинцеві солі для «хімії» широко застосовували й інші революційні угруповання. Так, паралельно існуючий «Союз російських соціал-демократів за кордоном» вважав найкращим складом симпатичного чорнила розчин азотно-свинцевої солі, який виявлявся не тільки нагріванням, але і нашатирем – водним розчином сірководню.

Цікаво, що у тому же 58-му томі «Брокгауза» був виписаний також і алгоритм виявлення хімічного листа: «Щоб розпізнати присутність штрихів, зроблених симпатичним чорнилом на білому папері або між рядками, написаними звичайним чорнилом, підозрілий папір поміщають між пластинками білого скла, сильно придавлюють останні один до одного та розглядають уважно при падаючому (від-



битому) і минаючому світлі. Нерідко це дає можливість прямо прочитати навіть зовсім безбарвні штрихи. У іншому випадку проводять по підозрілому паперу ряд непрямо-пересічних ліній за допомогою гусячих пер, що змочують у різні реактиви, наприклад, розведену оцтову кислоту, сірководневу воду, сірчистий амоній, йодну воду, розчини залізного, мідного купоросу, сулеми, азотно-срібної солі, хлорного заліза, жовтої і червоної кров'яної солі, свинцевого цукру, таніна й ін. Якщо який-небудь із реактивів дає позитивний результат, то неважко відшукати відповідний розчин для прояву всього написаного».

Тому головним завданням підпільників було не дати самого приводу запідозрити наявність стеганографії. А це вже залежало від їхньої майстерності. Саме в цьому конспіративному мистецтві Надія Крупська мала величезний практичний досвід.

Надалі революціонери істотно удосконалили технологію хімічного листування. З'явилися складні хімічні рецепти. Так, наприклад, у 1902 році Зінаїда Кржижанівська запропонувала такий рецепт: «Писати 1 %-спиртовим розчином b-нафтолу; чистити гумкою. Для прояву розчинити небагато паранітраніліна в розведеній соляній або сірчаній кислоті, додати туди трохи крапель розчину азотно-натрієвої або азотисто-калієвої солі та негайно за готовністю влити цю суміш у великий обсяг міцного розчину оцетнонатрієвої солі».

У 1904 році Мартин Лядов запропонував інший спосіб: «Пишіть надалі слабким розчином крохмалю, виявляється розчином йоду, від тепла не виявляється. Відзначайте листи, писані крохмалем, позначками під підписом».

У 1911 році секретар троцькістської газети «Правда» Віктор Копп в одному зі своїх листів написав інструкцію з ведення хімічного листування:

«Пишуть на шорсткуватому, не глянсовому папері. Пишуть спочатку звичайним чорнилом який-небудь незначний текст, тобто що-небудь зовсім необразливе, ні слова про справи. Коли цей лист написаний, то беруть зовсім чисте м'яке перо і пишуть між рядками, написаними чорнилом, уже те, що хочуть сказати про конспіративні справи. Цей конспіративний лист пишуть хімічним чорнилом, тобто розчином якої-небудь кислоти: або 1) Plumbum nitricum (азотно-кислим свинцем) – це найкращий склад, але отрута, і без рецепта цього препарату не видають; або 2) винно-кам'яною кислотою (цю кислоту можна купувати в будь-якому аптекарському або навіть бакалійному магазині: вона зовсім безпечна і покупка її не підозріла, тому що цю кислоту вживають у господарстві часто, наприклад, для лимонадів); нарешті, можна просто писати 3) лимонною кислотою. Яку б з цих кислот ви не взяли, ви повинні її розчинити у воді, написати що-небудь на чистому листі паперу, а потім нагріти цей папір на лампі, якщо розчин гарний, то написані букви від нагрівання стануть темніти і будуть майже чорними; якщо ж розчин недостатній, то потрібно додати ще кислоти і тільки тоді писати листа до нас».

З'являлися в революціонерів і нові оригінальні способи «хімії». Згідно з цирку-

ляром Департаменту поліції за січень 1914 року розповсюдженим способом листування підпільників став так званий «метод водяного тиску». Для цього на сирому нелінійованому аркуші паперу, накладеному на дзеркало, звичайним олівцем через інший, сухий, аркуш паперу писали потрібний лист, що при висиханні робився абсолютно невидимим. На ньому нерозчинним чорнилом писався маскувальний текст. Щоб приховане повідомлення проявилося, його знову занурювали у воду.

Заглянемо ж тепер у документ під № 99312 з архіву російської «охоронки»: «Листування хімією полягає в наступному. Пишуть на шорсткуватому, не глянсовому папері. Пишуть спочатку звичайним чорнилом який-небудь незначний текст, тобто що-небудь зовсім необразливе, ні слова про справи. Коли цей лист написаний, то беруть зовсім чисте м'яке перо та пишуть між рядками, написаними чорнилом, уже те, що хочуть сказати про конспіративні справи. Цей конспіративний лист пишуть хімічним чорнилом, тобто розчином якої-небудь кислоти».

Був також приведений витяг із листа, зробленого «хімією» революціонерами РСДРП, що був відправлений до Росії редакцією газети «Правда» з Відня. Виявити та прочитати цей тайнопис Департаменту поліції було не складно, адже саме в Росії розроблені та розвинуті способи читання прихованих і стертих текстів за допомогою фотографії та підбора висвітлення, що застосовуються й понині.

Використання вже складних хімічних рецептів поставило перед Департаментом поліції Росії серйозні проблеми. На початку XX століття один з провідних дешифрувальників Департаменту Іван Зибін в одній з доповідних записок описав рецепти прояву хімічного чорнила таким чином:

«1. Розчинити азотнокисле срібло при підкурюванні аміаком і при висвітленні вольтовою дугою.

2. Розчином ескуліна (флюоресцуючих місць непомітно при висвітленні вольтовою дугою).

3. 5-процентним розчином алізаринового чорнила (контроль – папір з чистою водою).

4. Розчином жовтої кров'яної солі (0,5 %).

5. Розчином сірчистого амонію (1 %).

6. Розчином аміаку (1 %).

7. Розчином червоної кров'яної солі з бромистим калієм (1 %).

Через проби (1, 2, 3) йодом, нагріванням і півторахлористим залізом як менш чуттєві і марні застосовані не були».

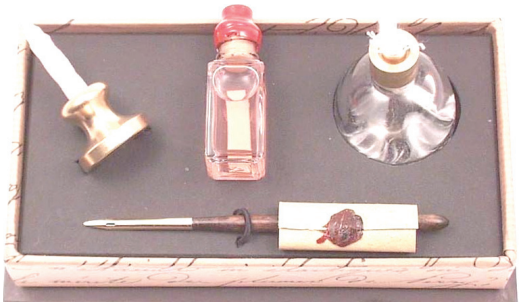
Однак з йодом Зибін помилився. На початку XX століття німці переконалися в ефективності застосування парів йоду для прояву стеганографічних послань. У подальшому, фізик Роберт Вуд запропонував використовувати для читання хімічних текстів явище люмінесценції, яке вразило своєю ефективністю англійські секретні служби, що займалися цією проблемою.

У 1917 році у американському дешифрувальному відділі «*MI-8*» було створене відділення стеганографії, що могло читати листи, написані з використанням більше 30 різних систем. Незабаром експерти-хіміки цього відділення зуміли продемонструвати своє мистецтво на практиці, знайшовши шпигунські послання, що були написані невидимим чорнилом, замаскованим під парфуми зі справжнім ароматом.

Пізніше німці замінили чорнило, що мали об'ємну і досить помітну форму рідини, хімічними речовинами, якими просочували шарфи, шкарпетки й інші предмети шпигунського одягу. Після цього їх потрібно було тільки намочити у воді, щоб одержати рідину для тайнопису. Вона була настільки ретельно складена, що вступала в реакцію тільки з одною визначеною хімічною речовиною, після чого текст можна було прочитати.

У відповідь американські хіміки створили реагент, що виявляв тайнопис із застосуванням будь-якого виду чорнила, навіть чистої води. Обережно нагріті кристали йоду при сублімації перетворювалися в пари фіолетового відтінку, що більш щільно осідали на волокнах паперу, порушені при будь-якому намоканні, і тим самим виявляли, як рухалося перо. Після того, як це стало відомо німцям, вони почали писати листи симпатичним чорнилом і потім змочувати ним весь лист. Американці у свою чергу почали піддавати смужки паперу хімічним перевіркам, що показували, чи була поверхня паперу намочена. Це було майже таким же доказом, як і фактичне виявлення листа, написаного симпатичним чорнилом. Хто, крім шпигуна, стане змочувати лист спеціальною рідиною для тайнопису?

Постійна боротьба між німецькими й американськими хіміками зайшла в тупик, коли обидві сторони створили універсальний хімічний реагент, що виявляв симпатичне чорнило при будь-яких умовах. На той час, коли з'явився цей реагент, відділення тайнопису «MI-8» піддавало перевірці 20 тисяч листів у тиждень з метою виявлення невидимих текстів і зуміло відшукати 50 дуже важливих шпигунських послань. Серед них виявилися листи, що привели до арешту якоїсь Марії Вікторії, чарівної німецької шпигунки, яка планувала ввезти вибухівку, що призначалася для саботажу, у пустотілих статуях Діви Марії та євангельських апостолів!



Незважаючи на давню популярність і слабку стійкість, симпатичні чорнила виявилися настільки зручними, що застосовувалися аж до Другої світової війни. Так, наприклад, граф Вільгельм Раутер, аме-

риканець німецького походження, який займався шпигунством на користь рідної Німеччини, був змушений використовувати сечу, коли в нього скінчився запас невидимого чорнила.

У грудні 1940 року англійська цензура виявила підозрілі за текстом листи та вирішила перевірити їх на використання невидимого чорнила. Традиційні перевірки за допомогою хімікалій, що виявляють звичайне симпатичне чорнило, дали негативні результати. Але хіміки зробили перевірку за допомогою парів йоду (цей метод був винайдений ще в Першу світову війну), і на зворотньому боці аркушів листів дійсно проступив таємний текст, що був написаний розчином пірамідону, який часто застосовувався як ліки від головного болю та продавався майже в будь-якій аптеці.

У листопаді 1941 року в цензури викликав підозру почерк листа, написаного по-іспанськи та відправленого з Гавани до Лісабона. Лист був перевірений із метою виявлення симпатичного чорнила, у результаті чого було знайдено довге повідомлення, у якому перераховувалися судна, що завантажувалися в порту Гавани, та зачіпалося питання про будівництво на Кубі військового аеродрому. Зібравши достатню кількість доказів, 5 вересня 1942 року американська поліція заарештувала Гейнця Лунінга. Він був посланий у Гавану з Німеччини у вересні 1941 року. З відправлених ним до Європи 48 листів англійські цензори перехопили 43.

Під час Другої світової війни американські цензори «смугували» всі листи, щоб виявити наявність у них невидимого чорнила. Лаборант водив по листу декількома скріпленими щітками, змоченими в розчинах різних проявників. Листи також проходили перевірку в інфрачервоних та ультрафіолетових променях. Написаний крохмалем текст, невидимий при денному або електричному світлі, починав світитися під впливом ультрафіолету. Інфрачервоні промені допомагали розрізняти кольори, які не відрізнялись при звичайному світлі, наприклад, зелені написи на зеленій поштовій марці.

За час війни до ФБР цензурою було передано більше 4,5 тисячі підозрілих листів, 400 з яких мали певну оперативну цінність. Проблеми, у яких місцеві відділення не могли розібратися самотужки, передавалися до лабораторії відділу безпеки. Одна з таких проблем полягала в тому, що німецькі агенти розшаровували лист паперу навпіл, писали текст невидимим чорнилом на внутрішній поверхні, а половинки потім знову з'єднували між собою. Оскільки чорнило знаходилося усередині листа, ніякий реагент, нанесений на його зовнішню поверхню, не міг їх виявити. Цей спосіб був виявлений лише після того, як один німецький агент використав для свого листа занадто багато чорнила, і їхній надлишок просочився крізь папір.

