

ОНАЦЬКИЙ О.В.

Комплексні системи захисту інформації





ІНФОРМАЦІЙНО-ДОВІДКОВІ МАТЕРІАЛИ ДО ЛЕКЦІЙ
ОК-24 Комплексні системи захисту інформації
Спеціальності 125 Кібербезпека та захист інформації
МГУ, 2025

№	Теми лекцій	Кількість годин	
		денна форма навчання	заочна форма навчання
1	Нормативно-правове забезпечення захисту інформації	2	2
2	Етапи створення КСЗІ. Порядок проведення робіт із створення КСЗІ в ІКС. Формування вимог до КСЗІ	4	
3	Обґрунтування необхідності створення КСЗІ. Категоріювання ІКС.	4	
4	Обстеження середовищ функціонування ІКС. Опис моделі порушника політики безпеки інформації. Опис моделі загроз для інформації.	4	2
5	Формування завдання на створення КСЗІ. Розробка політики безпеки інформації в ІКС	4	
6	Розробка технічного завдання на створення КСЗІ. Розробка проекту КСЗІ	4	
7	Введення КСЗІ в дію та оцінка захищеності інформації в ІКС. Супровід КСЗІ	4	2
Усього годин:		26	6





Тема 1

Нормативно-правове забезпечення захисту інформації

Питання захисту інформації в Україні регламентує низка законів і нормативних актів. Наведемо деякі з них.

Закон України «Про інформацію»

У цьому Законі наведені нижче терміни вживаються в такому значенні:

документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Стаття 9. Основні види інформаційної діяльності

1. Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, **охорона та захист інформації**.

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 (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.

Стаття 10. Види інформації за змістом

За змістом інформація поділяється на такі види:

- **інформація про фізичну особу;**

- інформація довідково-енциклопедичного характеру;

- інформація про стан довкілля (екологічна інформація);

- інформація про товар (роботу, послугу);

- науково-технічна інформація;

- податкова інформація;
 - правова інформація;
 - статистична інформація;
 - соціологічна інформація;
 - **критична технологічна інформація;**
- інші види інформації.

Стаття 11. Інформація про фізичну особу

1. **Інформація про фізичну особу (персональні дані)** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

2. **Конфіденційною є інформація про фізичну особу,** інформація, доступ до якої обмежено фізичною або юридичною особою.... Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

Закон України «Про доступ до публічної інформації»

Стаття 6. Публічна інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є:

- 1) **конфіденційна інформація;**
- 2) **таємна інформація;**
- 3) **службова інформація.**

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 внутрішню службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напрямку

діяльності установи або здійсненню контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідальної 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 державну таємницю»

У цьому Законі терміни вживаються у такому значенні:

державна таємниця (секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;

допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації;

доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;

Звід відомостей, що становлять державну таємницю – акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах;

ступінь секретності ("особливої важливості", "цілком таємно", "таємно") – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

Стаття 13. Строк дії рішення про віднесення інформації до державної таємниці

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. Він не може перевищувати для

інформації із ступенем секретності **"особливої важливості"** - **30 років**, для інформації **"цілком таємно"** - **10 років**, для інформації **"таємно"** - **5 років**.

Стаття 21. Режимно-секретні органи

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх дотриманням створюються на правах окремих структурних підрозділів **режимно-секретні органи (РСО)**, які підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства, установи, організації.

Закон України «Про захист персональних даних»

У цьому Законі терміни вживаються у такому значенні:

персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем;

база персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.

Стаття 5. Об'єкти захисту

1. **Об'єктами захисту є персональні дані.**

2. **Персональні дані можуть бути віднесені до конфіденційної інформації** про особу законом або відповідною особою.

Стаття 6. Загальні вимоги до обробки персональних даних

6. **Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди**, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Закон України «Про захист інформації в інформаційно-комунікаційних системах»

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

інформаційно- комунікаційна система - сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

захист інформації в системі - діяльність, спрямована на запобігання порушенню цілісності, конфіденційності і доступності інформації в системі;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно- технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації;

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

комплекс технічного захисту інформації - сукупність заходів, засобів технічного захисту інформації, призначених для захисту інформації від витоку технічними каналами в інформаційних, електронних комунікаційних та інформаційно- комунікаційних системах;

авторизована система з безпеки - інформаційна, електронна комунікаційна, інформаційно- комунікаційна, технологічна система або її окремі елементи, об'єкт критичної інформаційної інфраструктури, в яких запроваджені заходи та/або системи з безпеки інформації, що пройшли авторизацію з безпеки.

Стаття 8. Умови обробки інформації в системі

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, у системах, об'єктах критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, **мають оброблятися в авторизованих системах з безпеки** або шляхом отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності.

Концепція технічного захисту інформації в Україні

Концепція визначає поняття **технічного захисту інформації** таким чином: це діяльність, спрямована на забезпечення інженерно- технічними заходами конфіденційності, цілісності та доступності важливої для держави, суспільства і особи інформації.

Концепція визначає також такі терміни:

конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;

цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

доступність – властивість інформації бути захищеною від несанкціонованого блокування;

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

Основні законодавчі акти, що регулюють **захист критичної інфраструктури**:

1. Закон України «Про критичну інфраструктуру»;
2. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури» (в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1384);
3. Постанова Кабінету Міністрів України від 22 липня 2022 р. № 821 «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури»;
4. Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1174 «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури»;
5. Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1175 «Деякі питання подання інформації у сфері захисту критичної інфраструктури»;
6. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури».

Закон України «Про критичну інфраструктуру»

Стаття 19¹. Критична технологічна інформація

1. Критична технологічна інформація - дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об'єктів критичної інфраструктури.

3. Критична технологічна інформація за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту згідно із законом.

Стаття 9. Сектори критичної інфраструктури

4. До життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема:

- 1) урядування та надання найважливіших публічних (адміністративних) послуг;
- 2) енергозабезпечення (у тому числі постачання теплової енергії);
- 3) водопостачання та водовідведення;
- 4) продовольче забезпечення;
- 5) охорона здоров'я;

- 6) фармацевтична промисловість;
- 7) виготовлення вакцин, сталі функціонування біолабораторій;
- 8) інформаційні послуги;
- 9) електронні комунікації;
- 10) фінансові послуги;
- 11) транспортне забезпечення;
- 12) оборона, державна безпека;
- 13) правопорядок, здійснення правосуддя, тримання під вартою;
- 14) цивільний захист населення та територій, служби порятунку;
- 15) космічна діяльність, космічні технології та послуги;
- 16) хімічна промисловість;
- 17) дослідницька діяльність.

Стаття 10. Категоризація об'єктів критичної інфраструктури

1. Для визначення рівня вимог щодо забезпечення захисту об'єктів критичної інфраструктури відповідно до рівня їх важливості для забезпечення окремих життєво важливих функцій у межах секторів критичної інфраструктури здійснюється **категоризація об'єктів критичної інфраструктури** відповідно до категорій критичності, визначених цим Законом.

2. Установлюються такі категорії критичності об'єктів критичної інфраструктури:

- 1) I категорія критичності - особливо важливі об'єкти, **державного значення**;
- 2) II категорія критичності - життєво важливі об'єкти, **регіонального значення**;
- 3) III категорія критичності - важливі об'єкти, **місцевого значення**;
- 4) IV категорія критичності - необхідні об'єкти, **локального значення**.

Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури

VI. Категорія критичності об'єкта критичної інфраструктури

1. Категорія критичності об'єкта критичної інфраструктури визначається за такою процедурою:

1) робоча група ідентифікує всі об'єкти критичної інфраструктури свого сектору (підсектору) критичної інфраструктури згідно Порядку (постанова КМУ № 1109 від 2020 р.);

2) робоча група відповідно до Порядку для кожного об'єкта свого сектору (підсектору) критичної інфраструктури визначає, які основні послуги надає цей об'єкт;

3) робоча група разом з оператором критичної інфраструктури проводить **оцінку критичності об'єкта** критичної інфраструктури, використовуючи секторальні та міжсекторальні критерії визначення рівня негативного впливу.

