МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАТИКИ ТА ФІЗИКО-МАТЕМАТИЧНИХ ДИСЦИПЛІН

МЕТОДИЧНІ ВКАЗІВКИ

для виконання практичних робіт

з дисципліни

«БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ»

для студентів спеціальності

126 «Інформаційні системи та технології»

Ужгород – 2025

УДК 004.056/.5(076.5)(075.8)
Б 39

Безпека інформаційних систем: методичні вказівки до виконання практичних робіт для здобувачів другого (магістерського) рівня вищої освіти, спеціальності 126 Інформаційні системи та технології факультету інформаційних технологій УжНУ / Укладачі: д.т.н., доц. І.М. Лях, ст. викл. Н.Я. Шумило, асистент П.В. Яворський. Ужгород: УжНУ, 2025. 48 с.

У методичних вказівках до виконання практичних робіт з курсу «Безпека інформаційних систем» сформульовано теми завдань до виконання практичних робіт, вимоги до порядку виконання та змісту звіту по проробленій роботі. Також наведена програма навчальної дисципліни та перелік контрольних запитань на підсумковий контроль.

Укладачі: Лях І.М. – д.т.н., доцент, професор кафедри інформатики та фізико-математичних дисциплін факультету інформаційних технологій ДВНЗ «УжНУ»;

Шумило Н.Я. – ст. викладач кафедри інформатики та фізико-математичних дисциплін факультету інформаційних технологій ДВНЗ «УжНУ»;

Яворський П.В. – асистент кафедри інформатики та фізико-математичних дисциплін факультету інформаційних технологій ДВНЗ «УжНУ».

Рецензенти:

д.т.н., проф., завідувач кафедри інформаційних управляючих систем та технологій ДВНЗ «УжНУ» Міца О.В.;

д.т.н., проф., професор кафедри програмного забезпечення систем ДВНЗ «УжНУ» Поліщук В.В.

Рекомендовано кафедрою інформатики та фізико-математичних дисциплін від «27» січня 2025 р., протокол №8.

Розглянуто і схвалено науково-методичною комісією факультету інформаційних технологій УжНУ. Протокол №5 від 28.01.2025 р.

ЗМІСТ

ВСТУП

Актуальність вивчення дисципліни **«Безпека інформаційних систем»** є надзвичайно високою в умовах сучасного інформаційного суспільства, де інформація та інформаційні технології стали важливими ресурсами для розвитку економіки, науки, бізнесу та повсякденного життя.

Метою вивчення навчальної дисципліни **«Безпека інформаційних систем»** є формування компетентностей щодо засвоєння основних способів захисту конфіденційної інформації, протидіїнесанкціонованому доступу на прикладі послуг безпеки в інформаційних системах, грамотного застосування механізмів захисту інформації на основі сучасних процедур криптосистем для забезпечення доступності, цілісності, конфіденційності, автентичності транзакцій та даних.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ІНТ. Здатність розв’язувати задачі дослідницького та інноваційного характеру у сфері інформаційних систем та технологій.

ФК 1. Здатність розробляти та застосувати ІСТ, необхідні для розв’язання стратегічних і поточних задач.

ФК 6. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.

Програма навчальної дисципліни

Змістовий модуль 1.

Тема 1. Захист інформації в каналах зв’язку.

Тема 2. Засоби несанкціонованого доступу до інформації.

Тема 3. Виявлення несанкціонованих засобів доступу до інформації.

Тема 4. Методи боротьби ВОЛЗ.

Тема 5. Інформаційна безпека в мережах коміркового зв’язку.

Тема 6. Захист від несанкціонованого доступу мережі GSM.

Тема 7. Захист від прослуховування.

Тема 8. Конфіденційність локалізації абонента.

Змістовий модуль 2.

Тема 9. Види комп’ютерних мереж та їх основи функціонування.

Тема 10. Інциденти інформаційної безпеки.

Тема 11. Принципи організації безпеки комп’ютерних мереж.

Тема 12. Методи та засоби забезпечення вимог політики безпеки.

Тема 13. Види атак на інформаційні та програмно-технічні ресурси.

Тема 14. Виявлення атак на ресурси комп’ютерної мережі.

Тема 15. Захист приватної мережі від зовнішнього втручання.

Тема 16. Особливості забезпечення безпеки корпоративних мереж.

Самостійна робота

№ п/п	Назва теми
1.	Захист інформації в каналах зв’язку
2.	Засоби несанкціонованого доступу до інформації
3.	Виявлення несанкціонованих засобів доступу до інформації
4.	Методи боротьби ВОЛЗ
5.	Інформаційна безпека в мережах коміркового зв’язку
6.	Захист від несанкціонованого доступу мережі GSM
7.	Захист від прослуховування
8.	Конфіденційність локалізації абонента
9.	Види комп’ютерних мереж та їх основи функціонування
10.	Інциденти інформаційної безпеки
11.	Принципи організації безпеки комп’ютерних мереж
12.	Методи та засоби забезпечення вимог політики безпеки
13.	Види атак на інформаційні та програмно-технічні ресурси
14.	Виявлення атак на ресурси комп’ютерної мережі
15.	Захист приватної мережі від зовнішнього втручання
16.	Особливості забезпечення безпеки корпоративних мереж

Практична робота № 1.

Робота з обліковими записами користувачів і груп ОС Windows Server. Встановлення правил доступу до об’єктів файлової системи

Навчальна мета: Формування навичок створення та редагування облікових записів користувачів у Windows Server. Опанування змінення власників і налаштування прав доступу до об'єктів файлової системи для їхнього захисту (файлів, процесів).

Виховна мета: Формування відповідального ставлення до навчання та праці, розвиток інтелектуальних здібностей, моральних якостей, прагнення до самовдосконалення та розкриття індивідуального потенціалу.

Завдання:

1. Дослідити необхідність створення облікових записів користувачів із відповідними правами безпеки.
2. Створювати та редагувати облікові записи користувачів. Використовувати диспетчер завдань для керування процесами, зокрема завершення некоректно працюючих задач.

Необхідне обладнання: Індивідуальне робоче місце в комп’ютерному класі, оснащене ПК із встановленою операційною системою, веб-браузером та виділеним місцем для збереження даних.

Короткий теоретичний коментар до теми

Операційні системи Linux та Windows є багатокористувацькими, що означає можливість роботи з кількома обліковими записами одночасно. Користувачі можуть об’єднуватися в групи для спільного виконання завдань. Кожен користувач обов’язково належить до однієї або кількох груп, а всі команди виконуються від його імені в межах відповідної групи. Захист об’єктів файлової системи (файлів, процесів) є ключовим аспектом безпеки, оскільки дані одного користувача повинні бути захищені від несанкціонованого доступу інших.

Група користувачів — це набір облікових записів, що мають спільні права доступу та безпеки. Такі групи часто називають групами безпеки. Обліковий запис користувача може бути учасником декількох груп одночасно. Основні групи включають стандартних користувачів та адміністраторів, проте можуть існувати й інші категорії. Обліковий запис адміністратора має широкі можливості, включаючи створення нових груп, зміну складу груп, а також додавання та видалення облікових записів.

Обліковий запис містить інформацію, необхідну для ідентифікації та авторизації користувача в системі. До таких даних належать ім'я користувача, пароль або альтернативні засоби автентифікації, наприклад, біометричні дані чи секретні питання. Для підвищення безпеки пароль зазвичай зберігається у хешованому вигляді.

Додатково обліковий запис може включати персональну інформацію: ім'я, прізвище, електронну пошту, контактні дані, аватар або фотографію. Деякі системи також ведуть статистику активності користувача, зокрема час останнього входу, тривалість сесій, IP-адресу підключення, інтенсивність використання ресурсів та інші показники.

Завдання 1. Дослідити необхідність створення облікових записів користувачів із відповідними правами безпеки

Для роботи з комп’ютером, що працює під управлінням Windows, спочатку необхідно створити обліковий запис користувача. Він включає ім'я користувача та пароль. Якщо в системі активовано відповідну опцію, після натискання комбінації клавіш «CTRL+ALT+DEL» і введення облікових даних система перевіряє їхню правильність. У випадку, якщо обліковий запис був видалений, усі спроби входу з його використанням будуть заблоковані.

Щоб виконувати різні завдання на комп’ютері, користувачам необхідно мати відповідні права доступу. Використання груп облікових записів спрощує процес надання користувачам необхідних дозволів. Windows містить вбудовані групи користувачів, організовані відповідно до типових завдань. Додавання користувачів до певної групи автоматично надає їм відповідні права та дозволи.

Користувацькі права визначають перелік операцій, які можна виконувати на комп’ютері. Вони також регулюють можливість входу до системи, додавання та видалення користувачів у локальних групах. Вбудовані групи містять уже визначені права, і адміністратори можуть призначати їх шляхом включення облікового запису користувача до відповідної групи або створення нової групи з налаштованими дозволами. Користувачі, що входять до складу групи, автоматично отримують усі права, встановлені для цієї групи.

Контроль доступу до мережевих ресурсів здійснюється адміністратором, що дозволяє забезпечити безпеку системи. Це обмежує можливості користувачів та груп виконувати певні дії шляхом призначення їм відповідних дозволів. Дозвіл є правилом, яке визначає тип доступу до об'єкта (наприклад, файлу, папки чи принтера) для конкретного користувача або групи.