6.2. Маскування

Стеганографія також припускає, що таємний текст може «розчинятися» в повідомленні більшого розміру з абсолютно «стороннім» нетаємним змістом.

Першим методом такого маскування було застосування трафарету або решіток (винайдений у XVI столітті італійцем Джероламо Кардано).

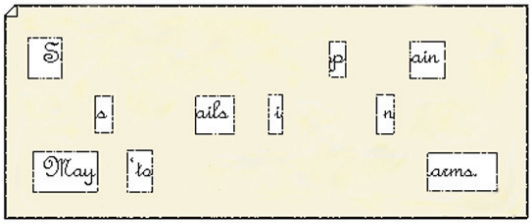
Зазвичай решітки являли собою лист із твердого матеріалу, у якому через неправильні інтервали були зроблені прямокутні вирізи висотою для одного рядка та різної довжини. Накладаючи ці решітки на аркуш паперу, можна було записувати у вирізи таємне повідомлення. Після цього, знявши решітки, потрібно було заповнити вільні місця, що залишилися, на аркуші паперу якимось текстом, що маскував таємне повідомлення. Подібним стеганографічним методом маскування повідомлення користувалися багато відомих історичних осіб, наприклад, французький кардинал Рішельє та російський дипломат і письменник О.С.Грибоєдов.

Так, Рішельє використовував прямокутник розміром 7x10. Для довгих повідомлень прямокутник використовувався декілька разів. Прорізи трафарету розміщувалися у позиціях (1,8), (2,9), (3,6), (4,5), (4,6), (5,1), (5,6), (5,7), (5,9), (6,2), (6,10), (7,9), (7,10).

	1	2	3	4	5	6	7	8	9	10
1								■		
2									■	
3						■				
4					■	■				
5	■					■	■		■	
6		■								■
7									■	■

Відомий російський письменник, суспільний діяч і дипломат Олександр Сергійович Грибоєдов, призначений у 1828 році на посаду російського представника в Персії, використовував решітки Кардано у своїх листах. Він писав своїй дружині «безневинні» листи, які, потрапивши до російської жандармерії, розшифровувалися та передавались царському уряду вже як секретні повідомлення.

Sir John regards you well and spekes again that
all as rightly 'vails him is yours now and ever.
May he 'tone for past d'lays with many charms.



Розкрилося це вже в радянські часи. Декого з біографів Грибоєдова засмутив той факт, що в окремих листах до своєї дружини порушувався характерний стиль знаменитого письменника. При дослідженні виявилося, що ці листи містили дипломатичні

послання Грибоєдова.

Розшифрували цю систему дуже просто. Склали листочки один на одний і освітили могутньою лампою. Букви, що стояли на місцях вікон решіток, давали темні плями, бо лежали суворо одна під одною. По цих плямах легко відновлювалися решітки, тобто ключ. Вони були зроблені через трафарет, що накладався на аркуш паперу, у якому були вирізані окремі віконця під букви. Написавши повідомлення через трафарет, Грибоєдов дописував розкидані на аркуші букви у зв'язний текст так, щоб він містив лист дружині, та відправляв його звичайною поштою.

Мабуть, дружина його не здогадувалася про подвійне призначення цих послань. Відзначимо велику дотепність застосованого шифру та достатню його надійність. Маючи окремий лист, розкрити шифр практично неможливо, а переписування тексту від руки руйнувало шифровку, оскільки букви неминуче зрушувалися за місцем розташування.

Другим методом маскування було читання таємного повідомлення за заздалегідь обговореними правилами. Так, наприклад, у XVII столітті сер Джон Тревеніон, прихильник англійського короля Карла I, що очікував неминучої страти від рук прихильників Кромвеля, одержав листа, який був ретельно вивчений його тюремниками, перш ніж був переданий йому в руки. Прочитавши в цьому листі кожну третю букву після кожного розділового знака, він довідався, що «у східній стіні каплиці відкривається одна панель». Під час вечірні Тревеніон утік.

Російські революціонери застосовували також такий прийом, як читання таємного повідомлення за заздалегідь обговореними місцями у «безневинному» тексті. Наприклад, вони домовлялися читати з отриманого нетаємного листа тільки кожне п'яте слово, що й складало таємне повідомлення. Відомий ідеолог анархізму П.Кропоткін послав своєму кореспонденту такий лист: «Вибач, що пишу поспіхом. Приходь до мене ввечері сьогодні. Завтра я повинен...». Читання тільки п'ятих слів дає початок таємного тексту: «Приходь завтра...»...

Прикладом такого маскування є також «акровірш» – вірш, у якому початкові букви рядків складають слово або фразу.

Російська партія соціалістів-революціонерів (есерів) використовувала для маскування свого таємного листування трафаретні вітання до дня народження, іменин, вступу в шлюб тощо. Текст листівок не мав ніякого значення, але мала значення ілюстрація, зображена на листівках. Так, зображення чоловічих фігур означало успішний хід підпільної роботи, а жіночих – труднощі і невдачі тощо.

Англійський філософ і державний діяч Френсіс Бекон (1561-1626) уперше запропонував свою систему стеганографічного маскування, назвавши її «двобуквеним» шифром. Практично це було «двійкове кодування» букв латинського алфавіту – те ж саме, яке використовується зараз у комп'ютерах.

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAABA	h	AABBB	o	ABBAB	u,v	BAABB
c	AAABB	i,j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

По суті, це була бінарна система маскування, оскільки за допомогою шрифтів двох видів (наприклад, «А» і «В») у букви довільного (нетаємного) тексту потай вносилася додаткова (таємна) інформація. Кожній букві таємного послання ставилося у відповідність п'ять букв звичайного відкритого тексту.

Розповідаючи про Френсіса Бекона, неможливо оминути також і те, що саме він, можливо, був автором усіх творів Уільяма Шекспіра. Справа в тому, що на початку XX століття були проведені криптоаналітичні дослідження творів Бекона та Шекспіра під керівництвом американця Фабіана в містечку Рівербенк штату Іллінойс. Підібрані ним криптоаналітики (у тому числі й видатний американський криптолог Уільям Фрідман) шукали докази того, що не Шекспір, а Бекон написав всесвітньо відомі п'єси.

В результаті цих дослідів знайшли спосіб, за допомогою якого вдалося розшифрувати таємні послання, приховані у творах Шекспіра та Бекона. І послання ці переконливо (принаймні, для Фабіана) свідчили, що насправді автором усіх шекспірівських творів був Френсіс Бекон, а єдиним внеском Шекспіра в літературу було лише його ім'я.

У період Другої світової війни полонені німецькі офіцери-підводники у своїх листах додому посилали таємні повідомлення, роблячи невеликі пробіли після кожної значимої букви. Один пильний англійський цензор помітив, що ці маленькі пробіли знаходилися в найбільш неприродних місцях, навіть у середині складів. Виявилося, що у своїх прихованих посланнях німці повідомляли про тактику, що застосовувалася англо-американськими союзниками в боротьбі з німецькими підводними човнами, а також про їхні технічні недоліки.

У цей же період американські військові у своїх листах додому пробували повідомляти своїх родичів про місце своєї служби, користуючись раніше домовленою системою листування. Так, наприклад, один солдат у п'яти листах додому як другий ініціал батька писав перші букви назви країни, де знаходився: Т, У, Н, І, С. На жаль, ці листи були отримані родичами у іншому порядку, а солдат забув поставити на листах дати. Тому родичі відповіли йому, що вони вивчили вес атлас, але країни з назвою «НУТСІ» не знашли. У 1943 році подібні спроби настільки почастішали, що керівництву ВМС США довелося попередити моряків про те, що використання «сімейних кодів» може призвести до суворого покарання.

Ще одним способом маскування, який був найбільш поширеним у російських

революціонерів, була розмітка потрібних букв повідомлення в друкованих рядках якої-небудь книги. Перше згадування про це ми знаходимо у 1872 році. Тобто для листування з арештованими товаришами використовувались книги, у яких голкою або гострим олівцем наколювалися або підкреслювалися букви так, щоб утворювалися потрібні слова.

У жовтні 1880 року Лев Гартман писав із лондонської еміграції народовольцям у Росію: «У випадку великих листів, надсилайте краще під копійчаною бандероллю брошурку, книжку, де, починаючи з 5 або 11 сторінки, відзначайте букви олівцем під ними. І читати легше, і шифру не треба і посилати не важко й не ризиковано».

Ще одним способом маскування, який застосовували революціонери, було ховати повідомлення у обкладинки книг або листи картону. Так, улітку 1895 року Володимир Ленін познайомив берлінських колег зі способом пресування і перетворення в палітурний картон літературних матеріалів, що підлягали таємному перевезенню: «Аркуші такої літератури або листів (тільки писаних тушшю), за цим рецептом з'єднуються особливим клеєм, накладаються один на інший до визначеної товщини, обкладаються зовні папером; у такому вигляді пресуються та сушаться, після чого виходить звичайний на вигляд картон, що не викликає підозри; коли ж заховану в цьому картоні літературу потрібно повертати в первісний стан, то картон кладуть у теплу воду й обережно розбирають на складові частини».

Збереглися два листи Леніна до Аксельрода у листопаді 1895 року, де Володимир Ілліч уточнює алгоритм використання цього способу:

1. «Писати треба китайською тушшю. Краще, якщо додати маленький кристалик хромпіка ($K_2Cr_2O_7$): тоді не змиється. Папір брати якомога тонший...»

2. «Необхідно вживати дуже рідкий клейстер: не більше чайної ложки крохмалю (картопляного, а не пшеничного, який занадто міцний) на склянку води. Тільки для верхнього листа та кольорового паперу потрібний звичайний клейстер, а папір тримається добре, під впливом преса, і при рідкому клейстері. У всякому разі, спосіб придатний, і його варто практикувати».

Зазначений Леніним «хромпік» являє собою кристали червоного кольору і відомий у хімії як вихідний матеріал для всіх інших з'єднань хрому. У XIX столітті ця речовина широко застосовувалася як окислювач у процесі фабричного фарбування тканин і у фотомеханічних способах друкування зображень. Тому «хромпік» був тоді цілком доступним для підпільників хімікатом.

Спосіб розклеювання подібної «посилки» ми знаходимо в одному з листів Надії Крупської у 1901 році: «Плетіння треба опустити в теплу воду, і коли воно стане розшаровуватися, почати відокремлювати аркуші, підставляючи під кран з киплячою водою, треба тільки не поспішати. Відділені в такий спосіб аркуші витерти губкою, щоб зняти клей, потім дати висохнути та вогкуватими покласти під прес».

У порівнянні з іншими, добре відомими російським жандармам способами

листування (хімія або крапки в буквах), метод закладення листів у картон, безумовно, був більш надійний, і революціонери високо цінували його. Звичайно, він був громіздкий, трудомісткий, вимагав визначених матеріальних витрат, але гарантував конспірацію. І молодий В.Ульянов свою революційну діяльність почав саме з цього надійного способу листування з еміграцією.

У 1900 році Володимир Акімов у своїй брошурі «Про шифри», у її другій главі «Як сховати шифр», описав декілька способів маскування шифрів:

«1. Відзначені букви [прим. – спосіб нанесення уколів у потрібних буквах друкованого книжкового тексту та метод запису цифрового шифру зазначеним способом].