5. Розраховується узагальнена нормована **оцінка рівня критичності** за такою формулою:

$$PK_{OKI} = \frac{\sum PK_i}{\sum PK_{max}},$$

PK_{OKI} – узагальнена нормована оцінка рівня критичності об'єкта критичної інфраструктури;

PK_i – сума балів, які отримав об'єкт критичної інфраструктури за всіма критеріями критичності;

PK_{max} – максимальна можлива сума балів (розраховується, виходячи з того, що об'єкт отримує максимальні бали за всіма критеріями оцінки рівня негативного впливу).

6. Рішення щодо категорії критичності об'єкта критичної інфраструктури приймається на основі узагальненої нормованої оцінки рівня критичності об'єкта критичної інфраструктури відповідно до такого правила:

I категорія критичності,	якщо $0,8 < PK_{OKI} \leq 1;$
II категорія критичності,	якщо $0,63 < PK_{OKI} \leq 0,8;$
III категорія критичності,	якщо $0,37 < PK_{OKI} \leq 0,63;$
IV категорія критичності,	якщо $0,2 < PK_{OKI} \leq 0,37;$
об'єкт не є критичним,	якщо $PK_{OKI} \leq 0,2.$

Крім законів і підзаконних актів впроваджено багато нормативних документів, які регламентують певні аспекти діяльності у сфері захисту інформації. Нижче наведено низку нормативних документів системи технічного захисту інформації (НД ТЗІ), які безпосередньо стосуються питань захисту інформації.

НД ТЗІ 1.1-003-99 Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу

НД ТЗІ 2.5-004-99 Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

НД ТЗІ 3.7-001-99 Методичні вказівки з розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу

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 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно- телекомунікаційних системах

НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі

НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно- комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці

НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації

НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

НД ТЗІ 3.6-007-21 Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

НД ТЗІ 2.3-025-24 Т1 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

НД ТЗІ 2.3-025-24 Т2 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

НД ТЗІ 2.3-025-24 Т3 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

НД ТЗІ 2.6-004-21 Порядок авторизації безпеки інформаційних систем

НД ТЗІ 3.6-008-21 Порядок моніторингу безпеки інформаційних систем

Положення документів обов'язкові до виконання всіма суб'єктами системи ТЗІ в Україні незалежно від їхньої організаційно- правової форми та форми власності, в ІКС яких обробляється інформація, що є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІКС обробляються інші види інформації, вимоги нормативних документів системи ТЗІ можна використовувати як рекомендації.

Також зазначимо **Положення про державну експертизу в сфері технічного захисту інформації**, затверджене наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93 та зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087.

4. Об'єктами експертизи є:

комплексні системи захисту інформації (КСЗІ), які є невід'ємною складовою інформаційної, електронної комунікаційної або інформаційно- комунікаційної системи (далі - ІКС);

апаратні, апаратно-програмні і програмні засоби, які реалізують функції ТЗІ та/або оцінки стану захисту інформації;

організаційно-технічне рішення (ОТР) для впровадження типової компоненти КСЗІ в ІКС - задокументоване уніфіковане рішення для багаторазового розгортання складових КСЗІ в ІКС, самодостатнє для вирішення певного завдання, що містить проектні рішення програмно- технічного комплексу, організаційно- технічні рішення щодо регламенту функціонування типової компоненти ІКС та опис (алгоритм) процедури впровадження (розгортання) компоненти КСЗІ в ІКС.

29. **Строк дії атестата відповідності** КСЗІ, експертного висновку на засіб ТЗІ або ОТР КСЗІ визначає Організатор:

для атестата відповідності КСЗІ автоматизованої системи класу 1 - безстроковий;

для атестата відповідності КСЗІ автоматизованої системи класів 2, 3 - до 5 років;

для експертного висновку на засіб ТЗІ - до 3 років;

для експертного висновку на ОТР КСЗІ - до 5 років.

Міжнародні стандарти

Міжнародний стандарт ISO/IEC 15408, відомий як «Загальні критерії» (Common Criteria), в Україні прийнято як національний стандарт **ДСТУ ISO/IEC 15408** (зокрема версія 2023 року). Він є

основою для оцінки безпеки ІТ- продукції, визначаючи функціональні вимоги та вимоги довіри, що дозволяє сертифікувати продукти на відповідність міжнародним стандартам. Впровадження ISO/IEC 15408 у формі ДСТУ є важливим кроком для безпеки критичної інфраструктури та сертифікації ІТ- рішень в Україні.

Ключові аспекти ДСТУ ISO/IEC 15408 в Україні:

Прийняття. Україна впроваджує стандарти ISO/IEC 15408 для гармонізації національної системи технічного захисту інформації з міжнародними вимогами, зокрема через оновлення стандартів, розроблених за участю Держспецзв'язку.

Структура (ДСТУ ISO/IEC 15408-1):

Частина 1: Вступ та загальна модель.

Частина 2: Функціональні вимоги безпеки.

Частина 3: Вимоги довіри безпеки (оцінка процесу розробки та функціонування).

Сертифікація. Стандарт використовується для оцінки того, чи задовольняє продукт заявленим вимогам безпеки. Профілі захисту (Protection Profiles) та Завдання з безпеки (Security Targets) є ключовими документами, що базуються на цьому стандарті.

Мета. Підвищення довіри до засобів захисту інформації, забезпечення сумісності ІТ- продуктів на міжнародному ринку та створення національної системи кібербезпеки.

CCRA (Common Criteria Recognition Arrangement): Україна активно працює над приєднанням до Угоди про визнання загальних критеріїв (CCRA), що дозволить взаємно визнавати сертифікати безпеки, видані в Україні та інших країнах- учасниках. Це є дуже важливим кроком для фахівців в області інформаційної безпеки, які сьогодні не можуть обійтися без знань відповідних стандартів.

ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ (ISO/IEC 18045:2008, IDT).

ДСТУ ISO/IEC 15408- 1:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408- 1:2009, IDT)»,

ДСТУ ISO/IEC 15408- 2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408- 2:2008, IDT),

ДСТУ ISO/IEC 15408- 3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408- 3:2008, IDT).

ДОДАТКОВО

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»

У цьому Законі наведені нижче терміни:

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;

об'єкт інформаційної діяльності - інженерно-технічна споруда (приміщення), транспортний засіб, де провадиться діяльність, пов'язана з державними інформаційними ресурсами та інформацією, вимога щодо захисту якої встановлена законом;

система технічного захисту інформації - сукупність суб'єктів, що провадять діяльність у сфері технічного захисту інформації, нормативно-правових актів, що регулюють їх діяльність, а також матеріально-технічної бази у цій сфері;

спеціальна інформаційно-комунікаційна система - інформаційно-комунікаційна система, яка забезпечує обробку інформації, що становить державну таємницю, та іншої інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, із застосуванням технічних засобів електронних комунікацій і засобів криптографічного захисту інформації;

засіб технічного захисту інформації - технічний або програмний засіб, у якому передбачено функції технічного захисту інформації або який спеціально розроблений для пошуку закладних пристроїв або контролю за ефективністю технічного захисту інформації;

засіб криптографічного захисту інформації - програмний, апаратно-програмний та апаратний засіб, призначений для криптографічного захисту інформації;

верифікація - комплекс заходів щодо перевірки відповідності програмних і технічних засобів вимогам, встановленим нормативними документами.



Тема 2

Етапи створення КСЗІ.
Порядок проведення робіт із
створення КСЗІ в ІКС.
Формування вимог до КСЗІ

Порядок проведення робіт із створення КСЗІ в ІКС.

НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі. Цей документ визначає основи організації та порядок виконання робіт із захисту інформації в інформаційно-комунікаційних системах (ІКС) – порядок прийняття рішень щодо складу комплексної системи захисту інформації залежно від умов функціонування ІКС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Дія цього нормативного документа системи технічного захисту інформації (НД ТЗІ) поширюється тільки на ІКС, в яких здійснюється обробка інформації автоматизованим способом. Отже, для таких ІКС чинні всі нормативно-правові акти та нормативні документи щодо створення автоматизованих систем (АС) та щодо захисту інформації в АС. НД ТЗІ не встановлює нових норм, а систематизує в одному документі вимоги, норми і правила, які безпосередньо або непрямым чином впливають з положень чинних нормативних документів.