Управління обліковими записами та групами здійснюється через службу "Керування комп’ютером" у Панелі керування (розділ "Адміністрування").

ЛОКАЛЬНІ КОРИСТУВАЧІ ТА ГРУПИ

У розділі "Локальні користувачі та групи" містяться дві папки: "Користувачі" та "Групи". У папці "Користувачі" представлено два вбудовані облікові записи — "Адміністратор" і "Гість", а також усі створені облікові записи користувачів. Обліковий запис адміністратора входить до групи адміністраторів, що дозволяє йому керувати системою.

Завдання 2. Створювати та редагувати облікові записи користувачів. Використовувати диспетчер завдань для керування процесами, зокрема завершення некоректно працюючих задач

Процес створення нового облікового запису можливий тільки при наявності адміністративних прав. Послідовність дій:

1. Відкрити "Пуск" → "Панель керування" → "Облікові записи користувачів".
2. У вікні "Облікові записи користувачів" вибрати "Створення облікового запису".

3. Вказати ім'я нового користувача та натиснути "Далі".
4. Вибрати тип облікового запису (наприклад, обмежений).
5. Натиснути "Створити обліковий запис".
6. Для створення другого користувача повторити ці ж дії.

ПРИЗНАЧЕННЯ ПАРОЛЯ КОРИСТУВАЧУ

1. Вибрати обліковий запис у вікні "Облікові записи користувачів".
2. Натиснути "Створити пароль".
3. Ввести пароль у відповідні поля та додати підказку.
4. Натиснути "Створити пароль".

ВИДАЛЕННЯ ЛОКАЛЬНОГО ОБЛІКОВОГО ЗАПИСУ

1. Відкрити "Панель керування" → "Облікові записи користувачів".
2. Вибрати користувача, якого потрібно видалити.
3. Натиснути "Видалення облікового запису".
4. Вибрати "Видалити файли".

КОНФІГУРУВАННЯ БЕЗПЕКИ В WINDOWS

Для налаштування доступу та прав користувачів необхідно:

- Використати утиліту control userpasswords2 для керування обліковими записами.
- Налаштувати доступ користувачів до файлів та директорій через вкладку "Безпека".
- Визначити розмежування прав доступу за допомогою secpol.msc.
- Налаштувати необхідні служби через services.msc.
- Виконати конфігурацію безпеки системи через msconfig.
- Відредагувати параметри завантаження у файлі C:\boot.ini.

- Встановити рівні безпеки Інтернету в браузері Windows Internet Explorer.
- Включити засоби автоматичного відновлення ОС.
- Налаштувати стандартний брандмауер Windows.
- Виконати захист даних через реєстр за допомогою RegEdit.

РЕКОМЕНДАЦІЇ ЩОДО ВИКОНАННЯ ПРАКТИЧНОЇ РОБОТИ

1. Виконати налаштування облікових записів користувачів і груп, супроводжуючи кроки скріншотами з поясненнями.
2. Описати внесені зміни, інструменти та утиліти, що використовувалися.
3. Дати відповіді на контрольні питання щодо типів облікових записів, способів їхнього налаштування та управління доступом.
4. Оформити звіт у форматі .odf, .doc або .docx.
5. Надіслати файл викладачеві в архіві, що містить звіт.

Практична робота № 2.

Застосування теорії чисел для забезпечення захисту інформації

Навчальна мета: ознайомити з основними поняттями теорії чисел та набути практичних навичок у шифруванні та дешифруванні повідомлень за допомогою відкритого та закритого ключа криптосистеми RSA, використовуючи теорію чисел.

Виховна мета: сприяти розвитку зібраності, самоконтролю та комунікабельності.

Завдання:

1. Ознайомити з прикладами використання теорії чисел у криптографії.
2. Провести розрахунок ключів криптосистеми RSA відповідно до індивідуальних варіантів.

Необхідне обладнання: персональне робоче місце в комп'ютерному класі, обладнане ПК із встановленою операційною системою, web-браузером та визначеним місцем для збереження даних.

Короткий теоретичний коментар до теми

Ключ у криптографії – це змінний елемент шифру, який використовується для кодування певних повідомлень.

Шифрування – це процес перетворення захищеної інформації в зашифроване повідомлення за встановленими правилами.

Шифр – метод трансформації даних для їхнього захисту від несанкціонованого доступу.

В **асиметричних алгоритмах шифрування** (криптографії з відкритим ключем) для кодування інформації застосовується один ключ (публічний), а для її розшифрування – інший (приватний). Ці ключі є унікальними та не можуть бути отримані один із іншого.

В асиметричному шифруванні використовується два ключі: **відкритий (публічний)**, який може бути доступний усім, і **закритий (приватний)**, який

зберігається на стороні отримувача. Взаємодія між ними забезпечує безпечну передачу даних: повідомлення, зашифроване одним ключем, можна розшифрувати тільки за допомогою іншого.

Такий метод дозволяє передавати відкритий ключ через незахищені мережі, оскільки без приватного ключа отримати вихідне повідомлення неможливо. Надійність шифрування залежить від довжини ключа, і збільшення довжини вдвічі значно підвищує криптографічну стійкість.

Асиметричне шифрування використовується в таких протоколах, як **SSH, SSL/TLS**, а також у системах, які забезпечують безпечне з'єднання або цифровий підпис.

Приклади алгоритмів асиметричного шифрування:

- **RSA** – алгоритм, що використовується як для шифрування, так і для цифрового підпису. Він застосовується, зокрема, в технології **SSL (Secure Sockets Layer)**, забезпечуючи захист каналів зв’язку.
- **Обмін ключами за методом Діффі-Геллмана (Diffie-Hellman Key Exchange)** – механізм для безпечної передачі криптографічних ключів через відкриті мережі.
- **Криптографія на еліптичних кривих (ECC - Elliptic Curve Cryptography)** – метод, подібний до RSA, але ефективніший для використання на мобільних пристроях та бездротових мережах.

Процедури генерації ключів, шифрування і дешифрування для цього алгоритму представлені на рис. 2.1.

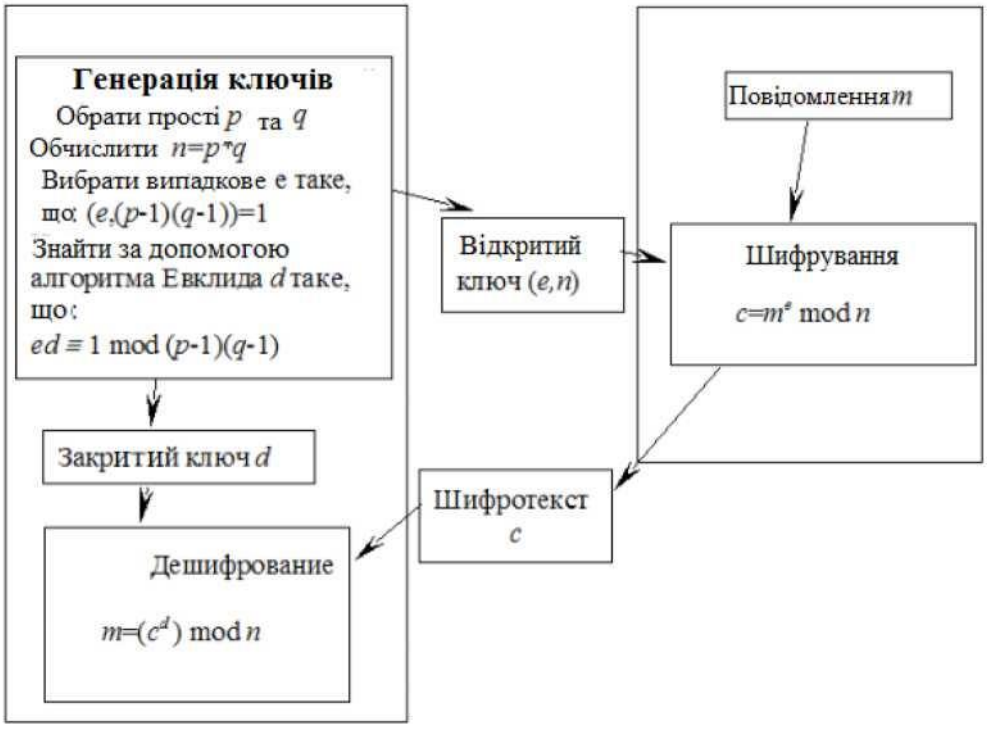

Рис. 2.1 Процедури генерації ключів, шифрування і дешифрування для алгоритму RSA

Основою безпеки **RSA** є складність факторизації великих чисел (понад 200 біт). Найпоширенішим алгоритмом асиметричного шифрування є **RSA**, який застосовується в **SSL/TLS** для захисту даних та електронного підпису.

Основи теорії чисел

Визначення 1. Число **a** ділиться на **b**, якщо існує ціле число **q**, таке що **a = bq**. У цьому випадку **a** називається кратним **b**, а **b** – дільником **a**.

Теорема 1 (про розподіл із залишком). Будь-яке ціле число **a** можна представити у вигляді:

$$a = bq + r, 0 \leq r < b$$

де **q** – неповна частка, а **r** – залишок від ділення **a** на **b**.

Визначення 2. Дільником чисел **a** і **b** називається будь-яке число, яке ділить обидва значення без залишку.