На сторінці книги з лівого боку в рядку ставлять крапку, що позначає чисельник дробу шифру. З правого боку на тім же рядку ставлять крапку, що позначає знаменник. Зручніше шифрувати двозначні числа. Менш помітні, ніж уколи і крапки, значки, поставлені не біля букв, а на їхньому чорному тлі. Олівець повинен бути гострий і твердий, при шифруванні його необхідно постійно підточувати наждачкою. Замість крапок краще ставити малесенькі риски, що непомітні, якщо дивитися перпендикулярно до площини книги, а видні, якщо глянути скоса, щоб промені йшли від букв до ока під дуже гострим кутом до площини книги. При цьому риски дають відблиск і стають помітними.

2. Цифри, що мають благонадійний вигляд [прим. – спосіб маскування шифру легальним текстом у вигляді рахунка, математичного завдання, торгівельного документа тощо].»

6.3. Мікрокрапки

Ще у 1644 році відомий англійський учений Роберт Хук в книзі «Мікрографія» писав: «Якщо спосіб мініатюрного листа став би простіше і доступніше, це знайшло б вдале застосування при пересиланні розвідувальних повідомлень без побоювання бути виявленими або викликати яку-небудь підозру».

Вже в XVIII столітті в Англії і Франції були створені спеціальні механічні пристрої для виконання мікронаписів. Один із таких приладів, «Peter's Machine for Microscopic Writing», зберігається в музеї Оксфордського університету. Він дозволяв виконувати напис з висотою символів усього в 2,5 мікрона! А в 1923 році американець Мак Івен, навіть, запатентував «Пристрій для написання розвідувальних повідомлень», сконструйований на основі вищезазначеної «Машини Пітера». На обкладинці журналу «*Scientific American*» за червень 1923 року, де з'явилася замітка про це пристосування, було на-

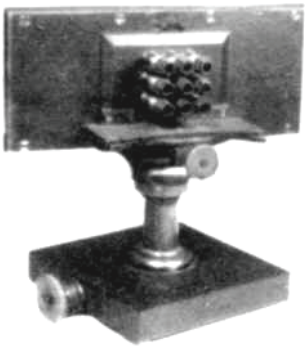
писано: «Напис для ока мікроскопа – як вигравіювати шпигунське повідомлення на капелюшку цвяха».

Девід Брюстер, один з укладачів восьмого видання Британської Енциклопедії, у статті про «мікроскопію» зробив воістину видатне зауваження: «...мікроскопічні копії дипломатичної пошти, інших важливих документів, а також різних планів і схем можна буде пересилати поштою. При цьому з метою збереження секретів ці повідомлення будуть займати на папері не більше місця, ніж крапка наприкінці речення або малопомітна чорнильна ляпка...» Так у жовтні 1857 року за багато років до її практичної появи була пердбачена не тільки сама «мікрокрапка», але спосіб її оперативного застосування.

У загальному випадку під «мікрокрапкою» розуміється сильно зменшене фотографічне зображення документа звичайних розмірів, наприклад, А4 (210х297 мм). Мікрокрапка є простим перекладом німецького терміна «*Mikrat*», уведеного її творцем Еммануїлом Голдбергом у 1925 році для позначення створеного ним мікроскопічного зображення. Це було зроблено за аналогією і видимою подібністю зі звичайною крапкою наприкінці речення, що звичайно при використанні друкарської машинки має діаметр порядку 0,8 мм. Таким чином, для того, щоб довести документ стандартних розмірів до величини машинописної крапки потрібне його зменшення в 275 разів.

У 1870 році у Франції з метою компактного збереження інформації був розроблений метод «мініатюрного фотографування». Текст із 300 тисяч букв уміщався на фотографії звичайного розміру. Вперше у військовій справі цей метод був використаний під час франко-прусської війни 1870-1871 років. Рене Дагрон організував мікрофільмування пошти й інших матеріалів, що передбачалися до пересилання «голубиною» поштою. Цікаво, що цей процес до 1890 року вважався французьким військовим секретом.

Листи і повідомлення виконувалися на прозорих аркушах, розділених на 12 секцій розміром 80х110 мм. Вони копіювалися вроздріб контактним способом на фотографічні пластинки, що після хімічної обробки повторно перезнімалися з великим зменшенням за допомогою спеціальної репродукційної камери з 20-а короткофокусними об'єктивами. У результаті виходили мікрозображення розміром не більш 1 мм, які вже цілком були схожими на реальну «мікрокрапку». Після обробки емульсія з мікрозображеннями знімалася зі скляної пластини у ванні з касторової олії.



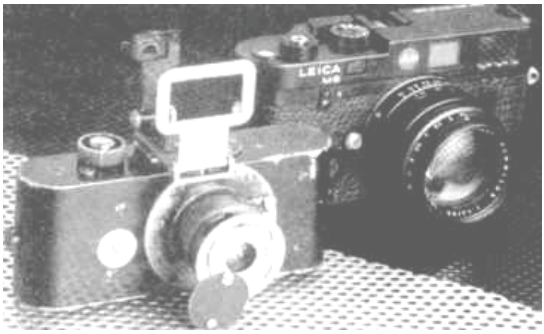
По суті, це була модифікація процесу, що застосовувався американцями задовго до цього. В архівах Конфедерації зберігся цікавий лист президенту жителів Півдня Д.Джеферсону від якогось Дж.Вінте-

ра з Алабами, датоване липнем 1861 року. У ньому містилася пропозиція використовувати мікрофотокопії різних повідомлень для забезпечення їхньої безпеки при доставці. І хоча не збереглося підтверджень, що ця пропозиція була реалізована, є докази, що конфедерати використовували в окремих випадках заховані мікрозображення, у тому числі в контейнерах, пристосованих для ковтання у випадку небезпеки.

До початку Першої світової війни фотографічний процес прийняв звичний для нас вигляд, однак можливості мікрофільмування використовували, мабуть, тільки німці. Існує навіть легенда, що справжньою задачею Оскара Барнака (1879-1936) було створення за завданням німецького МЗС і військових малоформатної 35 мм плівкової камери для мікрофільмування документів. Ідея камери, очевидно, ґрунтувалася на шведському прототипі 1911 року з форматом кадру 31х49 мм і запасом плівки 30 м. У 1913 році з'явилася перша модель фотокамери «*Ur-Leica*» (приставка «*Ur*» відповідає німецькому «*Urbild*», що означає «прототип»).

Мікрокрапка в її справжньому вигляді була створена талановитим німецьким вченим і інженером Еммануїлом Голдбергом. Син військового хірурга, що брав участь у Російсько-японській війні, народився в Москві 1 вересня 1881 року. Закінчивши Московський університет, він виїхав у Німеччину, де працював у Лейпцизі в Нобелівського лауреата В.Освальда. У 1906 році за дослідження іонної природи фотографічних процесів Голдберг одержав звання доктора наук. Два роки Голдберг працював у лабораторії Адольфа Міта над проблемами кольорової фотографії, а також був лектором у Військовій академії в Берліні з курсу фотограмметрії.

Подібно Гершелю та Брюстеру сторіччя назад, Голдберг так само задумувався про роль мікрофільмування для збереження та обробки зростаючого потоку друкованої інформації. У 1925 році на міжнародному конгресі з фотографії в Парижі доктор Голдберг продемонстрував створений ним процес з виготовлення «мікрокрапок» – мікрозображень із гранично можливими геометричними розмірами. До цього часу він був автором двох монографій: «Основи репродукційної техніки» і «Структура фотографічного зображення».



У німецькій розвідувальній системі був створений підрозділ «Geheimsache», що відповідав за розробку й виробництво засобів тайнопису, фальшивих документів і мікрофотографій. Для цього були всі передумови: високоякісні портативні 35 мм фотокамери «Лейка», «Кон-

такс» і особливо «Екзакта». До того ж приналежності для мікрозйомки і репродукції вироблялися саме в Німеччині.

У 1925-1937 роках з ініціативи «Geheimsache» у Німеччині розгорнулися роботи з удосконалення мікрокрапок – вищого досягнення в сфері мікрофільмування. Практично усі вони базувалися на первісних дослідженнях Голдберга 1906 року, найбільш успішно узагальнених і розвинутих ним наприкінці 20-х років.

Наприкінці 30-х років фахівці фірми «*Agfa*», одного з провідних світових виробників фотоматеріалів, розробили фотопластинки високої якості «HR» для астрофізики та спектрографії, відомі також за назвою «*Agfa-Mikrat-Platten*». Компанія «*Zeiss-Ikon*», де директором у свій час був творець «мікрокрапок» Голдберг, проводила роботи зі спрощення процесу одержання мікрозображень. Нею була випущена портативна репродукційна фотокамера для виготовлення ультра-мікрофільмів з оригіналів формату А4. Розмір зображення на плівці шириною 4 мм складав всього 2 мм^2!

18 листопада 1937 року випускник Берлінської вищої технічної школи Ханс Амман-Брас, швейцарець за походженням, одержав завдання абвера удосконалити технологію виготовлення мікрокрапок. У технічній записці ставилося завдання створити апарат для виготовлення мікрокрапок із кратністю зменшення до 1:750.

У період до і під час Другої світової війни засоби мікрофотографії найбільше активно використовували німецькі спецслужби. І справа не тільки в тому, що саме в Німеччині вони були доведені до того стану, коли практичне застосування не викликало труднощів у виконавців. Як відомо, основний потік інформації, що направлявся німцями відкритим поштовим каналом під час Першої світової війни, надходив у тайнописі.

Потреба в інформації була величезною – від загальнополітичних новин і соціологічних досліджень до економічних оглядів, наукових статей, інструкцій та технічних описів. Успішному збору матеріалів сприяв той факт, що після Першої світової війни до існуючих в усьому світі німецьких колоній та поселень додалися нові. У німецьких спецслужб був широкий вибір кандидатів на вербування із різних шарів суспільства. Залишалося тільки відпрацювати канали передачі інформації через треті країни.

Конверт с микроточкой, отправленный в 1941 г. немецкому агенту в США

Військова німецька розвідка (абвер), готуючись до Другої світової війни, усе частіше відправляла за кордон своїх агентів, навчених роботі з мікрокрапкою. Уже після ві-

йни з'ясувалося, що в багатьох німецьких посольствах у Латинській Америці були обладнані фотолабораторії – своєрідні фабрики мікрокрапок. Не менш важливою ланкою було застосування мікрокрапок для зв'язку Центра з агентом. Їм направлялися інструкції, завдання і навіть особисті листи. У випадку налагодженого поштового каналу мікрокрапки ставали винятково надійним і дешевим способом зв'язку, а в специфічних умовах Південної Америки 30-х років він був просто ідеальним.

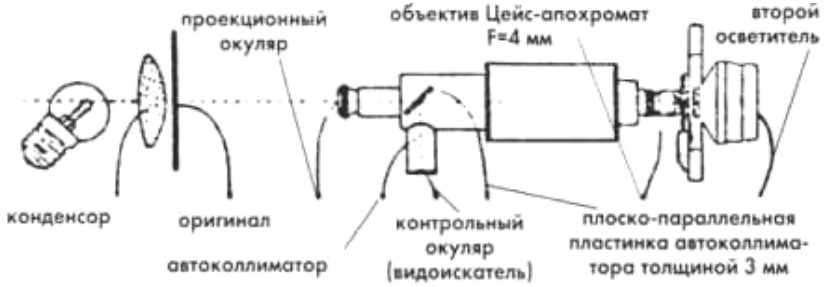
Так, наприклад, у столиці Мексики «звила гніздо» німецька розвідгрупа, що робила мікрофотознімки американських видань в галузі торгівлі та техніки, що заборонялося вивозити за кордон, та відправляла їх цілими партіями по таємних адресах у Європі, причому іноді в одному листі було до 20 мікрокрапок. У такий же спосіб через океан переправлялися викрадені технічні креслення та схеми.