НД ТЗІ 3.7-003-2023 призначено для суб'єктів інформаційних відносин (власників або розпорядників ІКС, користувачів), діяльність яких пов'язана з обробкою інформації, що підлягає захисту, розробників комплексних систем захисту інформації в ІКС, для постачальників компонентів ІКС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації щодо відповідності вимогам технічного захисту інформації (ТЗІ). Встановлений цим НД ТЗІ 3.7-003-2023 порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІКС яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІКС обробляються інші види інформації, то вимоги цього нормативного

документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

У цьому НД ТЗІ 3.7-003-2023 подано терміни та визначення:

інформаційна система - організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;

комунікаційна 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;

інтегрована система - сукупність двох або кількох взаємопов'язаних інформаційних та (або) комунікаційних систем, в якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Під **інформаційно-комунікаційною системою** в цьому НД ТЗІ слід розуміти будь-яка систему, яка відповідає одному з трьох наведених вище видів автоматизованих систем.

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

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

Порядок створення КСЗІ в ІКС розглядається цим НД як сукупність впорядкованих у часі, взаємопов'язаних, об'єднаних в окремі етапи робіт, виконання яких необхідне й достатнє для КСЗІ, що створюється. Послідовність виконання та типовий зміст робіт кожного з етапів створення КСЗІ повинні узгоджуватися з відповідними стадіями і етапами робіт зі створення ІКС, викладеними у розділі 6 НД ТЗІ 3.7-003-2023.

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

- витоку технічними каналами, до яких належать 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 та інше;

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

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

У випадках, визначених законодавством, роботи з проектування, розроблення, виготовлення, випробування, експлуатації ІКС мають виконуватися 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. Створення комплексів технічного захисту інформації від витoku технічними каналами здійснюється, якщо в ІКС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

Створення комплекс засобів захисту (КЗЗ) від несанкціонованого доступу (НСД) здійснюється в усіх ІКС, де обробляється інформація, що є власністю держави, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІКС, 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) ІКС з дотриманням вимог нормативно- правових актів щодо провадження діяльності у сфері захисту інформації. Якщо для створення КСЗІ необхідно виконувати декілька різних видів робіт, які підлягають ліцензуванню в межах господарської діяльності (отримання дозволу) з ТЗІ, то розробник КСЗІ повинен мати право на провадження хоча б одного з таких видів робіт. До виконання робіт, на провадження яких розробник КСЗІ не має ліцензії (дозволу), залучаються співвиконавці, які мають відповідні ліцензії.

Етапи створення КСЗІ.

Етапи робіт, які виконуються під час створення КСЗІ в конкретній ІКС, їх зміст та результати, терміни виконання визначаються ТЗ на створення КСЗІ на підставі цього НД. Дозволяється виключати окремі етапи робіт або поєднувати декілька етапів, а також вводити нові етапи робіт. У разі потреби дозволяється змінювати послідовність виконання окремих етапів - виконувати одночасно декілька етапів

робіт, окремі етапи виконувати до завершення попередніх тощо, якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання. При цьому зміст етапів має передбачати виконання всіх основних робіт, встановлених ДСТУ 3396.1-96 визначення й оцінка загроз для інформації, формування вимог, розроблення й реалізація проекту КСЗІ, проведення випробувань КСЗІ та введення її в експлуатацію в складі ІКС. Якщо у галузі впроваджені в установленому порядку і діють НД ТЗІ відомчого рівня або існують відповідні нормативні документи, чинність яких поширюється на організацію-власника ІКС або саму ІКС, то вони мають вищу силу і в першу чергу необхідно керуватися ними. Якщо певний вид робіт не нормовано національною нормативною базою з ТЗІ будь-якого з наведених рівнів, то допускається використання рекомендацій міжнародних стандартів в частині, що не суперечить нормативно-правовим актам та нормативним документам України.

НД ТЗІ 3.7-003-2023 визначає такі **етапи створення КСЗІ** та її документів:

1. Формування вимог до КСЗІ в ІКС

- 1.1. Обґрунтування необхідності створення КСЗІ і призначення СЗІ
- 1.2. Категорювання ІКС
- 1.3. Обстеження середовищ функціонування ІКС
- 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 ІКС

- 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

4. Розробка проекту КСЗІ

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

- 5.1. Підготовка КСЗІ до введення в дію:
- 5.2. Навчання користувачів:
- 5.3. Комплектування КСЗІ
- 5.4. Будівельно-монтажні роботи:
- 5.5. Пуско-налагоджувальні роботи:
- 5.6. Попередні випробування КСЗІ:
- 5.7. Дослідна експлуатація КСЗІ:
- 5.8. Державна експертиза КСЗІ:

6. Супровід КСЗІ

Формування вимог до КСЗІ в ІКС.

Прийняття рішень про створення КСЗІ і служби захисту інформації в ІКС. 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.

Для організації робіт зі створення КСЗІ в ІКС створюється служба захисту інформації (СЗІ), порядок створення, завдання, функції, структура та повноваження якої визначено в НД ТЗІ 1.4-001-2000. СЗІ створюється після прийняття рішення про необхідність створення КСЗІ.

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

Положення повинно складатись з таких розділів:

- загальні положення;
- завдання СЗІ;
- функції СЗІ;
- повноваження та відповідальність СЗІ;
- взаємодія СЗІ з іншими підрозділами організації та зовнішніми підприємствами, установами, організаціями;
- штатний розклад та структура СЗІ;
- 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 ін. 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).

Положення про службу захисту інформації в ІКС.

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 (СЗІ) - «Положення про СЗІ в ІКС».

В загальному випадку Положення повинно складатись з таких розділів:

- загальні положення;
- завдання служби захисту інформації;
- функції служби захисту інформації;
- повноваження і відповідальність служби захисту інформації;
- взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми підприємствами, установами, організаціями;
- штатний розклад та структура служби захисту інформації;
- організація робіт служби захисту інформації;
- фінансування служби захисту інформації.

В залежності від конкретних завдань і умов функціонування служби захисту інформації 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.

У 1-му розділі «Загальні положення» викладаються правові та організаційні питання:

1. Положення є нормативним документом організації та визначає завдання, функції, штатну структуру СЗІ, повноваження та відповідальність співробітників служби, взаємодію з іншими підрозділами організації та зовнішніми організаціями.

2. СЗІ є штатним або позаштатним підрозділом організації. СЗІ є самостійним структурним підрозділом з безпосередньою підпорядкованістю керівнику організації або структурною одиницею іншого підрозділу (РСО, ТЗІ, служби безпеки) організації.

В організаціях, де штатним розкладом не передбачено створення СЗІ, заходи щодо забезпечення захисту інформації в ІКС здійснюють призначені наказом керівника організації окремі працівники. У цьому випадку посадові (функціональні) обов'язки цих працівників повинні

включати положення, які б передбачали виконання ними вимог щодо діяльності СЗІ.

3. Метою створення СЗІ є організаційне забезпечення завдань керування КСЗІ в ІКС та здійснення контролю за її функціонуванням. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в ІКС, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в ІКС.

4. Правову основу для створення і діяльності СЗІ становлять Закон України «Про захист інформації в ІКС», «Правила забезпечення захисту інформації в ІКС», НД ТЗІ і накази Адміністрації Держспецзв'язку.

5. СЗІ у своїй діяльності керується Конституцією України, законами України, нормативно-правовими актами Президента України і Кабінету Міністрів України, іншими нормативно-правовими актами з питань захисту інформації, державними і галузевими стандартами, розпорядчими та іншими документами організації, а також цим Положенням. СЗІ здійснює діяльність відповідно до «Плану захисту інформації в ІКС», календарних, перспективних та інших планів робіт, затверджених керівником організації.

6. Для проведення окремих заходів з захисту інформації в АС, які пов'язані з напрямком діяльності інших підрозділів організації, керівник організації своїм наказом визначає перелік, строки виконання та підрозділи для виконання цих робіт.

7. У своїй роботі СЗІ взаємодіє з підрозділами організації (РСО, ТЗІ, служби безпеки), а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

У разі потреби, до виконання робіт можуть залучатися зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації.

