МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДВНЗ «Ужгородський національний університет»

Фізичний факультет

Кафедра твердотільної електроніки з/с інформаційної безпеки

**КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ:**

**проектування, впровадження, супровід**

Старший викладач: Гребенніков Вадим Вікторович

**ЗБІРНИК ЛЕКЦІЙ - 2013**

**Семестр 7 Модуль 1**

 1. Головні принципи та етапи захисту від загроз. Номативно-правове забезпечення захисту інформації

 2. Етапи створення КСЗІ в ІТС

 3. 1-й етап - формування вимог до КСЗІ

 4. Положення про службу захисту інформації в ІТС

###  5. Складання моделі порушника безпеки інформації в ІТС

###  6. Складання моделі загроз для інформації в ІТС

 7. Формування завдання та варіанту побудовиКСЗІ

 8. Основні вимоги до КЗЗ від НСД

#  9. Побудова і структура послуг безпеки інформації

# 10. Побудова і структура гарантій реалізації послуг безпеки

11. Вимоги щодо захисту інформації від НСД в АС класу 1

12. Особливості захисту секретної інформації в АС класу 1

**Семестр 8 Модуль 2**

13. 2-й етап - розробка політики безпеки інформації в ІТС

### 14. Складання Плану захисту інформації в ІТС

15. Вибір операційної системи, АВПЗ і КЗЗ

16. Опис КЗЗ від НСД, що мають експертні висновки

17. 3-й етап - технічне завдання на створення КСЗІ

### 18. 4-й етап - проектування КСЗІ в ІТС

19. 5-й етап - введення КСЗІ в дію та оцінка захищеності інформації

20. Попередні випробування та дослідна експлуатація КСЗІ

### 21. Державна експертиза КСЗІ в ІТС

### 22. 6-й етап - супровід КСЗІ в ІТС

23. Державний контроль за станом ТЗІ

24. Відповідальність за невиконання вимог захисту інформації

**Семестр 7 Модуль 1**

**1. Головні принципи та етапи захисту від загроз.**

**Номативно-правове забезпечення захисту інформації**

Загальний аналіз проблем організовування захисту від будь-яких загроз дає можливість визначити 4 головні принципи та етапи заходів:

1) організація зовнішніх рубежів безпеки з метою своєчасного виявлення загроз;

2) організація протидії загрозам та їх блокування, тобто зупинення та локалізації загроз під час їх реалізації;

3) забезпечення нейтралізації та ліквідації загроз, а також подолання наслідків загроз, які не вдалося блокувати;

4) попередження загроз, тобто аналіз відомих загроз та впровадження відповідних запобіжних заходів.

Стосовно автоматизованих (комп’ютерних) систем (далі - АС) ці принципи та етапи дають можливість також визначити 4 етапи та види захисту від загроз для електронних інформаційних ресурсів АС, які циклічно повторюються з метою постійного оновлення та підвищення ефективності заходів і засобів захисту.

**Виявлення ► Зупинення ► Нейтралізація ► Попередження**

**1. Етап виявлення**

*На організаційному рівні* – це забезпечення пропускного режиму, цілодобової охорони та контролю периметра безпеки, а також контррозвідувальних заходів служби безпеки установи.

*На інженерно-технічному рівні*– це використання інженерних споруд і технічних засобів пропускного режиму, охоронної сигналізації та відеоспостереження.

**2. Етап зупинення**

Ці заходи забезпечують апаратно-програмне блокування спроб несанкціонованого доступу (далі - НСД) порушника (хакера) до інформації в АС або ураження системи вірусами за допомогою спеціальних апаратних комплексів та програмних засобів захисту інформації. Для цього в АС встановлюються міжмережові екрани, файерволи (брандмауери), антивірусні програмні засоби та спеціальні комплекси засобів захисту інформації від НСД.

Зазначимо, що ці заходи можуть бути спрямовані на документування методів НСД до АС для наступного дослідження їх; збереження слідів правопорушення; взаємодію (у разі необхідності) з державними правоохоронними органами щодо виявлення та розкриття правопорушення (в тому числі за готування до злочину і за замах на злочин); сприяння притягненню винних до відповідної відповідальності (кримінальної, адміністративної, цивільно-правової, дисциплінарної).

**3. Етап нейтралізації**

*На організаційно-правовому рівні* – це дисциплінарне або адміністративне (кримінальне) розслідування правопорушення (злочину) та притягнення винних до відповідальності.

*На апаратно-програмному**рівні*– це подолання наслідків реалізації загроз у разі порушень:

- технологічих процесів - їх відновлення за допомогою плану аварійного відновлення та проведення ремонтних заходів;

- операційної системи та програмних засобів - їх відновлення за допомогою інсталяційних файлів (дисків);

- інформаійних ресурсів - їх відновлення за допомогою резервних і архівних копій, які зберігаються на зовнішніх носіях.

**4. Етап попередження**

*На організаційному рівні* – це проведення аналізу відомих загроз, прогнозування нових загроз і пошук відповідних запобіжних заходів, дезінформаційне легендування об’єктів захисту, розширення периметру безпеки, періодичне оновлення політики безпеки та плану захисту, постійне навчання та тренування персоналу.

*На інженерно-технічному рівні*– це застосування пасивних засобів захисту: закриття вікон та встановлення на них грат і штор (жалюзі), закриття та опечатування дверей, пломбування системних блоків, роз’ємів технічних засобів АС тощо, використання систем екранування, заземлення та зашумлення, а також модернізація наявної системи захисту та впровадження нових засобів ТЗІ.

**Номативно-правові акти України, які визначають необхідність створення КСЗІ в ІТС**

Історія захисту інформації в Україні розпочалася з Закону України **«Про захист інформації в автоматизованих системах»**, прийнятого постановою Верховної Ради України № 81/94-ВР від 5 липня 1994 року.

У тому же році постановою Кабінету Міністрів України (далі - ПКМУ) від 9 вересня 1994 року № 632 було затверджене **«Положення про технічний захист інформації в Україні»** (далі - ТЗІ), згідно якого була створена Державна служба України з питань ТЗІ.

Через 3 роки постановою КМУ від 8 жовтня 1997 року № 1126 була затверджена **«Концепція ТЗІ в Україні»**. Вонавизначає поняття ТЗІ таким чином: це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

А вже через 2 роки з’явилося нове **«Положення про ТЗІ в Україні»**, затверджене Указом Президента України від 27 вересня 1999 року № 1229. Пов’язане це було з тим, що питання ТЗІ були покладені на Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (скорочено - ДСТСЗІ СБУ), до складу якого і увійшла Державна служба з питань ТЗІ. Старе положення втратило чинність згідно постанови КМУ від 13 березня 2002 року № 281.

**«Положення про ТЗІ в Україні»** визначає поняття ТЗІ таким чином: це діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності важливої для держави, суспільства і особи інформації.

Воно визначає також такі терміни:

- **конфіденційність** - властивість інформації бути захищеною від несанкціонованого ознайомлення;

- **цілісність** - властивість інформації бути захищеною від несанкціонованого руйнування або знищення;

- **доступність** - властивість інформації бути захищеною від несанкціонованого блокування;

- інформаційна система - автоматизована система, комп'ютерна мережа або система зв'язку.

Тепер з'ясуємо, яку інформацію треба захищати:

**Закон України «Про інформацію» (1992)**

**Стаття 20. Доступ до інформації**

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

**Стаття 21. Інформація з обмеженим доступом**

1. Інформацією з обмеженим доступом (далі - ІзОД) є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

**Закон України «Про доступ до публічної інформації» (2011)**

**Стаття 7. Конфіденційна інформація**

1. Конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

2. Розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди - лише в інтересах національної безпеки, економічного добробуту та прав людини.

**Стаття 8. Таємна інформація**

1. Таємна інформація - інформація, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

**Стаття 9. Службова інформація**

1. До службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

2. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування».

**Закон України «Про захист персональних даних****» (2010)**

**Стаття 5. Об'єкти захисту**

1. Об'єктами захисту є персональні дані.

2. Персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом.

**Закон України «Про електронні документи та електронний документообіг****» (2003)**

**Стаття 15. Обіг електронних документів, що містять інформацію з обмеженим доступом**

В інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, які забезпечують обмін електронними документами, що містять інформацію, яка є власністю держави, або ІзОД, повинен забезпечуватися захист цієї інформації відповідно до законодавства.

*Таким чином, потрібно захищати ІзОД та інформацію, що є власністю держави та циркулює в інформаційно-телекомунікаційних системах.*

Закон України «**Про захист інформації в автоматизованих системах**» визначив термін захист інформації: це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. *Разом з тим, у законі ще не застосовувалось таке поняття як комплексна система захисту інформації.*

Також він визначив термін автоматизована система (далі - АС): це система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки та зв'язку), а також методи і процедури, програмне забезпечення.

**Згідно ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення»:**

АС - організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність.

Згідно НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»:

- АС - організаційно-технічна система, що реалізує інформаційну технологію та поєднує у собі: обчислювальну систему, фізичне середовище, персонал та інформацію, яка обробляється.

- захист інформації в АС - діяльність, спрямована на забезпечення безпеки оброблюваної в АС інформації та системи у цілому, що дає змогу запобігти реалізації загроз або унеможливити її, та зменшити ймовірність завдання збитків від реалізації загроз.

- комплексна система захисту інформації (далі - КСЗІ) - це сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Наступним етапним документом став **Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»**, який був прийнятийу2005 році на заміну Закону «Про захист інформації в АС».Він визначив багато нових термінів, зокрема, такі:

- КСЗІ - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

## - захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

- інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

- телекомунікаційна система - організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином;

- інформаційно-телекомунікаційна система (далі - ІТС) - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

- інформаційний ресурс - будь-які дані в електронному вигляді, які обробляються або зберігаються в інформаційно-телекомунікаційній системі.

**Закон України «Про захист інформації в ІТС»**

**Стаття 2. Об'єкти захисту в системі**

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

**Стаття 8. Умови обробки інформації в системі**

Інформація, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням КСЗІ з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення КСЗІ, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

**Стаття 9. Забезпечення захисту інформації в системі**

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

**Стаття 10. Повноваження державних органів у сфері захисту інформації в системах**

Вимоги до забезпечення захисту інформації, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

- розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

- визначає вимоги та порядок створення КСЗІ, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

- організовує проведення державної експертизи КСЗІ, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

- здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом;

- здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в ІТС та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту інформації, яка є власністю держави, або ІзОД, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

**Закон України «Про Державну службу спеціального зв'язку**

**та захисту інформації України» (2006)**

*Згідно цього закону ДСТСЗІ СБУ вийшов зі складу СБУ та був реорганізоваий у Державну службу спеціального зв'язку та захисту інформації України (скорочено – Держспецзв'язку), яка є спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.*

**Стаття 16.** На Держспецзв'язку згідно визначених завдань покладаються такі обов'язки:

3) розроблення порядку та вимог щодо захисту державних інформаційних ресурсів\* в ІТС, криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

***\*******державні інформаційні ресурси*** *- систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб’єктами владних повноважень.*

*У «Положенні про Реєстр ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління», затвердженому постановою Кабінету Міністрів України від 03.08.2005 № 688:*

***державні електронні інформаційні ресурси*** *- відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством.*

11) накопичення та аналіз даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІТС, а також про їх наслідки, інформування правоохоронних органів для вжиття заходів із запобігання та припинення кримінальних правопорушень у зазначеній сфері; оцінка стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, надання відповідних рекомендацій;

13) погодження проектів створення ІТС, в яких оброблятиметься інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, проведення їх експертної оцінки і визначення можливості введення в експлуатацію;

16) встановлення порядку і вимог щодо використання ІТС, у тому числі загального користування, органами державної влади, органами місцевого самоврядування, підприємствами, установами і організаціями незалежно від форм власності, які збирають, обробляють, зберігають та передають інформацію, яка є власністю держави, або інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законом;

32) видача атестата відповідності комплексних систем захисту інформації ІТС, із застосуванням яких обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вимогам нормативних документів з питань технічного захисту інформації.

**Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію**

(затверджена ПКМУ від 27.11.98 № 1893)

18. Використання ІТС для друкування документів з грифом «Для службового користування» та обробки конфіденційної інформації, що є власністю держави, може здійснюватися тільки після створення в ній КСЗІ та підтвердження відповідності створеної системи вимогам нормативних документів з питань технічного захисту інформації в порядку, встановленому законодавством.

Дозвіл на використання ІТС із зазначеною метою надається згідно з наказом керівника організації за наявності атестата відповідності КСЗІ.

Основний керівний нормативно-правовий акт:

**Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах**

(далі – Правила)(затверджені ПКМУ від 29.03.2006 № 373)

3. У Правилах наведені нижче терміни вживаються у такому значенні:

- автентифікація - процедура встановлення належності користувачеві інформації в системі (далі - користувач) пред'явленого ним ідентифікатора *(пароль)*;

- ідентифікація - процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою *(логін)*.

4. Захисту в системі підлягає:

- відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

- конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених Законом України "Про доступ до публічної інформації";

- службова інформація;

- інформація, яка становить державну або іншу передбачену законом таємницю (далі - таємна інформація);

- інформація, вимога щодо захисту якої встановлена законом.

5. Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

6. Під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

7. Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

11. У системі здійснюється обов'язкова реєстрація:

- результатів ідентифікації та автентифікації користувачів;

- результатів виконання користувачем операцій з обробки інформації;

- спроб несанкціонованих дій з інформацією;

- фактів надання та позбавлення користувачів права доступу до інформації та її обробки;

- результатів перевірки цілісності засобів захисту інформації.

Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі (адміністратор безпеки).

Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки.

Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.

12. Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

13. Передача службової і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

14. Порядок підключення систем, в яких обробляється службова і таємна інформація, до глобальних мереж передачі даних визначається законодавством.

15. У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації.

Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

**Організаційні засади забезпечення захисту інформації**

16. Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі - КСЗІ), яка призначається для захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень (далі - ПЕМВН), акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

- несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

- спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації.

Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято розпорядником інформації.

17. Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

18. Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації (далі - СЗІ), яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію КСЗІ, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

СЗІ утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

У разі коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

19. Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого СЗІ плану захисту інформації в системі.

План захисту інформації в системі містить:

- завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

- визначення моделі загроз для інформації в системі;

- основні вимоги щодо захисту інформації та правила доступу до неї в системі;

- перелік документів, згідно з якими здійснюється захист інформації в системі;

- перелік і строки виконання робіт службою захисту інформації.

20. Вимоги та порядок створення КСЗІ встановлюються Адміністрацією Держспецзв'язку (далі - Адміністрація).

Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або КСЗІ.

21. У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.

У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент проектування системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту.

22. Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією.

Органи виконавчої влади, які мають дозвіл на провадження діяльності з технічного захисту інформації для власних потреб, вправі за згодою департаменту організовувати проведення державної експертизи системи захисту на підприємствах, в установах та організаціях, які належать до сфери їх управління.

Порядок проведення такої експертизи встановлюється органом виконавчої влади за погодженням з Адміністрацією.

23. Виконавцем робіт із створення системи захисту може бути суб'єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері технічного захисту інформації, необхідність проведення якого визначено технічним завданням на створення системи захисту.

Для проведення інших видів робіт з технічного захисту інформації, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії.

Якщо для створення системи захисту необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензії на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

**2. Етапи створення КСЗІ в ІТС**

Основний керівний документ щодо створення КСЗІ в ІТС – це **НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»**

Він визначає порядок прийняття рішень щодо складу КСЗІ в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Побудований у вигляді керівництва, яке містить перелік робіт і посилання на діючі нормативні документи, у відповідності до яких ці роботи необхідно виконувати. Якщо якийсь з етапів чи видів робіт не нормовано, наводиться короткий зміст робіт та якими результатами вони повинні закінчуватись.

Дія цього НД ТЗІ поширюється тільки на ІТС, в яких здійснюється обробка інформації автоматизованим способом. Відповідно, для таких ІТС чинні всі нормативно-правові акти та нормативні документи щодо створення ІТС та щодо захисту інформації в АС. НД ТЗІ не встановлює нових норм, а систематизує в одному документі вимоги, норми і правила, які безпосередньо або непрямим чином витікають з положень діючих нормативних документів.

НД ТЗІ призначений для суб’єктів інформаційних відносин (власників або розпорядників ІТС, користувачів), діяльність яких пов’язана з обробкою інформації, що підлягає захисту, розробників КСЗІ в ІТС, для постачальників компонентів ІТС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам ТЗІ.

Встановлений цим НД ТЗІ порядок є обов’язковим для всіх суб’єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб’єкти системи ТЗІ можуть використовувати як рекомендації.

Порядок створенняКСЗІ в ІТС є єдиним незалежно від того, створюється КСЗІ в ІТС, яка проектується, чи в діючій ІТС, якщо виникла необхідність забезпечення захисту інформації або модернізації вже створеної КСЗІ.

Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.

Порядок створення КСЗІ в ІТС розглядається цим НД як сукупність впорядкованих у часі, взаємопов’язаних, об’єднаних в окремі етапи робіт, виконання яких необхідне й достатньє для КСЗІ, що створюється.

Створення КСЗІ повинно виконуватись у комплексі із заходами, щодо забезпечення режиму секретності, протидії технічним розвідкам, а також з режимними заходами щодо охорони інформації з обмеженим доступом, яка не є державною таємницею.

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

- несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів тощо;

- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом та умовами експлуатації ІТС.

Створення **комплексів технічного захисту інформації від витоку технічними каналами** здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

Створення **комплексу засобів захисту від несанкціонованого доступу** (далі – КЗЗ) здійснюється в усіх ІТС, де обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації.

Рішення щодо необхідності вжиття заходів захисту від спеціальних впливів на інформацію приймається власником інформації в кожному випадку окремо.

Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження діяльності у сфері захисту інформації.

Після прийняття рішення про необхідність створення КСЗІ в ІТС для організації цих робіт створюється Служба захисту інформації (далі - СЗІ) в ІТС.

**Цей НД ТЗІ визначає такі етапи створення КСЗІ та її документів:**

1. Формування вимог до КСЗІ в ІТС

1.1. Обґрунтування необхідності створення КСЗІ і призначення СЗІ:

 **-** наказ про порядок проведення робіт зі створення КСЗІ

 - наказ про створення СЗІ

 - положення про СЗІ

 - перелік інформації, що підлягає обробленню в ІТС та потребує захисту

1.2. Категоріювання ІТС:

 - наказ про призначення комісії з категоріювання

 - акт категоріювання

 1.3. Обстеження середовищ функціонування ІТС:

 - наказ про призначення комісії з обстеження

 - акт обстеження

 - формуляр ІТС

1.4. Опис моделі порушника політики безпеки інформації: модель порушника

1.5. Опис моделі загроз для інформації: модель загроз

1.6. Формування завдання на створення КСЗІ: звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ

2. Розробка політики безпеки інформації в ІТС

2.1. Вибір варіанту КСЗІ

2.2. Складання політики безпеки

2.3. Складання плану захисту

2.4. Складання календарного плану робіт із захисту інформації

3. Розробка Технічного завдання на створення КСЗІ:

- складання технічного завдання та погодження його з органами Держспецзв’язку

4. Проектування КСЗІ:

- складання документів ескізного проекту КСЗІ

- складання документів технічного проекту КСЗІ

- складання документів робочого проекту КСЗІ

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

5.1. Підготовка КСЗІ до введення в дію:

- інструкція про порядок введення в експлуатацію КСЗІ

5.2. Навчання користувачів:

- інструкція адміністратора безпеки в ІТС

- інструкція системного адміністратора ІТС

- інструкція користувача ІТС

- правила управління паролями в ІТС

- правила видачі, вилучення та обміну персональних ідентифікаторів, інших атрибутів розмежування доступу в ІТС

5.3. Комплектування КСЗІ

5.4. Будівельно-монтажні роботи:

- наказ про призначення комісії з приймання робіт

- акт приймання робіт

5.5. Пуско-налагоджувальні роботи:

- акт інсталяції та налагоджування АВПЗ і КЗЗ від НСД

- акт оцінки відповідності проведених робіт вимогам експлуатаційних документів

5.6. Попередні випробування КСЗІ:

- наказ про створення комісії з проведення випробувань

- програма та методика попередніх випробувань

- протокол про проведення попередніх випробувань

- акт про приймання КСЗІ у дослідну експлуатацію

5.7. Дослідна експлуатація КСЗІ:

- наказ про введення ІТС в дослідну експлуатацію

- акт про завершення дослідної експлуатації

- акт про завершення робіт зі створення КСЗІ

5.8. Державна експертиза КСЗІ:

- заявка на проведення державної експертиза КСЗІ

- експертний висновок щодо відповідності КСЗІ вимогам НД ТЗІ

- атестат відповідності КСЗІ вимогам НД ТЗІ

- наказ про дозвіл на обробку в ІТС інформації, яка підлягає захисту

**6. Супровід КСЗІ:**

- наказ про порядок забезпечення захисту інформації в ІТС

- інструкція щодо забезпечення правил обробки ІзОД в ІТС

- інструкція з антивірусного захисту інформації в ІТС

- інструкція про порядок використання засобів КЗІ в ІТС

- інструкція про порядок обліку та використання машинних носіїв інформації

- інструкція з правил управління паролями в ІТС

- інструкція про порядок створення і зберігання резервних копій інформаційних ресурсів ІТС

- інструкція про порядок проведення контролю режиму обробки та захисту інформації в ІТС

- інструкція про порядок супроводу та модернізації КСЗІ в ІТС

- інструкція про **порядок відновлювальних та ремонтних робіт** ІТС

- інші іструкції.

### 3. 1-й етап - формування вимог до КСЗІ

1-й етап - формування вимог до КСЗІ в ІТС - складається з таких заходів:

- обґрунтування необхідності створення КСЗІ і призначення СЗІ;

- категоріювання ІТС**;**

- обстеження середовищ функціонування ІТС;

- опис моделі порушника політики безпеки інформації;

- опис моделі загроз для інформації;

- формування завдання на створення КСЗІ.

Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

- оцінки можливих переваг (фінансово-економічних, соціальних тощо) експлуатації ІТС у разі створення КСЗІ.

На підставі **НД ТЗІ 2.5-005-99 «Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД»** за сукупністю характеристик ІТС виділено три ієрархічні класи, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

**Клас «1»** - одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності. Особливості такого класу:

- в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється;

- технічні засоби (носії інформації і засоби У/В ) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження і У/В всієї інформації.

Приклад - автономна ПЕОМ, доступ до якої контролюється з використанням організаційних заходів.

**Клас «2»** - локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Істотна відміна від попереднього класу - наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності. Приклад - ЛОМ.

**Клас «3»** - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності. Істотна відміна від попереднього класу - необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки. Приклад - глобальна мережа.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ, після чого відповідальний за ТЗІ організації-власника (розпорядника) ІТС готує для керівника організації 3 накази:

1) про створення **Служби захисту інформації в ІТС** (далі - СЗІ), порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000 «Типове положення про СЗІ в АС»;

2) про призначення **комісії з категоріювання ІТС**, завдання та повноваження якої визначено в НД ТЗІ 1.6-005-2013 «Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»;

3) про призначення **комісії з обстеження середовищ функціонування ІТС**, завдання та повноваження якої визначено в ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт».

До складу СЗІ, який визначається наказом, повинні призначатися фахівці з таких питань:

1. захисту інформації від витоку технічними каналами;
2. захисту каналів зв’язку і комутаційного обладнання,
3. налагодження і адміністрування засобів захисту інформації,
4. керування базами даних захисту інформації;
5. налагодження і керування активним мережевим обладнанням;
6. захищених технологій обробки інформації.

За функціональними обов’язками особовий склад СЗІ складається з таких спеціалістів (за рівнем ієрархії):

1. системний адміністратор ІТС;
2. мережевий адміністратор ІТС;
3. адміністратор безпеки інформації в ІТС;
4. адміністратор КСЗІ в ІТС.

Після призначення СЗІ її керівник складає «**Положення про СЗІ в ІТС**», що має бути оформлене у вигляді окремого документа згідно рекомендацій НД ТЗІ 1.4-001-2000 та затверджене керівником організації-власника (розпорядника) ІТС.

Положення повинно складатись з таких розділів:

1. загальні положення;
2. завдання СЗІ;
3. функції СЗІ;
4. повноваження та відповідальність СЗІ;

- взаємодія СЗІ з іншими підрозділами організації та зовнішніми підприємствами, установами, організаціями;

1. штатний розклад та структура СЗІ;
2. організація та фінансування робіт СЗІ.

В залежності від конкретних завдань і умов функціонування СЗІ дозволяється, у разі необхідності, поєднувати окремі розділи в один, вводити нові розділи або вилучати розділи, що не є актуальними.

До Положення у вигляді додатків можуть включатися нормативні документи, таблиці, схеми, графіки, необхідні для визначення заходів захисту інформації, плани об’єктів захисту з вказанням робочих місць та встановлених на них технічних засобів передачі, прийому, зберігання, обробки інформації, що підлягає захисту, та інші документи.

Положення має бути погоджене з юрисконсультом та керівниками підрозділів (служби безпеки, РСО, підрозділу ТЗІ) організації.

Зміни суттєвого характеру вносяться до Положення на підставі наказу керівника організації (підрозділу, до якого структурно входить СЗІ).

**Категоріювання ІТС**

Об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься ІзОД, підлягають обов’язковому категоріюванню. Об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься тільки відкрита інформація, категоріюванню не підлягають.

Об’єктами категоріювання є об’єкти інформаційної діяльності (далі - ОІД), в тому числі об’єкти електронно-обчислювальної техніки (далі - ЕОТ) ІТС. ОІД - це інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами ІзОД.

Категоріювання ІТС здійснюється комісією організації-власника (розпорядника) ІТС для визначення необхідного рівня захисту інформації, що обробляється на об’єктах ЕОТ ІТС. Категоріювання здійснюється за ознакою ступеня обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.

Згідно **ТПКО-95 «Тимчасове положення про категоріювання об'єктів»** установлюються 4 категорії об'єктів, на яких обробляється технічними засобами та/або озвучується ІзОД, що:

- становить державну таємницю, для якої встановлено гриф секретності «особливої важливості» - перша (І);

- становить державну таємницю, для якої встановлено гриф секретності «цілком таємно» - друга (ІІ);

- становить державну таємницю, для якої встановлено гриф секретності «таємно», а також інформація, що містить відомості, які становлять іншу передбачену законом таємницю - третя (ІІІ);

- не становить державної таємниці - четверта (ІV).

Категоріювання ОІД четвертої категорії здійснюється згідно вимог **НД ТЗІ 1.6-005-2013 «Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»**.

Категоріювання може бути первинним, черговим або позачерговим. Первинне категоріювання здійснюється у разі створення ІТС, де буде оброблятися ІзОД. Чергове - не рідше ніж один раз на 5 років. Позачергове - у разі зміни ознаки, за якою була встановлена категорія ІТС.

Комісія з категоріювання визначає ступень обмеження доступу до інформації, яка оброблятиметься в ІТС, та з урахуванням цього ступеня встановлює категорію ІТС. Встановлена категорія зазначається в Акті категоріювання ІТС, який складається комісією за результатами її роботи. Акт категоріювання є чинним протягом 5 років з моменту проведення категоріювання, якщо не змінилась ознака, за якою була встановлена категорія об’єкта.

В акті зазначається:

1. Підстава для категоріювання (рішення про створення КСЗІ, закінчення терміну дії акта категоріювання, зміна ознаки, за якою була встановлена категорія, та реквізити наказу про призначення комісії з категоріювання.

2. Вид категоріювання: первинне, чергове, позачергове (у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання, та реквізити акту, яким було встановлено цю категорію).

3. В ІТС здійснюється обробка ІзОД.

4. Ступінь обмеження доступу до ІзОД, що обробляється в ІТС (передбачена законом таємниця; службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, інша конфіденційна інформація, вимога щодо захисту якої встановлена законом).

5. Встановлена комісією категорія.

ІТС, яким комісія встановила відповідну категорію, вносяться до «**Переліку категорійованих об’єктів**», який ведеться власником (розпорядником, користувачем) ОІД.

### Обстеження середовищ функціонування ІТС

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

Під час проведення обстеження ІТС необхідно вивчити такі середовища:

- обчислювальне;

- інформаційне;

- користувацьке;

- фізичне (у разі обробки інформації, що становить державну таємницю).

При обстеженні обчислювального середовища ІТС повинні бути проаналізовані й описані:

* обладнання - ЕОМ та їхні складові частини (процесори, монітори, термінали, робочі станції та ін.), периферійні пристрої;
* програмне забезпечення - вихідні, завантажувальні модулі, утиліти, СКБД, операційні системи та інші системні програми, діагностичні і тестові програми тощо;

- види і характеристики каналів зв'язку;

- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного, можливі обмеження щодо використання засобів тощо.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням тощо.

 Повинні бути зафіксовані всі активні і пасивні об’єкти, які беруть участь у технологічному процесі обробки і тим чи іншим чином впливають на безпеку інформації. Для кожного активного об’єкту ІТС має бути визначено перелік пасивних об’єктів, які з ним взаємодіють.

Окрім компонентів ІТС, необхідно дати опис технології обробки інформації в ІТС, що потребує захисту, тобто способів і методів застосування засобів обчислювальної техніки під час виконання функцій збору, зберігання, обробки, передачі і використання даних, або алгоритмів окремих процедур.

При цьому рекомендується розробити структурну схему інформаційних потоків в ІТС, яка б відображала інформаційну взаємодію між основними компонентами ІТС (завданнями, об’єктами) з прив’язкою до кожного елемента схеми категорій інформації та визначених політикою безпеки рівнів доступу до неї.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС. Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, за типом їхнього представлення в ІТС, визначені й описані види її представлення в ІТС. Класифікація є підставою для визначення власником (розпорядником) інформації або ІТС методів і способів захисту кожного окремого виду інформації.

За режимом доступу інформація в АС має бути поділена на відкриту та з обмеженим доступом. Відкриту інформацію слід поділити на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.

За правовим режимом інформація з обмеженим доступом повинна бути поділена на таємну, службову та конфіденційну. До таємної інформації має бути віднесена інформація, що містить відомості, які становлять державну, а також іншу, передбачену законом таємницю. Правила доступу до службової та конфіденційної інформації, во­ло­діти, ко­ри­стувати­ся чи ро­з­по­ря­джати­ся якою можуть ок­ре­мі фі­зи­ч­ні, юри­ди­ч­ні осо­би або де­р­жа­ва, встановлює законодавство та її власник.

Конфіденційна інформація може мати велику цінність для її власника, втрата або передача якої іншим особам може завдати організації (власнику) значних збитків. З метою встановлення правил розмежування доступу до конфіденційної інформації необхідно класифікувати її, поділивши на декілька категорій за ступенем цінності (критерії розподілу можуть бути визначені під час оцінки ризиків).

Для встановлення правил взаємодії активних і пасивних об’єктів ІТС інформація повинна бути класифікована за типом її представлення в ІТС (для кожної з визначених категорій встановлюються типи пасивних об’єктів комп’ютерної системи, якими вона може бути представлена). Для кожного виду інформації і типу об’єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи ІТС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС.

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об’єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

За результатами обстеження інформаційного середовища складається «**Перелік інформації, що підлягає автоматизованому обробленню в ІТС і потребує захисту**», який оформлюється як окремий документ, затверджений керівником організації-власника (розпорядника) відповідної інформації, або як розділ у інших документах (Політика безпеки, План захисту, Технічне завдання на створення КСЗІ тощо).

У переліку має бути наведено перелік інформаційних ресурсів (видів інформації), що підлягають обробленню в ІТС, класифікований за такими ознаками:

* назва відповідного інформаційного ресурсу, який визначається цільовим призначенням відповідної інформації;
* характеристики інформації відповідно до встановленого законодавством правового режиму та режиму доступу (ІДТ, КІВД, КІ, ВІВД, ВІ);
* вищий ступінь обмеження доступу (для ІДТ) до інформації (ступінь секретності) відповідно до вимог Зводу відомостей, що становлять державну таємницю;
* критичні властивості інформації з погляду забезпечення її захищеності, визначені з урахуванням вимог Правил 373 і вимог власника (розпорядника) інформації;
* вимоги (за наявності) щодо обмеження доступу до інформації користувачів ІТС різних категорій, визначені з урахуванням, наприклад, вимог «Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в АС» або «Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».

Окрім зазначених вище, можуть бути використані додаткові класифікаційні ознаки, корисні з погляду подальшого формулювання політики безпеки інформації, оброблюваної в ІТС, наприклад, вид подання відповідних інформаційних ресурсів тощо.

При обстеженні користувацького середовища здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов’язків та рівня кваліфікації;

- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ;

- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС.

За результатами обстеження вище зазначених середовищ складається «**Формуляр ІТС**», який оформлюється як окремий документ і складається з таких розділів:

- загальні відомості про ІТС;

- склад технічних засобів ІТС;

- склад програмного забезпечення;

- відомості про програмно-апаратний КЗЗ від НСД;

- відомості про впровадження, випробування та приймання в експлуатацію;

- посадові особи, відповідальні за технічне обслуговування;

- посадові особи, відповідальні за забезпечення захисту інформації;

- реєстрація проведених робіт (технічне обслуговування, ремонт, модернізація тощо);

- відмітки про проведення перевірок КСЗІ;

- перелік технічних та експлуатаційних документів КСЗІ.

У разі обробки в ІТС інформації, що становить державну таємницю, обов’язково здійснюється також обстеження фізичного середовища, під час якого аналізується взаємне розміщення засобів обробки інформації ІТС на ОІД, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів.

Порядок проведення обстеження повинен відповідати ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт», а в частині, що стосується захисту інформації від витоку технічними каналами, - НД ТЗІ 3.1-001-07 «Створення комплексу технічного захисту інформації. Передпроектні роботи».

Аналізу підлягають такі характеристики фізичного середовища:

- характеристика об’єктів, де розташовані компоненти ІТС (дані про інженерно-технічну споруду, її частину або декілька споруд, приміщення тощо);

- архітектурно-будівельні особливості приміщень: огороджувальні будівельні конструкції: стеля, підлога, стіни, перегородки (матеріал, товщина); підвісна стеля (конструкція, матеріал); вікна, двері, інші отвори (кількість, матеріал, розміри).

 - дані про складові об’єктів, що можуть впливати на показники ефективності захищеності ІзОД і які можуть бути середовищем поширення за межі КЗ її носіїв (інженерні комунікації, обладнання, оргтехніка, телебачення, електроживлення, заземлення, газо-, водопостачання, опалення, вентиляції, кондиціонування повітря, водостоку, каналізації, технологічне обладнання, огороджувальні будівельні конструкції, світлопроникні отвори приміщень, будинків, споруд тощо).

- наявність систем безпеки в установі, до яких може бути інтегрована КСЗІ (відеоспостереження, пожежна та охоронна сигналізації, системи зв’язку);

- схеми розміщення комунікацій, обладнання систем електроживлення, у тому числі трансформаторної підстанції;

- дані про складові об’єктів, які виходять за межу КЗ або її перетинають, застосування яких не обґрунтовано виробничою необхідністю і які підлягають демонтуванню, у подальшому застосуванні яких відсутня необхідність);

- опис систем заземлення (дані про перелік технічних засобів ІТС, що підлягають заземленню);

- результати аналізу фізичного середовища та пропозиції щодо необхідності отримання додаткових даних про можливі місця розміщення засобів технічної розвідки; проведення випробувань (у т.ч. спеціальних досліджень технічних засобів, які оброблятимуть ІзОД); застосування організаційних, інженерно-технічних заходів захисту (у т.ч. застосування засобів оброблення ІзОД, інших технічних засобів у захищеному виконанні).

За результатами комісія складає «**Акт обстеження середовищ функціонування ІТС**», який затверджується керівником організації-власника (розпорядника) ІТС і складається з таких розділів:

- клас і склад обчислювальної системи,

- перелік і характеристики інформаційних ресурсів,

- перелік і повноваження користувачів,

- опис фізичного середовища (до акту додаються генеральний і ситуаційний плани, схеми систем життєзабезпечення та заземлення).

**4. Положення про службу захисту інформації в ІТС**

**НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в АС»** встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації (далі - СЗІ) - «Положення про СЗІ в ІТС».

Як правило, Положення складається з таких розділів:

* завдання і функції СЗІ;
* повноваження і відповідальність СЗІ;
* взаємодія СЗІ з іншими підрозділами організації та зовнішніми установами;
* штатний розклад і структура СЗІ;
* організація робіт СЗІ;
* фінансування СЗІ.

В залежності від конкретних завдань і умов функціонування СЗІ дозволяється, у разі необхідності, поєднувати окремі розділи в один, вводити нові розділи (підрозділи) або вилучати розділи, що не є актуальними.

До Положення у вигляді додатків можуть включатися нормативні документи, таблиці, схеми, графіки, необхідні для визначення заходів захисту інформації, плани об’єктів захисту з вказанням робочих місць та встановлених на них технічних засобів передачі, прийому, зберігання, обробки інформації, що підлягає захисту та ін. документи.

Положення має бути погоджене з юрисконсультом та керівниками підрозділів (служби безпеки, РСО, підрозділу ТЗІ) організації. Положення затверджується наказом керівника організації або підрозділу, до якого структурно входить СЗІ.

### 5. Модель порушника безпеки інформації в ІТС

На підставі Акту обстеженнята визначення загроз для ІТС СЗІ розробляє «**Модель порушника безпеки інформації в ІТС**», яка затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту.

Модель порушника - це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо. Як порушник розглядається особа, яка може одержати несанкціонований доступ (далі - НСД) до роботи з включеними до складу ІТС засобами.

Модель порушника повинна визначати:

1. можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту;
2. категорії персоналу, користувачів ІТС та сторонніх осіб, із числа яких може бути порушник;
3. припущення про кваліфікацію порушника;
4. припущення про характер його дій.

Метою порушника можуть бути:

1. отримання необхідної інформації у потрібному обсязі та асортименті;
2. мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
3. нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Порушники спочатку поділяються на дві основні групи: зовнішні та внутрішні.