Визначення 3. Найбільший спільний дільник (НСД) чисел **a** і **b** позначається як **НСД(a, b)**. Якщо **НСД(a, b) = 1**, то числа називаються взаємно простими.

Теорема 2. Якщо **a = bq + c**, то **НСД(a, b) = НСД(b, c)**.

Для обчислення **НСД(a, b)** застосовується **алгоритм Евкліда**, заснований на цій теоремі.

Алгоритм Евкліда

Щоб число **d** було найбільшим спільним дільником чисел **a1, ..., an**, повинні виконуватися три умови:

1. **d** менше або дорівнює будь-якому з чисел.
2. **d** ділить кожне число.
3. Якщо існує інше число, що задовольняє ці умови, то воно також дорівнює **d**.

Завдання 1. Ознайомитися з прикладами використання теорії чисел у криптографії

Дослідити поняття: прості числа, взаємно прості числа, модульна арифметика, обернені елементи за модулем.

Ознайомитися з використанням цих понять у криптографічних алгоритмах, таких як:

- RSA (шифрування та цифровий підпис)
- Алгоритм Диффі-Хеллмана (обмін ключами)
- Еліптичні криві в криптографії

Навести реальні приклади використання теорії чисел у сучасних криптосистемах (банківські операції, блокчейн, електронні цифрові підписи).

Завдання 2. Виконати розрахунок ключів криптосистеми RSA за власними варіантами

Для кожного варіанту виконайте такі дії:

1. Оберіть два простих числа p та q згідно з варіантом.
2. Обчисліть модуль $n = p \times q$.
3. Знайдіть функцію Ейлера $\varphi(n) = (p - 1) \times (q - 1)$.
4. Виберіть число e, яке є взаємно простим із $\varphi(n)$ (наприклад, 3, 5, 7, 17, 65537).

5. Обчисліть закритий ключ d як мультиплікативно обернене число до e за модулем $\varphi(n) = (d \cdot e \equiv 1 \; mod \; \varphi(n))$.
6. Використовуючи отримані ключі, зашифруйте числове повідомлення $M = 42$ за формулою:

- **Шифрування:** $C = M^e \; mod \; n$
- **Дешифрування:** $M = C^d \; mod \; n$

Варіанти завдань

Варіант	p	q
1	11	13
2	17	19
3	23	29
4	31	37
5	41	43
6	47	53
7	59	61
8	67	71
9	73	79
10	83	89

Порядок і рекомендації щодо виконання роботи

1. Вивчити теоретичні відомості по теорії чисел в криптографії.
2. Виконати розрахунки за власним варіантом. Результати розрахунків продемонструвати з покроковим виконанням.
3. Дати відповідь на контрольні питання:

- Яка довжина ключа RSA?
- З яких дій складається процедура генерації ключів?

4. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту практичної роботи

1. У звіті до цієї роботи повинні бути зазначені:

- Номер практичної роботи, прізвище та ініціали студента, шифр навчальної групи; мета роботи;
- Результати виконання завдань № 1,2;
- Відповіді на запитання (пункт 3 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт має бути оформлений в електронному вигляді у форматах *.odf, *.doc або *.docx.

3. Надіслати викладачу лист з архівом (файл назвати БІС_Pract_02_Прізвище_Ініціали*), який містить файл зі звітом.

Практична робота № 3.

Забезпечення безпеки локальної мережі під час використання утиліт для моніторингу трафіку

Навчальна мета: Ознайомитися з методами виявлення вторгнень у мережі Windows, виявлення сканування портів та сповіщення про спроби несанкціонованого доступу. На практиці вивчити механізми захисту локальних мереж за допомогою моніторингу трафіку. Для цього освоїти основи роботи з утилітами аналізу мережного трафіку, зокрема на прикладі **Network Monitor**.

Виховна мета: Формування інформаційної культури, розвиток навичок командної роботи та створення позитивного ставлення до навчального процесу.

Завдання:

1. Ознайомитися з можливостями та характеристиками утиліти **Network Monitor**, порівняти її функціонал із утилітою **Iris The Network Traffic Analyzer**.
2. Налаштувати **Network Monitor** для підвищення безпеки локальної мережі.

Необхідне обладнання: Індивідуальне робоче місце у комп'ютерному класі, оснащене ПК із встановленою операційною системою, веб-браузером та визначеним місцем для збереження даних.

Короткий теоретичний коментар до теми

Network Monitor представлений у двох версіях:

- **Спрощена версія**, яка інтегрована в Windows, дозволяє контролювати лише локальний трафік, тобто ті пакети, які приймає мережевий адаптер конкретної робочої станції.
- **Повна версія**, що входить до складу **Systems Management Server**, надає можливість моніторингу всього мережевого трафіку, а також дозволяє контролювати віддалені системи при підключенні до інших серверів або робочих станцій, на яких встановлено Network Monitor.

Програма містить набір інструментів для аналізу трафіку:

- **Фільтри** для виокремлення необхідної інформації у великих потоках даних.
- **Фільтри захоплення**, які дозволяють вибирати лише потрібні пакети.
- **Тригери**, що дають змогу автоматизувати певні дії з отриманими даними.

Після запуску утиліти користувач вибирає мережу для моніторингу через меню **Capture → Networks**, де відображаються всі доступні мережеві інтерфейси, адаптери, COM-порти та служби RAS (якщо вони встановлені).

Iris The Network Traffic Analyzer

Окрім стандартних функцій збору, фільтрації та аналізу мережних пакетів, створення звітів, ця утиліта має можливість **реконструювання даних**. Вона дозволяє відтворювати сесії користувачів із різними мережевими ресурсами.

Реконструкція даних реалізована через модуль дешифрування (**decode module**), який перетворює зібрані двійкові пакети у вихідний формат. Це значно розширює можливості моніторингу та аудиту.

Аналізатор пакетів у складі утиліти надає детальну інформацію про атаки:

- Дата і час події.
- IP-адреси та DNS-імена пристроїв зловмисників.
- Використані порти.

Цей аналізатор може відтворювати точну картину вторгнення, аж до натискань клавіш і рухів миші, що допомагає усунути наслідки атак і покращити заходи безпеки.

Network Monitor використовується для діагностики та виявлення проблем у мережі. Він реєструє та аналізує передані й отримані дані, надаючи їх у графічному вигляді. Записані кадри та пакети містять:

- Адреси відправника та одержувача.
- Порядкові номери пакетів.
- Контрольні суми.

Утиліта розшифровує цю інформацію, дозволяючи проводити глибокий аналіз мережного трафіку та вести журнал активності. Окрім даних канального

рівня, Network Monitor може відображати деяку інформацію прикладного рівня, наприклад, пакети протоколів **HTTP** або **FTP**.

Завдання 1. Ознайомитися з можливостями та характеристиками утиліти Network Monitor, порівняти її функціонал із утилітою Iris The Network Traffic Analyzer

1. **Запустіть утиліту Network Monitor** і ознайомтеся з її основними функціями для моніторингу мережного трафіку. Вивчіть налаштування, доступні в меню **View (Вид), Frames (Фрейми), Capture (Перехоплення), Filter (Фільтр)** та **Tools (Інструменти)**.

2. **Налаштуйте та запустіть перехоплення трафіку** відповідно до вашого варіанту. Для цього використовуйте **редактор фільтра запису (Capture Filter)** або **фільтра перегляду (Display Filter)**, доступні у вікні **Capture**. Через певний проміжок часу зупиніть перехоплення трафіку, вибравши відповідний пункт у меню **Capture**.

3. **Проаналізуйте зібрані дані** та зафіксуйте у протоколі правило фільтра, яке використовувалося під час перехоплення трафіку.

4. **Запустіть утиліту eEye Iris** та ознайомтеся з її основними функціями моніторингу, а також доступними налаштуваннями в головних пунктах меню.

5. **Розпочніть сканування трафіку**, а після певного часу зупиніть утиліту. Налаштуйте фільтри перегляду відповідно до поставленого завдання.

6. **Порівняйте роботу двох утиліт** (Network Monitor та eEye Iris), які ви використовували в практичній роботі. Внесіть до протоколу основні відмінності, переваги та недоліки кожної з них.

Завдання 2. Налаштувати Network Monitor для підвищення безпеки локальної мережі

1. Налаштуйте перехоплення трафіку між двома сусідніми робочими станціями.

2. Виконайте налаштування для фіксації трафіку між локальною та сусідньою робочою станцією.

3. Налаштуйте перехоплення трафіку, що використовує протокол ARP.

4. Задайте параметри для запису кадрів, що містять певний тип даних.

5. Активуйте перехоплення всього мережного трафіку.

6. Встановіть фільтр для фіксації лише зовнішнього трафіку.

7. Відфільтруйте кадри, щоб відобразити лише широкомовні пакети у мережі.

8. Виконайте фільтрацію кадрів для відображення адрес відправника та одержувача на канальному та мережному рівнях.

9. Налаштуйте фільтр для відображення кадрів, що передаються через протокол FTP.

10. Відобразьте кадри, які передані за допомогою протоколу TCP.

11. Відфільтруйте трафік, що використовує протокол IP.

12. Налаштуйте фільтрацію для відображення всього мережного трафіку, окрім широкомовних повідомлень.

Порядок і рекомендації щодо виконання роботи

1. Проаналізуйте записані дані та структуру кадрів у кожній з утиліт.