У 2-му розділі «Завдання СЗІ» наводиться перелік таких завдань СЗІ:

- захист законних прав щодо безпеки інформації організації, окремих її структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах з зовнішніми вітчизняними і закордонними організаціями;

- дослідження технології обробки інформації в ІКС з метою виявлення можливих каналів витоку та інших загроз для безпеки інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;

- організація та координація робіт, пов'язаних з захистом інформації в ІКС, необхідність захисту якої визначається її власником

або чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

- розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими повинен забезпечуватися захист інформації в ІКС;

- організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу ІКС;

- участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів ІКС з питань захисту інформації;

- формування у персоналу і користувачів розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;

- організація забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів з захисту інформації в ІКС та проведення контрольних перевірок їх виконання.

3-й розділ «Функції СЗІ» складається з 3-х таких підрозділів:

- функції під час створення КСЗІ;

- функції під час експлуатації КСЗІ;

- функції з організації навчання персоналу з питань забезпечення захисту інформації.

3.1. Функції під час створення КСЗІ:

- визначення переліків відомостей, які підлягають захисту в процесі обробки, інших об'єктів захисту в ІКС, класифікація інформації за вимогами до її конфіденційності або важливості для організації, необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформацією в ІКС;

- розробка та коригування моделі порушника безпеки інформації та моделі загроз для інформації, політики безпеки інформації та плану захисту інформації в ІКС;

- визначення і формування вимог до КСЗІ, організація і координація робіт з проектування та розробки КСЗІ, безпосередня участь у проектних роботах з створення КСЗІ;

- підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ;

- організація робіт і участь у випробуваннях КСЗІ, проведенні її експертизи;

- вибір організацій-виконавців робіт з створення КСЗІ, здійснення контролю за дотриманням встановленого порядку проведення робіт з захисту інформації, у взаємодії з підрозділом ТЗІ (РСО, службою

безпеки) погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт тощо);

- участь у розробці нормативних документів, чинних у межах організації і ІКС, які встановлюють дисциплінарну відповідальність за порушення вимог з безпеки інформації та встановлених правил експлуатації КСЗІ;

- участь у розробці нормативних документів, чинних у межах організації і ІКС, які встановлюють правила доступу користувачів до ресурсів ІКС, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій тощо).

3.2. Функції під час експлуатації КСЗІ:

- 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 ІКС, 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 ІКС (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 ІКС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;

- підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в АС, впровадження нових технологій захисту і модернізації КСЗІ;

- організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІКС або КСЗІ;

- участь в роботах з модернізації ІКС - узгодженні пропозицій з введення до складу ІКС 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 ІКС (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 ІКС і типові правила, встановлені для персоналу і користувачів ІКС;

- негайне втручання в процес роботи ІКС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;

- регулярне подання звітів керівництву організації- власника (розпорядника) АС про виконання користувачами ІКС вимог з захисту інформації;

- аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів для організації;

- контроль за виконанням персоналом і користувачами ІКС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації, у тому числі контроль за забезпеченням режиму секретності у разі обробки в ІКС інформації, що становить державну таємницю;

- контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;

- розробка і реалізація спільно з РСО (підрозділом ТЗІ, 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.

3.3. Функції з організації навчання персоналу з питань забезпечення захисту інформації:

- розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу ІКС;

- розроблення спеціальних програм навчання, які б враховували особливості технології обробки інформації в організації (ІКС), необхідний рівень її захищеності тощо;

- участь в організації і проведенні навчання користувачів і персоналу ІКС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;

- взаємодія з державними органами, учбовими закладами, іншими організаціями з питань навчання та підвищення кваліфікації;

- участь в організації забезпечення навчального процесу

необхідною матеріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою тощо.

4-й розділ «Повноваження та відповідальність СЗІ»
складається з 3-х таких підрозділів:

- права;
- обов'язки;
- відповідальність СЗІ.

4.1. СЗІ має право:

- здійснювати контроль за діяльністю будь-якого структурного підрозділу організації (ІКС) щодо виконання ним вимог нормативно-правових актів і нормативних документів з захисту інформації;

- подавати керівництву організації пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки, тощо у випадку виявлення порушень політики безпеки або у випадку виникнення реальної загрози порушення безпеки;

- складати і подавати керівництву організації акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;

- проводити службові розслідування у випадках виявлення порушень;

- отримувати доступ до робіт та документів структурних підрозділів організації (ІКС), необхідних для оцінки вжитих заходів з захисту інформації та підготовки пропозицій щодо їхнього подальшого удосконалення;

- готувати пропозиції щодо залучення на договірній основі до виконання робіт з захисту інформації інших організацій;

- готувати пропозиції щодо забезпечення ІКС (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації;

- виходити до керівництва організації з пропозиціями щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;

- узгоджувати умови включення до складу ІКС нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів АС;

- надавати висновки з питань, що належать до компетенції СЗІ, які необхідні для здійснення виробничої діяльності організації, особливо технологій, доступ до яких обмежено, інших проєктів, що потребують технічної підтримки з боку співробітників СЗІ;

- виходити до керівництва організації з пропозиціями щодо узгодження планів і регламенту відвідування ІКС сторонніми особами;

- інші права, які надані СЗІ у відповідності з специфікою та особливостями діяльності організації (ІКС).

4.2. СЗІ зобов'язана:

- організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів з захисту інформації в ІКС;

- вчасно і в повному обсязі доводити до користувачів і персоналу ІКС інформацію про зміни в галузі захисту інформації, які їх стосуються;

- перевіряти відповідність прийнятих в ІКС (організації) правил, інструкцій щодо обробки інформації, здійснювати контроль за виконанням цих вимог;

- здійснювати контрольні перевірки стану захищеності інформації в ІКС;

- забезпечувати конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в ІКС (організації);

- сприяти і, у разі необхідності, брати безпосередню участь у проведенні вищими органами перевірок стану захищеності інформації в ІКС;

- сприяти (технічними та організаційними заходами) створенню і дотриманню умов збереження інформації, отриманої організацією на договірних, контрактних або інших підставах від організацій-партнерів, постачальників, клієнтів та приватних осіб;

- періодично, не рідше одного разу на місяць, подавати керівництву організації звіт про стан захищеності інформації в ІКС і дотримання користувачами та персоналом АС встановленого порядку і правил захисту інформації;

- негайно повідомляти керівництво ІКС (організації) про виявлені атаки та викритих порушників;

- інші обов'язки, покладені на керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності ІКС (організації).

4.3. Відповідальність

1. Керівництво та співробітники СЗІ за невиконання або неналежне виконання службових обов'язків, допущені ними порушення встановленого порядку захисту інформації в ІКС несуть дисциплінарну, адміністративну, цивільно-правову, кримінальну відповідальність згідно з законодавством України.

Персональна відповідальність керівника та співробітників СЗІ визначається посадовими (функціональними) інструкціями.

2. Відповідальність за діяльність СЗІ покладається на її

керівника, який відповідає за:

- організацію робіт з захисту інформації в ІКС, ефективність захисту інформації відповідно до діючих нормативно-правових актів;

- своєчасне розроблення і виконання «Плану захисту інформації в ІКС»;

- якісне виконання співробітниками СЗІ завдань, функцій та обов'язків, зазначених у цьому Положенні, посадових інструкціях, а також планових заходів з захисту інформації, затверджених керівником організації;

- координацію планів діяльності підрозділів та служб ІКС (організації) з питань захисту інформації;

- створення системи навчання співробітників, користувачів, персоналу ІКС з питань захисту інформації;

- виконання особисто та співробітниками СЗІ розпоряджень керівника організації, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

3. Співробітники СЗІ відповідають за:

- додержання вимог нормативних документів, що визначають порядок організації робіт з захисту інформації, інформаційних ресурсів та технологій;

- повноту та якість розроблення і впровадження організаційно-технічних заходів з захисту інформації в ІКС, точність та достовірність отриманих результатів і висновків з питань, що належать до компетенції СЗІ;

- дотримання термінів проведення контрольних, інспекційних, перевірочних та інших заходів з оцінки стану захищеності інформації в ІКС, які включені до плану робіт СЗІ;

- якість та правомірність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок;

- інші питання персональної відповідальності, які покладені на керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності ІКС (організації).

У 5-му розділі «Взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми організаціями» викладаються такі питання:

1. СЗІ здійснює свою діяльність у взаємодії з науковими, виробничими та іншими організаціями, державними органами та установами, що займаються питаннями захисту інформації.