Зовнішніх порушників можна розділити на:

- добре озброєну та технічно оснащену групу, що діє зовні швидко і напролом;

- поодиноких порушників, що не мають допуску на об'єкт і намагаються діяти потайки й обережно, так як вони усвідомлюють, що сили реагування мають перед ним переваги.

Сторонні особи, що можуть бути порушниками:

- клієнти (представники організацій, громадяни);

- відвідувачі (запрошені з якого-небудь приводу);

- представники організацій, взаємодіючих з питань забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання тощо);

- представники конкуруючих організацій (іноземних служб) або особи, що діють за їх завданням;

- особи, які випадково або навмисно порушили пропускний режим (без мети порушити безпеку);

- будь-які особи за межами контрольованої зони.

Потенціальних внутрішніх порушників можна розділити на:

- допоміжний персонал об'єкту, що допущений на об'єкт, але не допущений до життєво важливого центру ІТС;

- основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);

- співробітників служби безпеки, які часто формально не допущені до життєво важливого центру ІТС, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

Серед внутрішніх порушників можна виділити такі категорії персоналу:

- користувачі (оператори) системи;

- персонал, що обслуговує технічні засоби (інженери, техніки);

- співробітники відділів розробки та супроводження програмного забезпечення (прикладні та системні програмісти);

- технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти ІТС);

- співробітники служби безпеки;

- керівники різних рівнів та посадової ієрархії.

Крім професійного шпигунства, можна виділити три основних мотиви порушень: безвідповідальність, самоствердження та корисливий інтерес.

При порушеннях, викликаних *безвідповідальністю*, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості. Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру заради *самоствердження* або у власних очах, або в очах колег.

Порушення безпеки ІТС може бути викликано *корисливим інтересом* користувача ІТС. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для несанкціонованого доступу до інформації в ІТС.

Усіх порушників можна класифікувати за такими ознаками:

1. за рівнем знань про ІТС;

- за рівнем можливостей;

- за часом дії;

- за місцем дії.

За рівнем знань про ІТС (в залежності від кваліфікації та професійної майстерності):

- володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС;

- володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування;

- володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС;

- знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості.

За рівнем можливостей (в залежності від методів і засобів, що використовуються):

- застосовує чисто агентурні методи отримання відомостей;

- застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

- використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні носії інформації, які можуть бути тайком пронесені крізь пости охорони;

- застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, перехоплення з каналів передачі даних, впровадження спеціальних програмних закладок).

За часом дії (в залежності від активності або пасивності системи):

- у процесі функціонування (під час роботи компонентів системи);

- у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т.д.);

- як у процесі функціонування, так і в період неактивності системи.

За місцем дії (в залежності від території доступу до засобів системи):

- без доступу на контрольовану територію організації;

- з контрольованої території без доступу до будівель та споруджень;

- усередині приміщень, але без доступу до технічних засобів;

- з робочих місць кінцевих користувачів (операторів);

- з доступом у зону даних (баз даних, архівів тощо);

- з доступом у зону управління засобами забезпечення безпеки.

Враховуються також такі обмеження та припущення про характер дій можливих порушників:

- робота з підбору та розстановки кадрів, а також заходи контролю за персоналом ускладнюють можливість створення коаліцій порушників, тобто злочинного угрупування (змови) і цілеспрямованих дій з подолання системи захисту двох і більше порушників;

- порушник, плануючи спробу НСД, приховує свої несанкціоновані дії від інших співробітників;

- НСД може бути наслідком помилок користувачів, адміністраторів, а також хиб прийнятої технології обробки інформації тощо.

Припускається, що в своєму рівні порушник - це фахівець вищої кваліфікації, який має повну інформацію про ІТС і засоби захисту. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

Під час формування моделі порушника обов'язково повинно бути визначено:

- ймовірність реалізації загрози,

- своєчасність виявлення,

- відомості про порушення.

Слід зауважити, що всі злочини, зокрема і комп’ютерні, здійснюються людиною. Користувачі ІТС, з одного боку, є її складовою частиною, а з іншого - основною причиною і рухаючою силою порушень і злочинів. Отже, питання безпеки захищених ІТС фактично є питанням людських відносин та людської поведінки.

**Модель порушників можна відобразити системою таблиць, наприклад:**

Для побудови моделі використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них вказується в дужках і оцінюється за 4-бальною шкалою.

**Таблиця 1. Категорії порушників, визначених у моделі**

|  |  |  |
| --- | --- | --- |
| Позначення | Визначення категорії | Рівень загроз |
|  | **Внутрішні по відношенню до ІТС** |  |
| ПВ1 | Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС | 1 |
| ПВ2 | Персонал, який обслуговує технічні засоби ІТС (інженери, техніки) | 2 |
| ПВ3 | Користувачі (оператори) ІТС | 2 |
| ПВ4 | Адміністратори ІТC, співробітники служби захисту інформації | 3 |
| ПВ5 | Співробітники служби безпеки установи та керівники різних рівнів | 4 |
|  | **Зовнішні по відношенню до ІТС** |  |
| ПЗ1 | Відвідувачі (запрошені з будь-якого приводу) | 1 |
| ПЗ2 | Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше) | 2 |
| ПЗ3 | Хакери  | 3 |
| ПЗ4 | Агенти конкурентів або закордонних спецслужб «під прикриттям» | 4 |

**Таблиця 2. Специфікація моделі порушника за мотивами здійснення порушень**

|  |  |  |
| --- | --- | --- |
| Позначення | Мотив порушення | Рівень загроз |
| М1 | Безвідповідальність | 1 |
| М2 | Самоствердження | 2 |
| М3 | Корисливий інтерес | 3 |
| М4 | Професійний обов’язок (ПЗ4) | 4 |

**Таблиця 3. Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС**

|  |  |  |
| --- | --- | --- |
| Позначення | Основні кваліфікаційні ознаки порушника | Рівень загроз |
| К1 | Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС | 1 |
| К2 | Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування | 2 |
| К3 | Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС | 3 |
| К4 | Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості  | 4 |

**Таблиця 4. Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту**

|  |  |  |
| --- | --- | --- |
| Позначення | Характеристика можливостей порушника | Рівень загроз |
| З1 | Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях | 1 |
| З2 | Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС | 2 |
| З3 | Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону | 3 |
| З4 | Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації  | 4 |

**Таблиця 5. Специфікація моделі порушника за часом дії**

|  |  |  |
| --- | --- | --- |
| Позначення | Характеристика можливостей порушника | Рівень загроз |
| Ч1 | Під час повної бездіяльності ІТС з метою відновлення та ремонту  | 1 |
| Ч2 | Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації  | 2 |
| Ч3 | Під час функціонування ІТС (або компонентів системи) | 3 |
| Ч4 | Як у процесі функціонування ІТС, так і під час призупинки компонентів системи | 4 |

**Таблиця 6. Специфікація моделі порушника за місцем дії**

|  |  |  |
| --- | --- | --- |
| Позначення | Характеристика місця дії порушника | Рівень загроз |
| Д1 | Усередині приміщень, але без доступу до технічних засобів ІТС | 1 |
| Д2 | З робочих місць користувачів (операторів) ІТС | 2 |
| Д3 | З доступом у зону зберігання баз даних, архівів тощо | 3 |
| Д4 | З доступом у зону керування засобами забезпечення безпеки ІТС | 4 |

**Виведемо два варіанти сумарного рівня загроз для окремих категорій можливих порушників:**

1) внутрішній порушник «ПВ» - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов’язків;

2) зовнішній порушник «ПЗ4» (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Посада | Кате-горія поруш-ника | Мо-тив пору-шення | Рівень обізнаності щодо ІТС | Можливості щодо подолання системи захисту | Можливості за часом дії | Можливості за місцем дії | Су-ма заг-роз |
| **прибир** | ПВ1 | М1 | К1 | З1 | Ч4 | Д1 | **9** |
| 1 | 1 | 1 | 1 | 4 | 1 |
| ПЗ4 | М4 | К4 | З4 | Ч4 | Д1 | **21** |
| 4 | 4 | 4 | 4 | 4 | 1 |
| **електр** | ПВ1 | М1 | К1 | З1 | Ч1 | Д1 | **8** |
| 1 | 1 | 1 | 1 | 3 | 1 |
| ПЗ4 | М4 | К4 | З4 | Ч1 | Д1 | **20** |
| 4 | 4 | 4 | 4 | 3 | 1 |
| **технік** | ПВ2 | М1 | К2 | З1 | Ч4 | Д3 | **12** |
| 2 | 1 | 2 | 1 | 4 | 2 |
| ПЗ4 | М4 | К4 | З4 | Ч4 | Д3 | **22** |
| 4 | 4 | 4 | 4 | 4 | 2 |
| **корист** | ПВ3 | М1 | К2 | З1 | Ч3 | Д2 | **11** |
| 2 | 1 | 2 | 1 | 3 | 2 |
| ПЗ4 | М4 | К4 | З4 | Ч3 | Д2 | **21** |
| 4 | 4 | 4 | 4 | 3 | 2 |
| **адмініс** | ПВ4 | М1 | К4 | З1 | Ч4 | Д4 | **17** |
| 3 | 1 | 4 | 1 | 4 | 4 |
| ПЗ4 | М4 | К4 | З4 | Ч4 | Д4 | **24** |
| 4 | 4 | 4 | 4 | 4 | 4 |
| **безпека** | ПВ5 | М1 | К1 | З1 | Ч4 | Д3 | **14** |
| 4 | 1 | 1 | 1 | 4 | 3 |
| ПЗ4 | М4 | К4 | З4 | Ч4 | Д3 | **23** |
| 4 | 4 | 4 | 4 | 4 | 3 |

Після зведення усіх даних 1-го варіанту в одну таблицю отримаємо таку табличну **«Модель внутрішнього порушника політики безпеки інформації»**:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Категорія порушника«ПВ» | Мо-тив пору-шень | Рівень обізнаності щодо ІТС | Можливості щодо подолання системи захисту | Можливості за часом дії | Можливості за місцем дії | Сума заг-роз |
| Служба безпеки | М1 | К1 | З1 | Ч4 | Д3 | **14** |
| Адмініст-ратор ІТС | М1 | К4 | З1 | Ч4 | Д4 | **17** |
| Користувач | М1 | К2 | З1 | Ч3 | Д2 | **11** |
| Технік ІТС | М1 | К2 | З1 | Ч4 | Д3 | **12** |
| Електрик | М1 | К1 | З1 | Ч1 | Д1 | **8** |
| Прибираль-ник | М1 | К1 | З1 | Ч4 | Д1 | **9** |

**Висновок:** з останньої таблиці видно, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адміністратор ІТС. Тому організація роботи цієї особи повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації.

Те, що основною загрозою для безпеки інформації в ІТС є персонал ІТС, підтверджують і дані, опубліковані у 2010 році американським інститутом комп′ютерної безпеки (Сан-Франциско, штат Каліфорнія), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

- несанкціонований доступ - 2%;

- ураження вірусами - 3%;

- технічні відмови апаратури мережі - 20%;

- цілеспрямовані дії персоналу - 20%;

- помилки персоналу (недостатній рівень кваліфікації) - 55%.

Таким чином, основною потенційною загрозою для інформації в ІТС слід вважати цілеспрямовані або випадкові деструктивні дії персоналу, оскільки вони становлять 75 % усіх випадків.

### 6. Модель загроз для інформації в ІТС

Після проведення обстеження всіх середовищ ІТС необхідно визначити всі можливі потенційні загрози для ІТС. Походження загроз може бути випадковим і навмисним.

Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в ІТС в процесі її функціонування. Найбільш відомими випадковими загрозами є стихійні лиха, відмови, збої, помилки та побічні впливи.

Сутність цих загроз (окрім стихійних лих, сутність яких незрозуміла) визначається таким чином:

- відмова - порушення працездатності системи, що призводить до неможливості виконання нею основних своїх функцій;

- збій - тимчасове порушення працездатності системи, наслідком чого може бути неправильне виконання у цей момент своїх функцій;

- помилка - неправильне виконання системою своїх функцій, що відбувається внаслідок її специфічного стану;

- побічний вплив - негативний вплив на систему, який чиниться будь-якими явищами, що відбуваються всередині системи або у зовнішньому середовищі.

Навмисне походження загроз обумовлюється зловмисними діями людей.

Передумови появи загрозможуть бути об'єктивними та суб'єктивними. Об'єктивні передумови можуть бути спричинені кількісною або якісною недостатністю елементів системи тощо. До суб'єктивних передумов відносяться різновиди людської діяльності: іноземна розвідка, промислове шпигунство, злочинні дії, неякісна робота персоналу ІТС.

Перераховані різновиди передумов інтерпретуються таким чином:

- кількісна недостатність - фізична нестача одного або декількох елементів системи, що викликає порушення технологічного процесу обробки даних і / або перевантаження наявних елементів.

- якісна недостатність - недосконалість конструкції (організації) елементів системи, в силу цього можуть з'являтися можливості випадкового або навмисного негативного впливу на оброблювану або збережену інформацію.

**Джерело загрози** - це безпосередній їх генератор або носій. Таким джерелом можуть бути люди, технічні засоби, моделі (алгоритми), а також - програми, технологічні схеми обробки, зовнішнє середовище.

Спробуємо тепер, спираючись на наведену системну класифікацію загроз безпеки інформації, визначити всю кількість загроз, потенційно можливих у сучасних ІТС. При цьому ми повинні врахувати не лише всі відомі загрози, але й ті загрози, що раніше не виявлялися, але потенційно можуть виникнути при застосуванні нових концепцій архітектурної побудови ІТС і технологічних схем обробки інформації.

Всі можливі канали витоку інформації (КВІ) класифікуються за двома критеріями:

- наявність доступу до ІТС;

- стан функціонування ІТС.

За першим критерієм КВІ можуть бути розділені на такі, що:

- не вимагають доступу, тобто дозволяють отримувати необхідну інформацію дистанційно (наприклад, шляхом візуального спостереження через вікна приміщень ІТС),

- вимагають доступу в приміщення ІТС. У свою чергу, такі канали можуть не залишити слідів в ІТС (наприклад, візуальний перегляд зображень на екранах моніторів або документів на паперових носіях), а можуть і залишити ті чи інші сліди (наприклад, розкрадання документів або машинних носіїв інформації).

За другим критерієм КВІ можуть бути розділені на:

- потенційно існуючі незалежно від стану ІТС (наприклад, викрадати носії інформації можна незалежно від того, в робочому стані знаходяться засоби АС чи ні);

- існуючі тільки в робочому стані ІТС (наприклад, побічні електромагнітні випромінювання та наведення).

В результаті такої класифікації отримаємо 6 класів КВІ, які мають таку орієнтовну характеристику:

- 1-й клас - КВІ, які проявляються безвідносно до обробки інформації без доступу до елементів ІТС ( підслуховування розмов, а також провокування на розмови осіб, що мають відношення до ІТС, і використання зловмисником візуальних, оптичних та акустичних засобів);

- 2-й клас - КВІ, які проявляються у процесі обробки інформації без доступу до елементів ІТС (електромагнітні випромінювання різних пристроїв ІТС, апаратури та ліній зв'язку, паразитні наведення в ланцюгах харчування, телефонних мережах, системах теплопостачання, вентиляції тощо);

- 3-й клас - КВІ, які проявляються безвідносно до обробки інформації з доступом до елементів ІТС, але без зміни останніх (всілякі види копіювання носіїв інформації і документів, а також розкрадання виробничих відходів);

- 4-й клас - КВІ, які проявляються у процесі обробки інформації з доступом до елементів ІТС, але без зміни останніх (запам'ятовування та копіювання інформації в процесі обробки, використання програмних закладок тощо);

- 5-й клас - КВІ, які проявляються безвідносно до обробки інформації з доступом до елементів ІТС і зі зміною останніх (підміна та розкрадання носіїв інформації й апаратури, впровадження у програмне забезпечення шкідливих кодів, вірусів тощо);

- 6-й клас - КВІ, які проявляються у процесі обробки інформації з доступом до елементів ІТС і зі зміною останніх (незаконне підключення до апаратури та ліній зв'язку, а також зняття інформації з ліній живлення різних елементів ІТС).

На підставі Акту обстеження та Моделі порушника політики безпеки СЗІ розробляє «**Модель загроз для** **інформації в ІТС**», яка затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ. Модель загроз має містити формалізований або неформалізований опис методів і засобів здійснення загроз для інформації, яка потребує захисту.

Модель загроз повинна визначити:

* перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);
* перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу.

Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

1. зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
2. збої та відмови у роботі технічних або програмних засобів (далі - ПЗ) ІТС;
3. наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);
4. помилки персоналу (користувачів) ІТС під час експлуатації;
5. навмисні дії (спроби) потенційних порушників.

Випадкові загрози суб’єктивної природи - це помилкові дії персоналу по неуважності, недбалості, незнанню тощо, але без навмисного наміру.

До них відносяться:

1. дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм тощо);
2. ненавмисне пошкодження носіїв інформації;
3. неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);
4. неумисне зараження ПЗ комп’ютерними вірусами;
5. невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;
6. помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
7. будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
8. неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);
9. наслідки некомпетентного застосування засобів захисту тощо.

Навмисні загрози суб’єктивної природи – це дії порушника, спрямовані на проникнення в систему та одержання можливості НСД до її ресурсів або дезорганізацію роботи ІТС та виведення її з ладу.

До них відносяться:

1. порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
2. порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);
3. порушення режимів функціонування ІТС (обладнання і ПЗ);
4. впровадження та використання комп’ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
5. використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;
6. крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
7. несанкціоноване копіювання носіїв інформації;
8. читання залишкової інформації з оперативної пам’яті ЕОТ, зовнішніх накопичувачів;
9. одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;
10. неправомірне підключення до каналів зв’язку, перехоплення даних, що передаються, аналіз трафіку тощо;
11. впровадження та використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);
12. інші.

Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити її спрямованість, джерело, механізм реалізації та можливі наслідки.

По-перше, на порушення яких властивостей інформації або ІТС загроза спрямована:

- конфіденційності - несанкціоноване ознайомлення з інформацією;

- цілісності - несанкціонована модифікація (спотворення, фальсифікація, викривлення) інформації;

- доступності - порушення можливості використання ІТС або оброблюваної інформації (відмова в обслуговуванні користувача);

- спостереженості ІТС - відмова в ідентифікації, автентифікації та реєстрації небезпечних дій.

По-друге, джерела виникнення загрози (які суб’єкти ІТС або суб’єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу):

- персонал і користувачі;

- технічні засоби;

- моделі, алгоритми, програми;

- технологія функціонування;

- зовнішнє середовище.

По-третє, можливі способи здійснення (механізм реалізації) загроз:

1. шляхом підключення до апаратури та ліній зв’язку,
2. маскування під зареєстрованого користувача,
3. подолання заходів захисту з метою використання інформації або нав’язування хибної інформації,
4. застосування закладних пристроїв чи програм, впровадження шкідливих кодів і вірусів.

По-четверте, опис моделі загроз (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації) має бути викладений настільки детально, щоб дозволяти (на етапі аналізу ризиків, пов’язаних з реалізацією загроз) однозначне визначення як можливих наслідків у разі реалізації загрози, так і ймовірності її реалізації в певний спосіб.

**Перелік загроз з визначенням порушень властивостей інформації та ІТС**

|  |  |  |
| --- | --- | --- |
| **№****№** | **Потенційні загрози для інформації в ІТС** | **Ризики для** |
| **К** | **Ц** | **Д** | **С** |
| **1. Загрози об’єктивної природи** |
| 1.1. | Стихійні явища (пожежа, аварії) |  | + | + | + |
| 1.2. | Збої та відмови системи електроживлення  |  |  | + | + |
| 1.3. | Збої та відмови обчислювальної техніки  |  |  | + | + |
| 1.4. | Збої, відмови та пошкодження носіїв інформації  |  | + | + |  |
| 1.5. | Збої та відмови програмного забезпечення |  | + | + | + |
| **2. Загрози суб’єктивної природи** |
| **2.1** | **Зовнішні загрози** |  |  |  |  |
| 2.1.1 | Несанкціоноване підключення до технічних засобів  | + |  |  |  |
| 2.1.2 | Несанкціоноване підключення до каналів звязку | + |  |  |  |
| 2.1.3 | Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду документів | + |  |  |  |
| 2.1.4 | Несанкціоноване перехоплення інформації за рахунок витоку інформації за рахунок ПЕМВН | + |  |  |  |
| 2.1.5 | Несанкціонований перегляд інформації за рахунок візуально-оптичного каналу | + |  |  |  |
| **2.2** | **Порушення нормальних режимів роботи** |  |  |  |  |
| 2.2.1 | Зараження системи комп’ютерними вірусами |  | + | + | + |
| 2.2.2 | Втрата (розголошення) засобів розмежування доступу (паролів), магнітних носіїв інформації та резервних копій | + | + | + |  |
| 2.2.3 | Несанкціоноване внесення змін у технічні засоби, програмне забезпечення, компоненти інформаційного забезпечення тощо |  | + | + | + |
| 2.2.4 | Використання недозволеного програмного забезпечення або модифікація компонентів програмного та інформаційного забезпечення |  | + | + | + |
| 2.2.5 | Пошкодження носіїв інформації |  |  | + |  |
| 2.2.6 | Вхід у систему недопущених осіб (подолання систем захисту) | + | + | + |  |
| **2.3** | **Помилки персоналу** |  |  |  |  |
| 2.3.1 | Помилки користувачів (впровадження і використання програм, що не є необхідними для виконання службових обов’язків; запуск програм, здатних викликати критичні зміни в системі) | + | + | + |  |
| 2.4.2 | Помилки адміністраторів (неправильне конфігурування та адміністрування системи захисту, операційної системи; неправомірне відключення засобів захисту). | + | + | + |  |
| 2.3.3 | Порушення технології обробки, введення та виведення інформації, роботи з МНІ (резервними копіями, еталонами та дистрибутивами) | + | + | + |  |
| 2.3.4 | Недбале зберігання та облік документів, носіїв інформації, баз даних | + | + | + |  |
| 2.3.5 | Отримання сторонньою особою інформації у персоналу ІТС | + |  |  |  |

Зробимо розрахунок загроз з урахуванням 3-х рівнів ризиків і збитків:

- високий - якщо реалізація загрози надає великих збитків (3 бали);

- середній - якщо реалізація загрози надає помірних збитків (2 бали);

- низький - якщо реалізація загрози надає незначних збитків (1 бал).

**Модель загроз з визначенням рівня ризиків та збитків**

**1. Загрози конфіденційності інформації**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Механізм реалізації** | **Рівень** | **Сума загроз** |
| **ризиків** | **збитків** |
| К.1 | Ненавмисне ознайомлення з ІзОД під час співбесід персоналу ІТС зі сторонніми особами | середній2 | високий3 | 5 |
| К.2 | Втрата носіїв ІзОД з причини безвідповідального ставлення до виконання обв’язків | низький1 | високий3 | 4 |
| К.3 | Перегляд ІзОД на екранах моніторів або робочих місцях користувачів ІТС сторонніми особами | середній2 | високий3 | 5 |
| К.4 | Копіювання ІзОД на зовнішні носії з метою несанкціонованого ознайомлення сторонніх осіб | високий3 | високий3 | 6 |
| К.5 | Роздрукування ІзОД з метою несанкціонованого ознайомлення сторонніх осіб | середній2 | високий3 | 5 |
| К.6 | Викрадення носіїв ІзОД з метою несанкціонованого ознайомлення сторонніх осіб | низький1 | високий3 | 4 |
| К.7 | Безпосередній доступ до ІзОД будь-яким способом сторонніх осіб | низький1 | високий3 | 4 |

**2. Загрози цілісності інформації**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Механізм реалізації** | **Рівень** | **Сума загроз** |
| **ризиків** | **збитків** |
| Ц.1 | Помилки (ненавмисні) користувачів ІТС, які призвели до модифікації або спотворення інформації на жорсткому диску або зовнішніх носіях | середній2 | середній2 | 4 |
| Ц.2 | Несанкціонована (навмисне) модифікація або спотворення інформації персоналом ІТС на жорсткому диску або зовнішніх носіях | середній2 | середній2 | 4 |
| Ц.3 | Ненавмисне пошкодження носіїв інформації користувачами АС, яке призвело до модифікації або спотворення інформації | середній2 | середній2 | 4 |
| Ц.4 | Навмисне пошкодження носіїв інформації користувачами ІТС, яке призвело до модифікації або спотворення інформації | низький1 | середній2 | 3 |
| Ц.5 | Помилки (ненавмисні) адміністраторів ІТС при налагодженні засобів захисту та системного ПЗ, в наслідок яких стала можливою модифікація ІзОД  | середній2 | середній2 | 4 |
| Ц.6 | Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація інформації або її спотворення користувачами | середній2 | середній2 | 4 |
| Ц.7 | Безпосередній доступ до інформації будь-яким способом сторонніми особами | низький1 | середній2 | 3 |

**3. Загрози доступності інформації**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Механізм реалізації** | **Рівень** | **Сума загроз** |
| **ризиків** | **збитків** |
| Д.1 | Помилки (ненавмисні) користувачів ІТС, які призвели до знищення інформації або втрати доступу до неї | середній2 | середній2 | 4 |
| Д.2 | Помилки (ненавмисні) адміністраторів ІТС, які призвели до знищення інформації або втрати доступу  | середній2 | середній2 | 4 |
| Д.3 | Некоректне налагодження засобів захисту АБ, яке призвело до втрати доступу до інформації або ІТС | середній2 | середній2 | 4 |
| Д.4 | Пошкодження парольних носіїв персоналом ІТС, що призвело до втрати доступу до інформації | середній2 | середній2 | 4 |
| Д.5 | Навмисне пошкодження парольних носіїв персоналом ІТС, яке призвело до втрати доступу до інформації | середній2 | середній2 | 4 |
| Д.6 | Прояви помилок системного ПЗ, яке призвело до втрати доступу до інформації або ІТС | середній2 | середній2 | 4 |
| Д.7 | Безпосередній доступ до ІТС будь-яким способом сторонніх осіб | низький1 | середній2 | 3 |

**4. Загрози спостереженості ІТС**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Механізм реалізації** | **Рівень** | **Сума загроз** |
| **ризиків** | **збитків** |
| Н.1 | Помилки (ненавмисні) персоналу ІТС, які призвели до втрати спостереженості | низький1 | середній2 | 3 |
| Н.2 | Помилки (ненавмисні) адміністраторів ІТС, які призвели до втрати спостереженості | середній2 | високий3 | 5 |
| Н.3 | Некоректне налагодження засобів захисту адміністраторами ІТС, яке призвело до втрати спостереженості | низький1 | високий3 | 4 |
| Н.4 | Порушення спостережності користувачами ІТС внаслідок навмисного переповнення протоколів аудиту | середній2 | середній2 | 4 |
| Н.5 | Порушення спостереженості внаслідок пошкодження, у тому числі навмисного, поточних протоколів аудиту, архівів та носіїв з архівами протоколів аудиту | низький1 | високий3 | 4 |
| Н.6 | Прояви помилок системного ПЗ, яке призвело до втрати спостереженості | середній2 | високий3 | 5 |
| Н.7 | Безпосередній доступ до ІТС будь-яким способом сторонніх осіб | низький1 | високий3 | 4 |

**Модель загроз з розрахунком сумарного рівня ризиків та збитків:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Види загроз** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **Сума загроз** |
| 1 | конфіденційності | 5 | 4 | 5 | 6 | 5 | 4 | 4 | 33 |
| 2 | спостереженості | 3 | 5 | 4 | 4 | 4 | 5 | 4 | 29 |
| 3 | доступності | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 27 |
| 4 | цілісності | 4 | 4 | 4 | 3 | 4 | 4 | 3 | 25 |

**7. Формування завдання та варіанту побудови КСЗІ**

### Останні кроки 1-го етапу «Формування вимог до КСЗІ в ІТС» складаються з таких робіт:

1. Формування завдання на створення КСЗІв ІТС.

2. Аналіз ризиків реалізації загроз для інформації в ІТС.

3. Вибір варіанту побудови та складу КСЗІв ІТС.

4. Оформлення звіту за результатами проведеної роботи.

**7.1. Формування завдання на створення КСЗІ**

Під час цього кроку визначаються завдання захисту інформації та відповідні ним напрями забезпечення її захисту, в результаті чого визначається конкретний варіант **забезпечення** безпеки інформації.

Завданнями захисту інформації можуть бути:

1. забезпечення необхідних властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації ІТС;
2. своєчасне виявлення та ліквідація загроз для ресурсів ІТС, причин та умов, які спричиняють (можуть привести до) порушення її функціонування та розвитку;
3. створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні ІТС;
4. ефективне попередження загроз для ресурсів ІТС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;
5. керування засобами захисту інформації, керування доступом користувачів до ресурсів ІТС, контроль за їхньою роботою з боку персоналу СЗІ, оперативне сповіщення про спроби НСД до ресурсів ІТС;
6. реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;
7. створення умов для максимально можливого відшкодування та локалізації збитків, що завдаються неправомірними (несанкціонованими) діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками, зменшення негативного впливу наслідків порушення безпеки на функціонування ІТС.

Концепція безпеки інформації розкриває основні напрями забезпечення безпеки інформації та розробляється на підставі аналізу таких чинників:

1. правових засад;
2. вимог безпеки інформації;
3. загроз для інформації.

За результатами аналізу формулюються загальні положення безпеки, які впливають на технологію обробки інформації в ІТС:

1. мета і пріоритети, яких необхідно дотримуватись в ІТС під час забезпечення безпеки інформації;
2. загальні напрями діяльності, необхідні для досягнення цієї мети;
3. аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;
4. відповідальність посадових осіб та інших суб’єктів взаємовідносин в ІТС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.

**Вибір основних рішень** з безпеки інформаціїрозглядається на 3-х рівнях:

1. правовому;
2. організаційному;
3. технічному.

**На правовому рівні** забезпечення безпеки інформації повинні бути вироблені підходи щодо виконання вимог нормативно-правових актів з безпеки інформації. Цей рівень забезпечується виконанням таких заходів:

1. підтримка керівництвом організації заходів з безпеки інформації в ІТС, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподіл обов'язків співробітників СЗІ;
2. розробка політики безпеки, плану захисту та іншої документації згідно вимог нормативно-правових актів з безпеки інформації;
3. визначення процедури доведення до персоналу і користувачів ІТС основних положень політики безпеки інформації, їхнього навчання та підвищення кваліфікації з питань безпеки інформації;
4. система контролю за своєчасністю, ефективністю і повнотою реалізації в ІТС рішень з безпеки інформації, дотриманням персоналом і користувачами положень політики безпеки.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо організації та впровадження режимних заходів, регламентації доступу та навчання персоналу. Цей рівень забезпечується виконанням таких заходів:

1. застосування режимних заходів на об’єктах ІТС;
2. забезпечення фізичного захисту обладнання ІТС, носіїв інформації, інших ресурсів;
3. визначення порядку виконання робіт з безпеки інформації, взаємодії з цих питань з іншими суб’єктами системи ТЗІ в Україні;
4. регламентація доступу користувачів і персоналу до ресурсів ІТС;
5. організація навчання та підвищення кваліфікації персоналу і користувачів ІТС з питань безпеки інформації;
6. реалізація окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до ІТС, використання мереж передачі даних загального користування, зокрема Інтернет тощо).

На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування інженерно-технічних і програмно-апаратних засобів реалізації вимог безпеки. Під час розгляду різних варіантів реалізації рекомендується враховувати наступні аспекти:

1. інженерно-технічне обладнання приміщень, в яких розміщуються компоненти ІТС;
2. реєстрація санкціонованих користувачів ІТС, авторизація користувачів в системі;
3. керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів;
4. виявлення та реєстрація небезпечних подій з метою здійснення повсякденного контролю;
5. перевірка і забезпечення цілісності критичних даних на всіх стадіях їхньої обробки в ІТС;
6. забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;
7. резервне копіювання критичних даних, супроводження архівів даних і ПЗ;
8. відновлення роботи ІТС після збоїв, відмов, особливо для систем із підвищеними вимогами до доступності інформації;
9. захист ПЗ, окремих компонентів і ІТС в цілому від внесення несанкціонованих доповнень і змін;
10. забезпечення функціонування засобів контролю.

**7.2. Аналіз ризиків реалізації загроз**

Під час цього кроку здійснюється аналіз ризиків, який передбачає вивчення моделей загроз і порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди). В результаті аналізу ризиків реалізації загроз визначається перелік суттєвих загроз для ІТС.

Аналіз ризиків полягає в моделюванні картини появи несприятливих умов з урахуванням всіх можливих чинників, що визначають ризики, які називаються вхідними параметрами. До них відносяться активи, вразливості, загрози та збитки.

Активи - ключові компоненти ІТС, що залучені в технологічні процеси та мають певну цінність.

Вразливості - слабкості в засобах захисту, викликані помилками або недосконалістю процедур, які можуть бути використані для проникнення в ІТС або пошкодження активів.

Загрози - реалізація яких можлива за допомогою використання вразливостей.

Збитки - втрати після реалізації загрози з урахуванням витрат на відновлення пошкоджених активів.

Керування ризиками – це процес послідовного виконання трьох основних етапів:

- визначення початкових ризиків (в незахищеній ІТС);

- застосування засобів захисту для скорочення ризиків;

- прийняття залишкових ризиків.

З метою підвищення ефективності аналізу ризиків він проводиться по різних напрямах:

- для об'єктів ІТС;

- для процесів, процедур і програм обробки інформації;

- для каналів зв'язку;

- для побічних електромагнітних випромінювань і наведень;

- для механізмів керування системою захисту.

Процес аналізу ризиків включає оцінку:

- можливих втрат в результаті реалізації загроз;

- вірогідності виявлення вразливостей системи, що впливає на оцінку можливих втрат;

- витрат на впровадження заходів і засобів захисту, які скорочують ризик до прийнятного рівня.

Витрати на КСЗІ необхідно співвіднести з цінністю інформаційних ресурсів, які піддаються ризику, а також зі збитком, який може бути нанесений організації в результаті реалізації загроз. По завершенні аналізу ризиків реалізації загроз уточнюються допустимі залишкові ризики та витрати на заходи захисту інформації.

На даний час керування ризиками інформаційної безпеки визначає міжнародний стандарт **ISO/IEC 27005-2011 «Інформаційна технологія. Методи забезпечення безпеки. Керування ризиками інформаційної безпеки»**.

Згідно вимог цього стандарту керування ризиками складається з 4-х етапів:

1) визначення критеріїв;

2) аналіз ризиків;

3) обробка ризиків;

4) прийняття ризиків.

Кінцевою метою керування ризиком є ​​мінімізація ризику. Мета мінімізації ризику полягає в тому, що застосування ефективних заходів захисту призводить до прийняття залишкового ризику.

Мінімізація ризику складається з трьох частин:

- визначення областей, де ризик неприйнятний;

- вибір ефективних заходів захисту;

- оцінювання заходів захисту та визначення прийнятності залишкового ризику.

**8. Основні вимоги до розробки комплексу засобів захисту**

Згідно статті 8 **Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»** для створення КСЗІ, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері захисту інформації.

Тобто розроблений КЗЗ повинен пройти процедуру сертифікації в Українській державній системі сертифікації продукції (УкрСЕПРО) і отримати сертифікат відповідності, після чого він вноситься до Реєстру УкрСЕПРО. Здійснюється це згідно «**Правил проведення робіт із сертифікації засобів захисту інформації**», затверджених наказом Адміністрації Держспецз’язку та Державного комітету України з питань регуляторної політики підприємництва від 25.04.2007 № 75/91 і зареєстрованих у Міністерстві юстиції України 14.05.2007 за № 498/13765.

Для того, щоб розроблений КЗЗ отримав сертифікат відповідності він повинен відповідати вимогам **НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в КС від НСД»**, тобто забезпечити:

- безперервний захист;

- «модульність» КЗЗ;

- атрибути доступу;

- керування доступом.

Крім того, КЗЗвід НСД повинен реалізувати:

- концепцію диспетчера доступу;

- реєстрацію дій користувачів;

- послуги безпеки (функції захищеності);

- гарантії реалізації послуг безпеки.

# 9. Побудова і структура послуг безпеки інформації

Перелік функціональних послуг безпеки, їх структура і семантичне позначення наведені в **НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»**.

#

# 10. Побудова і структура гарантій реалізації послуг безпеки

Рівні гарантій функціональних послуг безпеки, їх структура і семантичне позначення наведені в **НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»**.

В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації.

З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю та доступністю. Виходячи з цього, кожний клас АС (Х=1,2,3) поділяється на підкласи, які визначають підвищені вимоги до забезпечення однієї чи декілька цих властивостей.

Таким чином, кількість сполучень з трьох властивостей зумовлює наявність семи груп підкласів АС:

1) підклас Х.К - конфіденційності інформації;

2) підклас Х.Ц - цілісності інформації;

3) підклас Х.Д - доступності інформації;

4) підклас Х.КЦ - конфіденційності та цілісності інформації;

5) підклас Х.КД - конфіденційності та доступності інформації;

6) підклас Х.ЦД - цілісності та доступності інформації.

7) підклас Х.КЦД - конфіденційності, цілісності та доступності інформації.

Якщо врахувати наявність в кожній групі трьох класів АС, сумарна кількість підкласів становить 21.

**НД ТЗІ 2.5-005-99 «Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД»** вводить таке поняття як «стандартний функціональний профіль захищеності» (далі - СФПЗ). Він являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних СФПЗ, яка може бути різною для кожного класу і підкласу АС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (К, Ц і Д). Зростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ ІТС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

СФПЗ будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які висуваються. Політика безпеки АС, що реалізує певний СФПЗ, має бути «успадкована» з документів, що встановлюють вимоги до порядку обробки певної інформації в АС.