2. Ознайомтеся з видами фільтрів відображення та додайте до звіту таблицю різних методів фільтрації.

3. Відповісти на контрольні питання:

a. На якому рівні семирівневої моделі OSI здійснюється збір даних у Network Monitor?

b. Яке призначення утиліти Microsoft Network Monitor?

c. Яку інформацію про передані та отримані дані адміністратор може отримати за допомогою Network Monitor?

d. Для чого використовується фільтр запису в Network Monitor і як він налаштовується?

e. Яке основне призначення утиліти eEye Iris?

f. Які параметри налаштувань і фільтри можна використовувати в eEye Iris?

g. Зробіть порівняльний аналіз Network Monitor та eEye Iris.

4. Оформіть звіт.

Вимоги щодо оформлення та порядку подання звіту практичної роботи

1. Звіт до цієї практичної роботи має містити:

- Номер практичної роботи, прізвище та ініціали студента, шифр навчальної групи, мету роботи.
- Результати виконання завдань №1 та №2.

До звіту необхідно додати інформацію про вибраний сегмент мережі відповідно до вашого завдання. Ці дані повинні включати:

- рівень завантаження мережі;
- кількість отриманих байтів за секунду;
- кількість отриманих кадрів за секунду.

Також у звіті повинні бути наведені такі відомості:

- статистика сеансу;
- статистика робочої станції;
- загальна статистика;
- відповіді на контрольні запитання (згідно з пунктом 3 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт оформлюється в електронному форматі (*.odf, *.doc або *.docx).
3. Надіслати викладачу архівований файл (назва файлу: **БІС_Pract_03_Прізвище_Ініціали**), який містить звіт.

Практична робота № 4.
Забезпечення безпеки механізму автентифікації під час перехоплення хешів паролів та їх розшифрування

Навчальна мета: освоєння практичних навичок роботи з утилітами для перехоплення та розшифровки парольних хешів за допомогою програми Cain&Abel (безкоштовне програмне забезпечення), при аутентифікації через

мережу, з метою перевірки коректності функціонування механізму аутентифікації.

Виховна мета: сформувати розуміння важливості конфіденційності та контролю доступу до особистих даних, сприяти розвитку компетентностей у використанні інформаційно-комунікаційних технологій.

Завдання:

1. Ознайомлення з призначенням, можливостями та принципом роботи утиліти Cain&Abel (безкоштовна версія ПЗ) — інструменту для відновлення паролів в операційних системах Windows, який дозволяє захищатися від вразливостей у кеші, методах аутентифікації та мережевих протоколах.
2. Виконання перебору паролів відповідно до заданого варіанту.

Необхідне обладнання: індивідуальне робоче місце в комп'ютерному класі з ПК, на якому встановлена операційна система, web-браузер та вказане місце для збереження файлів.

Короткий теоретичний коментар до теми

Автентифікація — це процес підтвердження приналежності користувача до конкретної інформації в системі на основі поданого ідентифікатора. З точки зору інформаційної безпеки, автентифікація є частиною процедури надання доступу до інформаційної системи, що йде після ідентифікації та передує авторизації.

Один із способів автентифікації в інформаційній системі полягає в попередній ідентифікації через користувацький ідентифікатор і пароль — конфіденційну інформацію, знання якої підтверджує право доступу до мережевого ресурсу. Після введення користувачем логіна та пароля комп'ютер порівнює їх з даними, збереженими в захищеній базі даних, і, у разі успішної автентифікації, здійснює авторизацію, надаючи користувачу доступ до роботи в системі.

Система ідентифікації та автентифікації є важливим компонентом інфраструктури захисту від несанкціонованого доступу (НСД) до будь-якої інформаційної системи. Під НСД розуміється доступ до інформації, який

порушує правила доступу і здійснюється за допомогою стандартних засобів обчислювальної техніки чи автоматизованих систем. НСД може бути як випадковим, так і навмисним. Основне завдання систем ідентифікації та автентифікації — це перевірка та підтвердження прав доступу користувача до системи.

Програма Cain&Abel призначена для відновлення паролів. Вона дозволяє відновити паролі до операційних систем, загальні паролі, паролі доступу до мережі та інші паролі, що зберігаються в системі чи зовнішніх файлах. Програма не використовує системні уразливості, але має потужні засоби для дешифрування.

Cain&Abel, хоча й не є мережевим сканером, демонструє методи, які використовуються зловмисниками для збору інформації про систему. Одна з таких методик — ARP Poison Routing (APR), за допомогою якої зловмисник може впровадити фальшиві зв'язки між мережевими та апаратними адресами, що призводить до перенаправлення трафіку через систему зловмисника. Cain&Abel дозволяє використовувати ARP спуфінг та перехоплювати RDP трафік між вузлами.

Cain&Abel може відновлювати паролі до операційних систем Windows і підтримує кілька методів відновлення: грубий перебір, підбір за словником, перегляд захованих паролів, а також аналіз перехоплених пакетів, запис мережевих перегонів та аналіз кеша. Крім того, програма здатна визначати паролі, заховані "зірочками", і має вбудований аналізатор мережевих протоколів.

Завдання 1. Ознайомлення з призначенням, можливостями та принципом роботи утиліти Cain&Abel (безкоштовна версія ПЗ) — інструменту для відновлення паролів в операційних системах Windows, який дозволяє захищатися від вразливостей у кеші, методах аутентифікації та мережевих протоколах

1. Запустіть програму та ознайомтесь із можливостями основних пунктів меню: "Конфігурація" (Configure) та "Сервіс" (Tools).

2. Створіть на вашій робочій станції кілька локальних користувачів з паролями різної довжини й складності. Під час створення користувачів не

встановлюйте прапорчик «User must change password at next logon». Також створіть загальний каталог з назвою «Test» і надайте створеним користувачам відповідні права доступу.

3. Перейдіть до меню "Конфігурація" (Configure), на вкладці "Sniffer" виберіть ваш мережевий адаптер і натисніть OK. Потім натисніть на кнопку "Start Sniffer", перейдіть на вкладку "Sniffer", а потім на вкладку "Passwords", щоб переглянути інформацію про перехоплені паролі.

4. Попросіть сусіда підключитися до вашого комп'ютера по мережі від імені створених користувачів. Для цього скористайтеся меню "Сервіс" (Service) та оберіть "Підключити мережевий диск" (Map Network Drive) із параметром «Підключити, використовуючи ім'я» (Connect using a different user name). Перевірте, чи є перехоплені парольні хеші в контейнері SMB.

5. Перегляньте кількість завантажених хешів. Для цього в контекстному меню "Send all to Cracker" виберіть перехоплені парольні хеші на вкладці "Cracker", потім оберіть меню (Dictionary Attack NTLM + Challenge), щоб побачити інформацію про кількість завантажених хешів.

6. Виконайте перебір паролів методом, відповідно до вашого варіанту.

7. Перевірте пароль за допомогою команди «Тестувати пароль» (Test Password) в контекстному меню.

8. Після завершення практичної роботи видаліть створених користувачів і мережеві диски.

Завдання 2. Виконання перебору паролів відповідно до заданого варіанту

1. Виконайте перебір паролів за допомогою словника. Для цього у вікні "Словник" (Dictionary Crack) виберіть опцію "Додати" (Add) і оберіть файл Wordlists.txt з директорії Wordlists, потім поверніться до меню "Словник" і натисніть "Почати" (Start), щоб побачити процес перебору паролів.

2. Виконайте перебір паролів методом "грубої сили". Для цього скористайтеся опцією "Атака" (Brute-Force Attack NTLM + Challenge) в контекстному меню. Оцініть час, необхідний для перебору пароля за допомогою утиліти Cain. Якщо час перебору надто великий, виберіть пароль з меншою

довжиною. За результатами роботи запишіть вимоги до пароля, які, на вашу думку, необхідно врахувати.

3. Проскануйте MAC-адреси робочих станцій у вашій локальній мережі. Для цього відкрийте вкладку "Sniffer", увійдіть в режим сніфінгу, виберіть "Start/Stop Sniffer" і додайте "SCAN MAC addresses". Після виявлення робочих станцій у локальній мережі перейдіть до вкладки "ARP". Додайте правила ARP Poison Routing, щоб ваша робоча станція стала сніфером між обраними сусідніми станціями. Не вимикаючи режим сніфера, виберіть "Start/Stop ARP" для відслідковування обміну пакетами і поступового заповнення рядків у "Passwords", поки поле ARP-RDP не зміниться на (1).

4. Використовуйте для перехоплення паролів меню "Конфігурація" (Configure), "Фільтр і перемикання портів" (Filters and Ports Tab), щоб захоплювати тільки аутентифікаційну інформацію. Відновіть пароль, переглядаючи сховані паролі.

5. Для перехоплення пароля використовуйте вкладку "HTTP Fields Tab", що містить список імені та поля пароля.

6. Виконайте перебір паролів за допомогою методу криптоаналізу (Cryptanalysis).

7. Виконайте перебір паролів за допомогою методу "грубої сили" (Brute-Force).

8. Переберіть паролі, використовуючи метод перехоплення інформаційних пакетів і їх наступний аналіз кешу.

9. Переберіть паролі, перехоплюючи інформаційні пакети та аналізуючи запис переговорів по мережі.