Для боротьби з німецькою агентурною мережею, що постійно розширювалася, у 1930-і роки був створений Британський координаційний комітет з безпеки на чолі з досвідченим контррозвідником Уільямом Стівенсоном. Англійці організували активну протидію каналам зв'язку німецьких агентів у Новому Світі. З цією метою на Бермудських островах, своєрідній перевалочній базі транспортного потоку з Америки в Європу, вони створили резидентуру для контролю зазначеної кореспонденції. Фактично здійснювався її огляд – перлюстрація.

За спогадами самого У.Стівенсона, багаж і пошта рейсів «*Pan-American*» ретельно переглядалися, поки йшло дозаправлення літака, а екіпаж розважався в яхт-клубі. Агенти англійської контррозвідки в скаженому темпі обстежували пошту та багаж, а пасажири чули лише вибачення за змушені затримки з тих або інших причин.

Найбільш творчими майстрами перлюстрації, природно, були дівчата – співробітниці британської контррозвідки «*MI-5*». У той час відрядження на Бермуди вважалося досить престижним. Але працювати доводилося з мікроскопами, досліджуючи всі підозрілі крапки в розкритих конвертах. Для мікрокрапок навіть існувала кличка «*duff*», оскільки їх шукали як родзинки у пудингу (англ. *plum duff*).

Зрозуміло, шукати голку в стозі сіна – мікрокрапку в загальному потоці кореспонденції в режимі вільного пошуку було безглуздо. Тому англійці довели до ФБР інформацію про мікрокрапку як засіб зв'язку німецьких агентів і способи її



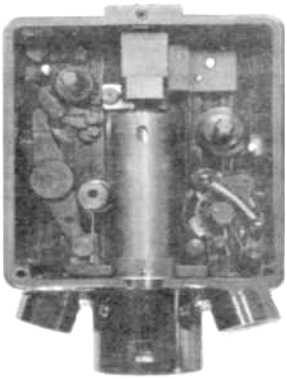
виготовлення на спеціальних апаратах. У відповідь ФБР інформувало своїх британських колег про підозрілих абонентів і кореспондентів: чию конкретно кореспонденцію доцільно взяти під контроль. Із зрозумілих причин співробітники ФБР на прохання англійців здійснили відповідні заходи безпеки, щоб не розкрити джерело інформації, і німці не догадалися, що їхній секрет виявлений.

Американська цензура лише в серпні 1941 року, завдяки тільки агентурним даним, знайшла першу мікрокрапку, що знаходилася на телеграфному бланку та була замаскована під розділовий знак машинописного шрифту. Коли агенти ФБР за допомогою невеликого мікроскопа ознайомилися зі знахідкою, один з контррозвідників викликнув: «Разюче! З цим я сам поїду у Вашингтон до Гувера. Упевнений, його це потішить...»

Але на цьому історія не закінчилася. Мікрокрапка містила не тільки дані про хід військового виробництва та постачання до Великобританії, але й опитувальник, присвячений системі оборони американської військово-морської бази Перл-Харбор, тієї самої, з нападу на яку для США почалася війна. У сполученні з показаннями, що цей опитувальник був складений провідним німецьким експертом з Японії бароном Гронау, інформація приймала лиховісний відтінок. Мабуть, директор ФБР Гувер, не доповів президенту Рузвельту повний зміст виявленої мікрокрапки.

Першою згадкою про використання мікрокрапки в 1950-і роки стало твердження про те, що інформація про постачання зброї чехословацького виробництва до Гватемали у 1954 році надійшла в американський Держдепартамент у вигляді мікрокрапки.

Але найбільш красномовно засоби мікрофотографії були розписані західною пресою при висвітленні процесів, пов'язаних із провалами радянських агентів-нелегалів. Так, Рудольф Абель виготовляв мікрокрапки, зменшуючи розмір кадру 35-міліметрової фотоплівки за допомогою лінзи з дуже малою фокусною відстанню. Щоб зберегти чіткість при такому зменшенні, він використовував найкращу фотоплівку з тих, які продавалися в магазинах.



Для пересилання підготовленого матеріалу Абель розшивав журнали з домоведення та садівництва, поміщав у їхній корінець мікрокрапки, знову переплітав ці журнали та посилав їх на визначену адресу до Парижа. З якихось причин ця прихована інформація не дійшла до адресата, і Москва попросила Абеля припинити відправлення подібних повідомлень. Однак він як і раніше продовжував одержувати інструкції з Центру у вигляді мікрокрапок.

У випадку з полковником шведських військово-повітряних сил (ВПС) Стігом Веннертстромом,

який у 1950-60-і роки співробітничав із радянською розвідкою, згадувалося, що інструкції він одержував у вигляді мікрокрапок. Для передачі військових таємниць С.Веннертстром активно використовував мікрофільмування.

Різноманітні фотографічні засоби фігурували і в іншій справі, пов'язаній із Портландською групою – «*Portland Ring*». Її керівником (резидентом) був знаменитий нелегал Конон Трохимович Молодий – Гордон Лонсдейл, з якого був списаний образ радянського нелегалу у фільмі «Мертвий сезон». Він мав прилад для читання мікрокрапок, який тримав у банці з тальком.

7 січня 1961 року британська контррозвідка заарештувала помічників К. Молодого – родину Олени і Пітера Крюгер (вони ж Лона і Моріс Коен), які на той час мали вже багаторічний досвід успішної нелегальної роботи. У схованці у ванній кімнаті було виявлено кілька фотоапаратів і велика кількість різних фотоматеріалів, а також приналежності для виготовлення мікрокрапок: солі хромової кислоти і целофан.

Говорячи про мікрокрапку, варто згадати про військовослужбовця ВПС США Роберта Томпсона, арештованого в 1965 році за обвинуваченням у шпигунстві на користь СРСР, за що він одержав 30 років в'язниці. При арешті в нього були вилучені фотоапарат «Minox B» і контейнер для збереження знятих мікрофільмів у каблуці. За словами Томпсона, у Радянському Союзі крім мікрофільмування його навчили і виготовленню мікрокрапки. Ось що він сам розповів про це:

«Документ, що підлягає зменшенню, перезнімався за допомогою 35 мм однооб'єктивної дзеркальної фотокамери. Для цього досить було покласти його на рівну поверхню, закріпити фотоапарат на спинці стільця за допомогою струбцини і, що дуже важливо, організувати рівномірне висвітлення оригіналу. Після прояву проміжний негатив затискувався між двома склами подібно звичайному слайду.

Паралельно з цим зі шматочка звичайного целофану за допомогою спеціальних хімікатів, якими агента постачали його «куратори», виготовлявся світлочутливий матеріал.

На певну горизонтальну поверхню містився лист білого паперу, на який установлювався спеціальний прилад, назвемо його умовно – камера для мікрокрапки або мікрокамера. Паралельно до цієї поверхні на висоті 60-80 см розташовувався проміжний негатив, затиснутий між склами. На нього ставили звичайну лупу силою 2,5-3х, що виконувала роль конденсора. Над негативом встановлювалася електрична лампа потужністю 100 Вт із прозорою колбою.

Усе це спорудження регулювалося таким

чином, щоб світло від лампи концентрувалося лупою і, проходячи через негатив, збиралося вузьким пучком у лінзову систему мікрокамери. Піднімаючи й опускаючи скло з негативом, треба було домогтися, щоб пучок світла збирався в крапку на аркуші білого паперу. Це місце позначалося хрестиком.

Після цього лампа виключалася. На місце, відзначене хрестиком, містився шматочок підготовленого целофану, а поверх нього – мікрокамера. Лампа знову включалася та вироблялася експозиція, що звичайно складала 3 хв. Проекспонований фотошар виявлявся в звичайному чорно-білому проявнику. Зображення являло собою мікроскопічну чорну крапку.

За допомогою шматочка бритвеного леза з відламаним гострим кінцем ця крапка вирізувалася і з особливими обережностями ховалася в деякому заздалегідь обумовленому з агентом місці. Звичайно для цього використовувалася звичайна поштова листівка. Треба було розщепити її кут на 2-3 мм, помістити в нього мікрокрапку та заклеїти клеєм зі звичайного борошна. На відміну від інших видів клею, цей не мав ефект люмінесценції в ультрафіолетових променях і не створював демаскуючих ознак. Для збереження мікрокрапок могли використовуватися різні контейнери в невеликих побутових предметах. Для читання мікрокрапок досить було невеликого мікроскопа або спеціального пристосування, закамуфльованого навіть у сигареті».

До речі, ізраїльська розвідка «Моссад» використовувала досить оригінальні контейнери для збереження та транспортування мікрокрапок: маленькі ємності з якою-небудь нешкідливою рідиною. У випадку небезпеки мікрокрапку можна було просто проковтнути разом із вмістом ємності. І якщо в звичайних умовах, впустивши на підлогу, її майже неможливо було знайти, то цього разу безпека була абсолютно гарантованою.

6.4. Цифрова стеганографія

Інтерес, що спостерігається в даний час до стеганографії як сукупності методів приховування інформації, виник у великій мірі завдяки інтенсивному впровадженню та широкому поширенню засобів обчислювальної техніки в усі сфери діяльності людини. У рамках обчислювальних мереж виникли досить широкі можливості з оперативного обміну різною інформацією у вигляді текстів, програм, звуку, зображень між будь-якими учасниками мережних сеансів незалежно від їхнього територіального розташування. Це дозволяє активно застосовува-

ти всі переваги, що дають стеганографічні методи захисту.

Стеганографічні методи знаходять усе більше застосування в оборонній і комерційній сферах діяльності завдяки їхньому легкому пристосуванню до вирішення завдань захисту інформації, а також відсутності явно виражених ознак засобів захисту, використання яких може бути обмежене або заборонено (як, наприклад, криптозасобів захисту).

Сьогодні стеганографічні технології активно використовуються для вирішення таких основних завдань:

- захист інформації з обмеженим доступом від несанкціонованого доступу;
- захист авторських прав на деякі види інтелектуальної власності;
- подолання систем моніторингу і керування мережними ресурсами;
- «камуфляж» програмного забезпечення;
- створення схованих каналів витоку чуттєвої інформації від законного користувача.

Використання стеганографічних систем є найбільш ефективним при вирішенні проблеми захисту інформації з обмеженим доступом. Так, наприклад, тільки одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і рівнем відліку 8 біт у стереорежимі дозволяє сховати за рахунок заміни молодших розрядів на приховуване повідомлення близько 10 Кбайт інформації. При цьому зміна значень відліків складає менше 1%. Така зміна практично не виявляється при прослуховуванні файлу більшістю людей.

Крім схованої передачі повідомлень, цифрова стеганографія є одним із найперспективніших напрямків для автентифікації та маркування авторської продукції з метою захисту авторських прав на цифрові об'єкти від піратського копіювання. На комп'ютерні графічні зображення, аудіопродукцію, літературні твори (програми в тому числі) наноситься спеціальна мітка, що залишається невидимою для очей, але розпізнається спеціальним програмним забезпеченням.

Мітка містить сховану інформацію, що підтверджує авторство. Схована інформація повинна забезпечити захист інтелектуальної власності. Як впроваджувану інформацію можна використовувати дані про автора, дату та місце створення добутку, номера документів, що підтверджу-

ють авторство, дату пріоритету тощо. Такі спеціальні відомості можуть розглядатися як докази при розгляді спорів про авторство або для доказу нелегального копіювання.

Нерідко методи цифрової стеганографії використовують для камуфлювання програмного забезпечення. У тих випадках, коли використання програм незареєстрованими користувачами є небажаним, воно може бути закамуфльоване під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано у мультимедійних файлах (наприклад, у звуковому супроводі комп'ютерних ігор).