2. Заходи щодо захисту інформації в ІКС повинні бути узгоджені СЗІ з заходами охоронної та режимно-секретної діяльності інших підрозділів організації.

СЗІ взаємодіє, узгоджує свою діяльність та встановлює зв'язки з:

- РСО організації;
- підрозділом ТЗІ організації;
- підрозділом інформаційних технологій та іншими підрозділами організації, виробнича діяльність яких пов'язана з захистом інформації або її автоматизованою обробкою;
- службою безпеки організації;
- зовнішніми організаціями, які є партнерами, користувачами, постачальниками, виконавцями робіт;
- підрозділами служб безпеки іноземних фірм (що є для організації партнерами, користувачами, постачальниками, виконавцями робіт), їхніми представництвами (на договірних або інших засадах);
- іншими суб'єктами діяльності у сфері захисту інформації.

3. СЗІ координує свою діяльність з регіональним органом Держспецзв'язку під час проведення перевірок стану захисту інформації в ІКС.

4. Взаємодію з іншими підрозділами організації з питань, що безпосередньо не пов'язані з захистом інформації, СЗІ здійснює у відповідності з наказами керівника організації.

У 6-му розділі «Штатний розклад та структура СЗІ» викладаються такі питання:

1. СЗІ є штатним або позаштатним підрозділом організації, безпосередньо підпорядкованим керівнику організації або його заступнику, що відповідає за забезпечення безпеки інформації. Або СЗІ є структурною (штатною або позаштатною) одиницею підрозділу ТЗІ (РСО або служби безпеки) організації.

2. Структура СЗІ, її склад і чисельність визначається фактичними потребами ІКС для виконання вимог політики безпеки інформації та затверджується керівництвом організації. Чисельність і склад СЗІ мають бути достатніми для виконання усіх завдань щодо захисту інформації в ІКС.

3. З метою ефективного функціонування та керування захистом інформації в ІКС СЗІ має штатний розклад, який включає перелік функціональних обов'язків усіх співробітників, необхідних вимог до рівня їхніх знань та навичок.

4. Безпосереднє керівництво роботою СЗІ здійснює її керівник. У випадку, коли СЗІ є структурною одиницею підрозділу ТЗІ (РСО або служби безпеки) – керівник цього підрозділу. Призначення та звільнення з посади керівника СЗІ здійснюється керівництвом організації за узгодженням з особами, що відповідають за забезпечення безпеки інформації.

На час відсутності керівника СЗІ (у зв'язку з відпусткою, службовим відрядженням, хворобою тощо) його обов'язки тимчасово виконує заступник керівника СЗІ, а у разі відсутності такої посади – найбільш кваліфікований співробітник СЗІ або керівник підрозділу

ТЗІ (РСО або служби безпеки). Призначення на цю посаду позаштатних або тимчасово працюючих співробітників забороняється.

5. Штат СЗІ комплектується спеціалістами, які мають спеціальну технічну освіту або спеціальні курси підвищення кваліфікації у галузі ТЗІ та практичний досвід роботи, володіють навичками з розробки, впровадження, експлуатації КСЗІ і засобів захисту інформації, а також реалізації організаційних, технічних та інших заходів з захисту інформації, знаннями і вмінням застосовувати нормативно-правові документи у сфері захисту інформації.

6. Функціональні обов'язки співробітників визначаються переліком і характером завдань, які покладаються на СЗІ керівництвом ІКС (організації).

7. В залежності від обсягів і особливостей завдань СЗІ до її складу можуть входити спеціалісти різного фаху з таких питань:

- захисту інформації від витоків технічними каналами;
- захисту каналів зв'язку і комутаційного обладнання;
- налагодження і керування активним мережевим обладнанням;
- керування базами даних захисту;
- адміністрування засобів захисту;
- захищених технологій обробки інформації.

8. За посадами співробітники СЗІ поділяються на такі категорії (за рівнем ієрархії):

- керівник СЗІ та його заступник;
- адміністратори - системний, мережевий, безпеки, КСЗІ тощо;
- спеціалісти служби захисту.

9. Зміна структури СЗІ здійснюється за рішенням керівництва організації та затверджується наказом керівника організації.

У 7-му розділі «Організація роботи СЗІ» викладаються такі питання:

1. Трудові відносини в СЗІ будуються на основі законодавства України з урахуванням положень статуту організації, правил внутрішнього трудового розпорядку та встановлених в організації норм техніки безпеки праці, гігієни і санітарії, інших розпорядчих документів організації.

2. СЗІ здійснює реалізацію основних організаційних та організаційно-технічних заходів щодо створення та забезпечення функціонування КСЗІ у відповідності з планами робіт. Підставою для розроблення планів робіт є «План захисту інформації в ІКС».

До планів включаться такі основні заходи:

- разові (які виконуються за умови перегляду прийнятих рішень з захисту інформації або виникнення певних змін в ІКС чи зовнішньому середовищі);

- періодичні (які виконуються з заданим інтервалом часу);

- постійні (які виконуються безперервно або дискретно у

випадковий чи заданий час).

Основними видами планів робіт СЗІ можуть бути:

- календарний план робіт (щодо реалізації заходів з проектування, реалізації, оцінювання, впровадження, технічного обслуговування, експлуатації КСЗІ та інших питань);

- план заходів з оперативного реагування на непередбачені ситуації (в тому числі надзвичайні та аварійні) та поновлення функціонування ІКС;

- поточний план робіт (на місяць, квартал, рік);

- перспективний план розвитку та удосконалення діяльності СЗІ з питань захисту інформації (до 5 років);

- план заходів з забезпечення безпеки інформації під час виконання окремих важливих робіт, при проведенні нарад, укладенні договорів, угод тощо.

Плани робіт складаються керівником СЗІ після обговорення на виробничій нараді СЗІ організаційно-технічних питань, що належать до її компетенції, і затверджуються керівником організації або керівником підрозділу, до складу якого входить СЗІ.

3. Реорганізація або ліквідація СЗІ здійснюється за рішенням керівництва організації. Реорганізаційна або ліквідаційна процедура здійснюється відповідною комісією, яка створюється за наказом керівника організації.

4. З метою забезпечення конфіденційності робіт, які виконуються співробітниками СЗІ, при прийомі на роботу (звільненні з роботи) вони дають письмові зобов'язання щодо нерозголошення відомостей, що становлять службову, комерційну або іншу таємницю, і які стали їм відомими в період роботи в організації.

5. Матеріально-технічну базу для забезпечення діяльності СЗІ складають належні їй на правах власності (оперативного управління, повного господарського відання) засоби захисту інформації, ПЗ, технічне і інженерне обладнання, засоби вимірювань і контролю, відповідна документація, а також інші засоби і обладнання, які необхідні для виконання СЗІ покладених на неї завдань.

Співробітники СЗІ відповідають за збереження майна, що є власністю або знаходиться у розпорядженні служби.

Засоби захисту інформації та захищені засоби, що використовуються співробітниками СЗІ при виконанні своїх службових обов'язків, повинні мати, одержаний у встановленому порядку документ, що засвідчує їхню відповідність вимогам НД ТЗІ.

Матеріально-технічне та інше спеціальне забезпечення СЗІ здійснюється відповідними підрозділами організації у встановленому порядку.

У 8-му розділі «Фінансування СЗІ» вказується, що СЗІ фінансується за рахунок:

- коштів, що виділяються в організації на утримання органів управління;
- прибутку організації (ІКС) та інших коштів за рішенням керівництва організації або рішенням загальних зборів акціонерів;
- коштів, отриманих за виконання СЗІ договірних робіт та надання послуг;
- інших джерел фінансування, не заборонених законодавством.

Структура інфографіки СЗІ показано на рис. 1.



Рисунок 1 – Структура служба захисту інформації відповідно до НД ТЗІ 1.4-001-2000



Тема 3

Обґрунтування необхідності створення КСЗІ. Категоріювання ІКС

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

- **обґрунтування необхідності створення КСЗІ і призначення СЗІ;**
- **категоріювання ІКС;**
- обстеження середовищ функціонування ІКС;
- опис моделі порушника політики безпеки інформації;
- опис моделі загроз для інформації;
- формування завдання на створення КСЗІ.

Обґрунтування необхідності створення КСЗІ і призначення СЗІ.