10. Виконайте перебір паролів за допомогою "атаки за маскою" (Mask Attack).

11. Виконайте перебір паролів за допомогою "гібридної атаки" (Hybrid Attack).

12. Виконайте перебір паролів за допомогою "атаки розподіленим перебором" (Distributed Brute-Force Attack).

Порядок і рекомендації щодо виконання роботи

1. У звіті до практичної роботи опишіть методи відновлення паролів, які використовуються в утиліті Cain&Abel, та поясніть, як ці функції реалізовані. Детально опишіть метод, який ви застосовували під час виконання роботи.

2. Розробіть план застосування механізмів для запобігання злому пароля з використанням подібних утиліт. Опишіть усі можливі заходи безпеки, які можуть запобігти злому паролів як з боку внутрішньої мережі, так і з глобальної мережі Інтернет.

3. Відповідайте на контрольні питання:

a. Опишіть призначення, можливості та принцип роботи утиліти Cain&Abel.

b. Поясніть, для чого використовується протокол ARP і як здійснюється атака за його допомогою.

c. Навіщо в утиліті Cain&Abel виконувати ARP-spoofing?

d. Які вимоги до паролів ви, як адміністратор безпеки, встановили б у вашій локальній мережі?

e. Якими методами можна відновити пароль за допомогою утиліти Cain&Abel?

f. Опишіть процес відновлення пароля за допомогою словникової атаки.

4. Оформіть звіт.

Вимоги щодо оформлення та порядку подання звіту практичної роботи

1. У звіті до цієї роботи повинні бути зазначені:

2. Номер практичної роботи, прізвище та ініціали студента, шифр навчальної групи; мета роботи;

3. Результати виконання завдань № 1,2;

4. Відповіді на запитання (пункт 3 «Порядок і рекомендації щодо виконання роботи»).

5. Звіт має бути оформлений в електронному вигляді у форматах *.odf, *.doc або *.docx.

6. Надіслати викладачу лист з архівом (файл назвати БІС_Pract_04_Прізвище_Ініціали*), який містить файл зі звітом.

Практична робота № 5.

Налаштування та адміністрування міжмережних екранів

Навчальна мета: ознайомлення з архітектурою, функціями та набуття практичних навичок налаштування та технічної експлуатації міжмережних екранів (брандмауерів) в локальних обчислювальних мережах (ЛОМ) та автоматизованих робочих місцях (АРМ).

Виховна мета: формування свідомого ставлення до праці та навчання, розвиток інтелектуальних здібностей, високих моральних якостей, самовдосконалення та індивідуальних навичок.

Завдання:

1. Ознайомитись з різними типами політик мережного доступу, методами технічної реалізації цих політик, вибором типів міжмережних екранів для забезпечення безпеки ЛОМ, а також з процесом їх впровадження та технічної експлуатації.
2. Ознайомлення з комплексом засобів міжмережного екрану Agnitum Outpost Firewall (як програмного, так і апаратного забезпечення), встановленого на ОС MS WINDOWS.

Необхідне обладнання: індивідуальне робоче місце в комп’ютерному класі, оснащене ПК з встановленою версією операційної системи, web-браузером та визначеним місцем для збереження інформації.

Короткий теоретичний коментар до теми

Міжмережевий екран (МЕ) або брандмауер — це програмний (або програмно-апаратний) засіб, який може бути локальним або розподіленим і здійснює контроль над інформацією, що надходить до інформаційної системи або виходить із неї. Брандмауер слугує захисним бар'єром між локальною мережею і зовнішнім середовищем, запобігаючи загрозам. Він контролює вхідний і вихідний трафік на комп'ютері чи в локальній мережі, зупиняючи майже всі типи мережевих атак, блокує рекламу, спливаючі вікна, і не дозволяє передавати інформацію про комп'ютер користувача стороннім серверам.

Функціонування брандмауера полягає в аналізі структури та вмісту інформаційних пакетів, що надходять з зовнішньої мережі, і в залежності від результатів аналізу дозволяється або блокується передача пакетів до внутрішньої мережі. Брандмауер під керуванням Windows ефективно працює, оскільки заміщає стандартний стек протоколів TCP/IP, що робить неможливим його порушення хакерами через спотворення протоколів зовнішньої мережі.

Архітектура Internet-систем базується на трирівневих структурах типу «клієнт-сервер», де WWW-сервер виконує роль проміжного шару. Завдяки такій структурі досягається висока ефективність механізмів безпеки, а також можливість атестації систем відповідно до діючих нормативних вимог. У цьому випадку WWW-сервер використовує екранування сервісів для створення незалежного засобу доступу та блокування дії шкідливих програмних закладок у сервері баз даних.

Основні компоненти брандмауера:

- Політика мережного доступу.
- Механізми посиленої автентифікації.
- Фільтрація пакетів.
- Прикладні шлюзи.

Існують різні конфігурації брандмауерів:

- Брандмауер з пакетною фільтрацією.
- Брандмауер зі шлюзом з двома адресами.
- Брандмауер з екранованим хостом.
- Брандмауер з екранованою мережею.
- Інші.

Порядок та методика виконання завдань практичної роботи

Завдання 1. Ознайомитись з різними типами політик мережного доступу, методами технічної реалізації цих політик, вибором типів міжмережних екранів для забезпечення безпеки ЛОМ, а також з процесом їх впровадження та технічної експлуатації

Брандмауер виконує такі функції:

- Фізично ізолює робочі станції та сервери внутрішньої мережі від зовнішніх каналів зв'язку.
- Ідентифікує вхідні запити до мережі на кількох етапах.
- Перевіряє права доступу користувачів до внутрішніх ресурсів мережі.
- Реєструє всі зовнішні запити до компонентів внутрішньої мережі.
- Контролює цілісність програмного забезпечення і даних.
- Оптимізує використання адресного простору мережі.
- Приховує IP-адреси внутрішніх серверів для захисту від атак.

Існує два основних типи брандмауерів: апаратні та програмні. Апаратний брандмауер — це пристрій, що фізично підключається до мережі і відстежує всі аспекти вхідного та вихідного обміну даними, а також перевіряє адреси джерела та призначення кожного пакету, що допомагає запобігти несанкціонованим проникненням. Програмний брандмауер виконує аналогічні функції, але на програмному рівні, без необхідності в зовнішньому пристрої, запускаючись на кінцевому комп'ютері або шлюзі. Програмні брандмауери є більш популярними.

Міжмережеві екрани можуть працювати на різних рівнях моделі OSI. На мережевому рівні фільтруються пакети за IP-адресами. На транспортному рівні — за номерами TCP портів і прапорцями в пакетах. На прикладному рівні — аналізуються протоколи (FTP, HTTP, SMTP) та контроль за змістом даних, що передаються (наприклад, блокування завантаження небажаних файлів).

Міжмережеві екрани поділяються на три основні типи:

- Пакетні фільтри.
- Сервера прикладного рівня.
- Сервера рівня з'єднання.

Пакетні фільтри приймають рішення про пропуск пакету, переглядаючи заголовки та інформацію про порти і адреси. Вони мають перевагу через низьку вартість і швидку обробку пакетів, але їхні недоліки включають видимість локальної мережі з Інтернету та можливість обходу фільтрації за допомогою IP-спуфінгу.

Сервера прикладного рівня використовують проксі-сервери для контролю доступу до конкретних сервісів, таких як TELNET або FTP. Вони

надають вищий рівень безпеки, приховуючи структуру мережі від зовнішніх користувачів і дозволяючи додаткові перевірки. Однак їхня продуктивність нижча, а вартість вища.

Сервери рівня з'єднання пропонують подібний захист, але на відміну від серверів прикладного рівня, вони можуть працювати з більшою кількістю протоколів. Проте вони не гарантують повну безпеку, оскільки не можуть запобігти таким загрозам, як віруси або фішинг.

Політика мережевої безпеки повинна включати:

1. Політику доступу до мережевих сервісів.
2. Політику реалізації міжмережевих екранів.

Політика доступу має визначати рівень доступу користувачів до Інтернету та внутрішніх ресурсів мережі, а також механізми обмеження доступу до небажаних сервісів.

Рішення щодо доступу до внутрішніх ресурсів мережі мають базуватися на одному з принципів: забороняти все, що не дозволено, або дозволяти все, що не заборонено.

Ефективність брандмауера залежить не тільки від політики безпеки, а й від вибору компонентів, які здійснюють доступ до мережевих сервісів.

Основні завдання адміністратора безпеки мережі при підключенні локальної мережі до глобальної — захист від несанкціонованого доступу, приховування структури мережі і контроль доступу між глобальною та захищеною мережею.

Завдання 2. Ознайомлення з комплексом засобів міжмережного екрану Agnitum Outpost Firewall (як програмного, так і апаратного забезпечення), встановленого на ОС WINDOWS

Outpost Firewall Free — це безкоштовний фаєрвол для захисту персонального комп'ютера від хакерських атак. Окрім забезпечення захисту від зовнішніх проникнень з мережі, Outpost Firewall Free також надає можливість запобігти нелегальному витоку конфіденційної інформації через програми, встановлені на комп'ютері (https://biblprog.org.ua/ru/outpost_firewall/). Для

виконання практичної роботи можна також використовувати Comodo Firewall (Free Firewall/Download Comodo Award Winning Free Firewall: https://www.comodo.com/home/internet-security/firewall.php).