У рамках комп'ютерної стеганографії розглядаються питання, зв'язані з прихованням інформації, що зберігається на носіях або передається по мережах телекомунікацій, з організацією схованих каналів у комп'ютерних системах і мережах, а також з технологіями цифрових водяних знаків і відбитка пальця.

Існують визначені відмінності між технологіями цифрових водяних знаків і відбитка пальця, з одного боку, і власне стеганографічними технологіями приховування секретної інформації для її наступної передачі або збереження. Найголовніша відмінність – це те, що цифрові водяні знаки і відбитки мають на меті захист самого цифрового об'єкта (програми, зображення, музичного файлу тощо), куди вони впроваджуються, та забезпечують доказ прав власності на даний об'єкт.

За аналогією з криптосистемами у стеганографії розрізняють системи з секретним ключем і системи з відкритим ключем. У стеганографічній системі з секретним ключем використовується один ключ, що повинен бути заздалегідь відомий абонентам до початку схованого обміну секретними повідомленнями або пересланий по захищеному каналу.

У стегосистемі з відкритим ключем для вбудовування та витягу таємного повідомлення використовуються різні ключі, причому вивести один ключ з іншого за допомогою обчислень неможливо. Один із ключів (відкритий) може передаватися вільно по незахищеному каналу зв'язку, а другий секретний ключ – по захищеному каналу. Дана схема добре працює при взаємній недовірі відправника та одержувача.

З огляду на все різноманіття стегосистем, вони можуть бути таких типів: безключові системи, системи з секретним ключем, системи з відкритим ключем і змішані системи.

Для підвищення безпеки безключових систем перед початком процесу стеганографічного приховання попередньо виконується шифрування інформації. Такий підхід збільшує захищеність усього процесу зв'язку, оскільки це ускладнює виявлення схованого повідомлення.

При використанні стегосистем із секретним ключем відправник, вставляючи секретне повідомлення в обраний контейнер, застосовує секретний стегоключ. Якщо використовуваний у стеганографічному перетворенні ключ відомий

одержувачу, він зможе витягти сховане повідомлення з контейнера. Без знання такого ключа будь-який інший користувач цього зробити не зможе. Даний тип стегосистем припускає наявність безпечного каналу для обміну стегоключами.

Стегосистеми з відкритим ключем не мають потреби в додатковому каналі ключового обміну. Для їхнього функціонування необхідно мати два стегоключі: один – секретний, який користувачі повинні зберігати в таємниці, а другий – відкритий, що зберігається в доступному для всіх місці. При цьому відкритий ключ використовується в процесі приховування інформації, а секретний — для її витягу.

Простим способом реалізації подібних стегосистем є використання криптосистем з відкритим ключем. Стегосистеми з відкритими ключами використовують той факт, що функція витягу схованої інформації може бути застосовна до будь-якого контейнера поза залежністю від того, чи знаходиться в ньому сховане повідомлення, чи ні. Якщо в контейнері відсутнє сховане повідомлення, то завжди буде відновлюватися деяка випадкова послідовність. Якщо ця послідовність статистично не відрізняється від шифротексту криптосистеми з відкритим ключем, тоді в безпечній стегосистемі можна ховати отриманий у такий спосіб шифротекст.

У змішаних стегосистемах застосовуються, як правило, безключові стегосистеми з використанням особливостей криптосистем з відкритим і (або) секретним ключем.

В цілому більшість методів комп'ютерної стеганографії базується на двох принципах. Перший полягає в тому, що файли, що не вимагають абсолютної точності (наприклад, файли з зображенням, звуковою інформацією тощо), можуть бути до визначеного ступеня видозмінені без втрати функціональності. Другий принцип заснований на відсутності спеціального інструментарію або нездатності органів почуттів людини надійно розрізняти незначні зміни в таких вихідних файлах.

В основі базових підходів до реалізації методів комп'ютерної стеганографії в рамках того або іншого інформаційного середовища лежить виділення малозначимих фрагментів середовища і заміна існуючої в них інформації на інформацію, що передбачається захистити. Оскільки в комп'ютерній стеганографії розглядаються середовища, що підтримуються засобами обчислювальної техніки та відповідних мереж, то все інформаційне середовище, в остаточному підсумку, може представлятися в цифровому вигляді.

Таким чином, незначущі для кадру інформаційного середовища фрагменти відповідно до того або іншого алгоритму або методики заміняються (змішуються) на фрагменти приховуваної інформації. Під кадром інформаційного середовища в даному випадку мається на увазі деяка її частина, виділена по визначених ознаках. Такими ознаками часто бувають семантичні характеристики виділеної частини інформаційного середовища. Наприклад, як кадр може бути обраний деякий окремий малюнок, звуковий файл, «Web»-сторінка тощо.

За способом добору контейнера розрізняють методи сурогатної, селектив-

ної та конструюючої стеганографії.

У методах сурогатної (безальтернативної) стеганографії відсутня можливість вибору контейнера та для приховування повідомлення вибирається перший випадковий контейнер, найчастіше не зовсім підходящий до повідомлення, до якого він вбудовується. У цьому випадку, біти контейнера заміняються бітами приховуваного повідомлення таким чином, щоб ця зміна не була помітною. Основним недоліком методу є те, що він дозволяє сховати лише незначну кількість даних.

У методах селективної стеганографії передбачається, що заховане повідомлення повинне відтворювати спеціальні статистичні характеристики шуму контейнера. Для цього генерують велике число альтернативних контейнерів, щоб потім вибрати найбільш придатний із них для конкретного повідомлення. Часткою такого підходу є обчислення деякої хеш-функції для кожного контейнера. При цьому для приховування повідомлення вибирається той контейнер, хеш-функція якого збігається зі значенням хеш-функції повідомлення (тобто стеганограмою є обраний контейнер).

У методах конструюючої стеганографії контейнер генерується самою стегосистемою. Тут може бути декілька варіантів реалізації. Так, наприклад, шум контейнера може моделюватися приховуваним повідомленням. Це реалізується за допомогою процедур, які не тільки кодують приховуване повідомлення під шум, але й зберігають модель первісного шуму. У граничному випадку за моделлю шуму може будуватися ціле повідомлення.

По способі доступу до приховуваної інформації розрізняють методи для потокових (безперервних) контейнерів і методи для контейнерів з довільним доступом (обмеженої довжини).

Методи, що використовують потокові контейнери, працюють з потоками безперервних даних (наприклад, інтернет-телефонія). У цьому випадку приховувані біти необхідно в режимі реального часу включати в інформаційний потік. Про потоковий контейнер не можна попередньо сказати, коли він почнеться, коли закінчиться і наскільки тривалим він буде. Більш того, об'єктивно немає можливості довідатися заздалегідь, якими будуть наступні шумові біти. Найбільшу проблему при цьому складає синхронізація початку схованого повідомлення.

Методи, що використовуються для контейнерів із довільним доступом, призначені для роботи з файлами фіксованої довжини (текстова інформація, програми, графічні або звукові файли). У цьому випадку заздалегідь відомі розміри файлу і його вміст. Приховувані біти можуть бути рівномірно обрані за допомогою певної псевдовипадкової функції. Недолік таких контейнерів полягає в тому, що вони мають набагато менші розміри, ніж потокові, до того ж відстані між приховуваними бітами рівномірно розподілені між найбільш короткими та найбільш довгими заданими відстанями, у той час як шум буде мати експонентний розподіл довжин інтервалу. Перевага таких контейнерів полягає в тому, то вони можуть бути заздалегідь

оцінені з погляду ефективності обраного стеганографічного перетворення.

За типом організації контейнери, подібно завадозахищеним кодам, можуть бути систематичними та несистематичними. У систематично організованих контейнерах можна вказати конкретні місця стеганограми, де знаходяться інформаційні біти самого контейнера, а де – шумові біти, призначені для приховуваної інформації (як, наприклад, у широко розповсюдженому методі найменшого значущого біта). При несистематичній організації контейнера такого розподілу зробити не можна. У цьому випадку для виділення схованої інформації необхідно обробляти зміст усієї стеганограми.

Основним напрямком комп'ютерної стеганографії є використання властивостей надмірності інформаційного середовища. Варто врахувати, що при приховуванні інформації відбувається перекручування деяких статистичних властивостей середовища або порушення її структури, який необхідно враховувати для зменшення демаскуючих ознак. В особливу групу можна також виділити методи, що використовують спеціальні властивості форматів представлення файлів:

• зарезервовані для розширення полю комп'ютерних форматів файлів, що звичайно заповнюються нулями і не враховуються програмою;

• спеціальне форматування даних (зсув слів, пропозицій, абзаців або вибір визначених позицій букв);

• використання незадіяних місць на магнітних носіях;

• видалення ідентифікуючих заголовків для файлу.

В основному, для таких методів характерний низький ступінь скритності, низька пропускна здатність і слабка продуктивність.

За призначенням розрізняють стегометоди власне для скритої передачі або скритого збереження даних і методи для приховування даних у цифрових об'єктах з метою захисту самих цифрових об'єктів. За типом інформаційного середовища виділяються стегометоди для текстового середовища, для аудіосередовища, а також для зображень (стоп-кадрів) і відеосередовища.

Розвиток мультимедійних засобів супроводжується великим потоком графічної інформації в обчислювальних мережах. При генерації зображення, як правило, використовуються значна кількість елементарних графічних примітивів, що становить особливий інтерес для стегометодів захисту. Візуальне середовище (цифрові зображення та відео) мають велику надмірність різної природи:

• кодовою надмірністю, що виникає при неоптимальному описі зображення;

• міжпіксельною надмірністю, що обумовлена наявністю значної кореляційної залежності між пікселями реального зображення;

• психовізуальною залежністю, що виникає через те, що орган зору людини не адаптований для точного сприйняття зображення та сприймає кожну ділянку з різною чутливістю.

Інформаційним відеопотокам, що складаються з послідовності окремих кадрів зображення, крім зазначених вище, властива також надмірність, обумовлена інформаційною, технічною, тимчасовою та функціональною (значеннєвою) залежністю між кадрами.

Принцип стегометодів полягає в заміні надлишкової, малозначимої частини зображення бітами секретного повідомлення. Для витягу повідомлення необхідно знати місце, де була розміщена приховувана інформація. Найбільш розповсюдженим методом цього класу є метод заміни найменшого значущого біта (далі – НЗБ).

Популярність методу НЗБ обумовлена його простотою й тим, що він дозволяє ховати у відносно невеликих файлах досить великі обсяги інформації. Даний метод звичайно працює з растровими зображеннями, що представлені у форматі без стиску (наприклад, «GIF» і «BMP»). Основним його недоліком є сильна чутливість до найменших перекручувань контейнера. Для ослаблення цієї чутливості часто застосовують завадостійке кодування.

Суть методу НЗБ полягає в заміні найменш значущих бітів пікселів зображення бітами секретного повідомлення. У найпростішому випадку проводиться заміна НЗБ усіх послідовно розташованих пікселів зображення. Але оскільки довжина секретного повідомлення зазвичай менше кількості пікселів зображення, то після його впровадження в контейнері будуть дві ділянки з різними статистичними властивостями (ділянка, у якій незначні біти були змінені, і ділянка, у якій вони не змінювалися). Це може бути легко виявлене за допомогою статистичних тестів.

Для створення еквівалентної зміни ймовірності всього контейнера секретне повідомлення зазвичай доповнюють випадковими бітами таким чином, щоб його довжина в бітах дорівнювала кількості пікселів у вихідному зображенні.