НД ТЗІ 2.5-005-99 визначає стандартний підхід до визначення ФПЗ АС шляхом вибору з множини СФПЗ, який базується на таких припущеннях:

- усі АС можна віднести до одного з трьох класів за наступними ознаками: конфігурація апаратних засобів, їх фізичне розміщення, кількість категорій оброблюваної інформації, кількість користувачів і категорій користувачів;

- у межах класу АС можна віднести до одного з підкласів, що визначені за критерієм необхідності забезпечення К, Ц і Д;

- вимоги до безпеки АС різних класів суттєво відрізняються, що дозволяє сформувати для їх підкласів множини СФПЗ, що знаходяться у ієрархічній залежності;

- для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної ІТС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

|  |  |  |
| --- | --- | --- |
| Клас АС | Кількість СФПЗ для підкласів АС | Загальна кількість СФПЗ |
| К | Ц | Д | КЦ | КД | ЦД | КЦД |
| 1 | 2 | 2 | 4 | 2 | 4 | 4 | 4 | 22 |
| 2 | 6 | 5 | 4 | 6 | 4 | 4 | 5 | 34 |
| 3 | 6 | 5 | 4 | 6 | 4 | 4 | 5 | 34 |

Стандартний підхід визначення ФПЗ вимагає таких етапів:

1. Визначення підкласу АС.

2. Визначення призначення АС та вибір підказки, яку треба використовувати у цьому випадку для вибору одного із СФПЗ, використовуючи довідковий додаток «А» з НД ТЗІ 2.5-005-99. Якщо призначення АС відрізняється від наведених у НД ТЗІ 2.5-005-99 необхідно власноруч обрати підмножину СФПЗ відповідно до підкласу АС.

3. Аналіз сутності вимог, відібраних СФПЗ.

4. Вибір одного із СФПЗ, який найбільш відповідає політиці безпеки.

5. У випадку, коли жоден із СФПЗ не підходить повною мірою, необхідно змінити рівень послуги, що міститься у СФПЗ, або додати нову послугу.

Така властивість як спостереженість не використовується для розбиття АС на підкласи. Цей факт пояснюється тим, що послуги спостереженості є необхідною умовою для реалізації інших послуг безпеки, а з іншого боку завжди важливі для АС.

**Згідно НД ТЗІ 2.5-005-99 кожний профіль має свій буквено-числовий ідентифікатор, який включає:**

- номер класу АС (1 - ПЕОМ, 2 - ЛОМ, 3 - РОМ),

- букви, що характеризує види загроз, від яких забезпечується захист (К, Ц, Д),

- номер профілю.

Всі частини ідентифікатора відділяються один від одного крапкою.

### Наприклад, СФПЗ АС класу «2» номер 1 з підвищеними вимогами до забезпечення конфіденційності інформації виглядає таким чином:

**2.К.1** = { КД-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1 }

А СФПЗ АС класу «1» номер 2 з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності інформації виглядає таким чином:

**1.КЦД.2** = { КА-1, КО-1, ЦА-1, ЦО-1, ДР-1, ДВ-1,

 НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }

Версія може служити, зокрема, для вказівки на підсилення певної послуги всередині профілю. Наприклад, нарощування можливостей реєстрації приведе до появи нової версії. Тим не менше, при внесенні деяких істотних змін, особливо додання нових послуг, може або привести до появи нового профілю, або до того, що профіль буде відноситись до іншого підкласу АС.

Найбільш складним профілем є профіль КЦД, до якого включається 22 послуги, причому це взагалі максимально можлива для профілів кількість послуг. Але не завжди є необхідність підтримувати відразу всі властивості інформації, що захищається, - іноді достатньо підтримувати лише деякі з них залежно від конкретної мети та завдань захисту інформації, а також очікуваних загроз інформації. Наприклад, у деяких випадках достатньо підтримувати властивість конфіденційності, яка може реалізуватися таким механізмом, як криптографія. Іноді, особливо в мережевих конфігураціях, найбільш важливою може бути підтримка властивості доступності.

ФПЗ по суті є варіантом технічної реалізації системи захисту інформації. За рахунок реалізації певного ФПЗ забезпечується виконання політики безпеки ІТС й зменшення збитку, що завдається АС впливом загроз. Вирішення завдання вибору оптимального ФПЗ включає формування множини припустимих варіантів ФПЗ, визначення сукупності показників якості та критерію оптимальності, а також вибір варіантів ФПЗ, оптимальних за цим критерієм.

Таким чином, завданням розробника КСЗІ є обстеження властивостей конкретної АС, як об'єкта захисту та вибір необхідного СФПЗ із списку, наведеного уНД ТЗІ 2.5-005-99. У випадку, коли жоден з наявних СФПЗ не підходить до конкретної АС, розробник має створити свій, найбільш придатний для нього ФПЗ, обґрунтувати й затвердити його.

**11. Вимоги до захисту інформації від НСД в АС класу 1**

Згідно НД ТЗІ 2.5-005-99 до АС класу 1 (далі – АС) відносяться системи, створені на базі одномашинного обчислювального комплексу (ПЕОМ – персональна електронно-обчислювальна машина), який кожного моменту може забезпечувати роботу тільки одного користувача.

**11.1. Типові умови функціонування АС**

Умови функціонування будь-якої АС визначаються такими її складовими:

- обчислювальна система,

- фізичне середовище,

- середовище користувачів,

- інформація, що обробляється,

- технології обробки інформації.

***Характеристика обчислювальної системи***

Обчислювальна система А складається з:

- стандартної ПЕОМ з периферійними пристроями введення, виведення, накопичення та відображення інформації (системний блок, клавіатура, монітор, миша, принтер тощо);

- ПЗ (системного та спеціалізованого для обробки інформації);

- КЗЗ від НСД (у тому числі антивірус).

Склад апаратного та програмного забезпечення АС вказується у формулярі АС.

Типові умови функціонування обчислювальної системи вимагають таке:

- ПЗ має відповідним чином оформлену ліцензію на право його легального використання;

- КЗЗ від НСД (у тому числі антивірус) має відповідним чином оформлений експертний висновок або сертифікат, який свідчить про відповідність КЗЗ вимогам НД ТЗІ;

- у разі обробки інформації, що становить державну таємницю, комплекс ТЗІ, який забезпечує захист інформації від витоку технічними каналами, має акт атестації, оформлений згідно вимог НД ТЗІ.

## *Характеристика фізичного середовища*

До фізичного середовища відноситься:

- приміщення, де розташована АС з усіма її компонентами (обчислювальна система, сховище носіїв інформації та ПЗ, робочі місця користувача та обслуговуючого персоналу);

- всі технічні засоби, встановлені в цьому приміщенні (засоби комунікації, сигналізації, електроживлення, заземлення, кондиціювання та побутові прилади).

Типові умови функціонування АС стосовно фізичного середовища вимагають таке:

- у приміщенні, де розташована АС з усіма її компонентами, запроваджений режим обмеження та контролю доступу згідно вимог діючого законодавства;

- у разі обробки інформації, що становить державну таємницю, всі технічні канали витоку інформації з АС блоковані засобами ТЗІ.

## Характеристика середовища користувачів

За рівнем повноважень доступу до інформації, характером та змістом робіт, які виконуються в процесі функціонування АС, суб’єкти, що мають доступ до АС, поділяються на такі групи:

- користувач, що має повноваження доступу до КЗЗ від НСД (адміністратор безпеки);

- користувачі, що мають повноваження доступу до інформації, що обробляється в АС;

- персонал, що забезпечує працездатність АС;

- персонал, що обслуговує приміщення, де розташована АС.

Повноваження користувачів першої та другої груп повинні бути фізично розділені, тобто виконуватися різними особами. Допускається виконання адміністратором безпеки додаткових функцій системного адміністратора.

Типові умови функціонування АС стосовно доступу користувачів до інформації вимагають таке:

- усі користувачі допущені до інформації, що обробляється в АС;

- доступ користувачів до службової інформації дозволяється після ознайомлення під розпис з вимогами «Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» (ПКМУ від 27.11.98 № 1893);

- доступ користувачів до інформації, що становить державну таємницю, дозволяється лише у разі наявності відповідного допуску згідно вимог «Порядок організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях» (ПКМУ від 02.10.2003 № 1561-12).

## *Характеристика інформації, що обробляється в АС*

Інформація згідно вимог захисту поділяється на такі групи:

- дані у вигляді файлів різних форматів, записів баз даних та інших структур машинного представлення (далі - дані), які містять ІзОД;

- дані, які не містять ІзОД;

- бази даних захисту (списки зареєстрованих користувачів, їх ідентифікаторів і повноважень, матриці доступу, журнали обліку тощо);

- дані, захищені ліцензійними умовами використання та розповсюдження, або такі, що належать деяким групам та окремим користувачам.

Типові умови щодо інформації, яка обробляється в АС, вимагають таке:

- дані, які входять до бази даних захисту, повинні бути віднесені до ІзОД із встановленням ступеня обмеження, не нижчим ступеня обмеження інформації, що обробляється в АС;

- реєстрація, обіг, зберігання та знищення ІзОД здійснюються згідно вимог діючого законодавства та відомчих інструкцій.

***Характеристика технологій обробки інформації***

ІзОД під час обробки в АС повинна мати атрибути з визначенням встановленого ступеня її обмеження відповідно до вимог діючого законодавства. Машинні носії, на які виводиться ІзОД, повинні мати встановлені відповідно до порядку забезпечення режиму обмеження реквізити.

Технології обробки ІзОД в АС вимагають реєстрацію її носіїв, видачу їх користувачу під розпис і зберігання в металевому сховищі. Якщо на носії зберігаються дані різних ступенів обмеження, гриф обмеження носія повинен відповідати вищому ступеню обмеження даних, що на ньому зберігаються.

Технології обробки інформації залежать від повноважень доступу користувачів до даних, розміщених на носії інформації, до якого вони мають доступ:

1) всі користувачі мають однакові повноваження;

2) користувачі мають різні повноваження, що ускладнює функціональний профіль захищеності (далі - ФПЗ) АС.

Прикладом першої (найпростішої) технології можуть бути випадки, коли:

- середовище користувачів складається лише з двох користувачів: звичайного та адміністратора безпеки;

- кожний користувач працює лише з особистим носієм інформації, до якого тільки він має доступ;

- кількість користувачів невелика, всі вони для виконання одного й того ж завдання організовані у групу користувачів і мають однакові повноваження щодо доступу до всіх даних в АС на весь час функціонування КСЗІ.

**11.2. Визначення ФПЗ**

Для умов середовищ АС можна визначити ФПЗ - мінімальний перелік послуг безпеки, які, за умови впровадження комплексу необхідних організаційних заходів, є функціонально достатніми для виконання завдань захисту інформації в АС.

Сукупність цих послуг забезпечує підтримання програмно-апаратними засобами АС процедур автентифікації користувачів АС, адміністративного розмежування доступу користувачів до даних, що зберігаються на носіях інформації, а також процедур контролю за діями користувачів із цими об’єктами.

На даний час у системі НД ТЗІ відсутній документ, що встановлює вимоги до КЗЗ від НСД в АС, де обробляється відкрита або конфіденційна інформація. Разом з тим, загальні вимоги захисту інформації висуваються «Правилами забезпечення захисту в ІТС», затвердженими ПКМУ від 29.03.2006 № 373 (далі - Правила). Тому вихідні дані для визначення ФПЗ отримаємо з цих Правил.

Так, пункт 5 Правил висуває такі вимоги:

1. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією, *що вимагає наявності послуги використання ресурсів (ДР)*.

2. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. *Це вимагає наявності послуг ідентифікації і автентифікації (НИ) і адміністративної цілісності (ЦА).*

3. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень або не підтверджені під час автентифікації пред'явленим ідентифікатором повинні блокуватися. *Це вимагає наявності послуги «одиночна ідентифікація і автентифікація» (НИ-2)**, для якої потрібна також послуга «однонаправлений достовірний канал» (НК-1).*

Пункт 11 Правил висуває такі вимоги:

1. У системі здійснюється обов'язкова автоматична реєстрація небезпечних для ІТС подій, *що вимагає наявності послуги реєстрації (НР)*.

2. Реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки, *що вимагає наявності послуги «захищений журнал» (НР-2)*.

3. Забезпечується можливість проведення аналізу реєстраційних даних виключно спеціально уповноваженим користувачем, *що вимагає наявності послуги виділення адміністратора (НО-1)*.

Пункт 15 Правил висуває такі вимоги:

1. У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. *Це вимагає наявності послуг самотестування (НТ), відкату (ЦО) і відновлення після збоїв (ДВ).*

2. Контролюється також цілісність програмних та технічних засобів захисту інформації, а у разі порушення їх цілісності обробка інформації в системі припиняється. *Це вимагає наявності послуги цілісності КЗЗ (НЦ).*

За умови наявності лише користувачів з однаковими повноваженнями доступу до інформації послуги безпеки базуються на довірчому розмежуванні доступу (КД і ЦД).

Виходячи з вище зазначеного, виписуємо всі визначені послуги безпеки в один рядок і обираємо схожий СФПЗ із НД ТЗІ 2.5-005-99 для АС класу 1. В результаті отримаємо необхідний СФПЗ для оброблення в АС відкритої інформації з мінімальними вимогами до забезпечення її цілісності та доступності:

**1.ЦД.1** = { ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }

А СФПЗ у разі оброблення службової інформації повинен мати мінімальні вимоги до забезпечення не тільки цілісності та доступності інформації, а ще її конфіденційності.

Так, пункт 6 Правил висуває такі вимоги:

Під час обробки службової інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення. У системі забезпечується можливість надання користувачу права на обробку службової інформації або позбавлення його такого права. *Це вимагає наявності послуг адміністративної конфіденційності (КА) та повторного використання об’єктів (КО-1).*

Виходячи з вище зазначеного, додаємо до СФПЗ **1.ЦД.1** послуг адміністративної конфіденційності (КА) та повторного використання об’єктів (КО-1)і в результаті отримаємо СФПЗ для обробки в АС службової інформації з мінімальними вимогами до забезпечення її конфіденційності, цілісності та доступності:

**1.КЦД.1** = { КА-1, КО-1, ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2,

 НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }

У випадку, коли усі користувачі допущені до обробки службової інформації в АС, реалізація послуги повторного використання об’єктів (КО-1) необов’язкова. А у разі наявності користувачів, що допущені до обробки лише відкритої інформації в АС, її реалізація обов’язкова.

## 11.3. Політика послуг безпеки ФПЗ

Опис послуг безпеки ФПЗ наведений в **НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»**.

Розподіл завдань захисту інформації між ФПЗ, організаційними (ОЗ) та інженерно-технічними заходами (ІТЗ), що можуть бути застосовані в АС, наведено в таблиці. Знаком «+» позначено необхідність впровадження заходів, визначених відповідними нормативно-правовими актами щодо захисту інформації, знаком «=» позначено необхідність впровадження заходів, визначених в експлуатаційній документації, що супроводжує впроваджений в АС КЗЗ. Для порівняння взяті дві ОС «Windows», які на даний час мають позитивний експертний висновок відповідності вимогам НД ТЗІ.

| **№** | **Загальні вимоги щодо****захисту інформації** | **І****Т****З** | **О****З** | **ФПЗ** | **Windows 8 Pro-fessional** | **Windows****Server 2012 R2** |
| --- | --- | --- | --- | --- | --- | --- |
| 1. | Захист від несанкціонованого |  |  |  |  |  |
| ознайомлення | + | = | КА-1КО-1ДВ-1 | -КО-1ДВ-2 | -КО-1ДВ-2 |
| розмноження |  | + |  |  |  |
| розповсюдження | + | + |  |  |  |
| копіювання | + | + |  |  |  |
| відновлення |  | + |  |  |  |
| спотворення | + | = | ЦА-1 | - | - |
| 2. | Надання доступу до ІзОД за умови достовірного розпізнавання користувачів |  | = | НК-1 НИ-2 | НК-1НИ-2 | НК-1НИ-2 |
| з урахуванням наданих згідно з службовою необхідністю повноважень |  | = | КА-1 НО-1 | -НО-3 | -НО-3 |
| 3. | Надання можливості своєчасного доступу зареєстрованих користувачів АС до ІзОД |  | = | НЦ-1 НТ-1 ДВ-1 | НЦ-2НТ-2ДВ-2 | НЦ-2НТ-2ДВ-2 |
| 4. | Контроль цілісності КЗЗ, а у разі її порушення припиняти обробку інформації |  | = | НЦ-1 | НЦ-2 | НЦ-1 |
| 5. | Забезпечення реєстрації дій всіх користувачів АС щодо обробки ІзОД |  | = | НР-2 | НР-2 | НР-2 |
| Забезпечення захисту реєстраційних даних від модифікації користувачами, які не мають адмін. повноважень |  | = | НР-2 НО-1 | НР-2НО-3 | НР-2НО-3 |
| 6. | Блокування доступу до ІзОД у разі порушення політики безпеки |  | = | НК-1 НИ-2 | НК-1НИ-2 | НК-1НИ-2 |
| 7. | Встановлення ступеня обмеження ІзОД під час її обробки в АС |  | + |  |  |  |
| 8. | Встановлення адміністратором обмежень на використання ресурсів користувачами |  | = | ДР-1 | ДР-1 | ДР-1 |
| 9. | Можливість модифікації та знищення ІзОД користувачами, яким надано відповідні повноваження |  | = | ЦА-1НИ-2 | -НИ-2 | -НИ-2 |
| 10 | Контроль цілісності ПЗ, що забезпечує обробку ІзОД, запобігання його несанкціонованій модифікації та ліквідація наслідків такої модифікації |  | = | НТ-1ЦО-1ДВ-1 | НТ-2ЦО-1ДВ-2 | НТ-2ЦО-1ДВ-2 |
| 12 | Забезпечення рівня гарантій реалізації ПБ |  |  | Г2 | Г2 | Г2 |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ АС-1 та механізмів захисту ОС «Windows», можна зробити такі висновки:

- КЗЗ обох ОС «Windows» нічим не відрізняються;

- ОС «Windows» може забезпечити захист відкритої інформації лише за умов впровадження ІТЗ і ОЗ;

- для забезпечення захисту службової інформації ОС «Windows» потребує використання додаткового КЗЗ (для забезпечення послуг КА-1 і ЦА-1).

**12. Особливості захисту секретної інформації в АС класу 1**

Інформація, що становить державну таємницю та оброболяється технічними засобами (у тому числі АС), згідно вимог НД ТЗІ підлягає захисту від витоку технічними каналами. Захист іншої ІзОД від витоку технічними каналами здійснюється за рішенням власника або розпорядника цієї інформації.

**12.1. Загальна|спільна| характеристика технічних каналів витоку**

**інформації,** **що обробляється** **в АС**

Витік інформації по технічних каналах треба розуміти як неконтрольоване поширення|розповсюдження| інформативного сигналу від його джерела через фізичне середовище|середу| до технічного засобу|кошту|, який здійснює перехоплення інформації.

Перехоплення інформації - це неправомірне отримання|здобуття| інформації з використанням технічного засобу|кошту|, який здійснює її виявлення та|та| обробку. В результаті|внаслідок,унаслідок| перехоплення інформації можливе неправомірне ознайомлення з|із| нею або неправомірний запис її на носій|носія|.

Разом з|поряд| технічними засобами|коштами| АС у приміщеннях|поміщеннях|, де вони встановлені|установлені|, як правило, знаходяться|перебувають| ще інші технічні засоби|кошти| і|та| системи, які в обробці інформації безпосередньої участі не беруть. До них відносяться: системи і|та| засоби|кошти| автоматичного телефонного зв'язку; відеонагляду та|та| сигналізації; сповіщення та|та| кондиціонування; прийому програм радіомовлення і|та| телебачення; засоби|кошти| електронної оргтехніки тощо.

Через приміщення|поміщення|, де встановлені|установлені| технічні засоби|кошти| АС, можуть проходити|минати,спливати| проводи|проводи| та|та| кабелі, що не відносяться до АС, та|та| інші струмопровідні металоконструкції (металеві труби систем опалювання, водопостачання тощо), які називаються сторонніми провідниками.

Електроживлення технічних засобів|кошти| здійснюється від розподільчих пристроїв|устроїв| і|та| силових щитів, які спеціальними кабелями з'єднуються з|із| трансформаторною підстанцією міської електромережі.

Усі технічні засоби|кошти|, що живляться|харчуються| від електромережі та мають металевий корпус, повинні бути заземлені. Типова система заземлення включає загальний|спільний| пристрій та кабель заземлення|, шини і|та| дроти|проводи|, що з'єднують пристрій заземлення| з|із| технічними засобами|коштами|.

З'єднувальні лінії АС, сторонні провідники, а також лінії електроживлення та|та| заземлення можуть виходити за межі контрольованої зони об'єкту (далі - КЗ), під якою розуміється простір (територія, будівля, частина|частка| будівлі), де виключено неконтрольоване перебування сторонніх осіб|лиць,облич| (відвідувачів|візитерів|, працівників комунальних служб тощо) та транспортних засобів.

 Межею|кордоном| КЗ може бути периметр території організації, що охороняється, а також огороджувальні конструкції будівлі або частини|частки| будівлі, що охороняється, якщо вона розміщена на території, що не охороняється.

При розгляді АС, як об'єкту захисту від витоку інформації по технічних каналах, його необхідно|треба| розглядати|розглядувати| як об'єкт, що включає :

- технічні засоби|кошти|, що безпосередньо обробляють інформацію, разом з їх з'єднувальними лініями (під ними розуміють сукупність дротів|проводів| і|та| кабелів, що прокладаються між окремими елементами АС);

- допоміжні технічні засоби|кошти| і|та| системи разом з їх з'єднувальними лініями;

- сторонні провідники;

- систему електроживлення;

- систему заземлення.

Сукупність джерела інформативного сигналу, технічного засобу|кошту|, що здійснює перехоплення інформації, і|та| фізичного середовища|середи|, в якому поширюється|розповсюджується| інформативний сигнал, називається технічним каналом витоку інформації (далі - ТКВІ).

Залежно від природи утворення інформативного сигналу ТКВІ можна розділити на:

- природні;

-|та| спеціально створювані.

Природні ТКВІ утворюються ненавмисно за рахунок побічних електромагнітних випромінювань і наведень (далі - ПЕМВН) АС. Вони складаються з електромагнітних та електричних ТКВІ.

Електромагнітні ТКВІ утворюються за рахунок побічних електромагнітних випромінювань (далі - ПЕМВ), що виникають при обробці інформації в АС.

Електричні ТКВІ утворюються внаслідок|унаслідок| наведень інформативних сигналів в лініях електроживлення, з'єднувальних лініях АС і|та| сторонніх провідниках.

Спеціально створювані ТКВІ утворюються навмисно шляхом впровадження в АС «закладних» електронних пристроїв перехоплення інформації та|та| шляхом високочастотного (далі - ВЧ) опромінення|опромінювання| АС.

***Електромагнітні ТКВІ***

Головними причинами виникнення електромагнітних ТКВІ в АС є:

- ПЕМВ, що виникають внаслідок|унаслідок| протікання інформативних сигналів по елементах АС;

- модуляція інформативним сигналом ПЕМВ генераторних або підсилювальних блоків АС із-за|через| паразитних зв'язків.

ПЕМВ виникають при таких|таких| режимах обробки інформації в АС:

- виведення даних на екран монітора;

- введення даних з клавіатури;

- запис даних на накопичувачі;

- зчитування даних з накопичувачів;

- обмін даними по каналах зв'язку;

- виведення даних на принтер;

- запис даних від сканера тощо.

При кожному режимі роботи АС виникають ПЕМВ, що мають свої характерні особливості. Діапазон можливих частот ПЕМВ АС може бути від 10 кГц| до 2 ГГц.

Для перехоплення ПЕМВ АС використовуються спеціальні стаціонарні, транспортні або ручні прийомні комплекси||устрої|, які називаються технічними засобами|коштами| розвідки побічних електромагнітних випромінювань і|та| наведень (далі - ТЗР ПЕМВН).

Типовий комплекс ТЗР ПЕМВН включає: спеціальний приймальний пристрій|устрій|, ноутбук, спеціальне програмне|програмове| забезпечення і|та| широкодіапазонну спрямовану|направлену| антену. Він може встановлюватися в будівлях або машинах, розташованих|схильних| за межами КЗ.

Найбільш небезпечним з точки зору|з| витоку інформації режимом роботи АС є виведення інформації на екран монітора. Враховуючи широкий спектр ПЕМВ відеосистеми АС (більше 100 Мгц) і|та| їх незначний рівень, перехоплення зображень, виводимих на екран монітора, є досить важким|скрутним| завданням|задачею|.

Дальність перехоплення ПЕМВ сучасних АС, як правило, не перевищує 50 метрів. Якість перехопленого зображення значно гірше якості зображення, що виводиться на екран монітора. Особливо важке|скрутне| завдання|задача| - перехоплення тексту, що виводиться на екран монітора та|та| написаний дрібним|мілким| шрифтом.

Простір навкруги|довкола,навколо| АС, за межами якого напруженість електромагнітного поля (далі - ЕМП) не перевищує допустимого (нормованого) значення, називається небезпечною зоною R2. Вона визначається інструментально-розрахунковим методом після спеціальних досліджень АС на наявність ПЕМВ і|та| вказується|указує| в приписі|розпорядженні| на її експлуатацію або сертифікаті відповідності.

Таким чином, для перехоплення електромагнітного ТКВІ АС необхідно, щоб відстань від АС до межі|кордону| КЗ була менше зони R2, в межах якої встановлений ТЗР ПЕМВ.

***Електричні ТКВІ***

Причинами виникнення електричних каналів витоку інформації є наведення інформативних сигналів, під якими розуміються струм|токи| і|та| напруга|напруження| в струмопровідних елементах, що викликаються|спричиняти,визивати| ПЕМВ, ємнісними та|та| індуктивними зв'язками.

Наведення інформативних сигналів за рахунок ПЕМВ можуть виникнути у:

- лініях електроживлення АС і|та| інших технічних засобів;

- лініях|цепах| заземлення АС|та|;

- з'єднувальних лініях АС і|та| інших технічних засобів;

- сторонніх провідниках (металевих трубах систем опалювання, водопостачання, металоконструкціях будівлі тощо).

Залежно від причин можливі наведення інформативних сигналів у:

- електричних колах|цепах| АС, викликані|спричиняти,визивати| ПЕМВ АС;

- з'єднувальних лініях технічних засобів і|та| сторонніх провідниках, викликані|спричиняти,визивати| ПЕМВ АС;

- електричних колах|цепах| АС, викликані|спричиняти,визивати| внутрішніми ємнісними та/або індуктивними зв'язками («витік» інформативних сигналів у колі|цепі| електроживлення через блоки живлення|харчування| АС);

- колах|цепах| заземлення АС, викликані|спричиняти,визивати| ПЕМВ АС, а також гальванічним зв'язком «схемної землі» та|та| блоків АС.

Різні|різноманітні| допоміжні технічні засоби|кошти|, їх з'єднувальні лінії, а також лінії електроживлення, сторонні провідники та|та| лінії|цепи| заземлення виконують роль випадкових антен, при підключенні ТЗР до яких можливе перехоплення наведених інформативних сигналів.

Випадкові антени можуть бути зосередженими та|та| розподіленими.

Зосереджена випадкова антена є компактним технічним засобом|коштом| (телефонний апарат, гучномовець оповіщення, датчик охоронної сигналізації, камера відеонагляду тощо), підключеним до лінії, що виходить за межі КЗ.

До розподілених випадкових антен відносяться кабелі, дроти|проводи|, металеві труби та|та| інші струмопровідні комунікації, що виходять за межі КЗ. Рівень сигналів, що наводяться в них, значною мірою|в| залежить не лише|не| від потужності випромінюваних сигналів, але йі відстані до них від засобів АС.

Простір навкруги|довкола,навколо| АС, за межами якого рівень наведеного від АС інформативного сигналу в зосереджених антенах не перевищує допустимого (нормованого) значення, називається небезпечною зоною r1, а в розподілених антенах - небезпечною зоною r1'.

На відміну від зони R2 розмір зони r1/r1' залежить не лише|не| від рівня ПЕМВ АС, але й від довжини випадкової антени (від приміщення|поміщення|, де встановлена|установлений| АС, до місця можливого підключення ТЗР).

Зони r1 і|та| r1' для кожної АС визначаються інструментально-розрахунковим методом, і|та| їх значення вказуються|указують| в приписі|розпорядженні| на експлуатацію АС.

Для виникнення електричного ТКВІ необхідно, щоб:

- відстань від АС до випадкової антени була менше зони r1/r1';

- випадкова антена виходила за межі КЗ і мала гальванічне підключення ТЗР.

***Спеціально створювані ТКВІ***

Разом з|поряд| пасивними способами перехоплення інформації, що обробляється АС, розглянутими|розглядувати| вище, можливе використання і|та| активних способів, зокрема, способу ВЧ опромінення|опромінювання|, при якому АС опромінюється спрямованим потужним|могутнім| ВЧ сигналом. Для цих цілей використовується ВЧ генератор із|із| спрямованою|направленою| антеною, що має вузьку діаграму спрямованості. При взаємодії опромінюючого ЕМП з|із| елементами АС відбувається|походить| модуляція інформативним сигналом вторинного|повторного| ВЧ випромінювання АС. Приймальний пристрій ТЗР приймає перевипромінений ВЧ сигнал і виділяє з нього інформативний сигнал.

Для перехоплення інформації, що обробляється в АС, можливо також використання «закладних» електронних пристроїв перехоплення інформації|устро, потайно|скритний| впроваджених|упроваджувати| в технічні засоби|кошти| АС.

Перехоплена за допомогою «закладних» пристроїв|устроїв| інформація або безпосередньо передається по каналу зв'язку на приймальний пристрій ТЗР, або записується|занотовує| в спеціальний запам'ятовуючий пристрій|устрій|, та передається тільки|лише| за сигналом дистанційного керування.

Для передачі інформації на приймальний пристрій можуть використовуватися радіоканал, оптичний (інфрачервоний) канал або лінії електроживлення АС.

«Закладні» пристрої|устрої| впроваджуються|упроваджують| в АС для перехоплення інформації, що:

- вводиться|запроваджує| з клавіатури;

- виводиться на екран монітора;

- виводиться на принтер;

- записується на жорсткий диск.

«Закладні» пристрої|устрої|, як правило, складаються з|із| блоків перехоплення, обробки, передавання, дистанційного керування та|та| живлення|харчування| (перетворювача AC/DC). Блок дистанційного керування призначений для прийому сигналів дистанційного включення|вмикання,приєднання| й|та| виключення «закладки»|закладення| та|та| встановлення параметрів роботи передавального блоку. Приймальний комплекс ТЗР ПЕМВН складається з|із| радіоприймального пристрою|устрою|, модему, ноутбука і|та| спеціального програмного|програмового| забезпечення.

Апаратна «закладка»|закладення| для перехоплення зображень з екрану монітора потайно|скритний| встановлюється, як правило, в корпусі монітора (можливе встановлення|настанова| і|та| в системному блоці) та|та| контактно підключається до кабелю монітора.

Перехоплена інформація (відеозображення) в цифровому вигляді|вигляді| передається по радіоканалу, лінії електромережі або виділеній лінії на приймальний комплекс ТЗР, де перехоплене зображення відновлюється та|та| відображається на екрані комп'ютера в реальному масштабі часу, створюючи «копію» екрану, а додаткова інформація може записуватися|занотовувати| на жорсткий диск для подальшої|дальшої| обробки.

Апаратна «закладка»|закладення| для перехоплення інформації, що вводиться|запроваджує| з клавіатури (далі - кейлогер|), потайно|скритний| встановлюється в корпусі клавіатури або всередині|всередині| системного блоку та|та| підключається до інтерфейсу клавіатури. Вона є найпоширенішою «закладкою»|закладення| та|та| призначена в основному для перехоплення паролів користувачів і|та| текстових документів, що набирають на клавіатурі. Перехоплена інформація може передаватися по радіоканалу або записуватися|занотовувати| на флеш-пам’ять|.

Кейлогер з|із| передачею інформації по радіоканалу складається з|із| блоку перехоплення, передавального або запам'ятовуючого блоку та|та| блоку управління. Живлення|харчування| кейлогера| здійснюється від інтерфейсу клавіатури. Він має невеликі розміри і|та| важить декілька грам.

Блок перехоплення здійснює перехоплення сигналів, що передаються з клавіатури до системного блоку при натисненні клавіші. Перехоплені сигнали в цифровому вигляді|вигляді| передаються по радіоканалу (наприклад, Bluetooth) на приймальний комплекс ТЗР, де в реальному масштабі часу відновлюються та|та| відображаються на екрані комп'ютера у вигляді символів, що набираються на клавіатурі.

Апаратні кейлогери|, що здійснюють запис перехопленої інформації на флеш-пам’ять |, складаються з|із| датчика перехоплення сигналів, що передаються з клавіатури до системного блоку при натисненні клавіші, мікроконтроллера|мікроконтролера| та|та| флеш-пам’яті |.

Вони працюють під управлінням будь-якої операційної системи та|та| не вимагають додаткового живлення, оскільки|харчування| живл|харчування|яться від клавіатури АС. При об'ємі|обсязі| пам'яті 1 МГб забезпечується запис до двох мільйонів натиснень клавіш або 500 сторінок тексту. Записана на флеш-пам’ять інформація шифрується з використанням 128-бітового ключа|джерела|.

Кейлогери випускаються у вигляді перехідних роз'ємів або подовжувачів, що підключаються в розрив кабелів, які з’єднують|з'єднують| клавіатуру та|та| системний блок. Їх встановлення|настанова| не вимагає спеціальних навичок|навиків| і|та| може бути зроблено|виробляти,справляти,проводити| за декілька секунд. За наявності великої кількості різних|різноманітних| кабелів, підключених до системного блоку, виявити факт встановлення |настанови| кейлогера| досить важко.

Апаратна «закладка»|закладення| для перехоплення інформації, що виводиться на принтер, встановлюється в корпусі принтера та|та| за принципом роботи аналогічна «закладкам»|закладення||закладенням|, розглянутим|розглядувати| вище.

Апаратна «закладка»|закладення| для перехоплення інформації, що записується на жорсткий диск, є найбільш складною з|із| розглянутих|розглядувати| вище. Вона потайно|скритний| встановлюється в системному блоці та|та| контактно підключається через блок перехоплення до інтерфейсу, що з’єднує|з'єднує| жорсткий диск з|із| материнською платою.

Перехоплені сигнали поступають|надходять| у блок обробки, що включає спеціалізований процесор, де здійснюється їх обробка за спеціальною програмою. Файли з|із| заданим розширенням (наприклад, \*.doc) записуються|занотовують| в оперативну або флеш-пам’ять.

За сигналом дистанційного керування записана в пам'яті інформація в цифровому вигляді|вигляді| по радіоканалу або лінії електромережі|сіті| передається на приймальний комплекс ТЗР, де у вигляді окремих файлів записується|занотовує| на жорсткий диск для подальшої|дальшої| обробки.

Таким чином, перехоплення інформації, що обробляється в АС, може здійснюватися шляхом|дорогою,колією|:

- перехоплення ПЕМВ, що виникають при роботі АС;

- перехоплення наведень інформативних сигналів з ліній електроживлення та|та| заземлення АС;

- перехоплення наведень інформативних сигналів із з’єднувальних ліній технічних засобів і|та| сторонніх провідників у приміщенні, де розташована АС;

- ВЧ опромінення засобів|опромінювання|»» АС;

- встановлення в засобах АС «закладних» пристроїв|устроїв|.

**12.2. Захист інформації в АС від витоку каналами ПЕМВН**

Для організації захисту ІзОД, що обробляється в АС, від **витоку каналами** ПЕМВН в Україні у 1995 році був розроблений нормативний документ **ТР ЕОТ - 95 «Тимчасові рекомендації з ТЗІ у засобах обчислювальної техніки, АС і мережах від витоку каналами ПЕМВН»**, в якому вказані рекомендації щодо захисту від перехоплення:

- випромінювань технічних засобів АС;

- наведень на системи, що мають вихід за межі КЗ;

- колами заземлення;

- колами електроживлення.

Крім того, ТР ЕОТ - 95 надає рекомендації щодо застосування:

- екранувальних конструкцій;

- системи просторового зашумлення.

У 2007 році в Україні були розроблені нормативні документи серії «**Захист інформації на об’єктах інформаційної діяльності** (далі - ОІД)» щодо створення комплексу ТЗІ:

- НД ТЗІ 1.1-005-07 Створення комплексу ТЗІ. Основні положення;

- НД ТЗІ 2.1-002-07 Випробування комплексу ТЗІ. Основні положення;

- НД ТЗІ 3.1-001-07 Створення комплексу ТЗІ. Передпроектні роботи;

- НД ТЗІ 3.3-001-07 Створення комплексу ТЗІ. Порядок розроблення та впровадження заходів із захисту інформації.

Ці НД ТЗІ вимагають застосування у складі комплексу ТЗІ лише тих засобів захисту інформації, які мають сертифікат відповідності Системи УкрСЕПРО вимогам НД ТЗІ або позитивний висновок державної експертизи у сфері ТЗІ.

Застосування імпортних засобів захисту інформації можливе лише за умови відсутності вітчизняних аналогів за умови наявності відповідних техніко-економічних обґрунтувань і проведення їх сертифікації або одержання позитивного експертного висновку.

**12.3. Створення комплексу технічного захисту інформації**

Основні вимоги до порядку створення комплексу ТЗІ виписані у НД **ТЗІ 1.1-005-07 «Захист інформації на ОІД. Створення комплексу ТЗІ. Основні положення»**.

Замовник (підрозділ установи) на створення комплексу ТЗІ разом із СЗІ готує та подає на затвердження керівнику установи-замовника:

- протокол про визначення вищого ступеня обмеження доступу до інформації;

- проект рішення щодо створення комплексу ТЗІ.

Створення комплексу ТЗІ передбачає такі основні етапи:

1) передпроектні роботи;

2) впровадження заходів захисту;

3) випробування комплексу ТЗІ.

**1-й етап: передпроектні роботи**

Він здійснюється згідно вимог НД ТЗІ 3.1-001-07 «Захист інформації на ОІД. Створення комплексу ТЗІ. Передпроектні роботи».