1. Запустіть програму Outpost Firewall і ознайомтесь з функціями вкладки контекстного меню «Параметри».

2. Налаштуйте функції програми Outpost Firewall відповідно до вимог, зазначених у вашому варіанті (рис. 5.1).

3. Налаштуйте журнал програми Outpost Firewall для відображення лише необхідної інформації, визначеної у вашому завданні.

Брандмауер дозволяє налаштовувати фільтри для пропуску трафіку за наступними критеріями:

1. **IP-адреса**. Кожен пристрій, що працює за протоколом IP, має унікальну адресу. Встановивши конкретну адресу або діапазон, можна заблокувати пакети з цих адрес або, навпаки, дозволити доступ тільки з них.

2. **Доменне ім'я**. Кожному сайту в Інтернеті присвоюється доменне ім'я, що набагато зручніше для запам'ятовування, ніж IP-адреса. Фільтр можна налаштувати на пропуск трафіку тільки до/від конкретного ресурсу або заблокувати доступ до нього.

3. **Порт**. Порти — це точки доступу програм до мережевих сервісів. Наприклад, FTP використовує порт 21, а браузери — порт 80. Це дозволяє обмежити доступ лише до певних сервісів і додатків або заблокувати доступ до небажаних.

4. **Протокол**. Брандмауер можна налаштувати на пропуск трафіку тільки для одного конкретного протоколу або заборонити доступ через інші протоколи. Тип протоколу визначає призначення програми та її параметри захисту, що дозволяє налаштувати доступ тільки для певного додатка, блокуючи небажані з'єднання.

Основні етапи налаштування міжмережевого екрана

Рис. 5.1. Вікно програми Outpost Firewall

Закладка "Загальні" (рис. 5.2). У верхній частині вікна знаходиться опція завантаження з трьома доступними варіантами на вибір: звичайне, фонове або без завантаження. За замовчуванням обрано перший варіант.

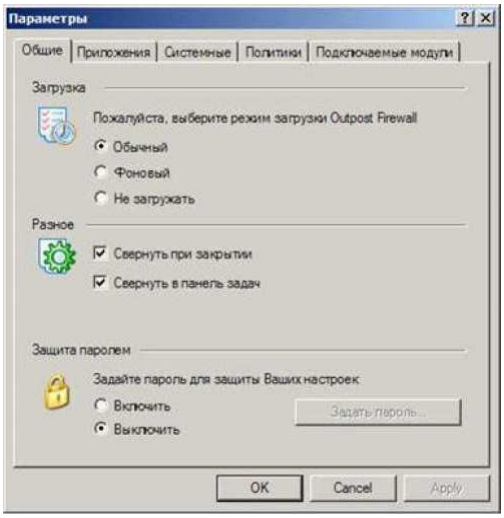

Рис. 5.2 Установчі параметри Outpost Firewall

Вкладка "Додатки" (рис. 5.3). У цьому вікні будуть відображатися програми, які запускаються вперше та виходять у мережу. Додатки поділяються на три категорії: заборонені, користувацький рівень і дозволені. "Заборонені" — це програми, яким адміністратор заблокував доступ до Інтернету; "Користувацький рівень" включає програми, для яких адміністратор визначив конкретні правила використання мережі (тобто не всі дії дозволені, а тільки певні); "Дозволені" — це програми, яким дозволено без обмежень використовувати мережу.

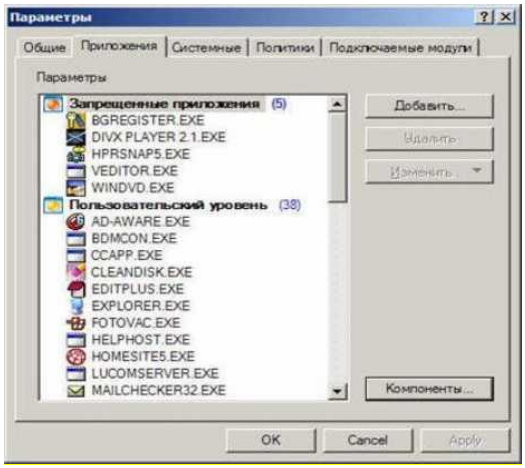

Рис. 5.3 Додатки Outpost Firewall

Кнопка "Компоненти" показує всі складові програм із цього вікна, такі як динамічні бібліотеки, запущені файли та інші елементи, які безпосередньо використовують мережу (рис. 5.4, 5.5).

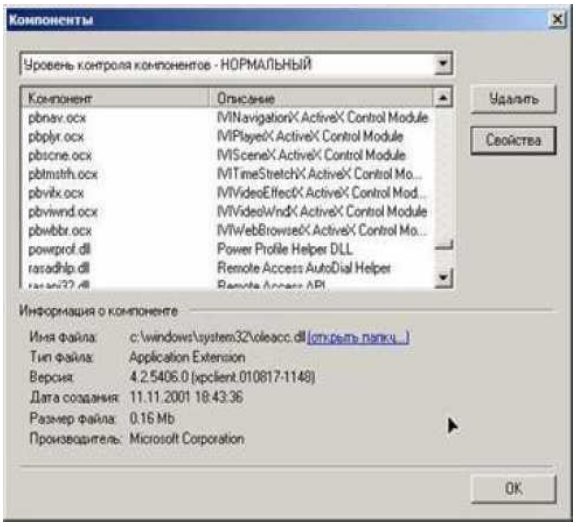

Рис. 5.4 Компоненти Outpost Firewall

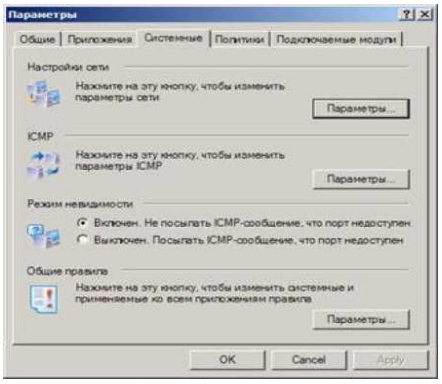

Рис.5.5. Мережеві налаштування

Вкладка "Системні" містить налаштування мережі (рис. 5.6), а також

параметри ICMP (Internet Control Message Protocol), який використовується для передачі повідомлень про помилки керування між комп'ютерами, з'єднаними в мережі (рис. 5.7). Ці налаштування за замовчуванням. Окрім того, є секція "Режим невидимості", де доступні два варіанти: увімкнений/вимкнений, причому за замовчуванням цей режим увімкнений.

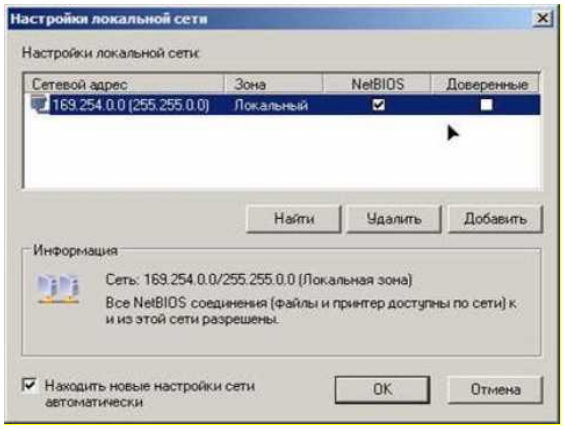

Рис.5.6. Налаштування ЛОМ

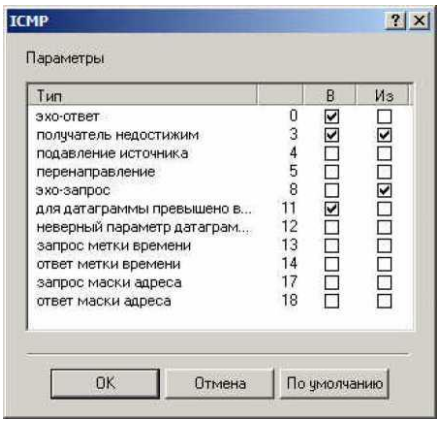

Рис. 5.7. Налаштування Internet Control Message Protocol

У цьому вікні відображаються наявні правила використання мережі, а також є можливість додавати власні правила, які будуть відноситися до категорії програм користувальницького рівня.

Варіанти завдань для виконання практичної роботи № 5

1. На робочих комп'ютерах користувачів потрібно заборонити відображення рекламних банерів у браузерах, а також інформувати користувачів про проведене сканування їхнього комп'ютера, навіть у разі одноразового сканування.

2. Необхідно налаштувати робочі комп'ютери користувачів для блокування відображення елементів ActiveX на Web-сторінках та запровадити блокування атакуючого вузла при виявленні підозри на атаку.

3. На робочих комп'ютерах користувачів слід заблокувати доступ до Web-сайтів, що містять певні слова, а також реалізувати автоматичне блокування підмережі, з якої були здійснені спроби атак.

4. На робочих комп'ютерах користувачів необхідно дозволити виконання Java та VB-сценаріїв, а також реалізувати захист від підміни ARP-адрес, приймаючи лише ті відповіді, для яких була відправлена відповідна адреса.

5. На робочих комп'ютерах користувачів слід заблокувати відображення інтерактивних рекламних оголошень у браузерах, а також реалізувати виявлення підміни IP-адреси і блокування атак.