Інший підхід, метод випадкового інтервалу, полягає у випадковому розподілі бітів секретного повідомлення у контейнері, в результаті чого відстань між двома вбудованими бітами визначається псевдовипадково. Ця методика найбільш ефективна при використанні потокових контейнерів (відео).

Для приховування даних можна також скористатися палітрою кольорів, що присутня у форматі зображення. У зображенні кожному пікселю привласнюється індекс у палітрі. Оскільки кольори в палітрі не завжди впорядковані, то приховувану інформацію можна кодувати послідовністю збереження кольорів у палітрі. Існує багато різних способів перестановки багатокольорової палітри, що цілком достатньо для приховування невеликого повідомлення.

У стеганографії застосовуються широкополосні методи, що ускладнюють виявлення схованих даних і їхнє видалення. Мета широкополосних методів збігається із завданням, що вирішує стегосистема: спробувати «розчинити» секретне повідомлення в контейнері та унеможливити його виявлення. Оскільки сигнали, розподілені по всій смузі спектра, важко видалити, стегометоди, побудовані на основі ши-

рокополосних методів, є стійкими до випадкових і навмисних перекручувань.

Основна перевага широкополосних стегометодів – це порівняно висока стійкість до перекручувань зображення та різного виду атакам, тому що прихована інформація розподілена в широкій смузі частот, і її важко видалити без повного руйнування контейнера.

Статистичні методи приховують інформацію шляхом зміни деяких статистичних властивостей зображення. Вони засновані на перевірці статистичних гіпотез. Суть методу полягає в такій зміні деяких статистичних характеристик контейнера, при якому одержувач зможе відрізнити модифіковане зображення від немодифікованого. Дані методи відносяться до «однобітових» схем, тобто орієнтовані на приховування одного біта секретної інформації.

Методи перекручування, на відміну від попередніх методів, вимагають знання про первісний вид контейнера. Схема приховування полягає в послідовному проведенні ряду модифікацій контейнера, що вибираються відповідно до секретного повідомлення. Для витягу схованих даних необхідно визначити всі розходження між стеганограмою та вихідним контейнером. За цими розходженнями відновлюється послідовність модифікацій, що виконувалася при приховуванні секретної інформації.

Методи перекручування легко застосовні до цифрових зображень. Як і в методах заміни, для приховування даних вибирається визначена кількість пікселів контейнера, що використовуються для приховування інформації. Такий вибір можна зробити, використовуючи датчик випадкових чисел (або перестановок).

Існує ще один підхід до реалізації методу перекручування зображення при приховуванні даних. Відповідно до даного методу при вставці приховуваних даних робиться спроба скоріше змінити порядок появи надлишкової інформації в контейнері, чим змінити його зміст. При приховуванні даних складається визначений «список пар» пікселів, для яких відмінність буде менше граничного. Цей список відіграває роль стегоключа – без нього не можна відновити секретне повідомлення. Якщо абонент має доступ до «списку пар», він завжди зможе провести зворотню процедуру.

Існує також стеганографічний метод, у якому приховування інформації проводиться на змістовному рівні з використанням структурних і інформаційних параметрів зображення. Суть методу полягає в проведенні послідовних перетворень фрагментів графічного зображення, що за остаточним підсумком приводить до формування прихованого тексту.

У даний час з'явилося безліч графічних пакетів програм і баз даних, за допомогою яких можна створювати різні графічні зображення, презентації, мультиплікацію тощо. У кожному графічному зображенні можна виділити окремі компоненти, що відповідно до його сфери інтерпретації мають своє інформаційне навантаження. Візуальний образ можна подати у вигляді цифрової послідовності, що потім легко перетвориться в текстове повідомлення. Це можливо, наприклад, у процесі покрит-

тя образа деяким графом, використовуючи інформаційну інтерпретацію його окремих компонентів. У першому наближенні вершинами такого графа можуть служити окремі компоненти малюнка, а ребрами – з'єднання.

Особливий розвиток мають методи цифрової стеганографії в аудіосередовищі. За їхньою допомогою забезпечується пересилання великих обсягів схованих даних у звукових повідомленнях, що транслюються по телевізійній, телефонній або радіомережі. Сучасні засоби телекомунікації дозволяють передавати звукові сигнали не тільки в реальному часі, але й у цифровому форматі через будь-яку мережу передачі даних.

Відомо, що слуховий апарат людини функціонує в широкому динамічному діапазоні. Він дуже чуттєвий до випадкових перешкод і здатний розрізняти відносну фазу, але зовсім нечутливий до абсолютної фази. Ці особливості слухового апарата дозволяють удало використовувати стегометоди в аудіосередовищі.

Метод НЗБ застосовується при цифровому поданні аудіосигналу та придатний для використання при будь-яких швидкостях зв'язку. При перетворенні звукового сигналу в цифрову форму завжди присутній шум дискретизації, що не вносить істотних перекручувань. «Шумовим» бітам відповідають молодші біти цифрового подання сигналу, які можна замінити прихованими даними. Наприклад, якщо звуковий сигнал представлений у 16-бітовому вигляді, то зміна чотирьох молодших бітів не приведе до помітного на слух перекручування. У якості стегоключа зазвичай використовується покажчик місця розташування бітів, у яких утримуються приховані дані.

Методи широкополосного кодування використовують ті ж принципи, що й методи приховування даних у зображеннях. Їхня суть полягає в незначній одночасній модифікації цілого ряду визначених бітів контейнера при приховуванні одного біта інформації. Ховати дані можна також шляхом упровадження луни в звуковий сигнал, оскільки при невеликих тимчасових зрушеннях луна-сигнал практично не розрізняється на слух.

Фазові методи приховування застосовуються як для аналогового, так і для цифрового сигналу. Вони використовують той факт, що плавну зміну фази на слух визначити не можна. У таких методах дані, що захищаються, кодуються або визначеним значенням фази, або зміною фаз у спектрі. Якщо поділити звуковий сигнал на сегменти, то дані зазвичай ховають тільки в першому сегменті при дотриманні двох умов:

- прихованість відносних фаз між послідовними сегментами;
- результуючий фазовий спектр стегосигналу повинен бути гладким, оскільки різкі стрибки фази є демаскуючим чинником.

Музичні стегосистеми забезпечують приховування інформації в музичному середовищі за аналогією з імпровізацією музичних творів. Імпровізація являє собою таку зміну музичного твору або його фрагментів, що зберігає основні теми первісного твору у вигляді мелодій, але при цьому розширює образ музичної теми іншими,

що доповнюють основний образ рисами, яких не було в основному музичному творі.

Основна відмінність музичної стеганографії від імпровізації полягає в тому, що метою є не розширення образів базового музичного твору, а внесення змін, що зберігають мелодію основного твору, відповідають усім правилам побудови даного твору та при цьому кодують приховане повідомлення, не спотворюючи головної теми твору.

На першому етапі роботи стегосистеми аналізується кількість мелодій (кількість її модифікацій) у рамках музичного твору в зіставленні з кількістю пропозицій повідомлення. На другому етапі здійснюється аналіз допустимості розширення деякої пропозиції музичного твору пропозиціями тексту повідомлення.

На наступному етапі здійснюється аналіз наступності фраз мелодій, окремих слів тексту та слів мелодії. Після позитивного вирішення завдань перерахованих рівнів формується нотне відображення розширеного музичного твору з впровадженим у нього прихованим повідомленням. На підставі нотного відображення розширення здійснюється його музична реалізація за допомогою сучасних комп'ютерних систем, що являють собою програмно-апаратні синтезатори звуку.

Подальша звукова обробка музичних записів, оброблених стегосистемою, не обов'язкова. Оскільки основна сфера застосування музичних стегосистем – це середовище «*Internet*», у якій музичні записи розміщаються в цифровому форматі на «*Web*»-сторінках, то досить, щоб розширений музичний твір сприймався сторонніми особами не як шум, а як певна музика, що має мелодію або сукупністю мелодій, що допускають ту або іншу тематичну інтерпретацію.

На завершення відзначимо, що саме цифровою стеганографією користуються міжнародні терористи для спілкування між собою та планування терактів. Так, стаття в газеті «*USA Today*» від 5 лютого 2001 року повідомляла про офіційну заяву американських і іноземних урядових чиновників про те, що «бен Ладен, обвинувачуваний в організації вибухів двох американських посольств у Східній Африці, так само як і інші терористи ховають фотографії та карти намічених цілей разом із відповідними інструкціями своїм соратникам у спортивних чатах, на порнографічних сайтах та інших ресурсах мережі Інтернет».

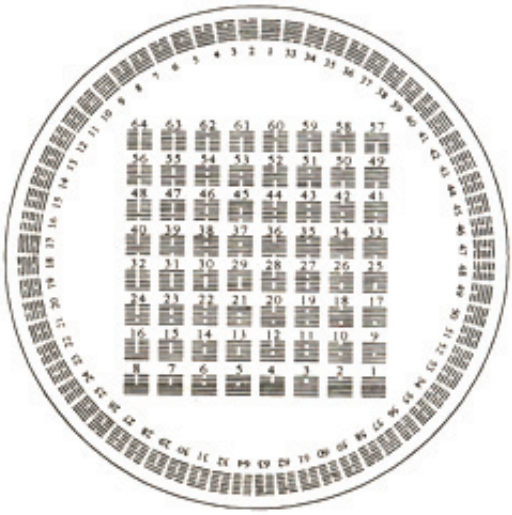
Виявлення повідомлень, захованих за допомогою цифрової стеганографії, – це серйозне технічне завдання для правоохоронних органів, що намагаються вистежити в такий спосіб терористів. При формуванні державного бюджету на кожний фінансовий рік ФБР США надає запит щодо збільшення асигнувань на вивчення нових технологій, які використовуються терористами.

ПІСЛЯМОВА

Ознайомившись з історією стеганографії та криптології – систем знань про тайнопис та способи його прочитання, доходиш висновку, що з огляду на експонентний ріст швидкостей обчислень та імовірність появи штучного інтелекту, потрібно бути в курсі її принципів та сучасних досягнень. Оскільки не виключено, що якщо не завтра, то вже післязавтра обов'язково наші комп'ютери будуть спілкуватися один з одним лише за допомогою цифрових «заклинань», недоступних людському розумінню.

Криптологія стає звичайною справою, і з розширенням сфери її застосування (ЕЦП, конфіденційність, ідентифікація, автентифікація, підтвердження вірогідності та цілісності електронних документів, безпека електронного бізнесу тощо) буде зростати і її роль. Усім нам треба цікавитися криптологією, тому що в майбутньому вона стане «третьою грамотою» нарівні з «другою грамотою» – володінням комп'ютером й інформаційними технологіями. До речі, ще в документах древніх цивілізацій говорилося, що тайнопис є одним із 64-х мистецтв, яким варто володіти як чоловікам, так і жінкам.

Цікаво, що давньокитайська «Книга змін» (І-цзин), поява якої датується 3-м тисячоліттям до н.е., описує природний хід будь-яких подій через послідовність 64 гексаграм - символів, що складаються з 6 ліній (суцільних або розірваних). «І-цзин» є одним з кращих в історії людства прикладів тайнопису з використанням двійкового кодування - універсальної системи зберігання інформації. Гексаграма - це типовий приклад 1 байту інформації, що зберігається за допомогою бінарного коду - суцільних і розірваних ліній - інформаційних бітів. До речі, перші комп'ютери працювали в 6-розрядній операційній системі, де 1 байт складався з 6 бітів - так само, як 1 гексаграма складається з послідовності 6 суцільних або розірваних ліній. Лише пізніше з'явились комп'ютери, що працюють з «октетом» - 8-бітовим байтом, який дозволяє використовувати не 64, а 256



комбінацій байтів для запису інформаційного потоку.