**2-й етап: впровадження заходів захисту**

Він здійснюється згідно вимог НД ТЗІ 3.3-001-07 «Захист інформації на ОІД. Створення комплексу ТЗІ. Порядок розроблення та впровадження заходів із захисту інформації».

**3-й етап: випробування комплексу ТЗІ**

Він здійснюється згідно вимог НД ТЗІ 2.1-002-07 «Захист інформації на ОІД. Випробування комплексу ТЗІ. Основні положення». Цей етап передбачає спочатку проведення випробувань, а після їх завершення - атестації комплексу ТЗІ.

**Перший варіант обладнання для комплексу ТЗІ в АС класу 1**

|  |  |
| --- | --- |
| Найменування обладнання | Вартість, грн. |
| Генератор ВЧ шуму комп’ютерний «РІАС-1К» | 7260 |
| Фільтр захисний протизавадний «ФЗП 103-2»  | 5526 |
| Засіб захисту інформації від НСД «Рубіж-РСО»  | 2730 |
| **Всього** | **13516** |

**Другий варіант обладнання для комплексу ТЗІ в АС класу 1**

|  |  |
| --- | --- |
| Найменування обладнання | Вартість, грн. |
| Генератор ВЧ шуму комп’ютерний «Базальт-5ГЕШ» | 7506 |
| Фільтр захисний протизавадний «ФЗП 103-1»  | 6174 |
| Засіб захисту інформації від НСД «Лоза-1» | 2880 |
| **Всього** | **16560** |

**Семестр 8 Модуль 2**

**13. 2-й етап - розробка політики безпеки інформації в ІТС**

Під час другого етапу створення КСЗІ складаються такі документи:

- політика безпеки інформації;

- план захисту інформації;

- календарний планробіт із захисту інформації.

Виходячи з міжнародного досвіду та вимог міжнародних стандартів в області інформаційної безпеки розрізняють три типи політики безпеки.

1. Програмна політики безпеки є політикою вищої ланки управління в організації. Об’єктом є організація в цілому, за розробку і здійснення програмної політики несе відповідальність керівництво організації. Програмна політика визначає стратегічні напрямки забезпечення інформаційної безпеки.

2. Системно - орієнтована політика – це структура, склад, вимоги до окремих компонентів, процедур і функцій ІТС, етапу документування, які визначені вітчизняними нормативними документами.

3. Проблемно - орієнтована політика спрямована на вирішення окремих проблем або завдань в області забезпечення інформаційної безпеки. Існує ряд областей діяльності організації, для яких необхідно розробити окремі політики: фізичної безпеки, керування доступом, адміністрування, криптозахисту, антивірусного захисту, інтернет-доступу тощо.

Опис політики безпеки інформації в ІТС здійснюється згідно вимог додатк**у «Методичні вказівки щодо структури та змісту Плану захисту інформації в АС»** до **НД ТЗІ 1.4-001-2000 «Типове положення про СЗІ в АС»**, затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ.

На підставі Плану захисту складається «**Календарний план робіт із захисту інформації в ІТС»**, який містить такі заходи:

1. організаційні;
2. контрольно-профілактичні;
3. інженерно-технічні;
4. кадрові.

Організаційні заходи - це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення захисту інформації. До плану можуть включатись заходи щодо:

1. розробки документів (інструкцій, методик, правил, розпоряджень тощо) з різних напрямів захисту інформації в АС;
2. внесення змін та доповнень до чинних в АС документів з урахуванням зміни умов (обставин);
3. розробки та впровадження нових організаційних заходів з захисту інформації;
4. обгрунтування необхідності застосування та впровадження нових засобів захисту інформації;
5. координації робіт та взаємодії з іншими підрозділами організації або зовнішніми організаціями на всіх етапах життєвого циклу ІТС;
6. розгляду результатів виконання затверджених заходів та робіт з захисту інформації;
7. інші.

До контрольних заходів можуть бути віднесені:

1. контроль за виконанням персоналом (користувачами) вимог відповідних інструкцій, розпоряджень, наказів;
2. контроль за виконанням заходів, розроблених за результатами попередніх перевірок;
3. контроль за станом зберігання та використання носіїв інформації на робочих місцях;
4. інші.

До профілактичних слід відносити заходи, спрямовані на формування у персоналу (користувачів) мотивів поведінки, які спонукають їх до безумовного виконання у повному обсязі вимог режиму, правил проведення робіт тощо, а також на формування відповідного морально-етичного стану в колективі.

До інженерно-технічних слід відносити заходи, спрямовані на налагодження, випробування і введення в експлуатацію, супроводження і технічне обслуговування КЗЗ від НСД, засобів захисту інформації від загроз її витоку технічними каналами, інженерне обладнання споруд і приміщень, в яких розміщуються засоби обробки інформації, у тому числі в процесі капітального будівництва тощо.

Планування роботи з кадрами включає заходи з підбору та навчання персоналу (користувачів) встановленим правилам безпеки інформації, новим методам захисту інформації, підвищення їхньої кваліфікації. Навчання персоналу (користувачів) може здійснюватись власними силами, з залученням спеціалістів зовнішніх організацій або в інших організаціях. Навчання повинно здійснюватися за програмою, затвердженою керівництвом організації. Навчальні програми повинні мати теоретичний і практичний курси. Доцільність і необхідність включення до програм окремих розділів визначається особливостями ІТС і технологіями захисту інформації, що використовуються в ній, функціональними завданнями спеціалістів, що входять до складу навчальних груп та іншими чинниками.

# Приклад календарного плану робіт із захисту інформації в ІТС

1. Організаційні заходи

|  |  |  |  |
| --- | --- | --- | --- |
| **Заходи** | **Виконавець** | **Регламент робіт** | **Терміни / період** |
| Розробка ТЗ на КСЗІ | СЗІАдміністра-тори | Згідно НД ТЗІ 3.7-001-99 | Після складання Плану захисту |
| Проектування КСЗІ  | Розробник КСЗІ | Згідно НД ТЗІ 3.7-003-05і НД ТЗІ 2.5-004-99 | Після погоджен-ня ТЗ з ДССЗЗІУ |
| Попередні випробування КСЗІ  | Розробник КСЗІ | Згідно ДСТУ 2853-94 і «Програми та методики попередніх випробувань» | Після пуско-налагоджуваль-них робіт КСЗІ  |
| Підготовка впровадження КСЗІ | Адміністра-тори  | Призначення відповідальних осіб і підготовка наказів щодо КСЗІ  | Під час попередніх випробувань КСЗІ  |
| Дослідна експлуатація КСЗІ | СЗІАдміністра-тори  | Відпрацювання технологій оброблення інформації, проведення навчання персоналу  | Після завершення попередніх випробувань  |
| Державна експертиза КСЗІ | Адміністра-ція ДССЗЗІУ | Згідно «Положення про державну експертизу»  | Після завершен-ня дослідної експлуатації |
| Введення в промислову експлуатацію | СЗІАдміністра-тори | Згідно «Інструкції з експлуатації ІТС в частині забезпечення захисту інформації» | Після отримання Атестату відповідності |
| Реєстрація МНІ і користувачів | Адміністра-тори | Заведення журналів обліку Реєстрація користувачів і МНІ в системі та журналах | Після наказу про введення ІТС в експлуатацію |
| Перегляд Плану захисту | СЗІАдміністра-тори | Розробка нових підходів до планування заходів захисту | щорічно |
| Супровід та модернізація КСЗІ | СЗІАдміністратори | Розробка техзавдань на модернізацію КСЗІ згідно НД ТЗІ 3.7-001 | згідно плану вдосконалення КСЗІ |
| Чергове кате-горіювання | Комісія установи | Згідно НД ТЗІ 1.6-005-2013 | через 5 років після первинного |
| Чергова державна експертиза | Адміністра-ція ДССЗЗІУ | Згідно вимог «Положення про державну експертизу» | через 5 років після первинної |

## 2. Контрольно-профілактичні заходи

| **Заходи** | **Виконавець** | **Регламент робіт** | **Термін/період** |
| --- | --- | --- | --- |
| Ознайомлення користувачів з порядком робіт та мірою відповідальності за дотримання політики безпеки  | Служба захисту | Оформлення допуску до роботи | після прийому на роботу |
| Адміністра-тор безпеки | Згідно «Інструкції користувачу»  | під час їх реєстрації в ІТС |
| Проведення занять з персоналом ІТС щодо виконання вимог політики безпеки в установі | Служба захисту | Згідно «Плану навчання в установі» | щоквартально |
| Контрольні заходи | Системний адміністратор | Перевірка справності ОС і ПЗ ІТС | щодня |
| Адміністра-тор безпеки | Перевірка виконання вимог політики безпеки користувачами | щомісячно |
| Служба захисту | Перевірка виконання політики безпеки адміністраторами | щоквартально |
| Перевірка стану захисту інформації | Комісія установи | Згідно «Положення про захист інформації в ІТС» | щорічно |
| Перевірка наявності МНІ | Комісія установи | Згідно «Інструкції про організацію діловодства» | щорічно |

## 3. Інженерно-технічні заходи

|  |  |  |  |
| --- | --- | --- | --- |
| **Заходи** | **Виконавець** | **Регламент робіт** | **Термін/період** |
| Пуско-нала-годжувальні роботи | Розробник КСЗІ | Згідно технічного завдання на КСЗІ | Після затвердження проекту КСЗІ |
| Попередні випробування КСЗІ  | Розробник КСЗІ | Згідно ДСТУ 2853-94 і «Програми та методики випробувань» | Після пуско-налагоджувальних робіт КСЗІ  |
| Дослідна експлуатація КСЗІ | СЗІАдміністра-тори  | Відпрацювання технологічних процесів в ІТС | Після завершення випробувань  |
| Державна експертиза КСЗІ | Експерт, призначений ДССЗЗІУ | Згідно «Програми та методики експертних випробувань» | Після дослідної експлуатації |
| Введення в промислову експлуатацію | СЗІАдміністра-тори  | Згідно «Інструкції з експлуатації ІТС в частині захисту» | Після отримання Атестату  |
| Супровід КСЗІ | Розробник КСЗІ | Гарантійне обслуговування | Гарантійний термін |
| Технічне обслугову-вання ІТС | Адміністра-тори  | Згідно «Регламенту технічного обслуговування» | згідно термінів регламенту |
| Резервування баз даних і фондів | Адміністратор безпеки | Згідно «Інструкції з резервування баз даних» | щомісячно |
| Поновлення антивірусних баз  | Адміністратор безпеки | Згідно «Інструкції з антивірусного захисту» | щодня |
| Перевірка МНІ і ІТС на наявність вірусів | Користувач (МНІ) | Згідно «Інструкції з антивірусного захисту» | щодня |
| Адміністратори (ІТС) | щотижня |
| Модернізація КСЗІ | Розробник КСЗІ | Заміна (додавання) окремих компонентів КСЗІ згідно НД ТЗІ 3.7-001-99 | згідно плану розвитку та вдосконалення КСЗІ |

##

## 4. Робота з кадрами

|  |  |  |  |
| --- | --- | --- | --- |
| **Заходи** | **Виконавець** | **Регламент робіт** | **Термін/період** |
| Вступне ознайомлення з положеннями політики безпеки інформації (під розпис) | СЗІ | Оформлення допуску до роботи | після прийому на роботу |
| Адміністра-тор безпеки | Згідно «Інструкції користувачу»  | під час їхньої реєстрації в ІТС |
| Підготовка та впровадження в рамках трудової угоди розділу відповідальності за виконання вимог політики безпеки | СЗІ | Згідно вимог трудового законодавства | за рішенням керівника установи |
| Інструктаж користувача щодо дій у випадку нештатної ситуації | Адміністратор безпеки | Згідно «Плану робіт у випадку нештатної ситуації»  | щорічно |
| Проведення занять з підготовки персоналу ІТС  | СЗІАдміністра-тори | Згідно «Плану професійної підготовки» | щотижня |
| Направлення на курси підвищення кваліфікації | СЗІ | Згідно «Плану підвищення кваліфікації» | згідно термінів плану |

**14. Складання Плану захисту інформації в ІТС**

План захисту інформації в ІТС розробляється на підставі:

- аналізу технологій обробки інформації;

- аналізу ризиків реалізації загроз;

- політики безпеки інформації.

План захисту визначає та документально закріплює:

- об’єкти захисту та завдання їх захисту;

- правила обробки інформації;

- мету побудови КСЗІ;

- заходи захисту інформації.

План захисту має фіксувати на певний момент часу:

- склад ІТС;

- перелік інформації, що обробляється;

- технологію обробки інформації;

- заходи та засоби захисту інформації;

- склад необхідної документації тощо.

План захисту повинен регулярно переглядатися та за необхідності змінюватись. Зміни та доповнення до Плану захисту затверджуються у тому ж порядку, що і основний документ.

Для АС, в яких обробляється інформація, що становить державну або іншу встановлену законом таємницю, службова інформація, інформація, яка належить до державних інформаційних ресурсів, або інформація, необхідність захисту якої встановлено законом, План захисту є обов’язковим документом. Склад і зміст Плану захисту для таких АС встановлено «**Положенням про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в АС**», затвердженим ПКМУ № 180-98.

План захисту повинен складатись з таких розділів:

1. Завдання захисту, класифікацію, опис технології обробки службової інформації.

2. Модель загроз інформації в АС.

3. Політика (основні правила) захисту інформації в АС.

4. Перелік нормативних, розпорядчих, організаційно-технічних та інших документів, згідно з якими реалізовано захист інформації в АС.

5. Календарний план робіт із захисту інформації в АС.

План захисту рекомендується розробляти і для всіх інших ІТС, в яких обробляється інформація, що підлягає захисту згідно з законодавством України, згідно вимог «**Правил забезпечення захисту інформації в ІТС**», затверджених ПКМУ № 373-2006.

План захисту повинен складатись з таких розділів:

1. Завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації.

2. Визначення моделі загроз для інформації в системі.

3. Основні вимоги щодо захисту інформації та правила доступу до неї в системі.

4. Перелік документів, згідно з якими здійснюється захист інформації в системі.

5. Перелік і строки виконання робіт службою захисту інформації.

Крім того, НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в АС»має додаток«**Методичні вказівки щодо структури та змісту Плану захисту інформації в АС**».

План захисту повинен складатись з таких розділів:

1. Завдання захисту інформації в АС.

2. Класифікація інформації, що обробляється в АС.

3. Опис компонентів АС та технології обробки інформації.

4. Загрози для інформації в АС.

5. Політика безпеки інформації в АС.

6. Система документів з забезпечення захисту інформації в АС.

# 15. Вибір ОС, АВПЗ і КЗЗ

Перед початком розробки технічного завдання на створення КСЗІ в ІТС здійснюється вибір технічних і програмно-апаратних засобів, які реалізують задані вимоги щодо надійного функціонування ІТС та захисту інформації, яка в ній обробляється.

До таких першочергових засобів в ІТС відносяться:

- операційна система (далі - ОС);

- антивірусне програмне забезпечення (далі - АВПЗ);

- комплекс засобів захисту від НСД (далі - КЗЗ) у разі потреби.

Стаття 8 Закону України «Про захист інформації в ІТС» визначає, що для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері захисту інформації.

Тобто засоби захисту інформації, інші технічні засоби та програмне забезпечення ІТС, що планується задіяти в КСЗІ, повинні мати підтвердження їхньої відповідності НД ТЗІ (сертифікат відповідності або експертний висновок) і використовуватись згідно цих вимог.

Здійснення сертифікації, підтвердження відповідності та проведення державної експертизи таких засобів здійснює Адміністрація Держспецзв'язку. Вона веде **«Перелік** **засобів** **ТЗІ**, **дозволених** **для** **забезпечення** **технічного** **захисту** **державних** **інформаційних** **ресурсів** **та** **інформації**, **вимога** **щодо** **захисту** **якої** **встановлена** **законом»** (далі - Перелік),який формується відповідно до пункту 17 «Положення про ТЗІ в Україні», затвердженого Указом Президента України від 27.09.99 № 1229.

Перелік призначений для використання суб'єктами системи ТЗІ під час час створення та модернізації КСЗІ в АС.

Перелік містить номенклатуру технічних засобів із захистом інформації, засобів ТЗІ, засобів контролю за ефективністю ТЗІ, засобів виявлення та індикації загроз безпеці інформації, відповідність яких вимогам нормативних документів з питань ТЗІ засвідчено сертифікатом відповідності або позитивним експертним висновком, одержаними у порядку, який встановлено такими нормативно-правовими актами:

- Правилами проведення робіт із сертифікації засобів захисту інформації, затвердженими спільним наказом Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 № 75/91 і зареєстрованими в Міністерстві юстиції України 14.05.2007 за № 498/13765;

- Положенням про державну експертизу в сфері ТЗІ, затвердженим наказом Адміністрації Держспецзв'язку України від 16.05.2007 № 93 і зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087.

Використання засобів з цього Переліку під час створення та модернізації КСЗІ в АС не увільняє від оцінювання відповідності досягнутого рівня захисту вимогам НД ТЗІ, яке здійснюється шляхом експертизи КСЗІ в АС.

Можливість подальшого використання засобів, які не ввійшли до цього Переліку, в діючій КСЗІ в АС визначається за результатом їх чергової експертизи.

Оновлення інформації, яка міститься в Переліку, здійснюється шляхом періодичного внесення змін до попередньої редакції. Перелік та його доповнення розміщуються на WEB-сайті *www.dsszzi.gov.ua.*

**Використання засобів ТЗІ, які на момент проектування КСЗІ**

**не мають підтвердження відповідності у сфері ТЗІ**

У разі необхідності використання в КСЗІ засобів ТЗІ, які на момент проектування КСЗІ не мали документа (сертифіката відповідності або експертного висновку), що підтверджує їх відповідність у сфері ТЗІ, ці засоби згідно з «Правилами забезпечення захисту інформації в ІТС», затвердженими ПКМУ від 29 березня 2006 року № 373, мають піддаватися відповідному оцінюванню під час проведення державної експертизи КСЗІ.

При цьому має оцінюватися відповідність засобів ТЗІ вимогам НД ТЗІ в обсязі показників тих функцій захисту, які реалізовані для захисту інформації, що обробляється в даній ІТС. Також має оцінюватися можливість створення цими засобами ТЗІ технічних каналів витоку інформації (в тому числі через закладні пристрої).

Має бути проведений аналіз особливостей застосування засобів ТЗІ в даній ІТС, за результатами якого мають бути встановлені (ідентифіковані, уточнені) функції захисту, які реалізовані для захисту інформації саме в даній ІТС, та показники цих функцій.

Програма та методика проведення державної експертизи КСЗІ має містити перелік робіт щодо визначення (вимірювання) встановлених за результатами аналізу показників функцій захисту засобів ТЗІ, оцінки відповідності цих показників вимогам НД ТЗІ та оцінки можливості створення цими засобами ТЗІ технічних каналів витоку інформації. Також мають бути наведені нормативні документи з питань ТЗІ, які визначають вимоги до цих показників.

Результати визначення (вимірювань) показників функцій захисту засобів ТЗІ, результати їх порівняння з вимогами нормативних документів та результати оцінювання можливості створення цими засобами ТЗІ технічних каналів витоку інформації мають відображатися у відповідних протоколах, які подаються на розгляд Експертної ради Адміністрації Держспецзв’язку разом з матеріалами державної експертизи КСЗІ (з Протоколом державної експертизи КСЗІ та Експертним висновком).

Засоби ТЗІ, які пройшли оцінювання під час державної експертизи КСЗІ, можуть використовуватись для захисту інформації виключно у складі цієї КСЗІ.

**1. Вибір ОС для робочої станції (АС класу 1)**

На даний час позитивний експертний висновок мають такі ОС: Windows 8 Professional і Windows 8.1 Enterprise. Крім цих, розглянемо ще захищену ОС «myLinux 3.1 ОКО», що отримала позитивний експертний висновок у 2006 році, дані яких для зручного порівняння викладемо у табличному вигляді.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Комплекс засобів захисту ОС** | **myLinux 3.1 ОКО** | **Windows 8****Professional** | **Windows 8.1****Enterprise** |
|  | Виробник | Україна, ТОВ «Майлінукс» | США, Microsoft Corporation | США, Microsoft Corporation |
|  | Рівень гарантій | Г3 | Г2 | Г2 |
| **Послуги конфіденційності** |
| 1 | базова адміністр. конфіденційність | КА-2 | - | - |
| 2 | базова довірча конфіденційність | КД-2 | КД-2 | КД-2 |
| 3 | повторне використання об’єктів | КО-1 | КО-1 | КО-1 |
| 4 | мінімальна конфіденційність при обміні  | КВ-1 | КВ-1 | КВ-1 |
| **Послуги цілісності** |
| 1 | базова адміністративна цілісність | ЦА-2 | - | - |
| 2 | базова / мінімальна довірча цілісність | ЦД-2 | ЦД-1 | ЦД-1 |
| 3 | обмежений відкат | ЦО-1 | ЦО-1 | ЦО-1 |
| 4 | мінімальна цілісність при обміні | - | ЦВ-1 | ЦВ-1 |
| **Послуги доступності** |
| 1 | використання ресурсів - квота | ДР-1 | ДР-1 | ДР-1 |
| 2 | стійкість при обмежених відмовах | ДС-1 | - | - |
| 3 | обмежена гаряча заміна | ДЗ-2 | ДЗ-2 | ДЗ-2 |
| 4 | автоматизоване відновлення | ДВ-1 | ДВ-2 | ДВ-2 |
| **Послуги спостережності** |
| 1 | захищений журнал | НР-2 | НР-2 | НР-2 |
| 2 | множинна / одиночна ідент. і автентифікація | НИ-3 | НИ-2 | НИ-2 |
| 3 | дво / однонаправлений достовірний канал | НК-2 | НК-1 | НК-1 |
| 4 | виділення адміністратора / розподіл обов'язків на підставі привілеїв | НО-2 | НО-3 | НО-3 |
| 5 | КЗЗ з контролем цілісності / гарантованою цілісністю | НЦ-1 | НЦ-2 | НЦ-2 |
| 6 | самотестування при старті | НТ-2 | НТ-2 | НТ-2 |
| 7 | автентифікація вузла | - | НВ-1 | НВ-1 |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених ОС, можна зробити такі висновки:

- КЗЗ ОС обох «Windows» однакові і забезпечують тільки довірче керування доступом;

- КЗЗ ОС «myLinux 3.1 ОКО» є найсильнішим, оскільки у порівнянні з «Windows» забезпечує вищий рівень гарантій Г-3 і послуги базової адміністративної конфіденційності КА-2 і цілісності ЦА-2, а також стійкості при обмежених відмовах ДС-1 і множинної ідентифікації та автентифікації НИ-3, що забезпечує надійний захист інформації від несанкціонованого і неконтрольованого ознайомлення, модифікації, знищення, копіювання та розповсюдження.

На жаль, на даний час ОС «myLinux 3.1 ОКО» не має позитивного експертного висновку.

Таким чином, КЗЗ ОС «Windows» не забезпечує виконання вимог пунктів 6 і 7 Правил щодо забезпечення захисту ІзОД від несанкціонованого і неконтрольованого ознайомлення, модифікації, знищення, копіювання, розповсюдження і забезпечення можливості надання користувачу права на виконання однієї або декількох операцій з оброблення конфіденційної інформації або позбавлення його такого права.

У разі використання тільки штатних засобів ОС «Windows» стає можливою навмисна або випадкова реалізація будь-яким авторизованим користувачем таких загроз:

- несанкціонованого копіювання файлів даних, що містять ІзОД, з використанням штатних засобів ОС (наприклад, програми «Провідник»), в каталоги жорсткого диска, які містяться у профайлі користувача (наприклад, каталог «Мої документи»), з отриманням можливості самостійно надавати права доступу до відповідного файлу іншим користувачам, а також безконтрольно його поширювати, що приведе до порушення конфіденційності ІзОД;

- несанкціонованого експорту даних, ІзОД, що містять, на з'ємні носії, розмежування доступу до яких засобами ОС «Windows» не здійснюється, що приведе до порушення конфіденційності ІзОД;

- несанкціонованій модифікації файлів даних з використанням штатних засобів ОС (наприклад, програми «Блокнот»), які не призначені для обробки файлів даних відповідного типу, що не тільки приведе до порушення цілісності ІзОД, але може взагалі привести до блокування можливості подальшої роботи авторизованих користувачів з відповідним файлом даних, тобто до порушення доступності інформації.

**2. Вибір ОС для серверу (АС класу 2 і 3)**

На даний час позитивний експертний висновок мають такі ОС: Windows Server 2008 R2, Windows Server 2012 R2, OpenBSD шифр «BBOS». Розглянемо ці ОС, дані яких для зручного порівняння викладемо у табличному вигляді.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Комплекс засобів захисту****операційної системи** | **OpenBSD «BBOS»** | **Windows****Server 2008** | **Windows****Server 2012** |
|  | Виробник | Україна, ТОВ «АТМНІС» | США, Microsoft Corporation | США, Microsoft Corporation |
|  | Рівень гарантій | Г2 | Г2 | Г2 |
| **Послуги конфіденційності** |
| 1 | базова адміністративна конфіденційність | КА-2 | - | - |
| 2 | базова довірча конфіденційність | КД-2 | КД-2 | КД-2 |
| 3 | повторне використання об’єктів | КО-1 | КО-1 | КО-1 |
| 4 | конфіденційність при обміні (баз/мін) | КВ-2 | КВ-1 | КВ-1 |
| **Послуги цілісності** |
| 1 | мінімальна адміністративна цілісність | ЦА-1 | - | - |
| 2 | мінімальна довірча цілісність | ЦД-1 | ЦД-1 | ЦД-1 |
| 3 | обмежений відкат | ЦО-1 | ЦО-1 | ЦО-1 |
| 4 | мінімальна цілісність при обміні | ЦВ-1 | ЦВ-1 | ЦВ-1 |
| **Послуги доступності** |
| 1 | незахоплення ресурсів / квота | ДР-2 | ДР-1 | ДР-1 |
| 2 | стійкість з погіршенням характеристик / при обмежених відмовах | ДС-2 | ДС-1 | ДС-1 |
| 3 | обмежена гаряча заміна | ДЗ-2 | ДЗ-2 | ДЗ-2 |
| 4 | автоматизоване відновлення | ДВ-2 | ДВ-2 | ДВ-2 |
| **Послуги спостережності** |
| 1 | захищений журнал | НР-2 | НР-2 | НР-2 |
| 2 | одиночна ідентифікація і автентифікація | НИ-2 | НИ-2 | НИ-2 |
| 3 | однонаправлений достовірний канал | НК-1 | НК-1 | НК-1 |
| 4 | виділення адміністратора / розподіл обов'язків на підставі привілеїв | НО-1 | НО-3 | НО-3 |
| 5 | КЗЗ з контролем цілісності / гарантованою цілісністю | НЦ-1 | НЦ-2 | НЦ-2 |
| 6 | самотестування при старті | НТ-2 | НТ-2 | НТ-2 |
| 7 | автентифікація вузла | НВ-1 | НВ-1 | НВ-1 |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених ОС, можна зробити такі висновки:

- КЗЗ ОС обох «Windows» однакові і забезпечують тільки довірче керування доступом;

- КЗЗ ОС «OpenBSD» є найсильнішим, оскільки у порівнянні з «Windows» забезпечує послуги адміністративної конфіденційності і цілісності, що дає можливість захисту інформації від несанкціонованого і неконтрольованого ознайомлення, модифікації, знищення, копіювання та розповсюдження.

**3. Вибір АВПЗ**

На даний час позитивний експертний висновок мають такі АВПЗ: Kaspersky, Dr.Web, ESET, AVAST, McAfee, Symantec, Zillya! Розглянемо три АВПЗ під керуванням найпоширенішої ОС «Windows», дані яких для зручного порівняння викладемо у табличному вигляді.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Програмне забезпечення антивірусного захисту інформації під керуванням «Windows»** | **Kaspersky Endpoint Security 10 for Windows** | **McAfee Endpoint Protection Suite** | **Zillya! Антивірус для Бізнесу версія 1.1** |
|  | Виробник | Росія, ЗАТ «Лаборатория Касперского» | США, «McAfee Inc.» | Україна, ТОВ«Олайті Сервіс» |
|  | Рівень гарантій | Г2 | Г2 | Г2 |
| **Послуги конфіденційності** |
| 1 | базова адміністративна конфіденційність | КА-2 | КА-2 | КА-2 |
| **Послуги цілісності** |
| 1 | мінімальна адміністративна цілісність | ЦА-1 | ЦА-1 | ЦА-1 |
| 2 | обмежений відкат | ЦО-1 | ЦО-1 | - |
| 3 | мінімальна цілісність при обміні | ЦВ-1 | ЦВ-1 | ЦВ-1 |
| **Послуги доступності** |
| 1 | використання ресурсів - квота | ДР-1 | - | - |
| 2 | стійкість при обмежених відмовах | ДС-1 | ДС-1 | ДС-1 |
| 3 | модернізація | ДЗ-1 | ДЗ-1 | ДЗ-1 |
| 4 | ручне відновлення | ДВ-1 | ДВ-1 | ДВ-1 |
| **Послуги спостережності** |
| 1 | захищений журнал | НР-2 | НР-2 | НР-2 |
| 2 | одиночна ідентифікація і автентифікація | НИ-2 | НИ-2 | НИ-2 |
| 3 | однонаправлений достовірний канал | НК-1 | НК-1 | НК-1 |
| 4 | виділення адміністратора  | НО-1 | НО-2 | НО-1 |
| 5 | КЗЗ з контролем цілісності  | НЦ-1 | НЦ-1 | НЦ-1 |
| 6 | самотестування при старті | НТ-2 | НТ-2 | НТ-2 |
| 7 | автентифікація вузла | НВ-1 | НВ-1 | - |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених АВПЗ, можна зробити такі висновки:

- «Kaspersky Endpoint Security» є найсильнішим ПЗ, оскільки у порівнянні з іншими має найбільшу кількість послуг безпеки та додатково забезпечує послугу використання ресурсів ДР-1 (квота);

- «Zillya! Антивірус» є найслабкішим ПЗ, оскільки у порівнянні з іншими має найменшу кількість послуг безпеки та не забезпечує послуг обмеженого відкату ЦО-1, використання ресурсів ДР-1 і автентифікації вузла НВ-1.

**Порядок оновлення антивірусних програмних засобів,**

**які мають позитивний експертний висновок**

**за результатами державної експертизи в сфері ТЗІ**

(затверджений наказом Адміністрації Держспецзв'язку від 26.03.2007 № 45 і зареєстрований в Мін’юсті 10.04.2007 за № 320/13587)

3. Поняття, що використовуються у цьому Порядку, мають таке значення:

- центр антивірусного захисту інформації (далі - ЦАЗІ) - організаційно-технічний комплекс, призначений для вирішення питання захисту ІТС від комп'ютерних вірусів з подальшим розвитком комплексного підходу до проблеми антивірусного захисту ІТС;

- комп'ютерний вірус - програма, що здатна створювати свої копії, модифіковані копії, які можуть цілком не відповідати оригіналу, і впроваджувати їх у різні об'єкти/ресурси ІТС безвідома користувача, й направлена на деструктивну дію;

- антивірусний програмний засіб (далі - АВПЗ) – програмне забезпечення, яке призначене для захисту об'єктів/ресурсів ІТС відушкодження комп'ютерними вірусами;

- антивірусне оновлення АВПЗ - складова частина АВПЗ, яка розробляється після створення засобу та призначена для пристосування АВПЗ до захисту об'єктів/ресурсів ІТС від ушкодженнята зараження новими вірусами.

5. Оновлення АВПЗ здійснюється шляхом організації та забезпечення процесу отримання та впровадження в АВПЗ антивірусних оновлень.

 6. Оновлення АВПЗ, який пройшов державну експертизу та має позитивний експертний висновок Адміністрації Держспецзв'язку, здійснюється з використанням антивірусних оновлень, які розміщуються на веб-сайті ЦАЗІ (*www.cazi.dsszzi.gov.ua*).

7. На веб-сайті ЦАЗІ розміщуються тільки антивірусні оновлення АВПЗ, які пройшли експрес-експертизу. Крім того, на веб-сайті можна подивитись перелік АВПЗ, що отримало позитивний експертний висновок Держспецзв'язку.

8. Експрес-експертиза антивірусного оновлення АВПЗ здійснюється ЦАЗІ шляхом перевірки АВПЗ з впровадженим антивірусним оновленням на його відповідність експертному висновку, виданому за результатами державної експертизи.

У подальшому під антивірусним оновленням АВПЗ розуміється антивірусне оновлення АВПЗ, яке пройшло експрес-експертизу.

9. Органи державної влади та місцевого самоврядування, утворені відповідно до законів України військові формування та організації державної форми власності:

- не менше ніж раз на день отримують антивірусні оновлення АВПЗ за допомогою веб-серверу ЦАЗІ;

- інсталюють отримані за допомогою веб-серверу ЦАЗІ антивірусні оновлення АВПЗ відповідно до технічної документації АВПЗ;

- для забезпечення авторизованого доступу до ресурсів веб-серверу ЦАЗІ щороку до 1 березня надають до Адміністрації Держспецзв'язку відомості щодо кожного користувача у паперовому вигляді за визначеною формою (у разі внесення змін - протягом 3-х днів).

10. Адміністрація Держспецзв'язку:

- організовує за допомогою спеціалізованого ПЗ отримання органами державної влади та місцевого самоврядування, утвореними відповідно до законів України військовими формуваннями та організаціями державної форми власності антивірусних оновлень для АВПЗ, які мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ, та забезпечує функціонування веб-серверу ЦАЗІ;

- заносить надану органами державної влади та місцевого самоврядування, утвореними відповідно до законів України військовими формуваннями та організаціями державної форми власності реєстраційну інформацію до бази даних користувачів ЦАЗІ. Реалізує автентифікацію та ідентифікацію користувачів відповідно до цієї бази даних;

- проводить експрес-експертизу антивірусних оновлень АВПЗ;

- розробляє рекомендації щодо тримання антивірусних оновлень АВПЗ та їх розміщення на веб-сайті ЦАЗІ;

- використовує механізм ЕЦП для підтвердження цілісності антивірусних оновлень АВПЗ та ідентифікації підписувача після впровадження в органі державної влади та місцевого самоврядування, утворених відповідно до законів України військових формуваннях та організаціях державної форми власності ЕЦП.

**4. Вибір КЗЗ від НСД**

**4.1. Системи захисту в АС класу 1**

На даний час позитивний експертний висновок мають такі КЗЗ: «Лоза-1», «Гриф» і «Рубіж-РСО». Розглянемо два КЗЗ, дані яких для зручного порівняння викладемо у табличному вигляді.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1** | **Система захисту інформації** | **Лоза-1****версія 4** | **Рубіж-РСО****версія 2** | **Гриф****версія 3** |
| 2 | Виробник | ТОВ НДІ «Автопром» | ПАТ «КП ОТІ» | ТОВ «ІКТ»м. Київ |
| 4 | Рівень гарантій | Г4 | Г3 | Г4 |
| **Послуги конфіденційності** |
| 1 | повна / базова адмін. конфіденційність  | КА-3 | КА-2 | КА-2 |
| 2 | повторне використання об’єктів | КО-1 | КО-1 | КО-1 |
| **Послуги цілісності** |
| 1 | мінімальна / базова адмін. цілісність | ЦА-1 | ЦА-1 | ЦА-2 |
| 2 | обмежений відкат | - | - | ЦО-1 |
| **Послуги доступності** |
| 1 | використання ресурсів - квота | - | - | ДР-1 |
| 2 | стійкість при обмежених відмовах | ДС-1 | - | ДС-1 |
| 3 | модернізація | ДЗ-1 | - | ДЗ-1 |
| 4 | ручне відновлення | ДВ-1 | ДВ-1 | ДВ-1 |
| **Послуги спостережності** |
| 1 | захищений журнал / детальна реєстрація | НР-2 | НР-2 | НР-2 |
| 2 | множинна ідентифікація і автентифікація | НИ-3 | НИ-3 | НИ-3 |
| 3 | однонаправлений достовірний канал | НК-1 | НК-1 | НК-1 |
| 4 | розподіл обов'язків адміністратора  | НО-2 | НО-2 | НО-2 |
| 5 | КЗЗ з гарантованою цілісністю  | НЦ-2 | НЦ-1 | НЦ-2 |
| 6 | самотестування при старті | НТ-2 | НТ-2 | НТ-2 |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених КЗЗ, можна зробити такі висновки:

- усі КЗЗ забезпечують послуги адміністративної конфіденційності КА та цілісності ЦА, тобто гарантують захист інформації від несанкціонованого і неконтрольованого ознайомлення, модифікації, знищення, копіювання та розповсюдження;

- «Гриф» є найсильнішим КЗЗ, оскільки у порівнянні з іншими має найбільшу кількість послуг безпеки та додатково забезпечує послуги обмеженого відкату ЦО-1 і використання ресурсів ДР-1 (квота);

- «Рубіж-РСО» є найслабкішим КЗЗ, оскільки у порівнянні з іншими має найменшу кількість послуг безпеки.