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 ІКС у разі створення КСЗІ.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ. Після прийняття такого рішення відповідальний за ТЗІ організації-власника (розпорядника) ІКС готує для керівника організації 3 накази:

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

2) про призначення **комісії з категоріювання ІКС**, 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 ІКС**, завдання та повноваження якої визначено в ДСТУ 3396.1 Технічний захист інформації. Порядок проведення робіт.

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

- захисту інформації від витоку технічними каналами;
- захисту каналів зв'язку і комутаційного обладнання,
- налагодження і адміністрування засобів захисту інформації,
- керування базами даних захисту інформації;
- налагодження і керування активним мережевим обладнанням;
- захищених технологій обробки інформації.

За функціональними обов'язками особовий склад СЗІ поділяється на такі категорії (за рівнем ієрархії):

- керівник СЗІ та його заступник;
- системний адміністратор ІКС;
- мережевий адміністратор ІКС;
- адміністратор безпеки інформації в ІКС;
- адміністратор КСЗІ в ІКС.

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 (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 пропускну 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 пропускну режиму, охоронної сигналізації та відеоспостереження.

2. Етап зупинення

Ці заходи забезпечують апаратно-програмне блокування спроб несанкціонованого доступу (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:

- технологічних процесів - їх відновлення за допомогою плану аварійного відновлення та проведення ремонтних заходів;
- операційної системи та програмних засобів - їх відновлення за допомогою інсталяційних файлів (дисків);
- інформаційних 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 ґрат 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.

Категоріювання ІКС.

Об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом (ІзОД) підлягають обов'язковому категоріюванню. Об'єктами категоріювання є об'єкти інформаційної діяльності, в тому числі об'єкти електронно-обчислювальної техніки (ЕОТ) ІКС.

Категоріювання ІКС здійснюється комісією організації-власника (розпорядника) ІКС для визначення необхідного рівня захисту інформації (рис. 1), що обробляється на об'єктах ЕОТ ІКС, згідно вимог НД ТЗІ 1.6-005-2013 «Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці».

НАКАЗ

" ____ " _____ 202_р.

№ ____

Про призначення комісії з
категоріювання

З метою проведення заходів щодо технічного захисту інформації відповідно до вимог Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці (НД ТЗІ 1.6-005-2013), затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 15.04.2013 року № 215

НАКАЗУЮ:

1. Призначити комісію з категоріювання об'єкта інформаційної діяльності –

(повна назва АС) (скорочена назва АС), що буде розташована в

(місце розташування АС), у складі:

Голова комісії: _____
(ПІБ та посада працівника)

Члени комісії: _____
(ПІБ та посада працівника)

(ПІБ та посада працівника)

2. Комісії провести категоріювання об'єкта інформаційної діяльності.

3. За результатами розгляду умов функціонування об'єкта інформаційної діяльності скласти акт категоріювання та подати його на затвердження.

Керівник органу _____

Рисунок 1 – Зразок наказу

Положення визначає загальні вимоги з категоріювання, ознаки, за якими здійснюється категоріювання, а також порядок категоріювання об'єктів інформаційної діяльності, в тому числі об'єктів електронно-обчислювальної техніки.

Положення є обов'язковим для органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, органів судової влади, правоохоронних та інших державних органів, військових формувань, а також підприємств, установ, закладів і організацій незалежно від форми власності, на об'єктах яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці.

У НД ТЗІ 1.6-005-2013 використано такі терміни та визначення:

власник об'єкта інформаційної діяльності – юридична або фізична особа, якій належить право власності на об'єкт інформаційної діяльності;

інформація з обмеженим доступом, що не становить державної таємниці – інформація, яка становить передбачену законом таємницю (крім державної), службова інформація, конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації”, та інша конфіденційна інформація, вимога щодо захисту якої встановлена законом;

категоріювання – сукупність дій зі встановлення категорії об'єкта;

категорія (об'єкта) – класифікаційна характеристика важливості об'єкта, за якою визначається необхідний (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівень захисту інформації, що обробляється технічними засобами та/або озвучується на цьому об'єкті;

користувач (розпорядник) об'єкта інформаційної діяльності – юридична або фізична особа, якій надано право користуватися (розпоряджатися) об'єктом інформаційної діяльності;

об'єкт електронно-обчислювальної техніки (об'єкт ЕОТ) – об'єкт інформаційної діяльності, на якому здійснюється обробка інформації розташованими на ньому засобами електронно-обчислювальної техніки інформаційних (автоматизованих), телекомунікаційних або інформаційно-телекомунікаційних систем та/або іншими технічними засобами;

об'єкт інформаційної діяльності (ОІД) – інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється

озвучення та/або обробка технічними засобами інформації з обмеженим доступом;

обробка інформації – здійснення за допомогою технічних засобів однієї або декількох операцій з інформацією, зокрема: створення, введення, збирання, записування, передавання, приймання (отримання), копіювання, перетворення, реєстрація, розмноження, дублювання, сканування (зчитування), роздрукування, зберігання, відображення (візуалізація, показ), відтворення, виготовлення (друкування) графічних та текстових документів, знищення тощо;

технічні засоби обробки інформації – засоби електронно-обчислювальної техніки інформаційних (автоматизованих), телекомунікаційних або інформаційно-телекомунікаційних систем та інші технічні засоби, на яких здійснюється обробка інформації.

Категоріювання здійснюється за ознакою ступеня обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД. Визначено 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 (I);
- становить державну таємницю, для якої встановлено гриф секретності «цілком таємно» - друга (II);
- становить державну таємницю, для якої встановлено гриф секретності «таємно», а також інформація, що містить відомості, які становлять іншу передбачену законом таємницю - третя (III);
- не становить державної таємниці - четверта (IV).

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

Комісія з категоріювання визначає ступень обмеження доступу до інформації, яка оброблятиметься в ІКС, та з урахуванням цього ступеня встановлює категорію ІКС. Встановлена категорія зазначається в Акті категоріювання ІКС, 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 (рис. 2) 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 ІКС здійснюється обробка ІзОД.

4. Ступінь обмеження доступу до ІзОД, що обробляється в ІКС (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.

ІКС, яким комісія встановила відповідну категорію, вносяться до «Переліку категоріюваних об'єктів», який ведеться власником (розпорядником, користувачем) ОІД.

Гриф обмеження доступу

Прим. № ____

ЗАТВЕРДЖУЮ

Керівник установи-власника
(розпорядника, користувача) об'єкта

(посада, підпис, ініціали, прізвище)

____. _____. 20 ____

М.П.

АКТ

категоріювання _____
(найменування об'єкта категоріювання)

1. Підстава для категоріювання _____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,

зміна ознаки, за якою була встановлена категорія об'єкта, тощо;

посилання/реквізити на розпорядчий документ 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; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється _____
(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті

(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія _____

Голова комісії _____
(підпис)

(ініціали, прізвище)

Члени комісії: _____
(підпис)

(ініціали, прізвище)

_____. _____. 20 ____

Рисунок 2 – Зразок акту категоріювання об'єкта



Тема 4

Обстеження середовищ функціонування ІКС. Опис моделі порушника ПБІ

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

- обґрунтування необхідності створення КСЗІ і призначення СЗІ;
- категоріювання ІКС;
- **обстеження середовищ функціонування ІКС;**
- **опис моделі порушника політики безпеки інформації;**
- опис моделі загроз для інформації;
- формування завдання на створення КСЗІ.

Обстеження середовищ функціонування ІКС.

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІКС 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 ІКС необхідно вивчити такі середовища:

- обчислювальне;
- інформаційне;
- користувацьке;
- фізичне (у разі обробки інформації, що становить державну таємницю).

При обстеженні обчислювального середовища ІКС 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 ІКС має бути визначено перелік пасивних об'єктів, які з ним взаємодіють.

Окрім компонентів ІКС, необхідно дати опис технології обробки інформації в ІКС, 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 ІКС, яка б відображала інформаційну взаємодію між основними компонентами ІКС (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 ІКС, 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 ІКС. Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, за типом їхнього представлення в ІКС, визначені й описані види її представлення в ІКС. Класифікація є підставою для визначення власником (розпорядником) інформації або ІКС 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 ІКС інформація повинна бути класифікована за типом її представлення в ІКС (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 ІКС (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 ІКС.