Взагалі двійковий код лежить в основі природного сприйняття навколишньої реальності, яка має полюси - крайності. Чоловіче – жіноче, світле – темне, гаряче – холодне, день – ніч, літо – зима, північ – південь, так - ні та інші протилежності закодовані в базовій системі часових і просторових координат. Дуалізм життя допомагає структурувати потік всієї інформації, що обрушується на людину. Яке би поняття або явище ми не розглядали, майже все можна звести до набору протилежностей та записати як двійковий код, прикладом чого є комп'ютер, який може містити величезну кількість інформації, зведеної до послідовності одиниць і нулів - інформаційних бітів.

Американський скульптор Джеймс Сенборн віддав належне історичній важливості тайнопису, створивши дві своєрідні зашифровані скульптури на честь криптології. Перша, відома під назвою «Кріптос» (англ. *Kryptos*), була відкрита 3 листопада 1990 року перед штаб-квартирою ЦРУ в Ленглі, штат Віргінія. Центральним її елементом є зігнутий у вигляді латинської букви «*S*» мідний сувій, прикріплений до окам'янілого дерева. Сувій має висоту 3 метри, а на обох боках його висічений зашифрований текст - всього трохи більше 1800 знаків. Починаючи з моменту відкриття скульптури, навколо неї постійно ходять дискусії про розгадку зашифрованого повідомлення.

Скульптура продовжує створювати безліч розбіжностей службовцями ЦРУ і криптоаналітиками, що намагаються розшифрувати шифр. Не дивлячись на те, що з моменту установки пройшло більше 20 років, текст послання все ще далекий від розшифрування. Світова спільнота криптоаналітиків, нарівні з працівниками ЦРУ і ФБР, за весь цей час змогли розшифрувати тільки перші 3 секції. До цього часу не розшифрованими залишаються 97 символів останньої частини (відомою як К4). Четверта частина, що залишилася, є однією з найвідоміших у світі нерозгаданих проблем.

Друга скульптура Сенборна під назвою «Кирилічний проектор» (англ. *Cyrillic Projector*), значно менш відома, була споруджена на основі букв кирилиці та знайшла свій постійний притулок лише у 1997 році, в Університеті штату Північна Кароліна.

Композиція є порожнистим бронзовим циліндром діаметром півтора і заввишки близько трьох метрів. У металі прорізані сотні крізних букв шифру, та ночами яскравий світильник усередині циліндра проектує букви на мостову і стіни довколишніх будинків.

До розшифрування написів «кирилічного проектора» справа дійшла лише в травні 2003 року. Тоді таємною скульптурою зацікавилася міжнародна група любителів криптографії, об'єднуюча більше 70 осіб з різних країн світу. Шифр, треба сказати, був вибраний скульптором нескладний, і розкрили його досить легко. Ну а прочитані російські написи, як виявилось, є фрагментами двох розсекречених на початку 1990-х років документів КДБ СРСР.

У одному мовиться про те, що радянський академік Сахаров підготував звернення до учасників Пагуошської конференції світових вчених і що «прийнятими заходами спланована супротивником ворожа антирадянська акція була зірвана». Інший напис є цитатою чи то з секретного підручника, чи то з якоїсь інструкції КДБ по роботі з джерелами інформації: «Високим мистецтвом в секретній розвідці вважається здатність розробити джерело, яке ти контролюватимеш і яким цілком розпоряджатимешся. Таке джерело, як правило, поставляє найнадійнішу інформацію». Далі мовиться, що знайти таке джерело і встановити над ним повний психологічний контроль - справа непроста. Але вже коли ти цього добився, то тебе чекають «підвищення по службі та зростання авторитету серед колег».

Крім того, увійшовши у величезний будинок ЦРУ, відвідувач через декілька кроків бачить біблейські слова (Іоанн 8:32), вищерблені в мармурі головного холу: «І та узрішь ти істину, і істина зробить тебе вільним» (англ. *And ye shall know the*

truth, and the truth shall make you free). Цей напис можна трактувати, мабуть, і так: хто скоріше перехопить та розшифрує повідомлення (тобто, знання) супротивника, той першим отримає важливу інформацію (тобто, істину) для прийняття правильного рішення в інформаційній війні, яка постійно триває між нами та «ними». В результаті перший буде перемагати і мати право керувати обставинами та вирішувати долю супротивника, тобто переможець стане незалежним від нього і таким чином стане вільним.

Така інформаційна перевага, яку забезпечує потужна криптослужба, дає змогу правильно реагувати на будь-які події та випереджати дії супротивника, тобто «володіти» ситуацією. Тому держава, яка не шкодує витрат на шифрувально-дешифрувальну службу, завжди буде стійкою до політичного «тиску» інших країн, тобто незалежною та вільною у своїх діях, що завжди веде до перемоги у політичних «війнах».

Разом з тим, якщо ми обернемо свій погляд на природу, то при створенні живих і неживих істот ми побачимо присутність процесів, що відбуваються за схожею з криптографією логікою шифрування. Як приклад можна привести виробництво білків у результаті розшифрування нуклеїнових кислот (ДНК, РНК), що містять зашифровані (крипто) повідомлення генетичних даних, в рибосомах (органи синтезу білків).

У закодованих в ДНК шифрах і шифруванні, що проводиться під час доставки необхідній інформації в рибосоми для синтезу білків за зашифрованою інформацією, захована велика мудрість і глибокий сенс. Якщо порівняти молекули ДНК, яка утворює геном живої істоти, з книгою, то можна позначити написані в книзі букви такими символами, як A, T, G, C. Ця символічна мова з хімічних молекул чотирьох видів використовується в шифруванні генетичної програми, яка визначає основну модель і форму живого організму.

Геном кожного живого організму є сукупністю цих букв, написаних в різних числах усередині певної програми. Наприклад, якщо число букв в геномах людини і миші приблизно рівне 3 мільярдам, то число букв в геномі одного виду бактерій складає приблизно 4-5 мільйонів. Якщо дивитися в загальному порядку, не дивлячись на те, що різниця комбінацій між рядами геномів двох людей складає тільки один відсоток, то за зовнішнім виглядом чоловік не схожий ні на одну іншу людину.

Кількість генів в людині і тваринах демонструє

цікаві зміни. Багаті шифрувальні технології, які використовуються в ДНК, є основним біологічним механізмом, задіяним як завіса при утворенні генетичного різновиду в живих організмах. Програмна книжка, звана геномом, в описуваних у «Святих Писань» рамках є зразком книги уселенських законів на цьому світі. Ідентичність в живих організмах, з багатьох точок зору, алфавіту, загальних правил побудови пропозиції і функціонування, які використовуються в шифруванні програми, розміщеної в клітках живих організмів для отримання ними життя та її продовження, показує, що всі вони вийшли з-під однієї руки. При утворенні білків ми також стаємо свідками певного шифрування, яке служить приводом для передачі правильного повідомлення рибосомі під час перенесення зареєстрованих кодів у ДНК в рибосоми.

Розвиток криптології, як науки, не обмежується тільки забезпеченням конфіденційності інформації, воно також допомагає зрозуміти функціонування божественних процесів у світі живих істот. Шифрування в ДНК за допомогою системи 4-х букв, правильне розшифрування цієї зашифрованої інформації клітки та проведення відповідних до цього розшифрування синтезів інформації, які послужили приводом для забезпечення різноманітності в живих істотах, показує, що всі творіння Небесного Творця, безперечно, несуть в собі дуже глибокий сенс.

В результаті, у світлі божественних заяв «Святих Писань», ми повинні створити ідейну платформу для роздумів на основі цієї уселенської книги та її безкрайніх знань...

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Антонов В., Карпов В. Тайные информаторы Кремля. Нелегалы. М., 2002.
2. Бабаш А., Баранова Е. Специальные методы криптографической деятельности после второй мировой войны // Технологии техносферной безопасности № 4 (38). 2011.
3. Бабаш А., Шанкин Г. История криптографии. Часть I. М., 2002.
4. Бабаш А., Шанкин Г. Криптография. Аспекты защиты. М., 2002.
5. Бабаш А., Гольев Ю., Ларин Д., Шанкин Г. О развитии криптографии в XIX веке // Защита информации. Конфидент № 5. 2003.
6. Бабаш А., Гольев Ю., Ларин Д., Шанкин Г. Криптографические идеи XIX века // Защита информации. Конфидент № 1. 2004.
7. Бабаш А., Гольев Ю., Ларин Д., Шанкин Г. Криптографические идеи XIX века. Русская Криптография // Защита информации. Конфидент № 3. 2004.
8. Бабаш А., Гольев Ю., Ларин Д., Шанкин Г. Шифры революционного подполья России XIX века. // Защита информации. Конфидент. № 4. 2004.
9. Бабаш А., Гольев Ю., Ларин Д., Шанкин Г. Криптография в XIX веке // Информатика № 33 (466). М., 2004.
10. Батюшин Н. Тайная военная разведка и борьба с ней. София, 1939.
11. Берд Киви. Книга о странном. М., 2003.
12. Блоч Дж., Фитцджеральд П. Тайные операции английской разведки. М., 1987.
13. Бэмфорд Д. Дворец загадок. М., 1999.
14. Бобылев П., Алябьев А. Защита цифровой информации методами стеганографии. Тамбов, 2005.
15. Бутырский Л., Гольев Ю., Ларин Д., Никонов Н., Шанкин Г. Криптографическая деятельность в Швеции. От викингов до Хагелина // Защита информации. INSIDE.
16. Волкова Ю. Алхимия защиты // CIO № 9 від 20.09.2004.
17. Воронин П. Воспоминания // Электросвязь № 3. 1995.
18. Габис С. Тайна «Магдебурга». Морской исторический сборник. Выпуск 2. СПб., 1991.
19. Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Криптографическая деятельность в период наполеоновских войн // Защита информации. Конфидент № 5. 2004.
20. Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Криптографическая деятельность в США XVIII-XIX веков // Защита информации. Конфидент № 6. 2004.
21. Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Научно-технический прогресс и криптографическая деятельность в России XIX века. // Защита информации. INSIDE № 2. 2005.

22. Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Начало войны в эфире // Защита информации. INSIDE № 3. 2005.
23. Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Криптографическая деятельность во время гражданской войны в России // Защита информации. INSIDE № 4. 2005.
24. Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Криптографическая деятельность революционеров в 20-х - 70-х годах XIX века в России: успехи и неудачи // Защита информации. INSIDE № 5. 2005.
25. Гольев Ю., Ларин Д., Шанкин Г. Криптографическая деятельность организаций «Земля и Воля» и «Народная Воля» в России в 1876-1881 годах // Защита информации. INSIDE № 6. 2005.
26. Гольев Ю., Ларин Д., Шанкин Г. Криптографическая деятельность революционеров в России. 1881-1887 годы: агония «Народной Воли» // Защита информации. INSIDE № 2. 2006.
27. Гольев Ю., Ларин Д., Шанкин Г. Криптографическая деятельность революционеров в России в 90-е годы XIX века: // Защита информации. INSIDE № 4. 2006.
28. Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Служба наблюдения Кригсмарине // Защита информации. INSIDE № 5, № 6. 2006.
29. Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Криптография. Страницы истории тайных операций. М., 2008.
30. Горбовский А. Загадки древнейшей истории. М., 1971.
31. Дело Старовойтова - Монастырецкого // Московский комсомолец. 14.04.1998.
32. Джеймс П., Торп Н. Тексты с тайным смыслом. 2004.
33. Жельников В. Криптография от папируса до компьютера. М., 1997.
34. Жигадло В. Телекоммуникационные сети военного назначения США и стран НАТО.
35. Зданович А., Измозик В. Сорок лет на секретной службе. Жизнь и приключения Владимира Кривоша. М., 2007.
36. Зелинский Ф. Сказочная древность Эллады. М., 1993.
37. Зима И. Расшифрованный Нострадамус. М., 1988.
38. Ильинский М. Тайны спецсвязи Сталина. М., 2004.
39. Исаев П. Некоторые алгоритмы ручного шифрования.
40. Калачёв К. В круге третьем (Воспоминания и размышления о работе Марфинской лаборатории в 1948-1951 годах). М., 1999.
41. Кан Д. Взломщики кодов. М., 2000.
42. Кан Д. Война кодов и шифров. История 4 тысячелетий криптографии. М., 2004.
43. Карпов Е. Углов А.Т. - радиоинженер, изобретатель, организатор.
44. Карпов М. Из фронтового блокнота.
45. Клепов А. Информационное оружие Гитлера. Информационное оружие Сталина.