**4.2. Системи захисту в АС класу 2**

На даний час позитивний експертний висновок мають такі КЗЗ: Лоза-2, Гриф-Мережа, VTI-Рубіж. Розглянемо два КЗЗ, дані яких для зручного порівняння викладемо у табличному вигляді.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Система захисту інформації** | **ЛОЗА-2****версія 4** | **VTI-Рубіж версія 2** | **Гриф-****Мережа** |
|  | Виробник | ТОВ НДІ «Автопром» | ПАТ «КП ОТІ» | ТОВ «ІКТ»м. Київ |
|  | Рівень гарантій | Г4 | Г3 | Г4 |
| **Послуги конфіденційності** |
| 1 | повна / базова адмін. конфіденційність  | КА-3 | КА-2 | КА-2 |
| 2 | повторне використання об’єктів | КО-1 | КО-1 | КО-1 |
| **Послуги цілісності** |
| 1 | мінімальна / базова адмін. цілісність | ЦА-1 | ЦА-2 | ЦА-2 |
| 2 | обмежений відкат | - | ЦО-1 | ЦО-1 |
| **Послуги доступності** |
| 1 | використання ресурсів - квоти | - | - | ДР-1 |
| 2 | стійкість при обмежених відмовах | ДС-1 | ДС-1 | ДС-1 |
| 3 | модернізація | ДЗ-1 | ДЗ-1 | ДЗ-1 |
| 4 | ручне відновлення | ДВ-1 | ДВ-1 | ДВ-1 |
| **Послуги спостережності** |
| 1 | детальна реєстрація / аналіз у реальному часі | НР-4 | НР-4 | НР-5 |
| 2 | множинна ідентифікація і автентифікація | НИ-3 | НИ-3 | НИ-3 |
| 3 | однонаправлений достовірний канал | НК-1 | НК-1 | НК-1 |
| 4 | розподіл обов'язків адміністратора  | НО-2 | НО-2 | НО-2 |
| 5 | КЗЗ з гарантованою цілісністю  | НЦ-2 | НЦ-2 | НЦ-2 |
| 6 | самотестування при старті | НТ-2 | НТ-3 | НТ-2 |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених КЗЗ, можна зробити такі висновки:

- «Гриф-Мережа» є найсильнішим КЗЗ, оскільки у порівнянні з іншими має найбільшу кількість послуг безпеки та додатково забезпечує послугу використання ресурсів ДР-1 (квота) та вищий рівень послуги реєстрації НР-5 (аналіз у реальному часі);

- «Лоза-2» є найслабкішим КЗЗ, оскільки у порівнянні з іншими має найменшу кількість послуг безпеки та не забезпечує послуг обмеженого відкату ЦО-1 і використання ресурсів ДР-1.

**4.3. Системи захисту Web-ресурсів**

На даний час позитивний експертний висновок мають такі КЗЗ: Портал Менеджер і Тайфун-Web. Розглянемо їх, дані яких для зручного порівняння викладемо у табличному вигляді.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Система захисту інформації** | **Портал Менеджер 1.0** | **Тайфун-Web вер. 1.хх** |
|  | Виробник | ТОВ «Софтлайн ІТ», м. Київ | ТОВ «ІКТ», м.Київ |
|  | Рівень гарантій | Г2 | Г4 |
| **Послуги конфіденційності** |
| 1 | базова адміністративна конфіденційність  | КА-2 | КА-2 |
| 2 | повторне використання об’єктів | КО-1 | КО-1 |
| 3 | базова конфіденційність при обміні | - | КВ-2 |
| **Послуги цілісності** |
| 1 | мінімальна адміністративна цілісність  | ЦА-1 | ЦА-1 |
| 2 | обмежений відкат | ЦО-1 | - |
| 3 | базова цілісність при обміні | - | ЦВ-2 |
| **Послуги доступності** |
| 1 | стійкість при обмежених відмовах | - | ДС-1 |
| 2 | модернізація | - | ДЗ-1 |
| 3 | ручне відновлення | ДВ-1 | ДВ-1 |
| **Послуги спостережності** |
| 1 | захищений журнал / зовнішній аналіз | НР-2 | НР-1 |
| 2 | одиночна / зовнішня ідентифікація і автентифікація | НИ-2 | НИ-1 |
| 3 | однонаправлений достовірний канал | НК-1 | - |
| 4 | розподіл обов'язків / виділення адміністратора  | НО-2 | НО-1 |
| 5 | КЗЗ з контролем цілісності | НЦ-1 | НЦ-1 |
| 6 | самотестування при старті | НТ-2 | НТ-2 |
| 7 | автентифікація вузла / джерела даних | НВ-1 | НВ-2 |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених КЗЗ, можна зробити такі висновки:

- «Тайфун-Web» є найсильнішим КЗЗ, оскільки у порівнянні з іншим має найбільшу кількість послуг безпеки, вищий рівень гарантій та забезпечує додатково послуги базової конфіденційності при обміні КВ-2, базової цілісності при обміні ЦВ-2, стійкості при обмежених відмовах ДС-1 і модернізації ДЗ-1;

- «Портал Менеджер» є найслабкішим КЗЗ, оскільки у порівнянні з іншим має найменшу кількість послуг безпеки.

Разом з тим, «Портал Менеджер» у порівнянні з іншим забезпечує додатково послуги обмеженого відкату ЦО-1 і однонаправленого достовірного каналу НК-1, а також вищий рівень послуг ідентифікації і автентифікації НИ-2 (одиночна), реєстрації НР-2 (захищений журнал), розподілу обов’язків НО-2 (адміністраторів).

Крім того, головна відмінність КЗЗ «Тайфун-Web» від КЗЗ «Портал Менеджер» є застосування симетричних криптоалгоритмів для захисту конфіденційності та цілісності інформації, що передається між клієнтом та сервером.

Кінцевий результат вибору ОС, АВПЗ і КЗЗ залежить від необхідності та достатності послуг безпеки, які повинні забезпечити обраний ФПЗ ІТС.

**5. Вибір комплексу ТЗІ**

Інформація, що становить державну таємницю та оброболяється технічними засобами (у тому числі АС), згідно вимог законодавства підлягає захисту від витоку технічними каналами за рахунок побічних електромагнітних випромінювань і наведень (далі – ПЕМВН). Закриття технічних каналів витоку інформації (далі - ТКВІ) забезпечується пасивними або активними методами і засобами:

* пасивні - здійснюють ослаблення рівня інформаційних сигналів АС, що забезпечується екрануванням технічних засобів обробки інформації або приміщень, де вони розташовані;
* активні - здійснюють зменшення відношення сигнал/завада (далі - С/3) АС у місцях можливого розміщення технічних засобів розвідки до рівня, який унеможливлює виділення інформації, що забезпечується електромагнітним зашумленням.

***Пасивні засоби***

Одним з пасивних засобів захисту інформації в АС від ПЕМВН є електронні обчислювальні машини (далі - ЕОМ) у захищеному виконанні. Вони виготовляються з використанням сучасних пасивних методів захисту у поєднанні з оригінальними схемотехнічними рішеннями, що|вирішеннями,розв'язаннями,розв'язуваннями| забезпечують їх захист від ПЕМВН і|та| зовнішнього|навмисної| електромагнітного впливу, спрямованого|направленої| на знищення інформації або порушення її працездатності|чинить|.

Розроблені технології включають нанесення екрануючого покриття з використанням методів іонно-плазмового напилення на внутрішні поверхні пластмасових корпусів моніторів, клавіатур, маніпуляторів «миша» та нанесення прозорих екрануючих покриття на захисні стекла моніторів, а також використання спеціальної конструкції корпусів системних блоків, протизавадних фільтрів, спеціальних екранованих кабелів і електроз’єднувачів. При цьому забезпечується збереження початкового зовнішнього вигляду ЕОМ, а рівень захищеності не залежить від їх конкретних конфігурацій.

ЕОМ у захищеному виконанні призначена для обробки інформації будь-якого рівня секретності на одній і тій же ЕОМ на об’єктах будь-якої категорії без використання дорогих і небезпечних для здоров'я персоналу екранованих приміщень (внаслідок відбивання та складання випромінювань).

Крім того, використання розробленої технології дозволяє забезпечити додатковий захист користувачів від високочастотного електромагнітного випромінювання ЕОМ, яке не регламентується стандартами безпеки «ТСО», але при довготривалій дії також є шкідливим, оскільки електромагнітні випромінювання в дециметровому і сантиметровому діапазоні найбільш «ефективні» за дією на організм людини, особливо на нервову систему і органи зору.

Використанню підлягають тільки ті пасивні засоби, які мають сертифікат відповідності у сфері ТЗІ. На даний час українські виробники пропонують такі захищені ПЕОМ, які мають сертифікат відповідності:

* електронна обчислювальна машина «ЕОМ-П0» (робоча станція) і «ЕОМ-П1» (сервер) - ЗАТ «Інформаційні комп'ютерні системи» (Київ);
* персональний комп'ютер із захистом інформації «Expert» - ТОВ «Епос» (Київ);
* універсальне автоматизоване робоче місце у захищеному виконанні  ЗОТ «Плазма-ЗВ-АРМ» - ТОВ «НВП “Плазмотехніка”» (Київ).

***Активні засоби***

Пристрої просторового зашумлення застосовуються у разі, коли пасивні заходи не забезпечують необхідної ефективності захисту інформації, що становить державну таємницю, яка обробляється в АС.

При цьому треба розуміти, що застосування генераторів шуму негативно впливає на центральну нервову та серцево-судинну систему людини, а також демаскує місцезнаходження об’єкта та час обробки інформації, не забезпечуючи захист інформативних сигналів у вищому гігагерцовому діапазоні. До того ж, захисна дія генераторів шуму може бути взагалі компенсована сучасними методами обробки сигналів.

До складу засобу просторового зашумлення входять:

- надширокосмугові генератори електромагнітного шуму;

- система антен;

- пульт сигналізації справності роботи системи.

Використанню підлягають тільки ті активні засоби, які мають позитивний експертний висновок у сфері ТЗІ. На даний час українські виробники пропонують такі генератори, які мають позитивний експертний висновок:

- «БАЗАЛЬТ- 5ГЕШ» - ДП «Укрспецтехніка система» (Київ);

- «РІАС-1К» - ПП «РІАС» (Київ);

- «ІЗ-2000» - ТОВ «Інфозахист» (Київ);

- «УЗОР-ПЕ» - ТОВ «Галтехноком» (Львів);

- «DELTA-7» - ТОВ «Discovery defence enjineering» (Київ).

**Порівняльний аналіз характеристик генераторів**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Назва | Габаритні розміри, мм | Вага, кг | Частотний діапазон  | Споживана потужність | Ціна,тис.грн |
| БАЗАЛЬТ- 5ГЕШ | 750×750×50  | 1,1 | 100 кГц - 1 ГГц | 6 Вт | 7,5 |
| РІАС-1К | 198×190×70  | 2,5  | 0,18 кГц - 2 ГГц | 20 Вт | 8,0 |
| DELTA-7 | 220×60×40  | 0,8  | 9 кГц - 3,3 ГГц | - | - |
| ІZ-2000 | - | - | 100 кГц - 2 ГГц | 60 Вт | - |

**16. Опис функцій і можливостей КЗЗ від НСД**

**1. Системи захисту в АС класу 1**

**1.1. «Рубіж-РСО» (версія 2)**

Комплекс призначений для забезпечення захищеної інформаційної технології в частині збирання, оброблення, зберігання і представлення інформації з обмеженим доступом в АС класу 1.

**ФПЗ комплексу:**

**КА-2, КО-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-1, НТ-2**

**Рівень гарантій – Г-3.**

Розробник: ПАТ «КП ОТІ», м. Київ

Експертний висновок № 422 дійсний до 01.03.2016

**Комплекс** може використовуватися у якості програмно-технічного ядра КСЗІ в АС класу 1 для обробки конфіденційної інформації, а також інформації, що становить державну таємницю, при виконанні відповідних організаційних заходів та забезпеченні захисту від витоку інформації технічними каналами.

**Використання передбачається: на робочих станціях «Intel» архітектури в середовищі операційної системи (далі - ОС) Windows 2000 / XP.**

**При автентифікації в Windows використовуються логін і пароль та додатково перевіряється PIN-код на оптичному носії CD-R/RW, який повинен бути зареєстрований адміністратором безпеки в базі даних комплексу за правилами обліку носіїв. Тільки при наявності усіх цих чинників може бути здійснена автентифікація користувача АС.**

**Технологія обробки конфіденційної інформації передбачає виконання таких вимог:**

**- ІзОД зберігається тільки на зйомних магнітних (Flash диски) та оптичних носіях (CD-R/RW), які зареєстровані адміністратором в базі даних;**

**- на одному носії зберігаються дані одного ступеню конфіденційності, який відповідає встановленому для носія грифу конфіденційності.**

**Комплекс забезпечує вирішення таких функцій захисту:**

* можливість доступу до інформації тільки за умови достовірного розпізнавання користувача з урахуванням наданих йому повноважень;
* виключення неконтрольованого та несанкціонованого ознайомлення, копіювання та відновлення інформації;
* виключення неконтрольованої та несанкціонованої модифікації та видалення інформації;
* ведення обліку дій користувачів та реєстрацію спроб порушення встановленого порядку доступу до інформації, блокування доступу до інформації у разі виявлення таких спроб, а також можливість здійснення контролю за доступом до інформації з боку адміністратора безпеки (відповідальної особи);
* **контроль роботи комплексу ТЗІ від витоку фізичними каналами, при включенні до складу КЗЗ приладу контролю активності «РІАС-4КА»;**
* **контроль цілісності комплексу ТЗІ.**

**Комплекс складається з:**

**- комплексу технічних засобів обробки ІзОД;**

**- засобів захисту інформації від витоку фізичними каналами, які підключаються до певних входів приладу;**

**- «РІАС-4КА» -** пристрою автоматизованого контролю працездатності засобів просторового та лінійного захисту інформації з видаванням сигналів на КЗЗ**.**

**Опис функціонування**

**Посилена автентифікація – при спробі користувача авторизуватись в ОС відбувається перевірка КЗЗ від НСД. Якщо виявлені порушення, то користувач, що не є Адміністратором безпеки не зможе здійснити вхід до системи.**

**Моніторинг – вмикається тоді, коли адміністратор безпеки переведе КЗЗ в режим роботи Нормальний, і, вимикається, коли КЗЗ переводиться в режим роботи Службовий.**

**Інформування – у випадку виявлення порушень функціонування Комплексу буде надано користувачеві інформативне повідомлення з певним часом аварійного завершення сеансу на виявлення та можливого вирішення ситуації зі сторони користувача, якщо це можливо, та здійснений запис в базу даних КЗЗ.**

**Якщо час аварійного завершення сеансу вийшов і Комплекс не був відновлений, система примусово завершить сеанс користувача і переведеться в режим Службовий.**

**Обробка ІзОД передбачає виконання такої послідовності дій:**

**- отримати носій у відповідального за зберігання носіїв працівника;**

**- пройти процес автентифікації при вході в ОС;**

**- створити або скопіювати з носія до власної робочої папки необхідні для роботи документи;**

**- виконати планові операції з документами (створення, перегляд, редагування, друк та збереження);**

**- скопіювати необхідні документи на носій;**

**- всі документи робочих папок та тимчасово створені файли знищити;**

**- завершити сеанс роботи;**

**- здати носій на зберігання працівнику РСО.**

**1.2. «Лоза-1**» **(версія 4)**

**Система** - це програмний засіб захисту інформації від НСД в АС класу 1, який працює під керуванням **ОС** Windows XP / Vista / 7.

**Система постачається у двох конфігураціях:**

- «Підвищена безпека» - для захисту інформації, що становить державну таємницю;

- «Стандартна безпека» - для захисту службової та конфіденційної інформації (в тому числі персональних даних).

**ФПЗ системи у конфігурації «Підвищена безпека»:**

КА-3, КО-1, ЦА-1, ДВ-1, ДЗ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2.

**ФПЗ системи у конфігурації «Стандартна безпека»:**

КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДВ-1, ДЗ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2.

**У конфігурації «Стандартна безпека» рівень надання послуги безпеки «Ідентифікація та автентифікація» залежить від значення параметра конфігурації «*Перевіряти ключовий диск під час входу до Windows*». Якщо для нього встановлене значення «Так», зазначена послуга надається на рівні НИ-3 «Множинна ідентифікація та автентифікація».**

**У протилежному випадку послуга надається на рівні НИ-2 «Одиночна ідентифікація та автентифікація». У конфігурації «Підвищена безпека» послуга безпеки НИ-3 забезпечується автоматично. Як ключові диски можуть використовуватись модулі пам’яті USB Flash та CD/DVD-диски.**

Рівень гарантій: Г-4.

Експертний висновок № 540 дійсний до 08.08.2017**.**

Розробник: ТОВ НДІ «Автопром», м. Київ

***Система забезпечує:***

**1. Захист інформації від НСД:**

- дозволяє захистити будь-які дані на знімних та стаціонарних носіях; захист здійснюється на рівні папок Windows та знімних дисків;

- забезпечує надійний захист документів Microsoft Word та Microsoft Excel за рахунок тісної інтеграції з Microsoft Office (відключаються небезпечні команди, макроси, шаблони тощо); підтримуються версії Microsoft Office XP / 2003 / 2007 / 2010;

- дозволяє контролювати роботу із знімними дисками: компакт-дисками та флешками; для флешек дозволи на доступ до диска можуть встановлюватись для окремих носіїв (вони ідентифікуються за «залізним» серійним номером);

- дозволяє встановлювати дозволи або заборони на запуск процесів.

**2. Контроль друку та експорту:**

- забезпечує можливість встановлення дозволу/заборони друку та експорту на рівні окремих документів;

- для підсилення контролю дозволяє забезпечити присутність адміністратора або іншої уповноваженої особи під час друку та експорту (за рахунок необхідності введення пароля).

**3. Контроль входу користувачів до системи:**

- у конфігурації «Підвищена безпека» вхід здійснюється тільки після введення пароля та встановлення ключового диска (може використовуватись флешка або диск); діє жорстка політика паролів та політика блокування користувачів, яка протидіє підбору паролів;

- у конфігурації «Стандартна безпека» для входу достатньо ввести пароль; політика паролів менш жорстка, ніж в конфігурації «Підвищена безпека».

**4. Реєстрацію подій:**

- веде захищений журнал, в якому реєструються всі події, важливі для захисту інформації;

- аналіз журналу та протоколів роботи не потребує спеціальної кваліфікації;

- журнал подій ніколи не перезаписується: після досягнення граничного розміру журналу всі події зберігаються у файлі на жорсткому диску;

- забезпечує докладну реєстрацію подій друку та експорту; поряд із стандартною інформацією у журналі фіксуються гриф та обліковий номер документа, а також серійний номер носія, на якому зберігається документ, та носія, на який здійснюється експорт; адміністратор має можливість формування протоколу друку документів.

**1.3. «Гриф» (версія 3)**

Комплекс призначений для забезпечення захисту ІзОД від НСД при її обробці в АС класів 1 і 2 під керуванням **ОС** Windows XP / Vista / 7 / Server 2008 / Server 2008 R2.

Рівень гарантій - Г-4.

Розробник: ТОВ «Інститут комп'ютерних технологій», м. Київ

Експертний висновок № 450 дійсний до 12.07.2016.

Комплекс повністю замінює штатні засоби адміністрування ОС власними засобами, що підтримують реалізацію адміністративного розмежування доступу до захищених ресурсів.

Комплекс забезпечує захист інформації, представленої у вигляді файлів даних довільного типу (електронних документів, електронних таблиць, конструкторських креслень, цих геоінформаційних систем тощо).

ФПЗ комплексу :

КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-3, НО-2

Комплекс реалізує такі основні функції захисту :

* ідентифікацію і аутентифікацію користувачів на підставі логіна, пароля і носія даних автентифікації (зйомного файлового носія або облаштування Touch Memory);
* розмежування обов'язків користувачів і виділення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрації ресурсів, реєстрації користувачів, надання прав доступу, обробки протоколів аудиту тощо);
* розмежування доступу користувачів до вибраних папок, розміщених на жорсткому магнітному диску ПЕОМ, і файлів, які містяться в них, що дозволяє організувати спільну роботу декількох користувачів, що мають різні службові обов'язки і права по доступу до ІзОД;
* керування потоками інформації і блокування потоків інформації, що призводять до зниження рівня її конфіденційності;
* контроль за виведенням інформації на друк з можливістю маркування друкарських аркушів документів згідно вимог чинних нормативних документів в області охорони державної таємниці;
* контроль за експортом інформації на зйомні носії з забезпеченням можливості їх реєстрації та обмеження (для певних користувачів) їх переліку тільки зареєстрованими;
* контроль за імпортом інформації зі зйомних носіїв;
* гарантоване видалення ІзОД шляхом затирання вмісту файлів при їх видаленні;
* розмежування доступу застосовних програм до вибраних папок і файлів, що містяться в них, що дозволяє забезпечити захист ІзОД від випадкового видалення або модифікації і дотриматися технології її обробки;
* контроль цілісності прикладного ПЗ і ПЗ комплексу, а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів і дотримання технології обробки ІзОД;
* контроль за використанням дискового простору користувачами (квоти), що унеможливлює блокування одним з користувачів можливості роботи інших;
* можливість блокування облаштувань інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;
* контроль цілісності і самотестування комплексу при старті;
* відновлення функціонування комплексу після збоїв, що гарантує доступність інформації при дотриманні правил доступу до неї;
* реєстрацію, аналіз і обробку інформації про критичні для безпеки події (входу користувача в ОС, спроб несанкціонованого доступу, фактів запуску програм, роботи з ІзОД, імпорту/експорту інформації, виводу на друк і т.п.), що дозволяє адміністраторам контролювати доступ до ІзОД, стежити за тим, як використовується комплекс, а також правильно його конфігурувати;
* ведення архіву зареєстрованих даних аудиту;
* взаємодія з прикладними програмними системами (ППС) через визначений інтерфейс, що дозволяє забезпечити безперервність захисту ІзОД при її обробці як штатними засобами ОС, так і засобами різних ППС.

**Операційні системи, в середовищі яких працюють КЗЗ**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Windows | NT | 2000 | XP | Vista | 7 | Server 2008 | Touch Memory | Захист папок |
| Рубіж-РСО |  | + | + |  |  |  |  |  |
| Лоза-1 |  |  | + | + | + |  |  | + |
| Гриф |  |  | + | + | + | + | + | + |

**Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Комплекс засобів захисту** | **ФПЗ****АС-1** | **Windows 7 ЕЕ SP1** | **Лоза-1****вер.4** | **Гриф вер.3** |
| 1 | рівень гарантій | **Г2** | Г2 | Г4 | Г4 |
| 2 | повна / базова адмін. конфіденційність | **КА-1** | - | КА-3 | КА-2 |
| 4 | повторне використання об’єктів | **КО-1** | КО-1 | КО-1 | КО-1 |
| 5 | мінімальна адміністративна цілісність | **ЦА-1** | - | ЦА-1 | ЦА-2 |
| 6 | обмежений відкат | **ЦО-1** | ЦО-1 | - | ЦО-1 |
| 7 | використання ресурсів - квоти | **ДР-1** | ДР-1 | - | ДР-1 |
| 8 | стійкість при обмежених відмовах | **-** | - | ДС-1 | ДС-1 |
| 9 | модернізація | **-** | ДЗ-2 | ДЗ-1 | ДЗ-1 |
| 10 | ручне відновлення | **ДВ-1** | ДВ-2 | ДВ-1 | ДВ-1 |
| 11 | захищений журнал / детальна реєстрація | **НР-2** | НР-2 | НР-2 | НР-2 |
| 12 | один. / множ. ідентифікація і автентифікація | **НИ-2** | НИ-2 | НИ-2/3 | НИ-3 |
| 13 | однонаправлений достовірний канал | **НК-1** | НК-1 | НК-1 | НК-1 |
| 14 | розподіл обов'язків на підставі привілеїв / розподіл обов'язків адміністратора  | **НО-1** | НО-3 | НО-2 | НО-2 |
| 15 | КЗЗ з гарантованою цілісністю / контролем цілісності | **НЦ-1** | НЦ-2 | НЦ-2 | НЦ-2 |
| 16 | самотестування при старті / у реальному часі | **НТ-1** | НТ-2 | НТ-2 | НТ-2 |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту ОС і вище зазначених КЗЗ, можна зробити такі висновки:

- разом з послугами безпеки ОС усі КЗЗ забезпечують визначений ФПЗ АС-1;

- «Гриф» є найсильнішим КЗЗ, оскільки у порівнянні з «Лозою» забезпечує вищий рівень послуги адміністративної цілісності ЦА-2 і додаткові послуги обмеженого відкату ЦО-1 і використання ресурсів ДР-1, а також автентифікацію користувачів з використанням технології «Touch Memory»;

- «Лоза» у порівнянні з «Гриф» забезпечує вищий рівень адміністративної конфіденційністі КА-3.

**2. Системи захисту в АС класу 2**

**2.1. «VTI-Рубіж» (версія 2)**

Комплекс призначений для реалізації механізмів захисту інформації від НСД, автоматизації процесів керування ними та створення захищеної технології оброблення, зберігання та представлення ІзОД в АС класів 1 і 2.

**ФПЗ комплексу:**

КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-3

**Рівень гарантій – Г-3.**

Експертний висновок № 482 дійсний до 13.12.2016.

Комплекс може розглядатися як централізована багаторівнева ієрархічна система захисту інформації від НСД, яка складається з КЗЗ рівнів та засобів забезпечення їх взаємодії.

До складу КЗЗ кожного рівня входять монітор безпеки (МБ) у складі автоматизованого робочого місця (АРМ) адміністратора безпеки та серверу МБ. Крім МБ в комплекс входять агенти МБ, які інсталюються на кожному з хостів і здійснюють взаємодію з програмно-технічними та проблемно-орієнтованими засобами захисту (ПОЗЗ).

МБ є програмно-технічним ядром системи захисту, яке забезпечує централізоване управління КЗЗ та взаємодію його елементів.

МБ інтегрує в єдину систему керування захистом такі засоби:

- захисту домену;

- захисту функціональних робочих місць у складі засобів автентифікації, захисту ОС та управління фізичним доступом до робочих станцій - «Рубіж-РС»;

- підсистеми управління фізичним доступом до території та приміщень вузла АС - «Рубіж-Ф»;

- захисту баз даних (БД) рівня АС;

- захисту комунікаційної мережі зв'язку;

- криптографічного захисту інформації;

- антивірусного захисту;

- резервного копіювання та відновлення інформації КЗЗ, операційного середовища та БД.

Сервер МБ забезпечує:

- реалізацію бізнес-логіки функціонування системи захисту інформації АС від НСД,

- зберігання параметрів моделі системи захисту, конфігурації системи, ведення та обробку журналів подій,

- зберігання параметрів аудиту системи та реагування на критичні події, автентифікацію адміністраторів (агентів),

- мережеву взаємодію з АРМ адміністратора безпеки та агентами МБ,

- формування команд для взаємодії з ПОЗЗ,

- відслідковування подій та видачу інформації на АРМ адміністратора безпеки для керування КЗЗ.

Взаємодія МБ з ПОЗЗ з проблемно-орієнтованими засобами захисту (функціональних АРМ, контролера домену, операційних систем та СКБД) забезпечується його структурним елементом - сервером МБ за схемою: АРМ адміністратора ↔ сервер МБ ↔ агент монітора безпеки ↔ ПОЗЗ.

Взаємодія з програмно-технічними та проблемно-орієнтованими засобами захисту інформаційних ресурсів кожного з хостів здійснюється через окремі функціональні компоненти - агенти МБ, які інсталюються на окремих серверах та робочих станціях АС. Кожний агент для взаємодії з проблемно-орієнтованими засобами захисту має набір драйверів відповідно до складу ПОЗЗ.

Агенти МБ призначені для:

- керування механізмами захисту ПОЗЗ;

- видачі інформації на АРМ про параметри системи захисту за запитами адміністратора безпеки;

- реєстрації подій ПОЗЗ;

- видачі повідомлень на АРМ адміністратора безпеки про події, що зв’язані з безпекою системи.

Агент МБ приймає команди на адміністрування ПОЗЗ від АРМ адміністратора, виконує команди і відправляє монітору безпеки інформацію про результати їх виконання. Крім того, агент МБ відслідковує події на ПОЗЗ, видає інформацію про події монітору безпеки і забезпечує реагування на критичні події.

У випадку відсутності зв’язку з МБ (або його непрацездатністю) агент МБ автономно виконує функції захисту інформаційних ресурсів хосту, відслідковує події, забезпечує реагування на критичні події. При відновленні зв’язку з МБ всю необхідну інформацію агент пересилає на МБ для подальшої обробки і прийняття відповідних рішень.

Програмні засоби АРМ адміністратора безпеки забезпечують зручний та інтуїтивно зрозумілий інтерфейс для адміністратора безпеки і представляють собою програмні модулі, що функціонують у середовищі Windows NT / 2000.

Інтерфейс забезпечує введення та відображення інформації, необхідної для налагодження та керування механізмами захисту АРМ адміністратора безпеки, а також відслідкування подій, що впливають на стан захищеності АС.

Засоби комплексу забезпечують автоматизовану побудову моделі захищеної системи, яка включає:

* структуру системи, що захищається;
* структуру власне СЗІ;
* структуру суб'єктів інформаційної діяльності;
* структуру об'єктів захисту;
* правила розмежування доступу;
* правила забезпечення спостереженості за станом систем;
* правила реагування на критичні події.

Об’єктами захисту комплексу є:

* системні ресурси АС – ресурси операційних систем, системних та мережних служб, власне СЗІ;
* інформаційні ресурси АС (об'єкти СКБД, файли);
* інформаційні ресурси власне КЗЗ АС (об'єкти БД КЗЗ: параметри моделі і конфігурація системи захисту, параметри автентифікації користувачів, журнали подій, журнали дії адміністраторів, архіви журналів, звіти про стан захищеності системи, параметри аудиту подій, параметри реагування на події тощо);
* прикладні ресурси (програмне забезпечення АС).

Правила розмежування доступу визначаються встановленою власником АС політикою безпеки і полягають у наданні повноважень суб'єктам АС на доступ до ресурсів, які захищаються, а також у встановленні типів доступу суб'єктам до об'єктів захищеної системи. На основі такої інформації за внутрішніми алгоритмами перевірки повноважень диспетчери доступу ПОЗЗ реалізують санкціонування доступу суб'єкта до об'єкта. Таким чином забезпечується довірчий та адміністративний принципи керування доступом.

**2.2. «Лоза-2» (версія 4)**

**Система** - це програмний засіб захисту інформації від несанкціонованого доступу в АС класу 2 (ЛОМ). Система може працювати під керуванням операційних систем Windows XP / Vista / 7 / Server 2003 / Server 2008 / Server 2008 R2.

Система може працювати як в одноранговій мережі, так і в мережі, побудованій на основі домену. Один із комп’ютерів мережі повинен виконувати роль сервера системи. В одноранговій мережі серверна частина системи може бути встановлена на будь-якому з комп’ютерів мережі.

В мережі, побудованій на основі домену, серверна частина системи встановлюється на первинному контролері домену. На всіх інших комп’ютерах встановлюється клієнтська частина системи.

**ФПЗ д**ля конфігурації «Стандартна безпека»:

КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-2, НК-1, НО-2, НЦ-2, НТ-2

**ФПЗ д**ля конфігурації «Підвищена безпека»:

КА-3, КО-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-2

**Рівень гарантій:**Г-4.

Експертний висновок № 383 дійсний до 16.10.2015

**Система забезпечує ті ж функції, що й «Лоза-1»:**

**- захист інформації від НСД;**

**- контроль друку та експорту;**

**- контроль входу користувачів до системи;**

**- реєстрацію подій.**

**2.3. «Гриф-Мережа»** **(версія 3)**

Комплекспризначений для забезпечення захисту інформації з обмеженим доступом, що обробляється в ЛОМ і РОМ. До складу мережі можуть входити файлові сервери, що функціонують під управлінням ОС Windows Server 2003 / Server 2008 / Server 2008 R2, і робочі станції, що функціонують під управлінням ОС Windows XP / Vista / 7, об'єднані в єдиний домен Active Directory.

Рівень гарантій Г-4.

Експертний висновок № 402 дійсний до 19.12.2015

Комплекс дозволяє створити на базі ЛОМ спеціалізовану АС класу 2 для обробки ІзОД і забезпечити її захист від загроз порушення цілісності, конфіденційності і доступності при реалізації політики адміністративного керування доступом до інформації.

Комплекс поставляється у двох конфігураціях: базовій і підвищеної спостереженості. Відмінність між вказаними конфігураціями комплексу полягає в тому, що у конфігурації підвищеної спостереженості реалізована можливість збору і аналізу в реальному часі інформації про критичні з точки зору захищеності інформації події, зареєстровані на серверах, робочих станціях і активних мережевих пристроях, що функціонують у складі захищеної ЛОМ.

ФПЗ у базовій конфігурації:

КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-3, НО-2

У базовій конфігурації в реальному часі виконується тільки збереження інформації про критичні з точки зору захищеності інформації події, зареєстровані на серверах і робочих станціях, що функціонують у складі захищеної ЛОМ, її аналіз виконується у відкладеному режимі.

Комплекс у базовій конфігурації доцільно застосовувати для захисту інформації в ЛОМ, кількість робочих станцій в яких відносно невелика (до 30) і при цьому усі робочі станції розташовуються в одному або декількох суміжних приміщеннях.

ФПЗ у конфігурації підвищеної спостереженості:

КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-5, НК-1, НЦ-2, НТ-2, НИ-3, НО-2

Комплекс доцільно застосовувати для захисту інформації в ЛОМ, кількість робочих станцій в яких досить велика (більше 30) або в яких робочі станції розташовуються у великій кількості територіально рознесених приміщень (наприклад, по декілька робочих станцій на різних поверхах багатоповерхової будівлі).

Комплекс реалізує такі функції:

* ідентифікацію і автентифікацію користувачів на підставі логіна, пароля і персонального носія даних автентифікації (Touch Memory, Flash Drive тощо) при завантаженні ОС робочої станції до завантаження будь-якого ПЗ з дисків, що дозволяє заблокувати використання робочої станції сторонньою особою, а також упізнати авторизованого користувача та надалі реагувати на його запити згідно його повноважень;
* розмежування обов'язків користувачів і виділення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрації ресурсів, реєстрації користувачів, пнадання прав доступу, обробки протоколів аудиту тощо);
* блокування облаштувань інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;
* контроль цілісності та самотестування КЗЗ при старті і за запитом адміністратора, що дозволяє забезпечити стійке функціонування КЗЗ і не допустити обробку ІзОД у разі порушення його працездатності;
* розмежування доступу користувачів до вибраних папок, розміщених на робочих станціях і файлових серверах ЛОМ, і файлів, які знаходяться в них, що дозволяє організувати одночасну спільну роботу декількох користувачів ЛОМ, що мають різні службові обов'язки і права по доступу до ІзОД;
* керування потоками інформації і блокування потоків інформації, що призводять до зниження її рівня конфіденційності;
* контроль за виведенням інформації на друк з можливістю маркування друкарських аркушів документів, що виводяться, згідно вимог чинних нормативних документів в області охорони державної таємниці;
* контроль за експортом інформації на зйомні носії з можливістю обмеження переліку використовуваних змінних носіїв;
* контроль за імпортом інформації зі зйомних носіїв;
* гарантоване видалення інформації шляхом затирання вмісту файлів при їх видаленні;
* розмежування доступу застосовних програм до вибраних папок і файлів, що знаходяться в них, що дозволяє забезпечити захист ІзОД від випадкового видалення, модифікації і дотриматися технології її обробки;
* контроль цілісності прикладного і системного ПЗ і ПЗ КЗЗ, а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів і дотримання технології обробки ІзОД;
* контроль за використанням користувачами дискового простору файлових серверів (квоти), що унеможливлює блокування одним з користувачів можливості роботи інших;
* відновлення функціонування КЗЗ після збоїв, що гарантує доступність інформації із забезпеченням дотримання правил доступу до неї;
* безперервну реєстрацію, аналіз і обробку подій (входу користувачів в ОС, спроб НСД, фактів запуску програм, роботи з ІзОД, виводу на друк і т.п.) в спеціальних протоколах аудиту, що дозволяє адміністраторам контролювати доступ до ІзОД, стежити за тим, як використовується КЗЗ, а також правильно його конфігурувати;
* ведення архіву зареєстрованих даних аудиту;
* негайне сповіщення адміністратора безпеки про всі виявлені порушення ПРД (у конфігурації підвищеної спостереженості).

**Операційні системи, в середовищі яких працюють КЗЗ**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Windows | NT | 2000 | XP | Vista | 7 | Server 2003 | Server 2008 | Touch Memory | Захист папок |
| VTI-Рубіж | + | + |  |  |  |  |  |  |  |
| Лоза-2 |  |  | + | + | + | + | + |  |  |
| Гриф-Мережа |  |  | + | + | + | + | + | + | + |

**Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Комплекс засобів захисту** | **ФПЗ****АС-2** | **Windows****Server** | **Лоза-2****вер.3** | **Гриф вер.3** | **Гриф-Мережа** |
| 1 | рівень гарантій | **Г2** | Г2 | Г4 | Г4 | Г4 |
| 2 | базова адмін. конфіденційність | **КА-2** | - | КА-2 | КА-2 | КА-2 |
| 3 | базова довірча конфіденційність | **КД-2** | КД-2 | КД-2 | - | - |
| 4 | повторне використання об’єктів | **КО-1** | КО-1 | КО-1 | КО-1 | КО-1 |
| 5 | базова адміністративна цілісність | **ЦА-2** | - | ЦА-1 | ЦА-2 | ЦА-2 |
| 6 | мінімальна довірча цілісність | **ЦД-1** | ЦД-1 | ЦД-1 | - | - |
| 7 | обмежений відкат | **ЦО-1** | ЦО-1 | - | ЦО-1 | ЦО-1 |
| 8 | використання ресурсів - квоти | **ДР-1** | ДР-1 | - | ДР-1 | ДР-1 |
| 9 | стійкість при обмежених відмовах | **ДС-1** | ДС-1 | ДС-1 | ДС-1 | ДС-1 |
| 10 | модернізація | **ДЗ-1** | ДЗ-2 | ДЗ-1 | ДЗ-1 | ДЗ-1 |
| 11 | ручне відновлення | **ДВ-1** | ДВ-2 | ДВ-1 | ДВ-1 | ДВ-1 |
| 12 | захищений журнал / детальна реєстрація / аналіз у реальному часі | **НР-2** | НР-2 | НР-4 | НР-2 | НР-2/5 |
| 13 | одиночна / множинна ідентифікація і автентифікація | **НИ-2** | НИ-2 | НИ-2/3 | НИ-3 | НИ-3 |
| 14 | однонаправлений достовірний канал | **НК-1** | НК-1 | НК-1 | НК-1 | НК-1 |
| 15 | розподіл обов'язків на підставі привілеїв / розподіл обов'язків адміністратора  | **НО-2** | НО-3 | НО-2 | НО-2 | НО-2 |
| 16 | КЗЗ з гарантованою цілісністю / контролем цілісності | **НЦ-2** | НЦ-2 | НЦ-2 | НЦ-2 | НЦ-2 |
| 17 | самотестування при старті / у реальному часі | **НТ-2** | НТ-2 | НТ-2 | НТ-2 | НТ-2 |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту ОС і вище зазначених КЗЗ, можна зробити такі висновки:

- разом з послугами безпеки ОС КЗЗ «Гриф» забезпечують визначений ФПЗ АС-2 у повному обсязі, а «Лоза» не забезпечує рівень послуги ЦА-2;

- «Гриф-Мережа» у конфігурації підвищеної спостереженості є найсильнішим КЗЗ, оскільки у порівнянні з «Лоза» забезпечує вищий рівень послуги адміністративної цілісності ЦА-2 і реєстрації НР-5 (аналіз у реальному часі), а також додаткові послуги обмеженого відкату ЦО-1 і використання ресурсів ДР-1 та автентифікацію користувачів з використанням технології «Touch Memory»;

- «Лоза» у порівнянні з «Гриф» і «Гриф-Мережа» у базовій конфігурації забезпечує додаткові послуги довірчої конфіденційності КД-2 і цілісності ЦД-1 та вищий рівень послуги реєстрації НР-4 (захищений журнал).