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 ІКС 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 ІКС, 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 ІКС 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 ІКС, 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 ІКС, доступу до ІКС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ;

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

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

- загальні відомості про ІКС;

- склад технічних засобів ІКС;

- 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 ІКС інформації, що становить державну таємницю, обов'язково здійснюється також **обстеження фізичного середовища**, під час якого аналізується взаємне розміщення засобів обробки інформації ІКС 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 3.6-003-2016 «Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації».

Аналізу підлягають такі характеристики фізичного середовища:

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

- архітектурно-будівельні особливості приміщень: огорожувальні 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, водосток, каналізація, технологічне обладнання, огорожувальні будівельні конструкції, світлопроникні отвори приміщень, будинків, споруд тощо).

- наявність систем безпеки в установі, до яких може бути інтегрована КСЗІ (відеоспостереження, пожежна та охоронна сигналізація, 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 ІКС, 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 ІКС»**, який затверджується керівником організації-власника (розпорядника) ІКС 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).

Опис моделі порушника політики безпеки інформації.

На підставі Акту обстеження та визначення загроз для ІКС СЗІ розробляє **«Модель порушника безпеки інформації в ІКС»**, яка затверджується керівником організації-власника (розпорядника) ІКС, 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 та місце дії тощо. Як порушник розглядається особа, яка може одержати несанкціонований доступ (НСД) до роботи з включеними до складу ІКС засобами.

Модель порушника повинна визначати:

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

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- 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 ІКС;
- основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);
- співробітників служби безпеки, які часто формально не допущені до життєво важливого центру ІКС, 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 ІКС);
- співробітники служби безпеки;
- керівники різних рівнів та посадової ієрархії.

Можна виділити також 3 основних мотиви порушень: безвідповідальність, самоствердження та з корисною метою.

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

Усіх порушників можна класифікувати за рівнем знань про ІКС:

- знає функціональні особливості ІКС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

- має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням;

- має високий рівень знань в області програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

- знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (методам та засобам, 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 магнітні носії інформації, які можуть бути тайком пронесені крізь пости охорони;

- застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).

За часом дії:

- 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:

- 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 кадрів і спеціальні заходи утруднюють можливість створення коаліцій порушників, тобто злочинного

угруповання (змови) і цілеспрямованих дій по подоланню 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 ІКС і засоби захисту. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

За результатами формування моделі порушника обов'язково повинні бути визначені: імовірність реалізації загрози, своєчасність виявлення та відомості про порушення.

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

Структура інфографіки моделі порушника показано на рис. 1.



Рисунок 1 – Структура моделі порушника відповідно до НД ТЗІ 1.4-001-2000



Тема 5
Формування завдання на
створення КСЗІ.
Опис моделі загроз для інформації.
Розробка політики безпеки
інформації в ІКС

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

- обґрунтування необхідності створення КСЗІ і призначення СЗІ;
- категоріювання ІКС;
- обстеження середовищ функціонування ІКС;
- опис моделі порушника політики безпеки інформації;
- **опис моделі загроз для інформації;**
- **формування завдання на створення КСЗІ.**

Опис моделі загроз для інформації.

Після проведення обстеження середовищ ІКС необхідно визначити всі можливі потенційні загрози для ІКС.

Походження загроз може бути **випадковим** і **навмисним**.

Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в ІКС в процесі її функціонування. Найбільш відомими подіями цього плану є відмови, збої, помилки, стихійні лиха та побічні впливи. Сутність перерахованих подій (окрім стихійних лих, сутність яких незрозуміла) визначається таким чином:

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

- збій - тимчасове порушення працездатності якого-небудь елемента системи, наслідком чого може бути неправильне виконання ним у цей момент своєї функції;

- помилка - неправильне (разове або систематичне) виконання елементом однієї або декількох функцій, що відбувається внаслідок специфічного (постійного або тимчасового) його стану;

- побічний вплив - негативний вплив на систему в цілому або окремі її елементи, чиниться будь-якими явищами, що відбуваються всередині системи або у зовнішньому середовищі.

Навмисне походження загроз обумовлюється зловмисними діями людей.

Передумови появи загроз можуть бути об'єктивними (кількісна або якісна недостатність елементів системи) і суб'єктивними. До

останніх відносяться діяльність розвідувальних органів іноземних держав, промислове шпигунство, діяльність кримінальних елементів, дії недобросовісного персоналу ІКС.

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 повне безліч погроз, потенційно можливих у сучасних автоматизованих системах. При цьому ми повинні врахувати не лише всі відомі (раніше проявлялися) загрози, але й такі загрози, які раніше не виявлялися, але потенційно можуть виникнути при застосуванні нових концепцій архітектурного побудови АС і технологічних схем обробки інформації.

Всі можливі **канали витоку інформації** (КВІ) можна класифікувати за двома критеріями: необхідністю доступу до елементів ІКС для реалізації того чи іншого КВІ і залежністю появи КВІ від стану ІКС.

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 ІКС),

- вимагають доступу в приміщення ІКС. У свою чергу, такі канали можуть не залишити слідів в ІКС (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 ІКС (наприклад, викрадати носії інформації можна незалежно від того, в робочому стані знаходяться кошти АС чи ні);

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

Наведемо орієнтовну характеристику каналів несанкціонованого отримання інформації виділених нами класів:

1-го класу - канали, які проявляються безвідносно до обробки інформації і без доступу зловмисника до елементів системи. Сюди може бути віднесено підслуховування розмов, а також провокування на розмови осіб, що мають відношення до ІКС, і використання зловмисником візуальних, оптичних та акустичних засобів.

2-го класу - канали, які у процесі обробки інформації без доступу зловмисника до елементів ІКС. Сюди можуть бути віднесені електромагнітні випромінювання різних пристроїв ІКС, апаратури та ліній зв'язку, паразитні наведення в ланцюгах харчування, телефонних мережах, системах теплопостачання, вентиляції тощо.

3-го класу - канали, які проявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІКС, але без зміни останніх. До них відносяться всілякі види копіювання носіїв інформації і документів, а також розкрадання виробничих відходів.

4-го класу - канали, які у процесі обробки інформації з доступом зловмисника до елементів ІКС, але без зміни останніх. Сюди може бути віднесено запам'ятовування і копіювання інформації в процесі обробки, використання програмних пасток тощо.

5-го класу - канали, які проявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІКС і зі зміною програмних або апаратних засобів. Серед цих каналів: підміна і розкрадання носіїв інформації й апаратури, включення до програм блоків типу троянський кінь, комп'ютерний черв'як тощо.

6-го класу - канали, які у процесі обробки інформації з доступом зловмисника до елементів ІКС і зі зміною останніх. Сюди може бути віднесено незаконне підключення до апаратури та ліній зв'язку, а також зняття інформації на шинах живлення різних елементів ІКС.

На підставі Акту обстеження та Моделі порушника політики безпеки СЗІ розробляє **«Модель загроз для інформації в ІКС»**, яка затверджується керівником організації-власника (розпорядника) ІКС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ. Модель загроз має містити абстрактний 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 ІКС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІКС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

Загрози для інформації, що обробляється в ІКС, 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 ІКС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

- збої та відмови у роботі технічних або програмних засобів (ПЗ) ІКС;

- наслідки помилок під час проектування та розробки компонентів ІКС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);

- помилки персоналу (користувачів) ІКС під час експлуатації;

- навмисні дії (спроби) потенційних порушників.

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неухважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, що призводять до відмови ІКС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);

- ненавмисне пошкодження носіїв інформації;

- неправомірна зміна режимів роботи ІКС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

- неумисне зараження ПЗ комп'ютерними вірусами;

- невиконання вимог до організаційних заходів захисту чинних в ІКС розпорядчих документів;

- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

- неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);

- наслідки некомпетентного застосування засобів захисту тощо.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи ІКС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

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

Перелік суттєвих загроз має бути максимально повним і деталізованим.