6. На робочих комп'ютерах користувачів потрібно заблокувати доступ до певних Web-сторінок та реалізувати захист від помилкових повідомлень типу «IP-адреса вже зайнята».

7. На робочих комп'ютерах користувачів слід заборонити відображення Java-аплетів у браузерах та налаштувати час для блокування DoS-атак.

8. На робочих комп'ютерах користувачів необхідно налаштувати фільтрацію .exe-файлів, що надходять через електронну пошту, а також налаштувати список системних портів для спостереження за підвищеною увагою для виявлення атак.

9. На робочих комп'ютерах користувачів необхідно налаштувати функцію, що дозволяє працювати з cookies лише за згодою користувача, а також визначити довірчі комп'ютери, порти та вузли, які не будуть розглядатися як шкідливі.

10. На робочих комп'ютерах користувачів потрібно налаштувати фільтрацію .bat-файлів, що надходять електронною поштою, та визначити список портів для спостереження з підвищеною увагою для виявлення атак.

11. На робочих комп'ютерах користувачів слід заборонити відображення спливаючих вікон у браузерах, а також реалізувати перевірку й блокування неправильних та наддовгих DNS-запитів.

12. На робочих комп'ютерах користувачів необхідно заблокувати відображення рекламних оголошень стандартного розміру в браузерах та реалізувати виявлення підміни MAC-адрес і блокування атак.

Порядок і рекомендації щодо виконання роботи

1. У звіті з практичної роботи слід детально описати функції, які ви налаштували для виконання завдання. Обґрунтуйте вибір налаштувань, застосованих для вирішення завдання.
2. Додайте до звіту результат виконання програми та налаштування журналу, які ви виконали.
3. Відповісти на контрольні питання:

   A. Опишіть призначення міжмережевих екранів. Які функції виконує програма Outpost Firewall?

   B. Поясніть призначення вкладок у вікні «Параметри».

   C. Для чого використовуються «Політики» в програмі Outpost Firewall? Охарактеризуйте політики, що є в програмі.

   D. На які категорії поділяються додатки в програмі Outpost Firewall і для яких цілей?

   E. Які дії потрібно виконати для перенесення додатку з однієї групи в іншу?

   F. Опишіть функції, що визначені в правилах програми Outpost Firewall.

   G. Які кроки потрібно зробити для створення користувацьких правил?

   H. Які умови можна визначити для протоколів? Опишіть їх призначення та особливості.

   I. Опис процесу налаштування системних протоколів. Які параметри можна вибрати, і яке їх функціональне значення?

   J. Для чого використовуються підключувані модулі? Охарактеризуйте роботу з ними.

   K. Дайте визначення терміну «брандмауер».

   L. Перерахуйте основні типи брандмауерів.
4. Оформіть звіт.

Вимоги щодо оформлення та порядку подання звіту практичної роботи

1. У звіті до цієї роботи мають бути вказані:

- Номер практичної роботи, прізвище та ініціали студента, шифр навчальної групи, а також мета роботи.
- Результати виконання завдань №1 та №2.
- Відповіді на запитання з пункту 3 «Порядок і рекомендації щодо виконання роботи».

2. Звіт повинен бути оформлений в електронному вигляді у форматах *.odf, *.doc або *.docx.
3. Надіслати викладачу листа з архівом, де файл зі звітом має бути названий як БІС_Pract_05_Прізвище_Ініціали*.

Практична робота № 6.

Методика створення захищеної телекомунікаційної мережі з використанням VPN

Навчальна мета: аналіз протоколів, що використовуються у віртуальних приватних мережах, з метою вибору оптимального рішення для віддаленого доступу до внутрішніх ресурсів корпоративної мережі.

Виховна мета: формування свідомого ставлення до праці та навчання, розвиток розумових здібностей, моральних якостей, самовдосконалення та індивідуальних талантів.

Завдання:

1. Огляд доступних рішень на ринку технологій VPN.
2. Налаштування підключення до віртуальної приватної мережі (VPN) на ОС Windows.

Необхідне обладнання: індивідуальне робоче місце в комп'ютерному класі, ПК з встановленою операційною системою, web-браузером та визначеним місцем для збереження інформації.

Короткий теоретичний коментар до теми

VPN виконують наступні функції:

- фізичне відокремлення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв'язку;
- ідентифікація запитів, що надходять у мережу, на кількох етапах;
- перевірка прав доступу користувача до внутрішніх ресурсів мережі;
- реєстрація всіх зовнішніх запитів до компонентів внутрішньої підмережі;
- контроль за цілісністю програмного забезпечення і даних;
- економія адресного простору мережі;
- приховування IP-адрес внутрішніх серверів для захисту від хакерських атак.

Існують два типи МЕ: апаратний і програмний. Апаратний тип являє собою пристрій, який фізично підключається до мережі і відслідковує всі аспекти вхідного та вихідного обміну даними. Цей пристрій також перевіряє адреси джерела і призначення кожного обробленого повідомлення, забезпечуючи

безпеку мережі та захищаючи від небажаних проникнень. Програмний тип виконує ті самі функції, але замість зовнішнього пристрою використовує програму, запущену на кінцевому комп'ютері або шлюзі. Найбільш поширений саме програмний тип реалізації МЕ.

МЕ можуть працювати на різних рівнях моделі OSI. На мережевому рівні здійснюється фільтрація пакетів за IP-адресами: блокуються пакети, що надходять з Інтернету і направлені до серверів, доступ до яких зовні заборонено. На транспортному рівні фільтрація відбувається також за номерами портів TCP і прапорцями в пакетах (наприклад, запити на встановлення з'єднання). На прикладному рівні проводиться аналіз прикладних протоколів (FTP, HTTP, SMTP) та контроль вмісту даних, наприклад, заборона отримання певних типів файлів, таких як реклама або виконувані програмні модулі.

Завдання 1. Огляд доступних рішень на ринку технологій VPN

1. Провести аналітичний огляд сучасних технологій VPN, що використовуються на сьогоднішній день, зокрема найбільш популярних, враховуючи як вітчизняний, так і зарубіжний ринки.

2. Представити аналіз у вигляді графіків та діаграм.

Завдання 2. Налаштування підключення до віртуальної приватної мережі (VPN) на ОС Windows

1. Натисніть кнопку "Пуск", потім виберіть "Панель управління" або "Пуск" → "Налаштування" → "Панель управління".

Якщо ваша Панель управління має інший вигляд, зліва виберіть "Переключення до класичного вигляду". У відкритій Панелі управління двічі клацніть на значок "Мережеві підключення" (рис. 6.1).

Архітектурно інтернет-системи є трирівневими "клієнт-сервер", де WWW-сервер виступає як проміжний шар. Оскільки саме трирівневі системи використовуються для найбільш ефективного забезпечення безпеки, можна бути впевненими в успішному впровадженні механізмів безпеки в інтернет-системи.

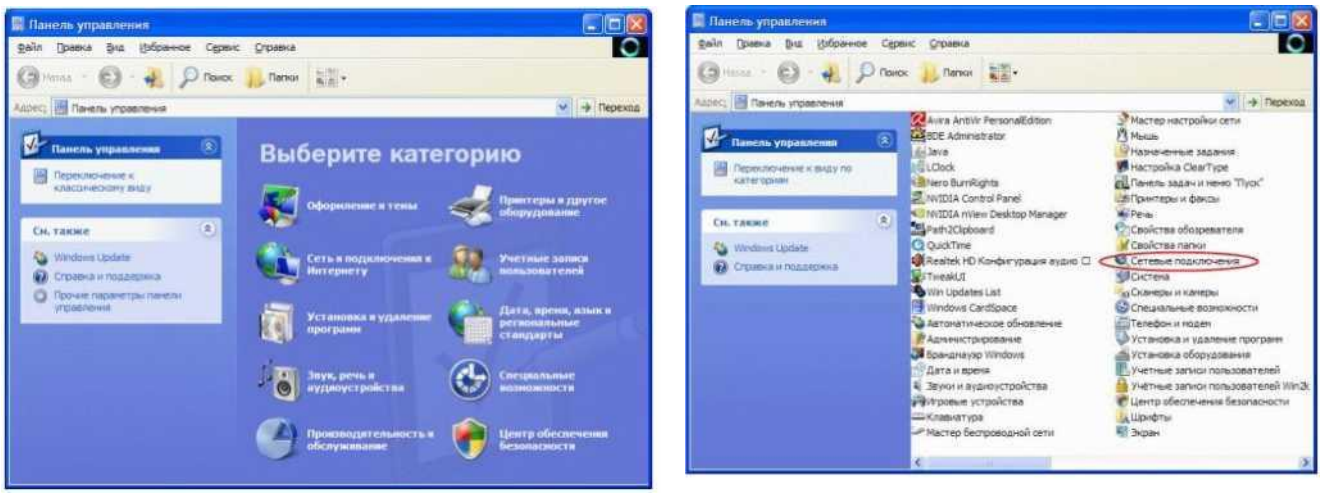

Рис. 6.1 Виклик Панелі управління та "Мережеві підключення"

Додатковою перевагою цього підходу є можливість атестації таких систем відповідно до чинного законодавства. У цьому випадку WWW-сервер застосує механізм екранування сервісів для створення незалежного засобу доступу та блокування дії програмних закладок у програмному забезпеченні сервера баз даних.