**3. Системи захисту Web-ресурсів від НСД**

**3.1. «Megapolis. Portal Manager»**

Системазабезпечує керування адміністративною частиною, зовнішнім виглядом та наповненням будь-якого Web-ресурсу. Однією з його головних переваг є простота і гнучкість використання.

ФПЗ системи:

КА-2, ЦА-1, ЦО-1, ДВ-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НВ-1

Рівень гарантій: Г-2.

Розробник: ТОВ «Софтлайн ІТ», м. Київ

Експертний висновок № 327 дійсний до 02.12.2014.

Системана Web-порталі забезпечує розподіл прав доступу користувачів до визначених ресурсів, надає ці права, в залежності від «ролей» користувачів (відвідувач порталу, адміністратор або контент-менеджер), стежить за дотриманням цих прав доступу згідно встановлених правил.

Системареалізує технологію «MDI Framework», який потрібен для того, щоб у зручному форматі відображати інформацію, яку сервіси отримують із будь-яких джерел за допомогою технологічних інтерфейсів.

Основні характеристики системи:

* реалізація в архітектурі клієнт-сервер, що забезпечує роботу в «багато-користувацькому» режимі;
* простота та зручність налаштувань за рахунок використання стандартного інтерфейсу користувача файлових менеджерів (папки, дерева тощо);
* можливість роботи з сучасними промисловими СКБД;
* забезпечення роботи віддаленого адміністрування порталів;
* розподіл прав доступу користувачів до елементів порталу;
* модульність побудови системи, що дозволяє більш гнучко настроювати керування кожним конкретним порталом.

Система має такі властивості:

* керування сервісами порталу за допомогою модулів, які входять до складу кожного сервісу;
* інформація про складові кожного сервісу (елементи), що зберігається у відповідних записах;
* однотипні записи складають окремий реєстр;
* всі реєстри складають базу даних усіх записів (елементів);
* керування контентом порталу здійснюється за допомогою модулів, в яких створюються записи в реєстрах;
* реєстри можуть бути в довільний спосіб пов’язані між собою;
* над записами будь-якого реєстру можна виконувати наступні операції:
* створення нових записів;
* редагування існуючих записів;
* видалення записів;
* пошук з можливістю урахування морфології;
* фільтрація записів реєстрів за різноманітними критеріями;
* групування записів;
* інтеграція з програмними пакетами Microsoft Office для підготовки матеріалів публікацій;
* автоматична публікація вже готових матеріалів;
* можливість одночасної роботи з декількома реєстрами або модулями кожного сервісу.

**3.2. «Тайфун-Web»**

Комплекспризначений для криптографічного захисту та розмежування доступу до інформації, оброблюваної в ІТС, побудованих на базі Web-технологій.

ФПЗ комплексу:

КА-2, КВ-2, ЦА-1, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-1, НИ-1, НО-1, НЦ-1, НТ-2, НВ-2

Рівень гарантій: Г-4.

Розробник: ТОВ «Інститут комп’ютерних технологій», м. Київ

Експертний висновок № 336 дійсний до 29.12.2014.

При використанні комплексу забезпечується:

- взаємна автентифікація (підтвердження справжності) клієнта та сервера за протоколом, побудованим з використанням асиметричних криптоалгоритмів;

- захист конфіденційності та цілісності інформації, що передається між клієнтом та сервером, з використанням симетричних криптоалгоритмів і вироблення/перевіряння кодів автентифікації повідомлень;

- розмежування доступу користувачів до інформаційних ресурсів, представлених у вигляді статичних або динамічних Web-сторінок, що зберігаються та оброблюються на захищених Web-серверах.

Реалізована технологія інтеграції серверної та клієнтської компонентів комплексу до стеку мережевих протоколів ОС, які реалізують функції «Winsock», забезпечує незалежність від використовуваних Web-браузерів та Web-серверів. Для забезпечення сумісності із засобами «MS Internet Information Server» (IIS), в якому функції «Winsock» не використовуються, реалізована можливість підключення серверної компоненти комплексу безпосередньо до «MS IIS» через інтерфейс «ISAPI».

Програмні засоби комплексу функціонують на IBM-сумісних комп'ютерах (робочих станціях користувачів, Web-серверах, Proxy-серверах) в ОС Windows 2000 / XP / 2003 / Vista / 7 / Server 2008. При використанні засобів комплексу на Proxy-серверах, жодних обмежень щодо ОС Web-серверів, на яких зберігаються та оброблюються захищені Web-ресурси, не висувається.

Для керування ключовою інформацією (для вироблення відкритого та особистого ключів користувачів) у комплексі «Тайфун-Web» (у модулі адміністрування) використовуються програмні засоби генерації ключів та обслуговування сертифікатів користувачів комплексу «Тайфун-PKI».

Комплекс реалізує такі основні функції:

- ідентифікацію та автентифікацію користувачів комплексу на основі атрибутів, отриманих від ОС, що дозволяє однозначно встановити певного користувача та у подальшому коректно оброблювати його запити на доступ до захищеної інформації або до засобів адміністрування;

- виділення, на підставі результатів виконаної автентифікації, користувачів-адміністраторів, яким надані повноваження із керування засобами комплексу;

- сувору взаємну автентифікацію клієнтської та серверної компонентів комплексу та їхніх користувачів з використанням відповідних протоколів, у яких використовується механізм вироблення / перевірки ЕЦП за алгоритмом, установленим ДСТУ 4145, з використанням відповідних атрибутів;

- керування доступом користувачів до захищених Web-ресурсів (окремих Web-сторінок та їх сукупностей), представлених відповідними URL-адресами, на основі атрибутів доступу, призначених спеціально вповноваженими адміністраторами;

- зашифрування/розшифрування інформації, що передається між Web-браузером, який функціонує на робочій станції (РС) користувача, та захищеним Web-сервером (Proxy-сервером), що забезпечує захист конфіденційності інформації на всьому шляху її передачі по каналах мережі Internet;

- контроль цілісності інформації, що передається між Web-браузером, яке функціонує на РС користувача, та захищеним Web-сервером (Proxy-сервером), що забезпечує захист від її несанкціонованої модифікації на всьому шляху її передачі по мережі Internet;

- контроль цілісності та самотестування програмних засобів комплексу при старті та в процесі функціонування, що дозволяє забезпечити стійке функціонування засобів захисту та не допустити обробки повідомлень у випадку порушення працездатності;

- протоколювання критичних з погляду захищеності оброблюваної інформації подій у захищеному журналі ОС із забезпеченням можливості аналізу зареєстрованих даних аудита вповноваженими адміністраторами;

- можливість використання для збереження особистих (секретних) ключів користувачів, як незахищених (диск, flash-drive тощо), так і захищених носіїв (пристрій eToken Pro; SecureToken тощо).

**Операційні системи, в середовищі яких працюють КЗЗ**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Windows | 2000 | XP | 2003 | Vista | 7 | Server 2003 | Server 2008 | Крипто захист |
| Портал Менеджер |  |  |  |  |  |  |  |  |
| Тайфун-Web | + | + | + | + | + |  | + | + |

**Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Комплекс засобів захисту** | **ФПЗ****WEB** | **Windows****Server 2008 R2** | **Портал Менед-жер 1.0** | **Тайфун-Web****версія 1** |
| 1 | рівень гарантій | **Г2** | Г2 | Г2 | Г4 |
| 2 | базова адміністративна конфіденційність | **КА-2** | - | КА-2 | КА-2 |
| 3 | базова довірча конфіденційність | **КД-2** | КД-2 | - | - |
| 4 | мінімальна / базова конфіденційність при обміні  | **КВ-1** | КВ-1 | - | КВ-2 |
| 5 | мінімальна адміністративна цілісність | **ЦА-1** | - | ЦА-1 | ЦА-1 |
| 6 | обмежений відкат | **ЦО-1** | ЦО-1 | - | ЦО-1 |
| 7 | мінімальна / базова цілісність при обміні | **ЦВ-1** | ЦВ-1 | - | ЦВ-2 |
| 8 | використання ресурсів - квота | **ДР-1** | ДР-1 | - | - |
| 9 | ручне відновлення | **ДВ-1** | ДВ-2 | ДВ-1 | ДВ-1 |
| 10 | захищений журнал / зовнішній аналіз | **НР-2** | НР-2 | НР-2 | НР-1 |
| 11 | один. / множинна ідентифікація і автентифікація | **НИ-2** | НИ-2 | НИ-2 | НИ-1 |
| 12 | однонаправлений достовірний канал | **НК-1** | НК-1 | НК-1 | - |
| 13 | розподіл обов'язків адміністраторів / виділення адміністратора  | **НО-1** | НО-3 | НО-2 | НО-1 |
| 14 | КЗЗ з контролем цілісності | **НЦ-1** | НЦ-2 | НЦ-1 | НЦ-1 |
| 15 | самотестування при старті | **НТ-1** | НТ-2 | НТ-2 | НТ-2 |
| 16 | автентифікація вузла / джерела даних | **НВ-1** | НВ-1 | НВ-1 | НВ-2 |

Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених КЗЗ, можна зробити такі висновки:

- з урахуванням послуг безпеки ОС усі КЗЗ забезпечують визначений ФПЗ WEB;

- «Тайфун-Web» є найсильнішим КЗЗ, оскільки у порівнянні з іншим має найбільшу кількість послуг безпеки, вищий рівень гарантій та забезпечує додатково послуги базової конфіденційності при обміні КВ-2, базової цілісності при обміні ЦВ-2, стійкості при обмежених відмовах ДС-1 і модернізації ДЗ-1;

- «Портал Менеджер» є найслабкішим КЗЗ, оскільки у порівнянні з іншим має найменшу кількість послуг безпеки.

Разом з тим, «Портал Менеджер» у порівнянні з іншим забезпечує додатково послуги обмеженого відкату ЦО-1 і однонаправленого достовірного каналу НК-1, а також вищий рівень послуг ідентифікації і автентифікації НИ-2 (одиночна), реєстрації НР-2 (захищений журнал), розподілу обов’язків НО-2 (адміністраторів).

Крім того, головна відмінність КЗЗ «Тайфун-Web» від КЗЗ «Портал Менеджер» є застосування симетричних криптоалгоритмів для захисту конфіденційності та цілісності інформації, що передається між клієнтом та сервером.

### 17. 3-й етап - технічне завдання на створення КСЗІ в ІТС

### Технічне завдання на створення КСЗІ в ІТС розробляється згідно вимог НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення КСЗІ в АС».

### Погодження Технічного завдання

Після того, як Технічне завдання на створення КСЗІ в ІТС (далі - ТЗ) розроблене, воно має бути погоджено з органами Держспецзв’язку згідно вимог п.13 статті 16 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»:

13) погодження проектів створення ІТС, в яких оброблятиметься інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої
встановлена законом, проведення їх експертної оцінки і визначення можливості введення в експлуатацію.

На даний час є 2 варіанти погодження ТЗ в залежності від класу ІТС (АС).

***Погодження ТЗ для АС класу 1***

Погодження ТЗ для АС класу 1 **(**ПЕОМ) здійснює регіональний орган Держспецзв’язку згідно вимог п.2.2.14 «Положення про регіональний орган Держспецзв’язку», затвердженого наказом Адміністрації Держспецзв’язку від 17.08.2012 № 450 і зареєстрованого в Міністерстві юстиції України 10.09.2012 за № 1556/21868:

«Розглядає і погоджує (у межах своїх повноважень) технічні завдання на створення КСЗІ в ІТС, які призначені для захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, та контролює виконання вимог із технічного та криптографічного захисту інформації».

***Погодження ТЗ для АС класів 2 і 3***

Погодження ТЗ для АС класів 2 і 3 (ЛОМ і РОМ) здійснює Адміністрація Держспецзв’язку згідно вимог пунктів 24 і 31 розділу 4 «Положення про Адміністрацію Держспецзв’язку», затвердженого Указом Президента України від 30.06.2011 № 717:

24) погоджує проекти створення та розвитку інформаційно-телекомунікаційних систем, в яких оброблятиметься інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом;

31) здійснює погодження технічних завдань на проектування, будівництво і реконструкцію особливо важливих об'єктів, у процесі експлуатації або застосування яких збирається, обробляється, зберігається, передається чи приймається інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, незалежно від виду та змісту такої інформації.

Для цього ТЗ друкується у 2-х примірниках, які надсилаються для погодження на адресу регіонального органу або Адміністрації Держспецзв’язку. У разі відповідності ТЗ вимогам НД ТЗІ і погодження 1-й його примірник повертається до власника (розпорядника) ІТС або розробника КСЗІ (за його наявності). У разі невідповідності ТЗ вимогам НД ТЗІ і непогодження обидва його примірники повертаються для доопрацювання.

### Після того, як ТЗ повернулось погодженим органом Держспецзв’язку, воно затверджується розробником КСЗІ (за його наявності) та керівником установи-власника (розпорядника) ІТС.

18. 4-й етап - проектування КСЗІ в ІТС

Проект КСЗІ розробляється на підставі та у відповідності до погодженого та затвердженого «Технічного завдання на створення КСЗІ в ІТС»(далі - ТЗ)згідно вимог розділу 6.4 «Розробка проекту КСЗІ» **НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»**.

Під час розробки проекту обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації.

Проект виконується на таких стадіях створення ІТС: ескізна, технічна та робоча. Для всіх стадій розробки проекту склад документації визначається ТЗ, види та зміст - **ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем»** і **НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД»**.

Документація на програмні засоби складається згідно комплексу стандартів Єдиної системи проектної документації (далі - ЄСПД), а на технічні засоби - згідно з комплексом стандартів Єдиної системи конструкторської документації (далі - ЄСКД).

***Ескізний проект***

На цій стадії здійснюється розробка попередніх проектних рішень КСЗІ та, у разі необхідності, її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проектних рішень рівня ескізного проекту.

На цій стадії визначаються:

- функції КСЗІ в цілому та функції її окремих складових частин;

- склад заходів протидії технічним розвідкам, організаційних, правових та інших заходів захисту;

- склад КЗЗ від НСД;

- склад комплексів ТЗІ від витоку технічними каналами та спеціальних впливів;

- узагальнена структура КСЗІ та схема взаємодії складових частин.

Пропонуються попередні технічні рішення, за допомогою яких передбачається реалізація завдань і функцій КСЗІ. У документації ескізного проекту КСЗІ мають бути наведені відомості щодо попередніх проектних рішень, які визначають порядок реалізації вимог ТЗ щодо КСЗІ в цілому та, за необхідності, щодо її окремих складових частин.

Дозволяється вилучати стадію ескізного проекту, у такому випадку документація ескізного проекту не розробляється.

***Технічний проект***

На цій стадії виконується розробка:

- загальних проектних рішень, необхідних для реалізації вимог ТЗ;

- рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів);

- рішень щодо архітектури КЗЗ від НСД (у тому числі щодо АВПЗ, засобів виявлення та попередження про мережеві вторгнення тощо);

- рішень щодо механізмів реалізації послуг безпеки, визначених ФПЗ;

- рішень щодо алгоритмів, порядку та умов функціонування засобів захисту інформації, які використовуються у складі КЗЗ для реалізації певних функцій захисту.

Здійснюються організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ у відповідності до заданих рівнем гарантій реалізації послуг безпеки згідно вимог НД ТЗІ.

Виконується розробка, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ. Зміст та стиль проектної документації повинні бути достатніми для забезпечення реалізації вимог ТЗ.

Готується та оформляється документація на постачання засобів захисту або продукції, що містить їх у своєму складі, для комплектації КСЗІ. Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються технічні завдання) на розробку відповідних засобів.

Здійснюється розроблення, оформлення і затвердження завдань на проектування з суміжних питань, які пов’язані зі створенням КСЗІ або впливають на умови її функціонування (будівельні, електротехнічні, санітарно-технічні та інші підготовчі роботи).

***Робочий проект***

На цій стадії здійснюється розробка, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та, у разі необхідності, її окремих складових частин.

У документації робочого проекту КСЗІ мають бути наведені детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ та взаємодії її компонентів, а також відомості, необхідні для проведення пусконалагоджувальних робіт і тестування підсистем та засобів КСЗІ.

У разі обробки в ІТС секретної інформації до складу робочої документації на комплекси ТЗІ від витоку технічними каналами повинні входити схеми розміщення засобів ІТС, кабельного обладнання, мереж живлення та систем заземлення, які виконуються у відповідності до вимог НД ТЗІ. При цьому враховуються умови їх розміщення та мінімально допустимі відстані між засобами ІТС та іншими технічними засобами, що знаходяться у приміщеннях, де розташоване обладнання ІТС, та у суміжних приміщеннях (засоби зв’язку, системи та засоби кондиціювання, сигналізації, електроосвітлення тощо). Зазначені умови розміщення та мінімально допустимі відстані беруться з експлуатаційної документації, яка супроводжує сертифіковані засоби ІТС.

До складу робочої документації на КЗЗ повинні входити описи таких процедур:

- інсталяції та ініціалізації комплексу,

- налагодження всіх механізмів розмежування доступу користувачів до ресурсів ІТС,

- формування та актуалізації баз даних захисту,

- контролю за діями користувачів,

- контролю цілісності ПЗ та баз даних захисту.

Експлуатаційна документація включає настанови (інструкції) користувачам та опис порядку функціонування та супроводження КСЗІ впродовж життєвого циклу ІТС.

Зміст та склад документації кожної стадії проектування повинні бути достатніми для повного опису проектних рішень рівня відповідного проекту. Конкретний перелік документації визначається на підставі ГОСТ 34.201-89 і РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов» з урахуванням особливостей КСЗІ.

Документація кожної стадії проектування має бути затверджена розробником КСЗІ (за його наявності) та керівником установи-власника (розпорядника) ІТС.

Дозволяється поєднувати технічну та робочу стадії проектування в одну стадію техно-робочого проекту.

***Техно-робочий проект***

Згідно вимог вище зазначених стандартів техно-робочий проект повинен містити такі документи:

1) відомість проекту;

2) відомість виробів, що закуповуються;

3) пояснювальна записка до проекту;

4) опис завдань і функцій;

5) опис інформаційного забезпечення;

6) опис комплексу технічних засобів;

7) опис програмного забезпечення;

8) опис комплексу засобів захисту від НСД;

9) опис алгоритмів реалізації послуг безпеки;

10) опис організаційної структури;

11) відомість устаткування та матеріалів;

12) кошторисний розрахунок створення КСЗІ;

13) проектна оцінка надійності КСЗІ.

У разі проектування КСЗІ в АС класу 1 всі документи техно-робочого проекту можна об’єднати в один загальний документ під назвою **«Опис КСЗІ»**, який буде складатися з таких розділів:

1) зміст;

2) нормативні посилання;

3) загальні відомості;

4) завдання та функції КСЗІ;

5) опис АС та умов її функціонування;

6) опис інформаційної діяльності;

7) заходи антивірусного захисту;

8) заходи захисту інформації від НСД;

9) організаційні заходи захисту;

10) перелік розробленої документації.

19. 5-й етап - введення КСЗІ в дію та оцінка захищеності інформації

Введення КСЗІ в дію здійснюється на підставі та у відповідності до затвердженого «Техно-робочого проекту КСЗІ в ІТС»згідно вимог розділу 6.5 «Введення КСЗІ в дію та оцінка захищеності інформації в ІТС» **НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»**.

Цей етап складається з трьох періодів:

- підготовчий;

- монтажно-пусковий;

- випробувальний.

1. Підготовчий період складається з таких заходів:

### - підготовка КСЗІ до введення в дію;

- навчання користувачів;

- комплектування КСЗІ.

2. Монтажно-пусковий період складається з таких робіт:

### - будівельно-монтажні;

### - пуско-налагоджувальні.

3. Випробувальний період складається з таких заходів:

### - попередні випробування КСЗІ;

### - дослідна експлуатація КСЗІ;

- державна експертизаКСЗІ.

### 1. Підготовчий період

### 1.1. Підготовка КСЗІ до введення в дію

Проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС. Здійснюється створення СЗІ (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах.

В основному має бути завершена розробка і затверджені документи з питань захисту ІзОД в ІТС (за виключенням тих, для розробки яких необхідні результати наступних етапів робіт), а саме:

- інструкція щодо забезпечення правил обробки ІзОД в ІТС;

- посадові (функціональні) інструкції користувачів;

- технологічні інструкції щодо виконання завдань з адміністрування та обслуговування КСЗІ;

- інструкції про порядок використання засобів криптографічного захисту інформації.

Основною є **Інструкція щодо забезпечення правил обробки ІзОД в ІТС**, яка розробляється у випадку, якщо в ІТС передбачається обробка ІзОД. В ній має бути окреслений перелік заходів, спрямованих на дотримання визначеного вимогами чинної нормативно-правової бази режиму доступу до ІзОД, визначено порядок дій персоналу та користувачів ІТС з метою реалізації зазначених заходів, а також встановлено їх відповідальність у випадку порушення зазначених вимог.

Зокрема, в інструкції рекомендується у вигляді окремих розділів викласти:

* загальні відомості щодо організації захисту ІзОД в ІТС;
* опис порядку доступу до приміщень, в яких розташовані засоби ІТС;
* опис порядку захисту інформації від витоку технічними каналами;
* опис порядку захисту інформації від НСД;
* опис порядку здійснення антивірусного захисту;
* опис порядку впровадження і використання програмного забезпечення;
* опис порядку створення захищених інформаційних ресурсів, реєстрації користувачів та надання прав доступу до інформації користувачам ІТС;
* опис порядку контролю за дотриманням користувачами правил роботи із засобами ІТС;
* опис порядку обліку, зберігання, обігу, резервування, ротації та знищення матеріальних носіїв, що використовуються для зберігання ІзОД;
* опис порядку проведення ремонтних робіт та відновлення працездатності ІТС;
* опис порядку контролю за забезпеченням захисту ІзОД в ІТС;
* обов’язки користувачів та персоналу ІТС стосовно дотримання встановленого порядку оброблення ІзОД;
* відповідальність користувачів та персоналу ІТС за порушення встановленого порядку оброблення ІзОД.

В інструкції повинні бути враховані вимоги «*Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію*» щодо організації та порядку оброблення відповідної інформації в ІТС. Зокрема, мають бути враховані вимоги щодо використання журналів обліку та реєстрації сховищ та матеріальних носіїв ІзОД, а також визначено порядок та особливості використання відповідних журналів.

В інструкції мають бути враховані положення посадових (функціональних) інструкцій співробітників СЗІ, персоналу та користувачів ІТС, а також технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ.

Інструкція має бути погоджена з режимно-секретним органом установи, яка є власником (розпорядником) ІТС, погоджені з виконавцем робіт зі створення КСЗІ та затверджені керівником установи.

**Посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС** мають визначати їх обов’язки, відповідальність та порядок дій у процесі виконання ними завдань щодо керування засобами КСЗІ і ІТС, а також обробки в ІТС інформаційних ресурсів, що потребують захисту.

Перелік та зміст цих інструкцій повинні визначатися з урахуванням:

* структури та штатного розкладу СЗІ, визначених у Положенні про СЗІ;
* завдань, функцій та повноважень співробітників СЗІ, наведених у Положенні про СЗІ;
* категорій персоналу та користувачів ІТС, визначених політикою безпеки інформації щодо розподілу обов’язків користувачів та їх функціональних завдань;
* порядку дій співробітників СЗІ, персоналу та користувачів ІТС, який випливає з положень політики безпеки інформації, документації техноробочого проекту КСЗІ та експлуатаційної документації компонентів (складових частин) КЗЗ щодо забезпечення визначеного порядку функціонування ІТС та КСЗІ.

Як правило, у склад СЗІ входять всі визначені політикою безпеки адміністратори ІТС, тому для кожного з них складається своя настанова або інструкція, а саме:

* інструкція адміністратора безпеки;
* інструкція адміністратора системи;
* інструкція адміністратора мережі.

В посадових інструкціях необхідно у вигляді окремих розділів викласти:

* загальні положення, в яких визначено категорії персоналу, на яких поширюються їх вимоги;
* завдання та функції персоналу;
* обов’язки персоналу та порядок їх виконання;
* повноваження та відповідальність персоналу.

У посадових (функціональних) інструкціях персоналу ІТС повинні бути враховані положення технологічних інструкцій (настанов) з адміністрування та обслуговування КСЗІ.

Посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС мають бути погоджені з виконавцем робіт зі створення КСЗІ та затверджені керівником установи-власника (розпорядника) ІТС.

**Технологічні інструкції щодо виконання завдань з адміністрування та обслуговування КСЗІ** повинні детально визначати послідовність дій співробітників СЗІ та персоналу ІТС у процесі виконання відповідних завдань.

У технологічних інструкціях необхідно у вигляді окремих розділів викласти:

* загальні положення, в яких визначено завдання з адміністрування та обслуговування КСЗІ, порядок виконання яких встановлюється інструкцією, категорії співробітників СЗІ або персоналу ІТС, на яких поширюються вимоги відповідних інструкцій (настанов) та які є відповідальними за виконання відповідних завдань;
* послідовність і порядок здійснення технологічних операцій в ході виконання відповідальними особами певних завдань з адміністрування та обслуговування КСЗІ;
* порядок реєстрації фактів та результатів виконання певних завдань у відповідних реєстраційних журналах.

У технологічних інструкціях повинні бути враховані положення посадових (функціональних) інструкцій персоналу ІТС, а також визначені форми реєстраційних журналів, які планується використовувати (у додатках до інструкцій).

Інструкції мають бути погоджені виконавцем робіт зі створення КСЗІ та затверджені керівником установи-власника (розпорядника) ІТС.

**Інструкції про порядок використання засобів криптографічного захисту інформації** (далі - КЗІ)(за їх наявності у складі КСЗІ)повинні визначати порядок забезпечення безпеки, порядок керування ключовими даними використовуваних засобів КЗІ і порядок їх користування.

Перелік та зміст відповідних інструкцій визначаються вимогами чинної нормативно-правової бази у сфері КЗІ, зокрема «Положенням про порядок розроблення, виробництва та експлуатації засобів КЗІ», затвердженим наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141 і зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129.

Так, згідно вимог Положення розробник засобу КЗІ складає та погоджує з Держспецзв'язку такі інструкції:

- Інструкція із забезпечення безпеки експлуатації засобів КЗІ;

- Інструкція щодо порядку генерації ключових даних та поводження з ключовими документами.

**1.2. Навчання користувачів**

Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ тощо) в частині, що їх стосується, основним положенням документів Плану захисту, які необхідні їм для дотримання вимог політики безпеки інформації, правил експлуатації засобів захисту інформації тощо.

Після завершення навчання здійснюється перевірка знань користувачів ІТС всіх категорій та їх уміння користуватись впровадженими технологіями захисту інформації. За результатами цієї перевірки складається акт довільної форми.

**1.3. Комплектування КСЗІ**

Забезпечується придбання та отримання продукції (засобів захисту інформації, матеріалів, обладнання тощо) від постачальників та співвиконавців робіт згідно відомостей техно-робочого проекту створення КСЗІ.

Приймається рішення щодо підготовки до проведення оцінки на відповідність вимогам НД ТЗІ засобів захисту, які на момент проектування КСЗІ не мали відповідного сертифікату або експертного висновку, а також порядку проведення такої оцінки під час державної експертизи КСЗІ.

### 2. Монтажно-пусковий період

**2.1. Будівельно-монтажні роботи**

Як правило, будівельно-монтажні роботи виконуються для забезпечення інженерно-технічного захисту інформації, що становить державну таємницю та обробляється технічними засобами ІТС, від витоку технічними каналами за рахунок побічних електpомагнітних випpомінювань і наведень (далі - ПЕМВН).

 ПЕМВН - це електpомагнітні випpомінювання, що утвоpюються під час pоботи засобів забезпечення інфоpмаційної діяльності під впливом електpичних і магнітних полів на випадкові антени у пpоцесі акусто-електpичних пеpетвоpень, під час виникнення паpазитної високочастотної генеpації та паpазитної модуляції, шляхом взаємного впливу кіл технічних засобів ІТС і кіл електpоживлення, електpоосвітлення, заземлення, сигналізації тощо.

Роботи цього етапу виконуються під час переобладнання існуючих або при будівництві нових спеціалізованих споруд (приміщень), призначених для розміщення технічних засобів ІТС та персоналу, сховищ машинних носіїв інформації.

Виконання заходів захисту від ПЕМВН здійснюється згідно вимог таких НД ТЗІ:

- ТР ЕОТ - 95 Тимчасові рекомендації з ТЗІ у засобах обчислювальної техніки, АС і мережах від витоку каналами ПЕМВН;

- НД ТЗІ 2.4-007-08 Захист інформації на об’єктах інформаційної діяльності. Технічний захист інформації, яка обробляється засобами обчислювальної техніки, від витоку за рахунок ПЕМВН. Рекомендації з використання мережевих фільтрів;

- НД ТЗІ 2.7-007-08 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки щодо зашумлення ліній електроживлення технічних засобів.

Зокрема, передбачається виконання таких заходів в приміщеннях, де встановлені технічні засоби ІТС**:**

- незадіяні кабелі демонтуються;

- незадіяні проводи в кабелях закорочуються та заземлюються;

- необхідні кабелі прокладаються в екранованих конструкціях;

- монтується система заземлення, технічні засоби ІТС заземлюються;

- встановлюються завадозаглушувальні фільтри на лініях електроживлення технічних засобів ІТС;

- монтується комплекс ТЗІ, до складу якого входять системи просторового та лінійного зашумлення;

- здійснюється часткове або повне екранування серверного приміщення або технічних засобів ІТС.

Монтаж засобів ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.

Будівельно-монтажні роботи здійснюються силами установи-власника ІТС або будівельно-монтажними організаціями згідно з проектною документацією на будівництво, яка розробляється проектною організацією у відповідності до вимог Державних будівельних норм України **ДБН А.2.2-2-96** **«Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва»**.

Після завершення будівельно-монтажних робіт створюється комісія з прийняття робіт, до складу якої входять представники організації-замовника робіт та організацій-виконавців. За результатами роботи комісії складається за довільною формою акт приймання робіт з ТЗІ з оцінкою їх відповідності вимогам НД ТЗІ, який затверджується керівником організації-замовника робіт.

### 2.2. Пуско-налагоджувальні роботи

Метою пуско-налагоджувальних робіт є встановлення та налагодження всіх засобів захисту, перевірка їх працездатності та атестація комплексу ТЗІ.

Ці роботи виконуються у такій послідовності:

- інсталяція, ініціація та налагодження АВПЗ;

- інсталяція, ініціація та налагодження КЗЗ від НСД;

- інсталяція, ініціація та налагодження засобів КЗІ;

- перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії;

- атестація комплексу ТЗІ від витоку технічними каналами (у разі наявності).

Для захисту інформації використовуються засоби ТЗІ, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ, а засоби КЗІ - у сфері КЗІ.

Згідно з документацією техно-робочого проекту на створення КСЗІ в ІТС здійснюється інсталяція, ініціалізація та перевірка працездатності АВПЗ і КЗЗ від НСД, а у разі необхідності – засобів КЗІ. Інсталяція та ініціалізація засобів захисту, які мають експертний висновок щодо його відповідності вимогам НД ТЗІ, здійснюється у порядку, визначеному в експлуатаційній документації на ці засоби.

Під час інсталяції АВПЗ мають бути задіяні всі механізми моніторингу та контролю системи, мережі та встановленого ПЗ, а також цілісності АВПЗ, його антивірусних баз та встановлений режим їх поновлення.

Під час інсталяції КЗЗ мають бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності ПЗ та бази даних захисту КЗЗ.

До бази даних захисту вносяться відомості про користувачів ІТС, встановлюються їх повноваження щодо доступу до захищених об’єктів ІТС, їх створення, модифікації, архівування, знищення, експорту/імпорту тощо.

Під час інсталяції засобів КЗІ мають бути задіяні всі криптоалгоритми автентифікації, авторизації та обліку доступу користувачів до ресурсів ІТС, а також генерації та зберігання ключової інформації, алгоритмів шифрування/розшифрування даних, формування та перевірку ЕЦП.

Засобами КЗІ можуть бути електронні ключі автентифікації - носії ключової інформації, призначені для використання в системах інформаційного доступу, електронного документообігу, авторизації користувачів і захищеного зберігання ключової інформації.

Після отримання засобів КЗІ організація, яка їх експлуатує, кожний екземпляр засобу КЗІ бере на облік у відповідному журналі.

Одиницею обліку кожного екземпляра засобу КЗІ є:

- для апаратних засобів - конструктивно закінчений технічний засіб;

- для програмних засобів - інсталяційний компакт-диск тощо.

Підставою для початку експлуатації засобів КЗІ в організації (у тому числі її філіях або регіональних представництвах), яка здійснює експлуатацію засобів КЗІ, є відповідний наказ керівника цієї організації.

Передача засобів КЗІ здійснюється на підставі відповідних договорів, у яких указуються порядок установлення засобів КЗІ у користувачів та обслуговування цих засобів, забезпечення ключовими документами (ключовими даними), а також ужиття заходів щодо забезпечення режиму безпеки тощо.

Ефективність вжитих заходів із захисту інформації у разі створення комплексу ТЗІ повинна бути підтверджена результатами його інструментальної перевірки під час випробувань.

Спеціальні дослідження та інструментальні вимірювання рівня ПЕМВН виконуються підрозділом ТЗІ організації-власника ІТС або іншими суб’єктами господарювання за умови наявності ліцензії чи дозволу на здійснення відповідного виду робіт.

Інструментальна перевірка здійснюється згідно вимог таких НД ТЗІ:

- НД ТЗІ 2.2-005-08 Технічний захист інформації. Захист інформації, яку обробляють засобами електронної обчислювальної техніки на об’єктах інформаційної діяльності, від витоку інформації за рахунок ПЕМВН. Норми ефективності захисту;

- НД ТЗІ 2.3-014-08 Захист інформації на об’єктах інформаційної діяльності. Методика оцінки ефективності зашумлення ліній електроживлення технічних засобів;

- НД ТЗІ 2.3-015-08 Захист інформації на об’єктах інформаційної діяльності. Технічний захист інформації, яка обробляється засобами обчислювальної техніки, від витоку за рахунок ПЕМВН. Методика оцінки захищеності об’єкта ЕОТ від витоку секретної інформації лініями електроживлення без використання на них засобів захисту;

- НД ТЗІ 2.3-016-08 Захист інформації на об’єктах інформаційної діяльності. Технічний захист інформації, яка обробляється засобами обчислювальної техніки, від витоку інформації за рахунок наведень побічних електромагнітних випромінювань на лінії та комунікації. Методика інструментального контролю ефективності захисту технічних засобів ЕОТ від витоку секретної інформації за рахунок ПЕМВН на лінії сигналізації та зв’язку, які виходять за межі контрольованої зони.

Оцінка повноти та якості виконання робіт з ТЗІ в приміщеннях проводиться шляхом атестації впровадженого комплексу ТЗІ від витоку технічними каналами, за результатами якої складається «Акт атестації комплексу ТЗІ».

Порядок здійснення атестації, зміст та форма Акту визначається НД ТЗІ 2.1-002-2007 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

Після завершення пуско-налагоджувальних робіт складається підсумковий акт, де зазначаються:

- обсяг виконаних робіт;

- оцінка відповідності проведення робіт вимогам експлуатаційних документів на засоби та нормативних документів;

- пропозиції щодо застосування додаткових заходів захисту (у разі необхідності).

До акту додаються:

- акт атестації комплексу ТЗІ (у разі наявності);

- акти інсталяції та налагодження всіх засобів захисту;

- схеми приміщень, де розташовані засоби ІТС, з указанням систем комунікацій та меж контрольованих зон;

- перелік технічних засобів і комунікацій, що знаходяться у цих приміщеннях.

Акт затверджується керівником організації - власника ІТС.

Після затвердження акту здійснюється впровадження додаткових заходів захисту, необхідність впровадження яких зафіксована в акті, та відповідне коригування проектної, робочої та експлуатаційної документації.

###

### 20. Попередні випробування та дослідна експлуатація КСЗІ

**1. Попередні випробування КСЗІ**

Попередні випробування КСЗІ в ІТС здійснюються згідно вимог розділу 6.5 «Введення КСЗІ в дію та оцінка захищеності інформації в ІТС» **НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»**.

Метою попередніх випробувань КСЗІ є перевірка її працездатності та визначення можливості прийняття у дослідну експлуатацію. Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ і НД ТЗІ. Порядок проведення попередніх випробувань може бути визначений наказом керівника установи-власника (розпорядника) ІТС.