46. Кузьмин Л. Не забывать своих героев // Защита информации. Конфидент № 1. 1998.
47. Кузьмин Л. ГУСС - этап в развитии советской криптографии // Защита информации. Конфидент № 4. 1998.
48. Кулинченко В. Русские против «Энигмы».
49. Куприянов А. IT&WWII.
50. Лайнер Л. Погоня за «Энигмой». Как был взломан немецкий шифр. М., 2004.
51. Лайнер Л. «Венона». Самая секретная операция американских спецслужб. М.,2006.
52. Ландер И. Негласные войны. История специальных служб. 1919-1945.
53. Ларин Д., Шанкин Г. Вторая мировая война в эфире: Некоторые аспекты операции «Ультра» // Защита информации. INSIDE № 1. 2007.
54. Лебедев А. Кому нужны «шифровальные средства».
55. Лекарев С., Порк В. Радиоэлектронный щит и меч. М., 2001.
56. Лота В. Секретный фронт Генерального штаба.
57. Лурье В., Кочик В. ГРУ: дела и люди. СПб., 2002.
58. Маклахлан Д. Тайны английской разведки (1939-1945). М., 1971.
59. Масленников М. Криптография и свобода.
60. Мозохин О., Гузо Л., Бычков В., Тертичко В. Спецтехника на защите государства. М., 2004.
61. Новик В. Франц Эпинус (краткая биографическая хроника, 1724-1802).
62. Окіпнюк В. Правові основи забезпечення режиму таємності органами ДПУ-УСРР. Київ.
63. Примаков Е., Лебедев С. Очерки истории внешней разведки в 5 томах. М., 1999.
64. Павлов В. Астрахан В., Чернега В., Чернявский Б. Правительственная электросвязь в истории России (1917-1945 гг.). М., 2001.
65. Павлов В. Сезам, откройся! Тайные разведывательные операции: Из воспоминаний ветерана внешней разведки. М., 1999.
66. Пестриков В. Искровые радиостанции Российской империи.
67. Первушин А. Оккультные тайны НКВД и СС. М., 2004.
68. Петров Н., Скоркин К. Кто руководил НКВД. 1934-1941. Справочник. М., 1999.
69. Петров Н., Кокурин А. Лубянка. Органы ВЧК-ОГПУ-НКВД-НКГБ-МГБ-МВД-КГБ. 1917-1991. Справочник. М., 2003.
70. Петров Н. Кто руководил органами госбезопасности. 1941-1954. Справочник. М., 2010.
71. Петров Н. Американская сеть «Эшелон» как угроза национальной безопасности России.
72. Полмар Н., Аллен Т. Энциклопедия шпионажа. М., 1999.

73. Пыхалов И. Агентство национальной безопасности (АНБ).
74. Риксон Ф. Коды, шифры, сигналы и тайная передача информации. М., 2011.
75. Рузайкин Г. Тайны Марфинской обители.
76. Саломаа А. Криптография с открытым ключом. М., 1995.
77. Семёнов В. К истории создания шифровальной службы в МИД России // Дипломатический вестник. 2001.
78. Сингх С. Книга шифров: тайная история шифров и их расшифровки. – М., 2007.
79. Синельников А. Шифры и революционеры России // www.cryptography.ru.
80. Соболева Т. Тайнопись в истории России. М., 1994.
81. Соболева Т. История шифровального дела в России. М., 2002.
82. Стефанович А. Засекреченная радиотелефонная связь США: история.
83. Стефанович А. История создания и становления Агентства безопасности связи Армии США (1914-1945 гг.) // www.ssl.stu.neva.ru.
84. Стефанович А. История успехов и неудач шведской радиоразведки (1914 – 1944 гг.) // www.agentura.ru.
85. Сумской А. «Энигма» и другие загадки противников и союзников.
86. Уинтерботем Ф. Операция «Ультра». М., 1978.
87. Ульфкотте У. Совершенно секретно: БНД. За кулисами Федеральной разведывательной службы Германии.
88. Фоменков Г. Криптокарта FORTEZZA – правительственные технологии в коммерческих приложениях.
89. Фролов Г. Тайна тайнописи. М., 1992.
90. Черкашин Н. Секретный кабель через два моря.
91. Черняк Е. Пять столетий тайной войны. М., 1991.
92. Чертопруд С. Американские субмарины – охотники за советскими военными сокровищами.
93. Чертопруд С. Говорите громче, вас плохо слышно. Организация системы шифровальной связи в Советском Союзе в период гражданской войны.
94. Черчхаус Р. Коды и шифры. Юлий Цезарь, «Энигма» и Интернет. М., 2005.
95. Циммерман Ф. Введение в криптографию.
96. Цыркун С. Весенние ночи 1937 года.
97. Хорошко В., Азаров О., Шелест М., Яремчук Ю. Основи комп'ютерної стеганографії. Вінниця, 2003.
98. Шелков В. История «микроточки». Кит Мэлтон и его музей «шпионской техники».
99. Эрли П. Семья шпионов. М., 1997.
100. Эндрю К., Гордиевский О. КГБ: История внешнеполитических операций от Ленина до Горбачёва. М., 1992.

ВИКОРИСТАНІ ВЕБ-СТОРІНКИ:

1. АНБ США // www.nsa.gov
2. Великие операции спецслужб // http://greatoperation.narod.ru
3. Виртуальный компьютерный музей http://www.computer-museum.ru
4. Госспецсвязи Украины // www.dsszzi.gov.ua
5. ЗАС и шифрослужба // http://scz.bplaced.net (нем.)
6. История Блетчли Парка // www.bletchleypark.org.uk
7. История отечественных спецслужб // http://shieldandsword.mozohin.ru
8. История криптографии и криптоанализа // http://crypto.hotbox.ru
9. Книга Памяти // http://www.uznal.org/book_of_memory
10. Криптомашины // http://jproc.ca/crypto
11. Криптомузей // www.cryptomuseum.com
12. История МВД России // http://mvd.ru/mvd/history
13. Музей телеграфной техники // http://w1tp.com
14. Проект «Агентура» // www.agentura.ru
15. Проект «Чекист» // www.chekist.ru
16. Разведка и контрразведка в лицах // http://rusrazvedka.narod.ru
17. История Спецсвязи ФСО России // www.fso.gov.ru/struktura/p2_1_2.html
18. ФСБ России // www.fsb.ru
19. ШКПС Великобритании // www.gchq.gov.uk
20. Центр генеалогических исследований // http://rosgenea.ru
21. Энциклопедия «ВикипедиЯ» // http://ru.wikipedia.org
22. Энциклопедия «Кругосвет» // www.krugosvet.ru/

РЕКОМЕНДОВАНІ ФІЛЬМИ

Документальні

1. Взломщики кодов. США, 2009.
2. Взломщики кодов: Забытые герои Блетчли Парка. Великобритания, 2011.
3. Гении и злодеи уходящей эпохи: Алан Тьюринг. Россия, 2007.
4. Германские субмарины: Морские волки. Железные гробы. Канада, 1997.
5. Две жизни Джорджа Блейка. Россия, 2012.
6. Дуэль разведок: Россия - Великобритания. Россия - США. Росія, 2005.
7. Живая история: Война дефекторов. Шпионы подземелья. Росія, 2009.
8. Документальное расследование: ФАПСИ. Росія, 1997.
9. Засекреченная любовь: Серебряная роза – Судьба нелегала. Росія, 2008.
10. Код Верченко. Росія, 2007.
11. Код Войнича. Самый загадочный манускрипт. Німеччина, 2010.
12. Кремль-9: Спецсвязь. Росія, 2009.
13. Найти и обезвредить: Кроты. Россия, 2012.
14. Открытая закрытая связь. Беларусь, 2006.
15. Секретная война: Всё ещё тайна. Англія, 1977.
16. Секреты второй мировой войны: Расшифровка кода «Энигма». Великобританія, 2003.
17. Тайны войны: Загадка японского кода. Загадка Роммеля. Оборона Британии. Уловки дня «Д». Холодная война. Великобританія, 1998-2002.
18. Тайны века: Зашифрованная война. Росія, 2003.
19. Шпионы и предатели: Берлинский туннель. Красные яблоки для Уокера. Последний из «Кембриджской пятёрки». Росія, 2008.
20. Breaking The Codes. Великобританія, 2009.
21. Decoding Nazi Secrets. Великобританія, 1999.
22. Secrets of War: Intelligence (The Ultra Enigma). США, 1998.
23. Secrets of World War II: The Enigma Secret. Великобританія, 1998.
24. Station X: 1. The keys to the reich. 2. The goose, that laid the golden eggs. 3. The Ultra secret. 4. The war of the machines. Великобританія, 1996.

Художні

1. В круге первом. Росія, 2010.
2. Говорящие с ветром. США, 2002.
3. Код убийства. Великобританія, 2012.
4. Мидуэй. США, 1976.
5 Подлодка U-571. США, 2000.
6. Поединки: Вербовщик. Выбор агента Блейка. Росія, 2011.
7. Смертельная схватка. Росія, 2010.
8. Тайна секретного бастиона. Польща, 2007.
9. Тайна шифра. Румунія, 1959.
10. Энигма. Франція, Великобританія, 1983.
11. Энигма. Великобританія, Німеччина, США, 2001.
12. Breaking the code. Великобританія, 1996.
13. Family of spies. США, 1990.
14. Sekret Enigmy. Польща, 1979.

З фільмами та іншими матеріалами з історії криптології та спеціальних видів зв'язку можна ознайомитись на офіційному сайті книги:
www.cryptohistory.ru

Науково-популярне видання

Гребенніков В.В.

ІСТОРІЯ КРИПТОЛОГІЇ & СЕКРЕТНОГО ЗВ'ЯЗКУ

**Видання друге,
виправлене,
доповнене,
ілюстроване**

Гребенніков В.В.

Г 79 Історія криптології & секретного зв'язку

Книга написана ветераном Державної служби спеціального зв'язку та захисту інформації України полковником Держспецзв'язку Гребенніковим Вадимом Вікторовичем, Головою Ради ветеранів Закарпатської обласної організації ветеранів урядового зв'язку, відміченим державною нагородою «За бездоганну службу» та багатьма відомчими нагородами, зокрема: «Хрестом заслуги».

У виданні розповідається про історію народження й розвитку криптології та стеганографії, спеціальних видів засекреченого зв'язку у провідних країнах світу (СРСР, США, Великобританія, Німеччина), утворення їхніх криптологічних служб та апаратури засекречування, «шпіонську» діяльність спецслужб СРСР і США та їхню боротьбу у «полюванні» за шифрами супротивника, а також сучасний стан криптології у світі.

Книга побудована виключно на відкритих матеріалах, зібраних автором із надрукованих книг та мережі Інтернет.

Офіційна веб-сторінка книги: *www.cryptohistory.ru*

ББК 32.811.4
УДК 519.711