Порядок і рекомендації щодо виконання роботи

1. Вивчити теоретичні відомості по можливостям захисту VPN.
2. Надати наочні результати аналізу технології VPN та результати налаштування віртуальної приватної мережі у вигляді скріншотів з поясненням виконання кожного кроку налаштування.
3. Дати відповідь на контрольні питання:
4. З яких дій складається процедура генерації ключів?
5. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту практичної роботи

1. Ознайомитися з теоретичними відомостями про можливості захисту віртуальних приватних мереж (VPN).
2. Надати наочні результати аналізу технології VPN та налаштування віртуальної приватної мережі у вигляді скріншотів, з поясненням кожного кроку налаштування.
3. Оформити звіт.

Практична робота № 7.

Методи криптографічного захисту даних: перестановка за допомогою ключа, подвійна перестановка, використання магічних квадраті

Навчальна мета: застосування криптографічного захисту інформації при розробці політики безпеки операційно-інформаційної системи з використанням надійної системи розподілу криптографічних ключів.

Виховна мета: сприяти розвитку компетентності у сфері використання інформаційно-комунікаційних технологій, навчанню ефективної співпраці в групі незалежно від інтелектуальних та творчих здібностей, виховувати відповідальність і самостійність при виконанні практичних і творчих завдань.

Завдання:

1. Виконати шифрування повідомлення за зразком, використовуючи методи простої перестановки по ключу, подвійної перестановки та метод магічних квадратів.
2. Зашифрувати текстове повідомлення, згідно з варіантами, визначеними викладачем, застосовуючи вивчені методи шифрування.

Необхідне обладнання: індивідуальне робоче місце в комп'ютерному класі з ПК, підключеним до мережі Інтернет, встановленою операційною системою, пакетом стандартних програм, браузерами та відведеним місцем для збереження інформації, мультимедійний проектор.

Короткий теоретичний коментар до теми

1. **Проста перестановка за допомогою ключа**

Ключем для шифрування та дешифрування є розмір таблиці та ключове слово. Повідомлення розташовується в таблиці по стовпцях, а для формування шифрованого тексту таблиця читається по рядках. Метод полягає в перестановці стовпців таблиці відповідно до ключового слова, фрази або набору чисел, що дорівнюють кількості стовпців. При дешифруванні текст записується в таблицю по рядках, стовпці переставляються за тим же ключем, і текст читається по стовпцях.

2. **Подвійна перестановка**

Для підвищення рівня захисту повідомлення може бути зашифроване двічі. Це відомий метод під назвою подвійна перестановка. Для цього використовуються дві таблиці, розмір яких відрізняється один від одного, причому їхні розміри мають бути взаємно простими. У першій таблиці переставляються стовпці, а в другій — рядки. Спочатку повідомлення записується в таблицю по стовпцях, потім переставляються стовпці, а потім рядки. При дешифруванні перестановки виконуються в зворотному порядку: спочатку переставляються рядки, потім стовпці. Число варіантів подвійної перестановки зростає разом із розміром таблиці:

- для таблиці 3x3 — 36 варіантів;
- для таблиці 4x4 — 576 варіантів;
- для таблиці 5x5 — 14400 варіантів.

Але ця техніка не забезпечує високої стійкості, оскільки шифр легко ламається при будь-якому розмірі таблиці.

3. **Магічні квадрати**

Магічні квадрати — це квадратні таблиці, у яких клітини заповнені натуральними числами від 1 і далі, так, що сума чисел по кожному рядку, стовпцю та діагоналі однакова (наприклад, 16 + 3 + 2 + 13 = 34). Текст шифрується шляхом вписування його в магічний квадрат відповідно до нумерації клітин. Прочитавши ці числа по рядках, отримаємо шифрований текст.

Завдання 1. Виконати шифрування повідомлення за зразком, використовуючи методи простої перестановки по ключу, подвійної перестановки та метод магічних квадратів

- **Проста перестановка за ключем**

- Виберіть ключове слово, наприклад, "КОД".
- Визначте порядок перестановки за алфавітним розташуванням букв ключового слова.
- Виконайте шифрування відповідно до отриманого порядку.

- **Подвійна перестановка**

- Використайте дві різні ключові фрази або двічі застосуйте перестановку до таблиці символів.

➢ **Шифрування за допомогою магічного квадрата**

- Побудуйте магічний квадрат заданого порядку (наприклад, 3×3 або 4×4).
- Розподіліть символи вихідного тексту по квадрату та запишіть шифртекст у порядку магічного квадрата.

Завдання 2. Зашифрувати текстове повідомлення, згідно з варіантами, визначеними викладачем, застосовуючи вивчені методи шифрування

Виконайте шифрування текстового повідомлення відповідно до свого варіанту, використовуючи один із вивчених методів:

- **Проста перестановка за ключем**
- **Подвійна перестановка**
- **Шифрування за допомогою магічного квадрата**

1. Використовуйте один із методів шифрування, вказаних у вашому варіанті.
2. Запишіть вихідний текст.
3. Виконайте повний процес шифрування, зазначаючи проміжні етапи.
4. Запишіть зашифрований текст.
5. Оформіть результати у вигляді звіту або реалізуйте процес у програмному коді.

Варіанти завдань:

Варіант	Вихідне повідомлення	Метод шифрування	Ключ (або квадратний

			розмір)
1	КРИПТОГРАФІЯ	Проста перестановка	Ключ: «КОД»
2	БЕЗПЕКА ДАНИХ	Подвійна перестановка	Ключі: «СЕКРЕТ», «ЗАХИСТ»
3	ШИФРУВАННЯ ІНФОРМАЦІЇ	Магічний квадрат	Розмір: 3×3
4	АЛГОРИТМ ШИФРУ	Проста перестановка	Ключ: «КРИПТО»
5	ЦИФРОВИЙ ПІДПИС	Подвійна перестановка	Ключі: «КОД», «БЕЗПЕКА»
6	ЗАХИСТ ІНФОРМАЦІЇ	Магічний квадрат	Розмір: 4×4
7	ПАРОЛЬНИЙ ЗАХИСТ	Проста перестановка	Ключ: «ШИФР»
8	ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ	Подвійна перестановка	Ключі: «ЛОГІН», «КЛЮЧ»
9	КОНФІДЕНЦІЙНІСТЬ	Магічний квадрат	Розмір: 5×5
10	СТЕГАНОГРАФІЯ	Проста перестановка	Ключ: «ПРИХОВАННЯ»

Порядок і рекомендації щодо виконання роботи

1. У звіті до практичної роботи надайте виконане завдання з шифрування індивідуального повідомлення, включаючи опис методів шифрування, які використовуються в даній роботі.

2. Відповісти на контрольні питання:

A. Що є ключем для шифрування та розшифрування при використанні методу простої перестановки?

B. Який елемент є ключем для шифрування в методі подвійної перестановки?

C. Що таке «магічні квадрати»?

D. Які основні принципи шифрування за допомогою простої перестановки по ключу?

E. Які основні принципи шифрування методом подвійної перестановки?

3. Оформити звіт.

Вимоги щодо оформлення та порядку подання звіту практичної роботи

1. У звіті до цієї роботи повинні бути вказані:

- номер практичної роботи, прізвище та ініціали студента, шифр навчальної групи, мета роботи;
- результати виконання завдань № 1 та 2;
- відповіді на запитання (п. 2 «Порядок і рекомендації щодо виконання роботи»).

2. Звіт має бути оформлений в електронному вигляді в одному з форматів: *.odf, *.doc або *.docx.
3. Звіт потрібно надіслати викладачу в архіві (файл назвати: БІС_Pract_07_Прізвище_Ініціали*), що містить файл зі звітом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. Горбатий І. В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи: навч. посіб./ І. В. Горбатий, А. П. Бондарєв. - Львів: Видавництво Львівської політехніки, 2016. - 336 с.

2. Грищук Р. В. Основи кібернетичної безпеки: монографія/ Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника, - Житомир: ЖНАЕ, 2016. - 636 с.

3. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. - К. : ДУТ, 2015. - 288 с.

4. Дегтярьова Л. Завдання та методичні рекомендації для виконання лабораторних робіт із дисципліни «Безпека інформаційних систем» для здобувачів вищої освіти за освітньо-професійною програмою «Інформаційні управляючі системи» спеціальності 126 Інформаційні системи та технології галузі знань 12 Інформаційні технології СВО «Бакалавр». Полтава: ПДАУ, 2021. 44 с.

5. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» https://zakon.rada.gov.ua/laws/show/3475-15#Text 2

6. Закон України «Про інформацію» https://zakon.rada.gov.ua/laws/show/2657- 12#Text

7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

8. Закон України «Про основні засади забезпечення кібербезпеки України» https://zakon.rada.gov.ua/laws/show/2163-19#Text

9. Постанова КМУ від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

10. Наказ Адміністрації Держспецзв'язку від 20.09.2021 № 576 «Про затвердження Вимог щодо рівня якості послуг рухомого (мобільного) зв'язку» https://zakon.rada.gov.ua/laws/show/z1298-21#Text

Формат 60x84/16. Гарнітура Times New Roman
Зам. № 49. Ум.друк.арк. 2,79.

Редакційно-видавничий відділ ДВНЗ «УжНУ»
88000, м. Ужгород, вул. Заньковецької, 89
E-mail: dep-editors@uzhnu.edu.ua