Попередні випробування проводяться згідно програми та методики випробувань (далі - Програма). Програму готує розробник КСЗІ, а узгоджує власник ІТС. Вона має бути погоджена керівником установи-власника (розпорядника) ІТС, та затверджена виконавцем робіт зі створення КСЗІ в ІТС. Попередні випробування організовує власник ІТС, а проводить розробник КСЗІ.

Для проведення попередніх випробувань КСЗІ керівником установи-власника (розпорядника) ІТС створюється комісія. Головою комісії попередніх випробувань КСЗІ призначається заступник керівника установи-власника (розпорядника) ІТС.

Програма призначена для встановлення даних, що забезпечують отримання та перевірку проектних рішень, визначення якості робіт, показників якості функціонування КСЗІ, перевірку відповідності системи вимогам політики безпеки, тривалість і режим випробувань. Вона розробляється та оформлюється згідно вимог РД 50-34.698-90 «*Автоматизированные системы. Требования к содержанию документов*».

Програма повинна містити перелік перевірок та опис методик виконання окремих перевірок КСЗІ. Успішне проведення цих перевірок повинно дозволити зробити однозначний висновок щодо відповідності створеної КСЗІ вимогам ТЗ. Якщо в ході створення КСЗІ здійснюються роботи зі створення певних компонентів КЗЗ, до складу Програми може бути введено Програму та методику випробувань ФПБ.

Методики випробувань КСЗІ розробляються на основі ТЗ і затверджених програм випробувань з використанням типових методик (за наявності). При цьому окремі положення типових методик випробувань можуть уточнюватися та конкретизуватися залежно від особливості системи і умов проведення випробувань. При проведенні випробувань у декілька етапів програми випробувань повинні бути оформлені у вигляді єдиного документа. Зміст розділів методик встановлює розробник КСЗІ.

Перелік перевірок, які повинні увійти до програми, включає:

- відповідність КСЗІ технічному завданню;

- комплектність КСЗІ та її документації;

- кількість і кваліфікація персоналу;

- ступінь виконання КСЗІ своїх функцій;

- контролездатність КСЗІ тощо.

Опис методів випробувань КСЗІ за окремими показниками рекомендується розташовувати в тій же послідовності, в якій ці показники розташовані в технічних вимогах.

Програма випробувань КСЗІ повинна містити такі основні розділи:

- об'єкт випробувань;

- мета випробувань;

- обсяг випробувань;

- умови та порядок випробувань;

- методи випробувань.

Залежно від особливостей КСЗІ допускається об'єднувати або виключати окремі розділи за умови викладу їх вмісту в інших розділах програми випробувань, а також включати в неї додаткові розділи (за необхідністю).

1. У розділі «Об'єкт випробувань» Програми вказується клас ІТС згідно класифікації НД ТЗІ 2.5-005-99, повне найменування та умовне позначення ІТС, в якій створена КСЗІ.

2. У розділі «Мета випробувань» Програми вказуються конкретні цілі та завдання, які повинні бути досягнуті та вирішені в процесі випробувань.

3. У розділі «Загальні положення» Програми вказуються:

- перелік керівних документів, на підставі яких проводять випробування;

- місце і тривалість випробувань;

- організації, що беруть участь у випробуваннях.

Якщо раніше вже проводились випробування, то також вказуються:

- перелік проведених випробувань;

- перелік документів, що пред'являються на випробування, відкоригованих за результатами проведених випробувань.

4. У розділі «Обсяг випробувань» Програми вказуються:

- перелік етапів випробувань і перевірок;

- послідовність проведення та режим випробувань;

- випробування ПЗ;

- перелік робіт, що проводяться після завершення випробувань.

5. У розділі «Умови та порядок проведення випробувань» Програми вказуються:

- умови проведення випробувань (умови початку та завершення окремих етапів, наявні обмеження тощо);

- вимоги до технічного обслуговування КСЗІ;

- вимоги до персоналу, що проводить випробування (порядок його допуску до випробувань);

- заходи забезпечення безпеки проведення випробувань.

Якшо до проведення випробувань залучаються сторонні організації та експерти, то також вказується:

- порядок взаємодії організацій, що беруть участь у випробуваннях;

- порядок залучення експертів для дослідження можливих пошкоджень під час випробувань.

6. У розділі «Методи випробувань» Програми вказуються описи використовуваних методів випробувань із зазначенням результатів проведення випробувань (переліків тестових прикладів, контрольних роздруківок тестових прикладів тощо).

7. У розділі «Матеріально-технічне забезпечення випробувань» Програми вказуються конкретні види матеріально-технічного забезпечення проведення випробувань з розподілом завдань і обов'язків організацій, які беруть участь у випробуваннях.

8. У розділі «Звітність» Програми вказується перелік звітних документів, які повинні оформлятися в процесі випробувань та після їх завершення, з визначенням порядку їх погодження і затвердження та термінів оформлення цих документів. До звітних документів відносяться акт, протокол або звіт про результати випробувань, акт технічного стану системи після випробувань тощо.

Після завершення попередніх випробувань складається «**Протокол попередніх випробувань КСЗІ в ІТС**», який повинен містити такі розділи:

1) об'єкт випробувань;

2) мета випробувань;

3) обсяг випробувань;

4) результати випробувань;

5) оцінка повноти та завершення випробувань;

6) висновок.

Обсяг викладання розділів Протоколу повинен відповідати обсягу розділів Програми.

Якщо під час випробувань були виявлені недоліки, вони та їхні причини обов’язково фіксуються у відповідних розділах Протоколу. У такому разі висновок Протоколу повинен містити рекомендації та термін усунення всіх виявлених недоліків. Після усунення недоліків проводяться чергові випробування, за результатами яких знову складається Протокол.

Після складання Протоколу з позитивним висновком оформлюється «Акт завершення попередніх випробувань КСЗІ в ІТС». Акт має бути підписаний членами комісії установи-власника (розпорядника) ІТС, представником виконавця робіт зі створення КСЗІ (за наявності) та затверджений керівником установи-власника (розпорядника) ІТС.

Про завершення проведення попередніх випробувань КСЗІ в ІТС необхідно зробити відповідний запис у формулярі ІТС.

**2. Дослідна експлуатація КСЗІ**

Дослідна експлуатація КСЗІ в ІТС здійснюється згідно вимог розділу 6.5 «Введення КСЗІ в дію та оцінка захищеності інформації в ІТС» **НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»**.

КСЗІ в ІТС приймається у дослідну експлуатацію після затвердження «Акту завершення попередніх випробувань» на підставі його позивного висновку. Порядок проведення дослідної експлуатації визначається наказом керівника установи-власника (розпорядника) ІТС, де вказується термін її проведення.

Для проведення дослідної експлуатації КСЗІ керівником установи-власника (розпорядника) ІТС створюється комісія. Головою комісії з дослідної експлуатації КСЗІ призначається заступник керівника установи-власника (розпорядника) ІТС.

Під час дослідної експлуатації КСЗІ:

- відпрацьовуються технології обробки інформації та обігу її носіїв, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та контролю за їх діями;

- співробітники СЗІ та користувачі ІТС засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів, набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації;

- у разі необхідності здійснюється доопрацювання ПЗ, додаткове налагоджування КЗЗ та коригування документації.

До складу експлуатаційної документації повинні входити документи, що визначають порядок інсталяції, ініціалізації, налаштування та експлуатації всіх компонентів КЗЗ, визначених у документації техно-робочого проекту КСЗІ.

Згідно вимог **НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД»** для КЗЗ (окремих компонентів) у вигляді окремих документів або розділів інших документів повинні бути розроблені:

- опис процедур інсталяції та ініціації КЗЗ;

- опис послуг безпеки, що реалізуються КЗЗ;

- настанови адміністратору з послуг безпеки;

- настанови користувачу з послуг безпеки.

Етап дослідної експлуатації завершується складанням «Акту завершення дослідної експлуатації КСЗІ в ІТС».

**«Акт завершення дослідної експлуатації КСЗІ в ІТС»** повинен містити перелік відпрацьованих заходів дослідної експлуатації та їх результати, а також висновки щодо можливості (або неможливості) представлення КСЗІ на державну експертизу.

Акт має бути підписаний членами комісії установи-власника (розпорядника) ІТС, представником виконавця робіт зі створення КСЗІ (за наявності) та затверджений керівником установи-власника (розпорядника) ІТС.Про завершення дослідної експлуатації КСЗІ необхідно зробити відповідний запис у формулярі ІТС.

Акт складається з таких розділів:

- заходи, відпрацьовані адміністраторами;

- заходи, відпрацьовані користувачами;

- заходи з ведення документації;

- заходи з налагоджування ПЗ (за необхідності);

- результати дослідної експлуатації;

- висновок.

Після затвердження «Акту завершення дослідної експлуатації**»** складається **«Акт завершення робіт зі створення КСЗІ в ІТС»**, який повинен містити:

- загальні відомості;

- перелік розроблених документів (вказуються реєстраційні номери, інші атрибути документів);

- перелік проведених робіт;

- висновок.

Акт має бути підписаний членами комісії установи-власника (розпорядника) ІТС, представником виконавця робіт зі створення КСЗІ (за наявності) та затверджений керівником установи-власника (розпорядника) ІТС.Про завершення робіт зі створення КСЗІ необхідно зробити відповідний запис у формулярі ІТС.

### 21. Державна експертиза КСЗІ в ІТС

16 травня 2007 року наказом Адміністрації Держспецзв’язку № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087, було затверджене «**Положення про державну експертизу в сфері ТЗІ**» (із змінами згідно наказу від 10.10.2012 № 567), яке визначає такі вимоги:

1.2. Державна експертиза в сфері ТЗІ (далі - експертиза) проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам НД ТЗІ та можливості їх використання для забезпечення ТЗІ.

1.3. Дія цього Положення поширюється на всіх юридичних та фізичних осіб, які є суб'єктами експертизи.

Суб'єктами експертизи є:

- юридичні та фізичні особи - власники (розпорядники) ІТС, технічних і програмних засобів, які реалізують функції ТЗІ, - замовники експертизи (далі - Замовники);

- Адміністрація Держспецзв'язку (далі - Адміністрація);

- підрозділи Держспецзв'язку, підприємства, установи та організації, які проводять експертизу (далі - Організатори);

- державні органи, які проводять експертизу в сфері свого управління;

- фізичні особи - виконавці експертних робіт з ТЗІ (далі - Експерти).

1.4. Об'єктами експертизи є:

- КСЗІ, які є невід'ємною складовою частиною ІТС;

- технічні та програмні засоби, які реалізують функції ТЗІ (далі - засоби ТЗІ).

1.5. Експертиза КСЗІ є процедурою підтвердження відповідності КСЗІ вимогам НД ТЗІ і проводиться шляхом експертних випробувань або шляхом аналізу декларації про відповідність КСЗІ вимогам НД ТЗІ (далі - декларація).

Експертиза засобів ТЗІ проводиться шляхом експертних випробувань.

1.6. Експертиза КСЗІ шляхом аналізу декларації проводиться у випадках, якщо:

- КСЗІ створено в ІТС, яка згідно з **НД ТЗІ 2.5-005-99** «**Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу**» класифікована як АС класу 1 і в якій передбачається обробка інформації, що не становить державної та іншої передбаченої законом таємниці, і де використовуються засоби захисту інформації, які мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ;

- закінчився строк дії атестата відповідності КСЗІ в ІТС вимогам НД ТЗІ (далі - Атестат), яка згідно з нормативними документами із ТЗІ класифікується як АС класу 1 і в якій передбачається обробка інформації, що не становить державної та іншої передбаченої законом таємниці.

У всіх інших випадках експертиза КСЗІ в ІТС проводиться шляхом експертних випробувань.

1.7. Експертиза може бути первинною, додатковою та контрольною.

Первинна експертиза є основним видом експертизи і передбачає виконання Організатором усіх потрібних заходів, визначених у розділі 3 цього Положення, для підготовки та прийняття рішення щодо об'єкта експертизи.

Додаткова експертиза проводиться стосовно об'єктів експертизи, щодо яких відкрилися нові наукові та науково-технічні обставини або в зв'язку з закінченням терміну дії документів, що засвідчують результати експертизи.

Контрольна експертиза проводиться іншим Організатором з ініціативи Замовника за наявністю у нього обґрунтованих претензій до висновку первинної чи додаткової експертизи або з ініціативи Адміністрації для перевірки висновку первинної чи додаткової експертизи.

**3. Порядок організації та проведення експертизи**

3.1. Для проведення експертизи шляхом експертних випробувань Замовник надсилає заяву на ім'я Голови Держспецзв'язку (крім випадків, передбачених у розділі 5 цього Положення) про проведення експертизи КСЗІ в ІТС або засобу ТЗІ, а шляхом аналізу декларації - декларацію про відповідність КСЗІ вимогам нормативних документів із ТЗІ (додаток 3), формуляр ІТС і акт про завершення робіт зі створення КСЗІ.

3.2. З метою розгляду декларацій і заяв, координації заходів і прийняття рішень щодо проведення експертиз в Адміністрації створюється експертна рада з питань державної експертизи у сфері технічного захисту інформації (далі - Експертна рада).

3.3. За результатами аналізу декларації і поданих разом із нею документів Експертна рада в місячний строк приймає рішення про реєстрацію декларації. Зареєстровану декларацію та інші подані документи Адміністрація повертає Замовнику.

3.4. У разі ненадання документів, зазначених у пункті 3.1 цього розділу, неповноти наданих у них відомостей або невідповідності порядку створення КСЗІ вимогам НД ТЗІ Адміністрація в місячний строк повертає Замовнику декларацію для доопрацювання.

3.5. Адміністрація має право в установленому порядку зупинити дію декларації або скасувати її реєстрацію

3.6. Строк дії зареєстрованої декларації є необмеженим. У разі внесення змін, не передбачених у технічному завданні на створення КСЗІ, Замовник зобов'язаний надіслати на ім'я Голови Держспецзв'язку декларацію в порядку, передбаченому в пункті 3.1 цього розділу.

3.7. За результатами розгляду заяви Експертна рада у місячний термін приймає рішення про доцільність проведення експертизи та визначає її Організатора.

3.8. У разі наявності у Замовника обґрунтованих претензій щодо порядку проведення або результатів експертизи він може звернутися до Адміністрації з пропозицією щодо здійснення контролю за проведенням Організатором експертних випробувань або із заявою на ім'я Голови Держспецзв'язку про проведення контрольної експертизи.

3.10. Основним документом, що регламентує відносини між Замовником і Організатором, є укладений між ними договір на проведення експертизи.

3.12. Результати, матеріали, висновки експертизи та створене або придбане за кошти Замовника матеріально-технічне забезпечення є його власністю, якщо інше не передбачено договором між Замовником і Організатором.

3.13. Термін проведення експертизи визначається договором і не повинен перевищувати, як правило, 6 місяців. У випадку значного обсягу експертних робіт термін проведення експертизи може бути продовжений за згодою Адміністрації та Замовника.

3.14. Список Експертів, які залучаються до виконання експертних робіт, визначається Організатором.

3.16. Організатор, за результатами аналізу наданих документів і з урахуванням загальних методик оцінювання задекларованих характеристик засобів ТЗІ і КСЗІ, формує програму і окремі методики проведення експертизи об'єкта та розробляє, у разі необхідності, порядок відбору зразків засобів ТЗІ для проведення випробувань і відповідне програмно-технічне забезпечення.

3.17. Програма проведення експертизи узгоджується із Замовником та Департаментом з питань захисту інформації в ІТС (далі – ДЗІ ІТС) Адміністрації, а окремі методики - з зазначеним департаментом.

3.18. Терміни розробки окремої методики та необхідних програмно-апаратних засобів залежать від характеру та складності об'єкта експертизи і визначаються у договорі на проведення експертизи.

3.19. Під час проведення експертизи кожний Експерт виконує експертні роботи тільки за дорученням Організатора та у відповідності з визначеною окремою методикою.

3.20. Результати роботи оформлюються у вигляді протоколу виконання робіт (додаток 6) за підписом Експертів, які її виконували. Протокол затверджується Організатором.

3.23. У протоколі можуть бути зафіксовані особливі думки Експертів відносно результатів виконаних робіт.

3.24. У разі виявлення невідповідності об'єкта експертизи вимогам НД ТЗІ Організатор може запропонувати Замовнику виконати доробку об'єкта.

3.26. Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами.

3.27. Результати робіт, визначених окремою методикою, узагальнюються Організатором в Експертному висновку.

3.28. Висновки щодо кожного пункту окремої методики, а також особливі думки Експертів, зафіксовані в протоколах, включаються до Експертного висновку як складові частини без унесення до них будь-яких змін.

3.29. За результатами проведених робіт Організатор складає Експертний висновок відповідного змісту щодо відповідності об'єкта експертизи вимогам НД ТЗІ, підписує його і разом із протоколами виконання робіт подає до Адміністрації.

**4. Порядок надання Експертного висновку та Атестата**

4.1. Експертний висновок на засіб ТЗІ розглядається Експертною радою і, у разі затвердження результатів експертизи, реєструється та видається Замовнику.

4.2. На підставі позитивного рішення щодо експертизи КСЗІ Замовнику видається зареєстрований Атестат відповідності за підписом Голови Держспецзв'язку.

4.3. Адміністрація має право в установленому порядку зупинити дію або скасувати Експертний висновок або Атестат.

**5. Особливості проведення експертиз КСЗІ державними органами**

5.1. Адміністрація надає державному органу повноваження з організації та проведення первинних або додаткових експертиз КСЗІ в ІТС шляхом експертних випробувань за умови погодження з Адміністрацією порядку їх здійснення.

5.2. Державні органи, які мають дозвіл Адміністрації на проведення робіт з ТЗІ для власних потреб та отримали від Адміністрації зазначені повноваження:

- здійснюють організацію та проведення експертиз КСЗІ в ІТС у сфері свого управління шляхом експертних випробувань;

- видають Атестат відповідності, який реєструється Адміністрацією.

19 березня 2009 року наказом Адміністрації Держспецзв'язку № 64 був затверджений «**Стандарт надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ**», метою якого є підвищення якості надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ.

До заяви про проведення первинної або додаткової експертизи додаються:

- технічне завдання на створення КСЗІ в ІТС;

- формуляр ІТС.

Прийняте Адміністрацією Держспецзв’язку рішення про можливість проведення експертизи КСЗІ в ІТС за заявою, поданою одержувачем, та про визначення організатора експертизи повідомляється одержувачу у термін, що не повинен перевищувати 15 робочих днів.

Атестат відповідності КСЗІ в ІТС вимогам нормативних документів з ТЗІ оформляється протягом 5 робочих днів на підставі позитивного рішення Адміністрації Держспецзв’язку щодо результатів експертизи. Зареєстрований атестат надсилається організатору експертизи для видачі одержувачу разом з експертним висновком.

Адміністративна послуга з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ надається безоплатно.

Інформація щодо порядку проведення експертизи КСЗІ в ІТС та форми заяв про проведення експертизи КСЗІ в ІТС розміщені на офіційному сайті Держспецзв’язку в мережі Інтернет (електронна адреса: *www.dsszzi.gov.ua*, розділ «Діяльність» - «Експертиза» - «Технічний захист інформації»).

1 жовтня 2010 року наказом Адміністрації Держспецзв’язку № 291 було затверджене «**Положення про Експертну раду з питань державної експертизи в сфері ТЗІ**», яка є постійно діючим колегіальним органом Адміністрації Держспецзв'язку з питань організації та проведення державної експертизи у сфері ТЗІ.

Метою діяльності Експертної ради є координація заходів з дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам нормативно-правових актів і НД ТЗІ та оцінювання результатів експертизи.

Формою роботи Експертної ради є засідання, які проводяться за потреби, але не рідше одного разу на місяць.

На підставі рішень Експертної ради про затвердження результатів державних експертиз оформляються, реєструються та надаються замовникам Експертні висновки на засоби ТЗІ, оформляються та видаються Атестати відповідності КСЗІ.

16 квітня 2008 року наказом Адміністрації Держспецзв'язку № 64 був затверджений «**Порядок формування Реєстру організаторів державної експертизи у сфері ТЗІ та Реєстру експертів з питань ТЗІ**»

До реєстру Організаторів вносяться всі підрозділи Держспецзв'язку, підприємства, установи та організації, визначені Експертною радою як Організатори, за результатами розгляду заяв замовників про проведення державної експертизи у сфері ТЗІ.

До реєстру Експертів вносяться всі фахівці з питань ТЗІ, які залучаються Організаторами до виконання експертних робіт під час проведення державних експертиз у сфері ТЗІ.

Картки реєстрації Організатора та Експертів зберігаються в окремій справі ДЗІ ІТС відповідно до встановлених у Держспецзв'язку вимог щодо ведення діловодства.

25 березня 2011 року наказом Адміністрації Держспецзв'язку № 65 був затверджений НД ТЗІ 2.6-001-11 «**Порядок проведення робіт з державної експертизи засобів ТЗІ від НСД та КСЗІ в ІТС**», який складається з таких основних розділів:

- вступні положення щодо порядку проведення експертизи засобів ТЗІ від несанкціонованого доступу та КСЗІ;

- опис порядку проведення робіт з експертизи засобів ТЗІ від несанкціонованого доступу;

- опис порядку проведення робіт з експертизи КСЗІ.

Він має такі додатки:

- рекомендації щодо складу та змісту проектної, експлуатаційної та нормативно-розпорядчої документації, яка надається Замовником при проведенні експертизи КСЗІ;

- вимоги щодо змісту програми проведення експертизи КСЗІ в ІТС;

- вимоги щодо змісту методики проведення експертизи КСЗІ в ІТС;

- рекомендації щодо викладення змістовної частини протоколу експертизи засобу ТЗІ від несанкціонованого доступу;

- рекомендації щодо викладення змістовної частини протоколу експертизи КСЗІ;

- рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи засобу ТЗІ від несанкціонованого доступу

- рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи КСЗІ.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, Організатор може запропонувати Замовнику виконати доробку об’єкта. Термін доробки об’єкта експертизи визначається спільним протоколом або додатковою угодою до договору між Замовником та Організатором. Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами. Після завершення передбачених актом робіт проводиться повторна експертиза.

Для інтегрованих ІТС може проводитись державна експертиза кожної складової частини (модуля) КСЗІ окремо. Державна експертиза КСЗІ інтегрованої ІТС полягає у перевірці взаємодії (адміністрування, обміну даними бази даних захисту тощо) вже оцінених модулів. Документи, що містять результати робіт кожного з етапів (протоколи, акти, атестати відповідності) для КСЗІ ІТС в цілому, оформлюються з урахуванням відповідних документів на складові частини КСЗІ.

Результати робіт, визначених методикою, узагальнюються Організатором в Експертному висновку. Висновки щодо кожного пункту методики, а також особлива думка Експерта, зафіксовані в протоколах, включаються до Експертного висновку як складові частини без унесення до них будь-яких змін.

За результатами проведених робіт Організатор складає Експертний висновок щодо відповідності об’єкта експертизи вимогам нормативних документів з ТЗІ, підписує його і разом із протоколами виконання робіт подає до Адміністрації.

На підставі позитивного рішення щодо експертизи КСЗІ Замовнику безоплатно видається зареєстрований Атестат відповідності за підписом Голови Держспецзв’язку згідно вимог «Переліку адміністративних послуг, які безоплатно надаються Адміністрацією Держспецзв'язку», затвердженого наказом Адміністрації Держспецзв'язку від 29.11.2011 № 350, зареєстрованого в Міністерстві юстиції України 15.12.2011 за № 1455/20193.

Згідно вимог п.1.6 Стандарту термін дії Атестату відповідності становить 5 років. Отримання Атестату фіксується відповідним записом у формулярі ІТС. Атестат відповідності є підставою для Замовника видати наказ про введення КСЗІ в ІТС в постійну експлуатацію, після чого в ІТС можна обробляти ІзОД.

**Особливості проведення експертизи шляхом декларації**

Шляхом аналізу декларації може проводитися державна експертиза КСЗІ в ІТС, яка складається з декількох компонентів, які організаційно поєднані в одну систему (окремих АРМ, які призначені для вирішення одного й того самого завдання, але функціонують автономно) і вимоги до захисту інформації від НСД кожної компоненти висуваються як для АС.

Процедурою державної експертизи шляхом аналізу декларації можуть скористатися будь-які суб’єкти: органи державної влади, місцевого самоврядування, установи, підприємства та організації незалежно від форми власності та підпорядкування, фізичні та юридичні особи (далі – установа).

Запровадження декларативного механізму проведення державної експертизи КСЗІ не зачіпає правових норм, що стосуються визначення вимог, організації робіт та порядку створення КСЗІ, не вносить жодних змін до порядку виконання робіт зі створення КСЗІ.

Декларація подається після завершення всіх робіт зі створення КСЗІ у повному обсязі і відображення їх результатів у Формулярі АС і Акті про завершення робіт зі створення КСЗІ, які повинні підтверджувати факт виконання всіх основних етапів та дотримання встановленого порядку виконання робіт.

Під словами «*всіх основних етапів робіт*» згідно вимог НД ТЗІ 3.7-003-05 розуміється, що мають бути виконані роботи з визначення й оцінки загроз для інформації, формування вимог, розроблення й реалізації проекту КСЗІ, проведення випробувань КСЗІ та введення КСЗІ в експлуатацію у складі АС.

Типові форми «Формуляру АС» і «Акту про завершення робіт зі створення КСЗІ в АС класу 1» можна знайти на сайті Держспецзв'язку.

Розділи формуляра мають бути заповнені відповідними відомостями з посиланням на технічні або розпорядчі документи (протоколи, акти тощо) установи з їх реєстраційними номерами, згідно з якими виконувалися або в яких зафіксовано результати виконання тих чи інших робіт. Наприклад, це може бути наказ установи про створення служби захисту інформації чи призначення відповідальних осіб за забезпечення захисту інформації в АС, акт (протокол, звіт тощо) про проведення власником АС випробувань КСЗІ, ТЗ на створення КСЗІ, техноробочий проект КСЗІ, опис КСЗІ, модель загроз для інформації тощо. Зазначаються випадки інтегрування декількох документів, що мають самостійне значення, в один документ.

До формуляра вносяться також відомості про проведення робіт із технічного обслуговування, модернізації КСЗІ, внесення інших змін до АС-1, які не впливають на технічні характеристики функціонування КСЗІ (наприклад, заміна окремих технічних засобів чи засобів обробки інформації іншими, нові призначення відповідальних осіб, зміна назви АС, місця розташування, адреси тощо).

Усі графи декларації мають бути заповнені.

До декларації вносяться відомості про повну назву установи-власника (розпорядника) ІТС, посаду, прізвище, ім’я та по батькові особи, що підписує декларацію (керівника установи), повну назву ІТС, в якій декларується створення і впровадження КСЗІ.

До декларації вноситься перелік назв з реєстраційними атрибутами розпорядчих, проектних і експлуатаційних документів (накази про призначення і виконання певних робіт, технічне завдання на створення КСЗІ, техно-робочий проект КСЗІ, опис КСЗІ, модель загроз для інформації, інструкції з експлуатації для адміністратора та користувача ІТС, інструкції з налаштування засобів захисту інформації тощо).

У графі «вид інформації за порядком доступу» вказується один або декілька видів інформації, які обробляються в ІТС (відкрита, конфіденційна, службова, персональні дані, інший вид інформації, вимога щодо захисту якої встановлена законом).

У графах з даними технічного завдання, проектних та експлуатаційних документів вказуються їх повні назви, реєстраційні атрибути, а також умовні позначення згідно з державним стандартом **ГОСТ 34.201-89** «**Виды, комплектность и обозначение документов при создании автоматизированных систем**» (у разі наявності).

Якщо документ потребує погодження з уповноваженим органом, зазначається назва органу, дата погодження, прізвище посадової особи, що його погодила.

Має бути документально підтверджено виконання обов’язкових вимог, установлених «Правилами забезпечення захисту інформації в ІТС», а також дотримання критерію щодо використання засобів захисту інформації, які мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ.

Використання КЗЗ з функціями розмежування доступу, який має чинний на момент подання декларації позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ, документально підтверджується відповідним записом у формулярі АС (вказати номер і дату експертного висновку, заводський номер і дату виготовлення впровадженого зразка засобу). Якщо у складі КСЗІ використовується засіб, термін дії експертного висновку якого закінчився, то необхідно додатково до запису у формулярі надати документ, який підтверджує легітимність засобу на момент його купівлі.

Формуляр повинен містити запис про впровадження антивірусних програм, які мають підтвердження відповідності. Застосування антивірусних засобів аналогічне тому, що і для засобів розмежування доступу.

Необхідно вказати реквізити розпорядчого документа установи, згідно з яким утворено службу захисту інформації або призначено відповідальних осіб.

Незаповнені графи у декларації та формулярі АС, відсутність висновків про позитивні результати впровадження заходів в акті завершення робіт зі створення КСЗІ, невідповідність наданих відомостей у різних документах, недостовірність відомостей є підставою для відмови у реєстрації декларації.

Адміністрація Держспецзв’язку не втручається у процес підготовки декларації, тому процес підготовки контролюється виключно власником (розпорядником) АС і тільки він є відповідальним за правильність оформлення та комплексність документів, достовірність поданих у декларації відомостей. Адміністрація Держспецзв’язку на прохання суб’єкта може тільки (і повинна) надавати необхідну консультативну та методичну допомогу з питань створення КСЗІ, оформлення результатів виконаних робіт, заповнення тексту декларації тощо.

Декларація складається власником (розпорядником) АС у 2-х примірниках і надсилається разом із «Формуляром АС» та «Актом про завершення робіт зі створення КСЗІ в АС» до Адміністрації Держспецзв’язку. Розгляд декларацій здійснюється Департаментом ТЗІ Адміністрації, яким перевіряється правильність заповнення декларації та дотримання відповідності порядку створення КСЗІ нормативним документам. Якщо декларація відповідає встановленим вимогам оригінал декларації реєструється Адміністрацією, кожен аркуш на звороті візується відповідальним співробітником зазначеного департаменту. Оригінал декларації, формуляр АС та акт завершення робіт зі створення КСЗІ повертається замовнику. Копія декларації залишається в Адміністрації Держспецзв’язку.

Процедура аналізу декларації Адміністрацією Держспецзв’язку є прозорою, ґрунтується на аналізі документів, визначених у Положенні, і не потребує додаткових перевірок упроваджених на об’єкті експертизи заходів і засобів захисту.

Зареєстрована декларація має таку ж саму правову силу, що і атестат відповідності, є законним документом, що підтверджує відповідність створеної КСЗІ в АС.

Відповідальність за достовірність внесених до декларації відомостей відповідно до статті 16 Закону України «**Про підтвердження відповідності**» несе подавець декларації.

Строк дії декларації не обмежений. Декларація зберігає свою чинність до того часу, доки внесені до неї відомості є достовірними. Зокрема, до втрати достовірності відомостей декларації може призводити модернізація КСЗІ, якщо вносяться зміни, які впливають на політику безпеку інформації. Наприклад, це може бути зміна видів об’єктів захисту, моделі загроз, ролей користувачів, правил розмежування доступу чи обраного для їх реалізації комплексу засобів захисту тощо.

У цьому разі власник (розпорядник) АС повинен задокументувати виконані роботи, внести відповідні відомості до декларації. Складена декларація надсилається до Адміністрації Держспецзв’язку для реєстрації. Розгляд та реєстрація складеної нової декларації здійснюється у тому ж порядку, що і під час первинної реєстрації. Власник (розпорядник) АС надсилає до Адміністрації Держспецзв’язку разом із складеною новою декларацією акт про завершення робіт зі створення КСЗІ, формуляр АС, оригінал чинної декларації. У супровідному листі вказуються причини подання нової декларації та заявляється необхідність скасування реєстрації чинної декларації.

Оригінал скасованої декларації повертається подавцю з відміткою «Скасовано», номером та датою рішення про скасування.

Адміністрація Держспецзв’язку має право перевіряти дотримання вимог НД ТЗІ під час експлуатації АС, КСЗІ яких мають зареєстровані декларації, та у разі виявлення порушень скасовувати їх реєстрацію або зупиняти дію до усунення цих порушень.

22. 6-й етап - супровід КСЗІ

Весь період функціонування КСЗІ забезпечується її супроводом, під час якого персоналом ІТС виконуються такі роботи щодо КСЗІ:

- керування КСЗІ згідно Плану захисту та експлуатаційної документації;

- вдосконалення та модернізації КСЗІ.

Крім того, під час супроводу КСЗІ здійснюються такі заходи:

- організаційне забезпечення працездатності ІТС;

- гарантійне та післягарантійне технічне обслуговування засобів КСЗІ;

- періодичне поновлення документів КСЗІ.

Всі заходи супроводу та модернізації КСЗІ вносяться до Календарного плану робіт із захисту інформації в ІТС, який щорічно поновлюється.

Він складається з 4-х розділів:

- організаційні заходи;

- контрольно-профілактичні заходи;

## - інженерно-технічні заходи;

## - кадрові заходи.

# Календарний план робіт із захисту інформації в ІТС

**1. Організаційні заходи**

Організаційні заходи - це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування КСЗІ.

|  |  |  |  |
| --- | --- | --- | --- |
| **Заходи** | **Виконавець** | **Регламент робіт** | **Терміни/період** |
| Коригування політики безпеки | СЗІАдміністра-тори | Коригування політикиРозробка додаткових інструкцій  | у разі змін умов функціонування ІТС |
| Коригування Плану захисту | СЗІАдміністра-тори | Розробка нових підходів до планування заходів захисту | щорічно |
| Планування модернізації КСЗІ | СЗІАдміністра-тори | Розробка ТЗ на модернізацію КСЗІ згідно НД ТЗІ 3.7-001-99 | згідно плану розвитку КСЗІ |
| Чергове категорію-вання | Комісія установи | Згідно НД ТЗІ 1.6-005-2013 | через 5 років після первинного |
| Чергова державна експертиза | Адміністра-ція ДССЗЗІУ | Згідно вимог «Положення про державну експертизу» | через 5 років після первинної |

**2. Контрольно-профілактичні заходи**

Контрольні заходи - це комплекс заходів контролю за виконанням персоналом ІТС вимог нормативно-правових актів України у сфері захисту інформації, розроблених в установі інструкцій і положень, а також заходів, розроблених за результатами попередніх перевірок.

Профілактичні заходи - це комплекс заходів, спрямованих на формування у користувачів мотивів поведінки, які спонукають їх на безумовне виконання у повному обсязі вимог правил проведення робіт із захисту інформації тощо, а також формування відповідного морально-етичного стану в колективі.

|  |  |  |  |
| --- | --- | --- | --- |
| **Заходи** | **Виконавець** | **Регламент робіт** | **Термін/період** |
| Проведення занять з персоналом ІТС щодо виконання вимог політики безпеки в установі | Служба захисту | Згідно «Плану навчання в установі» | щоквартально |
| Формування в трудовій угоді розділу відповідальності за виконання вимог політики безпеки | Служба захисту | Згідно вимог трудового законодавства | за рішенням керівника установи |
| Контроль працездатності та виконання вимог політики безпеки | Системний адміністратор  | Перевірка справності ОС і ПЗ ІТС | щодня |
| Адміністра-тор безпеки | Перевірка виконання вимог політики безпеки користувачами  | щомісячно |
| Служба захисту | Перевірка виконання політики безпеки адміністраторами | щоквартально |
| Перевірка стану захисту інформації  | Комісія установи | Згідно «Положення про захист інформації» | щорічно |
| Перевірка наявності МНІ | Комісія установи | Згідно «Інструкції про організацію діловодства» | щорічно |

## 3. Інженерно-технічні заходи

Інженерно-технічні заходи - це комплекс заходів, спрямованих на налагодження, випробування і введення в експлуатацію, супроводження і технічне обслуговування апаратних і програмних засобів захисту інформації в ІТС, інженерне обладнання споруд і приміщень, в яких розміщуються засоби ІТС.

|  |  |  |  |
| --- | --- | --- | --- |
| **Заходи** | **Виконавець** | **Регламент робіт** | **Термін/період** |
| Супровід КСЗІ | Розробник КСЗІ | Гарантійне обслуговування | Гарантійний термін |
| Технічне обслу-говування ІТС | Адміністратори  | Згідно «Регламенту техобслуговування» | згідно термінів регламенту |
| Резервування баз даних і фондів | Адміністратор безпеки | Згідно «Інструкції з резервування баз даних» | щомісячно |
| Поновлення антивірусних баз  | Адміністратор безпеки | Згідно «Інструкції з антивірусного захисту» | щодня |
| Перевірка МНІ і ІТС на наявність вірусів | Користувач (МНІ) | Згідно «Інструкції з антивірусного захисту» | щодня |
| Адміністратори (ІТС) | щотижня |
| Модернізація КСЗІ | Розробник КСЗІ | Заміна (додавання) окремих компонентів КСЗІ  | згідно плану розвитку КСЗІ |

## 4. Кадрові заходи

Кадрові заходи - це комплекс навчально-педагогічних заходів, спрямованих на розширення світогляду та підвищення професійної майстерності персоналу ІТС, що визначається її особливостями та технологіями захисту інформації, які використовуються в ній.

|  |  |  |  |
| --- | --- | --- | --- |
| **Заходи** | **Виконавець** | **Регламент робіт** | **Термін/період** |
| Вступне ознайомлення з положеннями політики безпеки інформації (під розпис) | Служба захисту | Оформлення допуску до роботи | після прийому на роботу |
| Адміністра-тор безпеки | Згідно «Інструкції користувачу»  | під час їхньої реєстрації в ІТС |
| Інструктаж користувачів щодо дій у випадку позаштатної ситуації | Адміністра-тор безпеки | Згідно «Плану робіт у випадку позаштатної ситуації»  | щорічно |
| Проведення занять з професійної підготовки персоналу ІТС  | Служба захистуАдміністра-тори | Згідно «Плану професійної підготовки в установі» | щотижня |
| Направлення на курси підвищення кваліфікації | Служба захисту | Згідно «Плану підвищення кваліфікації в установі» | згідно термінів плану |

Виконання Календарного плану забезпечується Службою захисту інформації в ІТС (далі - СЗІ), яка у процесі супроводу КСЗІ повинна виконувати такі функції:

* організація процесу керування КСЗІ;
* розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;
* вжиття заходів у разі виявлення спроб НСД до ресурсів ІТС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;
* забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;
* організація керування доступом до ресурсів ІТС (розподілення між користувачами необхідних реквізитів захисту інформації - паролів, привілеїв, ключів тощо);
* супроводження та актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об’єктів, ідентифікатори користувачів тощо);
* спостереження (реєстрація та аудит подій в ІТС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;
* підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в ІТС, впровадження нових технологій захисту і модернізації КСЗІ;
* організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІТС або КСЗІ;
* участь в роботах з модернізації ІТС - узгодженні пропозицій з введення до складу ІТС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;
* забезпечення супроводження і актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;
* проведення аналітичної оцінки поточного стану безпеки інформації в ІТС (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз тощо);
* інформування власників інформації про технічні можливості захисту інформації в ІТС і типові правила, встановлені для персоналу і користувачів ІТС;
* негайне втручання в процес роботи ІТС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;
* регулярне подання звітів керівництву організації про виконання користувачами ІТС вимог щодо захисту інформації;
* аналіз відомостей щодо засобів захисту інформації нового покоління, обгрунтування пропозицій щодо придбання засобів для організації;
* розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу ІТС;
* участь в організації і проведенні навчання користувачів і персоналу ІТС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;
* участь в організації забезпечення навчального процесу необхідною матеріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою тощо;
* контроль за виконанням персоналом і користувачами ІТС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації;
* контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;
* розробка та реалізація спільно з РСО та службою безпеки організації комплексних заходів з безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співробітництва з іноземними фірмами, а також під час проведення нарад, переговорів тощо, здійснення їхнього технічного та інформаційного забезпечення.

**Супровід КСЗІ** забезпечується виконанням вимог інструкцій та веденням журналів, які були розроблені при введенні КСЗІ в експлуатацію.

До складу супровідної документації КСЗІ входять:

- інструкції щодо забезпечення правил оброблення ІзОД в ІТС;

- інструкції співробітників СЗІ, персоналу та користувачів ІТС;

- технологічні інструкції щодо адміністрування та обслуговування КСЗІ;

* інструкція про порядок використання криптографічних засобів;
* інструкція про порядок супроводження та модернізації КСЗІ;
* інструкція про порядок резервування інформаційних ресурсів ІТС;
* порядок обліку і супроводження архівів та ротації носіїв інформації;
* інструкція про порядок оперативного відновлення функціонування ІТС;
* інструкція про організацію контролю за функціонуванням КСЗІ;
* інструкція про порядок проведення ремонтних робіт.
* порядок розробки, впровадження та модернізації ПЗ ІТС;
* правила видачі, вилучення та обліку персональних ідентифікаторів;
* правила управління паролями в ІТС;
* правила класифікації та класифікатор інформації і користувачів ІТС;
* формуляр (паспорт) ІТС;
* журнали, які використовуються для реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ.

Перелік та форми реєстраційних журналів повинні відповідати визначеним у технологічних інструкціях щодо виконання завдань з адміністрування та обслуговування КСЗІ.

Як приклади реєстраційних журналів можна розглядати такі:

- обліку користувачів ІТС;

- обліку роботи користувачів ІТС;

- обліку захищених інформаційних ресурсів ІТС;

- реєстрації проведених робіт з технічного обслуговування, ремонту, модернізації;

- реєстрації перевірок складу програмних засобів ІТС;

- реєстрації позаштатних ситуацій у роботі ІТС.

Якщо в ІТС передбачається оброблення службової інформації, під час функціонування ІТС використовуються журнали, форми та правила ведення яких встановлені «Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію», затвердженою постановою Кабінету Міністрів України від 27.11.98 № 1893.

Зокрема, необхідно вести такі журнали обліку службової інформації:

- обліку документів та видань з грифом «ДСК»;

- обліку машинних носіїв інформації з грифом «ДСК».

Якщо в ІТС передбачається оброблення секретної інформації, під час функціонування ІТС використовуються такі журнали, форми та правила ведення яких встановлені «Порядком організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях», затвердженим постановою Кабінету Міністрів України від 02.10.2003 № 1561-12.

Зокрема, необхідно вести такі журнали обліку секретної інформації:

- обліку сховищ матеріальних носіїв секретної інформації та ключів від них;

- здавання (приймання) з-під охорони режимних приміщень, сховищ матеріальних носіїв секретної інформації та ключів від них;

- обліку вхідних і підготовлених секретних документів;

- обліку робочих зошитів, спецблокнотів, окремих аркушів і бланків.

***Адміністратор безпеки під час супроводу КСЗІ зобов’язаний:***

- контролювати встановлення ПЗ, його працездатність та оновлення, конфігурування політики безпеки ІТС;

- забезпечувати конфігурування КЗЗ, ПЗ для захисту інформації, налагодження антивірусного ПЗ та елементів ІТС, які мають вбудовані функції захисту;

- забезпечувати надійне функціонування КЗЗ і ПЗ для захисту інформації, антивірусного ПЗ та контролювати його працездатність;

- встановлювати в ІТС обмежені права доступу до операційної системи та «BIOS»,

- визначати користувачів, їх ідентифікатори та паролі, встановлювати користувачам захищені каталоги;

- керувати обліковими записами та атрибутами користувачів,

- керувати правами доступу к захищеним каталогам з боку користувачів і програмних засобів;

- керувати рівнями конфіденційності та квотами на використання дискового простору ІТС;

- відновлювати роботу засобів захисту у разі їх збоїв або виходу з ладу;

- брати участь у впровадженні заходів захисту інформації в ІТС та здійснювати контроль умов використання ІТС відповідно до експлуатаційної документації та вимог приписів на експлуатацію об’єктів ІТС;

- здійснювати адміністрування в частині захисту інформації та оновлення баз даних захисту ІТС;

- забезпечувати проведення технічного обслуговування та контролю за функціонуванням засобів захисту інформації;

- здійснювати опечатування вузлів, блоків, усіх портів ІТС та щоденний контроль за його станом;

- проводити поточний контроль за забезпеченням режиму обробки та захисту інформації в ІТС згідно затвердженої інструкції;

- проводити інструктаж та навчання персоналу з питань дотримання вимог забезпечення режиму обробки та захисту інформації в ІТС;

- здійснювати контроль за роботою користувачів та виконанням ними вимог щодо захисту інформації шляхом періодичних спостережень за діями користувачів під час роботи в ІТС (вибірково);

- здійснювати контроль за проведенням робіт з ремонту та заміни технічних засобів ІТС або комплексу ТЗІ;

- вносити пропозиції та брати участь у проектуванні, створенні та дослідній експлуатації КСЗІ в ІТС;

- доповідати керівнику СЗІ про всі виявлені порушення режиму обробки та захисту інформації в ІТС.

***Системний адміністратор під час супроводу КСЗІ зобов’язаний:***

- встановлювати та настроювати ОС та необхідне для роботи апаратне й програмне забезпечення (далі - АПЗ);

- встановлювати на ІТС сертифіковане антивірусне програмне забезпечення (далі - ПЗ) та оновлювати його бази даних, після чого перевіряти ІТС на наявність комп’ютерних вірусів;

- підтримувати робочий стан ОС і АПЗ ІТС та контролювати їх працездатність;

- навчати користувачів роботі на ІТС і формуванню її інформаційного фонду;

- зберігати еталони ПЗ та резервні копії інформаційних фондів ІТС для відновлення її роботи після аварійних ушкоджень або ураження комп’ютерними вірусами;

- вести та оновлювати фонд дозволеного до використання ПЗ ІТС, щорічно проводити його інвентаризацію;

- щомісячно контролювати копіювання інформаційних фондів ІТС на зареєстровані зовнішні носії інформації згідно затвердженої інструкції;

- оперативно відновлювати працездатність ІТС при збоях і виході з ладу ОС і АПЗ ІТС згідно затвердженої інструкції;

- брати участь у проведенні інвентаризації ІТС;

- здійснювати контроль за проведенням ремонту та монтажу устаткування ІТС фахівцями сторонніх організацій;

- виявляти помилки користувачів та проводити їх інструктаж;

- готувати пропозиції з модернізації та придбання ІТС, АПЗ, розвитку автоматизації обробки даних;

- готувати пропозиції до планів роботи підрозділів стосовно заходів із забезпечення надійного та безперебійного функціонування ІТС;

- інформувати керівника СЗІ про випадки порушень правил експлуатації ІТС та обробки інформації.

***Користувач під час супроводу КСЗІ зобов’язаний:***

- використовувати надані інформацію ідентифікації та автентифікації (пароль) виключно для роботи з ІТС;

- зберігати особистий пароль (інформацію автентифікації) в таємниці, негайно інформувати адміністратора безпеки та безпосереднього начальника про факти компрометації (втрати, розголошення) паролю, при введенні пароля забезпечувати захист паролю від несанкціонованого спостереження іншими посадовими особами;

- виконувати вимоги нормативно-правових актів у сфері захисту інформації та НД ТЗІ щодо порядку поводження з МНІ та документами в електронному вигляді;

- при залишенні робочого місця на тривалий час здійснювати заходи щодо переведення системи в режим блокування;

- формувати перелік та періодично (щомісячно) здійснювати з залученням адміністратора ІТС резервне копіювання на з’ємні носії інформації, яка важлива для забезпечення службової діяльності установи;

- спільно з адміністратором ІТС визначати «папки» (файли) зі службовою інформацією, розпорядником якої є користувач, для встановлення аудиту прав доступу;

- негайно інформувати адміністратора про відхилення в нормальній роботі ІТС, системного та прикладного ПЗ, виходу із ладу або нестійкого функціонування технічних засобів ІТС, а також порушення цілісності або невідповідності печаток (пломб) вузлів та блоків, портів введення-виведення інформації технічних засобів ІТС.

Складовою супроводу КСЗІ є контроль за забезпеченням режиму під час обробки ІзОД в ІТС, який полягає у перевірці виконання персоналом ІТС вимог нормативно-правових актів з питань збереження ІзОД і нормативних документів з технічного та криптографічного захисту інформації.

Контроль режиму обробки ІзОД в ІТС здійснюється шляхом:

- планових перевірок;

- позапланових перевірок;

- повсякденного контролю.

Планові перевірки здійснюються комісіями, до складу яких входять начальники РСО і підрозділу ТЗІ, співробітники СЗІ та представники інших підрозділів установи. Головою комісії призначається керівник СЗІ. Підстави проведення перевірки, строки роботи і склад комісії, а також перелік об’єктів ІТС, які підлягають перевірці, зазначаються в наказі керівника установи.

Позапланові перевірки здійснюються у разі наявності відомостей щодо порушень виконання вимог «Інструкції щодо забезпечення правил оброблення ІзОД в ІТС», НД ТЗІ та інших нормативно-правових актів у сфері захисту інформації. Вони організовуються СЗІ та здійснюються комісіями, до складу яких входять начальники РСО і підрозділу ТЗІ, співробітники СЗІ та представники інших підрозділів установи.

Планова або позапланова перевірка проводиться у присутності начальника підрозділу установи, в якому проводиться перевірка, або особи, яка його заміщає, представника СЗІ та співробітника, відповідального за користування об’єкта ІТС.

Під час планових та позапланових перевірок перевіряється:

- дотримання користувачами ІТС встановлених вимог щодо забезпечення режиму обробки та захисту ІзОД;

- комплектація ІТС згідно з Формуляром;

- наявність та дотримання вимог приписів на експлуатацію об’єктів ІТС;

- виконання заходів щодо забезпечення захисту ІзОД від НСД на відповідність вимогам технічної та експлуатаційної документації, згідно з якими здійснюється експлуатація ІТС;

- відповідність ступеня обмеження доступу інформації, яка обробляється з використанням ІТС, наданій категорії об’єкта ІТС;

- відповідність ступеня обмеження доступу інформації, яка зберігається на машинних носіях даних, грифу обмеження доступу машинних носіїв даних;

- наявність атестата відповідності КСЗІ вимогам НД ТЗІ, організаційно-технічних документів та експлуатаційної документації.

За результатами перевірки складається акт, в якому зазначаються результати оцінки відповідності забезпечення режиму обробки та захисту ІзОД в ІТС вимогам НД ТЗІ та інших нормативно-правових актів у сфері захисту інформації, виявлені недоліки та рекомендації щодо їх усунення. Акт затверджується керівником установи, після чого з ним ознайомлюється начальник підрозділу, в якому проводилася перевірка.

Акт направляється в установленому порядку вищестоящому органу згідно з підпорядкованістю установи та регіональному органу Держспецзв’язку на його вимогу.

Повсякденний контроль за забезпеченням режиму під час обробки інформації в ІТС здійснюється СЗІ. Порядок його проведення та усунення виявлених недоліків або порушень вимог НД ТЗІ та інших нормативно-правових актів у сфері захисту інформаціївизначається окремою інструкцією, яка розробляється СЗІ, узгоджується з РСО і підрозділом ТЗІ та затверджується керівником установи.

Начальники підрозділів установи організовують усунення виявлених у ході перевірок недоліків та порушень. Контроль за виконанням зазначених заходів покладається на СЗІ.

**Особливості супроводу КСЗІ в ІТС державних установ**

Супровід системи антивірусного захисту як складової КСЗІ здійснюється згідно вимог «Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ», затвердженого наказом Адміністрації Держспецзв'язку від 26.03.2007 № 45, зареєстрованого в Міністерстві юстиції України 10.04.2007 за № 320/13587.

 Згідно з цим Порядком органи державної влади, органи місцевого самоврядування, утворені відповідно до законів України військові формування, підприємства, установи і організації державної форми власності зобов’язані:

- не менше ніж раз на день отримувати антивірусні оновлення АВПЗ за допомогою веб-серверу ЦАЗІ;

- інсталювати отримані за допомогою веб-серверу ЦАЗІ антивірусні оновлення АВПЗ відповідно до технічної документації АВПЗ;

- для забезпечення авторизованого доступу до ресурсів веб-серверу ЦАЗІ щороку до 1 березня та, у разі внесення змін, протягом 3 днів надавати до Адміністрації Держспецзв'язку відомості щодо кожного користувача у паперовому вигляді за визначеною формою.

Крім того, всі міністерства, інші центральні органи виконавчої влади, обласні державні адміністрації, а також підприємства, установи та організації, що належать до сфери їх управління, (далі – державні органи) подають відомості про створені ІТС, у тому числі, і АС класу «1», до Адміністрації Держспецзв'язку згідно вимог «Положення про Реєстр ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління», затвердженого постановою КМ України від 03.08.2005 № 688 із останніми змінами згідно постанови КМ України від 07.09.2011 № 938.

Це Положення визначає порядок утворення та функціонування Реєстру ІТС державних органів (далі - Реєстр), ведення якого забезпечує Адміністрація Держспецзв'язку як Адміністратор Реєстру згідно вимог «**Порядку формування й користування інформаційним фондом Реєстру ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління**», затверджений наказом Адміністрації Держспецзв'язку від 24.04.2007 № 72, зареєстрований в Міністерстві юстиції України 14.05.2007 за № 500/13767, із змінами згідно наказу Адміністрації Держспецзв’язку від 06.08.2012 № 425, зареєстрованого в Міністерстві юстиції України 22.08.2012 за № 1412/21724.

Цей Порядок визначає види та форми надання відомостей до інформаційного фонду Реєстру ІТС державних органів (далі - Інформаційний фонд) та правила користування ним. Відомості про ІТС подаються ще на стадії технічного проектування систем, а у разі модернізації функціонуючих ІТС - на стадії створення КСЗІ в цих системах. У разі введення в експлуатацію або припинення функціонування ІТС відповідний державний орган у 10-денний строк повідомляє про це адміністратора Реєстру.

Відомості до Інформаційного фонду подаються на оптичних носіях типу CD-R із супровідним листом за підписом керівника державного органу. Після впровадження в державному органі електронно-цифрового підпису зазначені відомості надаються з додержанням вимог чинного законодавства в електронному вигляді мережами передачі даних або надсилаються поштою на електронних носіях інформації. Носії інформації адресату не повертаються.

Державні органи двічі на рік (станом на 1 січня - до 1 лютого та станом на 1 липня - до 1 серпня) надають Адміністратору Реєстру узагальнені відомості про власні ІТС. Надалі в ті ж самі терміни державними органами надсилаються Адміністратору Реєстру відомості лише про ІТС, у яких відбулися зміни з моменту останнього надання інформації про них.

**23. Державний контроль за станом ТЗІ**

16 травня 2007 року наказом Адміністрації Держспецзв'язку № 87 було затверджене «**Положення про державний контроль за станом ТЗІ**», згідно якого державний контроль за станом ТЗІ полягає в перевірці виконання вимог НД ТЗІ та здійснюється з метою визначення стану ТЗІ в організаціях, виявлення порушень з ТЗІ та запобігання їм. Він здійснюється Держспецзв'язку шляхом організації та проведення контрольно-інспекторської роботи з питань ТЗІ.

**Організація проведення перевірок стану ТЗІ**

Перевірки стану ТЗІ поділяються на комплексні, цільові (тематичні) та контрольні. Зазначені перевірки можуть бути плановими та позаплановими.

При комплексній перевірці визначається відповідність комплексу ТЗІ (КСЗІ) та НД ТЗІ.

При цільовій (тематичній) перевірці перевіряються окремі складові комплексу ТЗІ (комплексної системи захисту інформації) на відповідність упроваджених заходів вимогам нормативних документів системи ТЗІ.

При контрольній перевірці перевіряється повнота та достатність проведених заходів щодо усунення недоліків, які були виявлені в ході проведення попередньої комплексної або цільової перевірки.

Контрольні перевірки проводяться за потреби, як правило, після отримання повідомлення про усунення недоліків.

Планові перевірки здійснюються згідно з річним планом контрольно-інспекторської роботи з питань ТЗІ, затвердженим Головою Держспецзв'язку.

Позапланові перевірки здійснюються у разі наявності відомостей щодо порушень виконання вимог НД ТЗІ або з метою визначення повноти та достатності вжитих заходів з ТЗІ. Зазначені перевірки можуть проводитися з попередженням або без попередження.

Керівництву органів, щодо яких здійснюється ТЗІ, повідомляється про проведення перевірки не менше ніж за 10 діб до її початку (за винятком проведення позапланової перевірки).

Підставою для допуску посадових осіб Держспецзв'язку до перевірки стану ТЗІ є наявність припису на право проведення перевірки за підписом начальника регіонального органу Держспецзв'язку.

**Порядок проведення перевірок стану ТЗІ**

Для проведення перевірки стану ТЗІ посадові особи Держспецзв'язку повинні пред'явити керівнику або вповноваженому представнику організації припис на право проведення перевірки та службові посвідчення.

За результатами перевірок посадовими особами Держспецзв'язку, які їх здійснювали, складаються акти перевірок стану ТЗІ.

Акт підписується посадовими особами Держспецзв'язку, якими проводилася перевірка, та затверджуються начальником регіонального органу Держспецзв'язку, який підписав припис на проведення перевірки.

 Ознайомлення керівника органу, щодо якого здійснюється ТЗІ, з актом здійснюється за його підписом.

У разі відмови керівника організації засвідчити факт ознайомлення з актом перевірки своїм підписом, посадовими особами Держспецзв'язку, що здійснювали перевірку, робиться в акті відповідний запис.

**Кваліфікація порушень з ТЗІ**

Порушення вимог з ТЗІ поділяються на 3 категорії, які визначають можливість реалізації загроз безпеці інформації:

1-а категорія - невиконання вимог НД ТЗІ, унаслідок чого створюється реальна загроза порушення конфіденційності, цілісності та доступності інформації;

2-а категорія - невиконання вимог НД ТЗІ, унаслідок чого створюються передумови до порушення конфіденційності, цілісності та доступності інформації;

3-я категорія - невиконання інших вимог з ТЗІ.

Порушення 1-ї категорії кваліфікується у разі встановлення такого факту:

- циркуляції ІзОД в ІТС за умов підтвердження інструментально-розрахунковими методами наявності технічного каналу поширення ІзОД;

- обробки ІзОД в ІТС, які мають вихід незахищеними каналами зв'язку за межі контрольованої зони, за умов відсутності атестата відповідності на КСЗІ;

- обробки ІзОД в ІТС, які не мають виходу за межі контрольованої зони, за умов доступу до її інформаційних ресурсів користувачів, які мають різні повноваження (права доступу до інформації), та відсутності атестата відповідності КСЗІ;

- обробки відкритої інформації, що є власністю держави, вимога щодо захисту якої встановлена законом, в ІТС, які мають підключення до мереж телекомунікацій (у тому числі загального користування), за умов відсутності атестата відповідності КСЗІ;

- несанкціонованого доступу користувачів ІТС до інформації, що є власністю держави, або ІзОД шляхом порушення встановлених правил розмежування доступу або подолання заходів захисту.

Порушення 2-ї категорії кваліфікується у разі встановлення такого факту:

- циркуляції ІзОД в ІТС за умов відсутності підтвердження інструментально-розрахунковими методами відповідності комплексу ТЗІ нормам та вимогам з ТЗІ;

- обробки ІзОД в ІТС, які мають вихід за межі контрольованої зони захищеними каналами, за умов відсутності атестата відповідності КСЗІ;

- обробки інформації, що є власністю держави, або ІзОД в ІТС, які не мають виходу за межі контрольованої зони, за умов відсутності атестата відповідності КСЗІ.

Невиконання вимог нормативно-правових актів щодо впровадження організаційних заходів з ТЗІ, а також інших норм та вимог у сфері захисту інформації, які не призводять до порушень 1-ї або 2-ї категорії, кваліфікується як порушення 3-ї категорії.

Для з'ясування причин, які призвели до порушень 1-ї категорії, а також притягнення осіб, які їх вчинили, до відповідальності посадові особи Держспецзв'язку, що здійснювали перевірку, ініціюють проведення службових розслідувань. У разі виявлення порушень 1-ї або 2-ї категорії вони у встановленому порядку можуть порушувати питання про припинення інформаційної діяльності на відповідних об'єктах.

З метою приведення стану ТЗІ у відповідність до вимог НД ТЗІ, а також виконання рекомендацій, наданих за результатами перевірки, керівниками органів, щодо яких здійснюється ТЗІ, у місячний термін після отримання акта перевірки затверджується план усунення недоліків, один примірник якого надсилається до органу Держспецзв'язку, посадовими особами якого було здійснено перевірку.

Повідомлення про виконання рекомендацій щодо приведення стану ТЗІ у відповідність до вимог НД ТЗІ надсилається керівнику органу Держспецзв'язку у терміни, зазначені в акті перевірки та плані усунення недоліків.

**24. Відповідальність за невиконання вимог захисту інформації**

Стаття 9Закону «**Про захист інформації в ІТС**» пише, що відповідальність за забезпечення захисту інформації в системі покладається на власника системи. А стаття 11 цього Закону визначає, що особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно чинного законодавства. Конкретизація таких порушень, їх правові та фінансові наслідки визначені у законодавстві України адміністративним та кримінальним кодексами.

**Кодекс України про адміністративний правопорушення (КУпАП)**

### Стаття 254. Складення протоколу про адміністративне правопорушення

Про вчинення адміністративного правопорушення складається протокол уповноваженою на те посадовою особою або представником громадської організації.

Протокол про адміністративне правопорушення, у разі його оформлення, складається у двох екземплярах, один з яких під розписку вручається особі, яка притягається до адміністративної відповідальності.

**Стаття 255.** У справах про адміністративні правопорушення, що розглядаються органами, зазначеними в статтях 218-221 цього Кодексу, протоколи про правопорушення мають право складати уповноважені на те посадові особи:

- органів Державної служби спеціального зв'язку та захисту інформації України;

- органів Служби безпеки України.

### Стаття 256. Зміст протоколу про адміністративне правопорушення

У протоколі про адміністративне правопорушення зазначаються: дата і місце його складення, посада, прізвище, ім'я, по батькові особи, яка склала протокол; відомості про особу, яка притягається до адміністративної відповідальності (у разі її виявлення); місце, час вчинення і суть адміністративного правопорушення; нормативний акт, який передбачає відповідальність за дане правопорушення; прізвища, адреси свідків і потерпілих, якщо вони є; пояснення особи, яка притягається до адміністративної відповідальності; інші відомості, необхідні для вирішення справи. Якщо правопорушенням заподіяно матеріальну шкоду, про це також зазначається в протоколі.

Протокол підписується особою, яка його склала, і особою, яка притягається до адміністративної відповідальності; при наявності свідків і потерпілих протокол може бути підписано також і цими особами.

У разі відмови особи, яка притягається до адміністративної відповідальності, від підписання протоколу, в ньому робиться запис про це. Особа, яка притягається до адміністративної відповідальності, має право подати пояснення і зауваження щодо змісту протоколу, які додаються до протоколу, а також викласти мотиви свого відмовлення від його підписання.

**1. Органи Державної служби спеціального зв'язку та захисту інформації України** - стаття 164 (у частині, що стосується правопорушень у галузі господарської діяльності, ліцензії на проведення якої видає ця Служба), пункт 9 частини першої статті 2122 та стаття 18831.

### Стаття 164. Порушення порядку провадження господарської діяльності

Провадження господарської діяльності без державної реєстрації як суб'єкта господарювання або без одержання ліцензії на провадження певного виду господарської діяльності, що підлягає ліцензуванню відповідно до закону, чи здійснення таких видів господарської діяльності з порушенням умов ліцензування, а так само без одержання дозволу, іншого документа дозвільного характеру, якщо його одержання передбачене законом (крім випадків застосування принципу мовчазної згоди), -

тягне за собою накладення штрафу від 20 до 100 неоподатковуваних мінімумів доходів громадян з конфіскацією виготовленої продукції, знарядь виробництва, сировини і грошей, одержаних внаслідок вчинення цього адміністративного правопорушення, чи без такої.

Дії, передбачені частиною першою цієї статті, вчинені особою, яку протягом року було піддано адміністративному стягненню за таке саме правопорушення, або пов'язані з отриманням доходу у великих розмірах, -

тягнуть за собою накладення штрафу від 100 до 500 неоподатковуваних мінімумів доходів громадян з конфіскацією виготовленої продукції, знарядь виробництва, сировини і грошей, одержаних внаслідок вчинення цього адміністративного правопорушення.

Надання суб'єктом господарювання дозвільному органу або адміністратору недостовірної інформації щодо відповідності матеріально-технічної бази вимогам законодавства -

тягне за собою накладення штрафу від 40 до 100 неоподатковуваних мінімумів доходів громадян.

***Примітка.****Отримання доходу у великих розмірах має місце, коли його сума у тисячу і більше разів перевищує неоподатковуваний мінімум доходів громадян. На даний час неоподатковуваний мінімум доходів громадян**складає 17 грн.*

### Стаття 18831. Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України

Невиконання законних вимог посадових осіб органів Держспецзв'язку щодо усунення порушень законодавства про захист державних інформаційних ресурсів, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, та законодавства у сфері надання послуг ЕЦП, а також створення інших перешкод для виконання покладених на них обов'язків -

тягнуть за собою накладення штрафу на посадових осіб від 50 до 100 неоподатковуваних мінімумів доходів громадян.

Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, -

тягнуть за собою накладення штрафу на посадових осіб від 100 до 150 неоподатковуваних мінімумів доходів громадян.

### Стаття 2122. Порушення законодавства про державну таємницю

Порушення законодавства про державну таємницю, а саме:

9) невиконання норм і вимог захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності, -

тягне за собою накладення штрафу на громадян від десяти до тридцяти неоподатковуваних мінімумів доходів громадян і на посадових осіб – від 30 до 100 неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення з числа передбачених частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню[, -](http://search.ligazakon.ua/l_doc2.nsf/link1/T991080.html)

тягне за собою накладення штрафу на громадян від 30 до 80 неоподатковуваних мінімумів доходів громадян і на посадових осіб - від 50 до 150 неоподатковуваних мінімумів доходів громадян.

**2. Органи Служби безпеки України** -стаття 164 (у частині, що стосується правопорушень у галузі господарської діяльності, ліцензії на проведення якої видає ця Служба), статті 1724-1729, 1955, 2122 (крім пункту 9 частини першої), 2125 і 2126.

### Стаття 2122. Порушення законодавства про державну таємницю

Порушення законодавства про державну таємницю, а саме:

1) недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

2) засекречування інформації:

- про стан довкілля, про якість харчових продуктів і предметів побуту;

- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися та загрожують безпеці громадян;

- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти та культури населення;

- про факти порушень прав і свобод людини і громадянина;

- про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових осіб;

- іншої інформації, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена;

3) безпідставне засекречування інформації;

4) надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненадання грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;

5) порушення встановленого законодавством порядку надання допуску та доступу до державної таємниці;

6) невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;

7) провадження діяльності, пов'язаної з державною таємницею, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов'язаних з державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

8) недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведення роботи з ними.

**Стаття 2126. Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем**

Здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах[, -](http://search.ligazakon.ua/l_doc2.nsf/link1/T041703.html)

тягне за собою накладення штрафу від 5 до 10 неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу, або без такої.

Та сама дія, вчинена особою, яку протягом року було піддано адміністративному стягненню за порушення, передбачене в частині першій цієї статті, -

тягне за собою накладення штрафу від 10 до 20 неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу.

Дія, передбачена частиною першою цієї статті, вчинена стосовно інформаційних (автоматизованих) систем, призначених для зберігання та обробки інформації з обмеженим доступом, -

тягне за собою накладення штрафу від 30 до 100 неоподатковуваних мінімумів доходів громадян з конфіскацією програмних або технічних засобів, що використовувалися для незаконного доступу.

Незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі -

тягне за собою накладення штрафу від 10 до 25 неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно виготовлених копій баз даних.

Безоплатне незаконне розповсюдження інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі -

тягне за собою накладення штрафу від 5 до 20 неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно розповсюджених чи призначених для розповсюдження копій баз даних.

Незаконний збут інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі -

тягне за собою накладення штрафу від 20 до 100 неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно збутих чи призначених для збуту копій баз даних, а також грошей, отриманих від їх продажу.

**Кримінальний кодекс України**

**Розділ XVI. Злочини у сфері використання ЕОМ (комп’ютерів),**

**систем та комп’ютерних мереж і мереж електрозв’язку**

**Стаття 361. Несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку**

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, -

карається штрафом від 600 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від 2 до 5 років, або позбавленням волі на строк до 3 років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 2 років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від 3 до 6 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

***Примітка.*** *Значною шкодою у статтях 361-3631, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.*

**Стаття 3611. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут**

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -

караються штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до 2 років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк до 5 років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

**Стаття 3612. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації**

1. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, -

караються штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до 2 років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від 2 до 5 років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

**Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї**

1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, -

караються штрафом від 600 до 1000 неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до 2 років з конфіскацією програмних або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, -

караються позбавленням волі на строк до 3 років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк від 3 до 6 років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до 3 років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

**Стаття 363. Порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється**

Порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, -

караються штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до 3 років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

**Стаття 3631. Перешкоджання роботі ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку**

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -

карається штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до 3 років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, -

караються обмеженням волі на строк до 5 років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до 3 років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, які є власністю винної особи.

**Стаття 3761. Незаконне втручання в роботу автоматизованої системи документообігу суду**

1. Умисне внесення неправдивих відомостей чи несвоєчасне внесення відомостей до автоматизованої системи документообігу суду, несанкціоновані дії з інформацією, що міститься в автоматизованій системі документообігу суду, чи інше втручання в роботу автоматизованої системи документообігу суду, вчинене службовою особою, яка має право доступу до цієї системи, або іншою особою шляхом несанкціонованого доступу до автоматизованої системи документообігу суду, -

караються штрафом від 600 до 1000 неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від 2 до 5 років, або позбавленням волі на строк до 3 років, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк від 1 до 3 років.

2. Дії, передбачені частиною першою цієї статті, вчинені за попередньою змовою групою осіб, -

караються обмеженням волі на строк від 3 до 5 років або позбавленням волі на строк від 3 до 6 років, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк від 2 до 3 років.

На даний час при вчиненні громадянами України, іноземцями, особами без громадянства адміністративних правопорушень, передбачених статтею 18831 та пунктом 9 статті 2122 КупАПспівробітники Держспецзв'язку мають право складати адмінпротокол згідно вимог «**Інструкції про порядок оформлення та складання Державною службою спеціального зв'язку та захисту інформації України матеріалів про адміністративні правопорушення**», затвердженої наказом Адміністрації Держспецзв'язку від 29.05.2007 № 100, зареєстрованим в Міністерстві юстиції України 12.06.2007 за № 618/13885. Після складання протокол надходить до суду, де він розглядається та виноситься відповідна постанова.

**Рекомендована література**

**1. Закони України**

Про інформацію

Про доступ до публічної інформації

Про захист інформації в інформаційно-телекомунікаційних системах

Про захист персональних даних

Про електронні документи та електронний документообіг

Проелектронний цифровий підпис

**2. Державні стандарти України та Росії**

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

ДСТУ 2851-94 Програмні засоби ЕОМ. Документування результатів випробувань

ДСТУ 2853-94 Програмні засоби ЕОМ. Підготовлення і проведення випробувань

ДСТУ 3396 0-96 Технічний захист інформації. Основні положення.

ДСТУ 3396 1-96 Технічний захист інформації. Порядок проведення робіт.

ДСТУ 3396.2-97 Технічний захист інформації. Терміни та визначення.

ГОСТ 34.201-89 Виды, комплектность и обозначение документов при создании автоматизированых систем

РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов

**3. Укази Президента України**

Положення про технічний захист інформації в Україні, затверджене УП України від 27.09.99 № 1229/99 із останніми змінами згідно УП України від 11.04.2008 № 333/2008

**4. Постанови Кабінету Міністрів України**

Концепція технічного захисту інформації в Україні, затверджена постановою КМ України від 08.10.97 № 1126 із останніми змінами згідно постанови КМ України від 07.09.2011 № 938

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМ України від 29.03.2006 № 373 із останніми змінами згідно постанови КМ України від 07.09.2011 № 938

Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, затверджена постановою КМ України від 27.11.98 № 1893 із останніми змінами згідно постанови КМ України від 20.10.2011 № 1109

Перелік послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню, затверджений постановою КМ України від 18.05.2011 № 517

Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу, затверджений постановою КМ України від 26.05.2004 № 680 із останніми змінами згідно постанови КМ України від 27.05.2013 № 371

Порядок застосування електронного цифрового підпису органами державної влади, рганами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності, затверджений постановою КМ України від 28.10.2004 № 1452 із останніми змінами згідно постанови КМ України від 05.10.2011 № 1022

Порядок обов'язкової передачі документованої інформації, затверджений постановою КМ України від 28.10.2004 № 1454 із змінами згідно постанови КМ України від 02.11.2011 № 1122

Типовий порядок здійснення електронного документообігу в органах виконавчої влади, затверджений постановою КМ України від 28.10.2004 № 1453 із змінами згідно постанови КМ України від 08.12.2006 № 1700

Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, затверджене постановою КМ України від 03.08.2005 № 688 із останніми змінами згідно постанови КМ України від 07.09.2011 № 938

Порядок підключення до глобальних мереж передачі даних, затверджений постановою КМ України від 12.04.2002 № 522

**5. Накази Адміністрації Держспецзв’язку**

Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб, затверджений наказом ДСТСЗІ СБ України від 23.02.2002 № 9 і зареєстрований в Міністерстві юстиції України 13.03.2002 за №245/6533

Положення про державну експертизу в сфері технічного захисту інформації, затверджений наказом Адміністрації Держспецзв’язку від 16.05.2007 № 93, зареєстрований в Міністерстві юстиції України 16.07.2007 за № 820/14087, із змінами, затвердженими наказом Адміністрації Держспецзв’язку від 10.10.2012 № 56, зареєстрованим в Міністерстві юстиції України 06.11.2012 за № 1863/22175

Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, затверджений наказом Адміністрації Держспецзв’язку від 26.03.2007 № 45, зареєстрований в Міністерстві юстиції України 10.04.2007 за № 320/13587

Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Наказ від Наказ від 02.12.2014 № 660, зареєстрований в Мін’юсті 28.01.2015 за № № 90/26535

Перелік адміністративних послуг, які безоплатно надаються Адміністрацією Держспецзв'язку», затверджений наказом Адміністрації Держспецзв'язку від 29.11.2011 № 350, зареєстрований в Міністерстві юстиції України 15.12.2011 за № 1455/20193

Стандарт надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС, затверджений наказом Адміністрації Держспецзв'язку від 19.03.2009 № 64

Порядок формування й користування інформаційним фондом Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, затверджений наказом Адміністрації Держспецзв’язку від 24.04.2007 № 72, зареєстрований в Міністерстві юстиції України 14.05.2007 за № 500/13767

Положення про державний контроль за станом ТЗІ, затверджений наказом Адміністрації Держспецзв'язку від 16.05.2007 № 87, зареєстрований в Міністерстві юстиції України 10.07.2007 за № 785/14052,з останніми змінами згідно наказу Адміністрації від 20.05.2013 № 275, зареєстрованого в Міністерстві юстиції України04.06.2013 за № 876/23408

**6. Нормативні документи системи ТЗІ**

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу

НД ТЗІ 1.1-005-2007 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення (із змінами згідно наказу Адміністрації Держспецзв’язку від 03.11.2011 № 93/ДСК)

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806)

НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці

НД ТЗІ 2.1-002-2007 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806)

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від НСД (зі зміною № 1)

НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від НСД під час оброблення в автоматизованих системах класу «2» (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806)

НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806)

НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів ТЗІ від НСД та КСЗІ в ІТС (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806)

НД ТЗІ 2.7-009-2009 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806)

НД ТЗІ 2.7-010-2009 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

НД ТЗІ 3.1-001-2007 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Передпроектні роботи

НД ТЗІ 3.3-001-2007 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Порядок розроблення та впровадження заходів із захисту інформації

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів ТЗІ від НСД (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806)

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806)

НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806)