Для кожної з загроз необхідно визначити:

1) на порушення яких властивостей інформації або ІКС вона спрямована:

- загрози конфіденційності - несанкціоноване ознайомлення з інформацією;
- загрози цілісності - несанкціонована модифікація (спотворення, фальсифікація, викривлення) інформації;
- загрози доступності - порушення можливості використання ІКС або оброблюваної інформації (відмова в обслуговуванні користувача);
- загрози спостережності та керованості ІКС - відмова в ідентифікації, автентифікації та реєстрації небезпечних дій;

2) джерела виникнення (які суб'єкти ІКС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

- персонал ІКС;
- технічні засоби ІКС;
- моделі, алгоритми, програми ІКС;
- технологія функціонування ІКС;

- зовнішнє середовище.

З) можливі способи здійснення (механізм реалізації) загроз:

- 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, вкорінення комп'ютерних вірусів.

Опис моделі загроз (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації рис. 1), має бути викладений настільки детально, щоб дозволяти (на етапі аналізу ризиків, пов'язаних з реалізацією загроз для інформації в ІКС) однозначне визначення як збитків, що завдаються у випадку успішної реалізації загрози, так і ймовірності реалізації загрози (здійснення атаки) в певний спосіб.

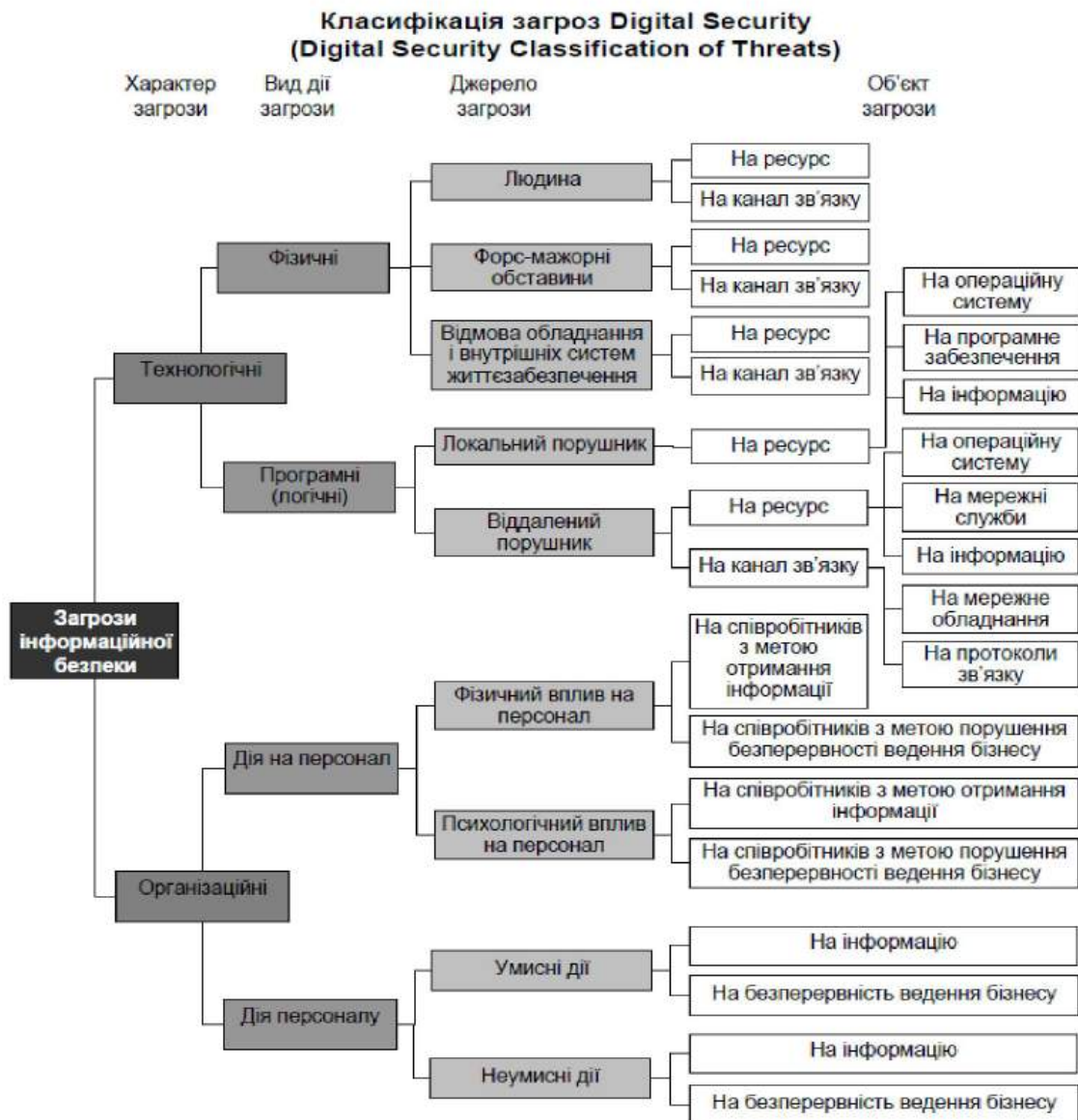


Рисунок 1 – Класифікація загроз Digital Security

Формування завдання на створення КСЗІ.

Останній крок 1-го етапу «Формування вимог до КСЗІ в ІКС» складається з таких робіт:

- 1. Формування завдання на створення КСЗІ в ІКС.**
- 2. Аналіз ризиків реалізації загроз для інформації в ІКС.**
- 3. Вибір варіанту побудови та складу КСЗІ в ІКС.**
- 4. Оформлення звіту за результатами проведеної роботи.**

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

1. Формування завдання на створення КСЗІ в ІКС.

Завданнями захисту інформації можуть бути:

- забезпечення необхідних властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації ІКС;

- своєчасне виявлення та знешкодження загроз для ресурсів ІКС, причин та умов, які спричиняють (можуть привести до) порушення її функціонування та розвитку;

- створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні ІКС;

- ефективне знешкодження (попередження) загроз для ресурсів ІКС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;

- керування засобами захисту інформації, керування доступом користувачів до ресурсів ІКС, контроль за їхньою роботою з боку персоналу СЗІ, оперативне сповіщення про спроби НСД до ресурсів ІКС;

- реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;

- 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 ІКС.

Концепція безпеки інформації розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після вибору варіанту концепції створюваної ІКС і виконується на підставі аналізу таких чинників:

- правових і (або) договірних засад;
- вимог до забезпечення безпеки інформації згідно з завданнями і функціями ІКС;
- загроз, яким зазнають впливу ресурси ІКС, що підлягають захисту.

За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію обробки інформації в ІКС:

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

Вибір основних рішень щодо забезпечення безпеки інформації розглядається на 3-х рівнях:

- **правовому;**
- **організаційному;**
- **технічному.**

На правовому рівні повинні бути вироблені підходи щодо:

- підтримки керівництвом організації заходів з забезпечення безпеки інформації в ІКС, виконання правових вимог з захисту інформації, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподілу обов'язків співробітників СЗІ;

- процедур доведення до персоналу і користувачів ІКС основних положень політики безпеки інформації, їхнього навчання і підвищення кваліфікації з питань безпеки інформації;

- системи контролю за своєчасністю, ефективністю і повнотою реалізації в ІКС рішень з захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.

На організаційному рівні повинні бути вироблені підходи щодо:

- застосування режимних заходів на об'єктах ІКС;
- забезпечення фізичного захисту обладнання ІКС, носіїв інформації, інших ресурсів;

- порядку виконання робіт з захисту інформації, взаємодії з цих питань з іншими суб'єктами системи ТЗІ в Україні;

- виконання робіт з модернізації ІКС (окремих компонентів);
- регламентації доступу сторонніх користувачів до ресурсів ІКС;
- регламентації доступу власних користувачів і персоналу до ресурсів ІКС;

- здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки, попередження появи вірусів тощо);

- реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад,

організація віддаленого доступу до ІКС, використання мереж передачі даних загального користування, зокрема Інтернет тощо).

На технічному рівні повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації. Під час розгляду різних варіантів реалізації рекомендується враховувати наступні аспекти:

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

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) і визначається перелік суттєвих загроз для ІКС.

Аналіз ризиків полягає в моделюванні картини появи несприятливих умов за допомогою обліку всіх можливих чинників, що визначають ризик, які можна назвати вхідними параметрами:

- активи - ключові компоненти інфраструктури ІКС, що залучені в технологічний процес і мають певну цінність;
- вразливості - слабкості в засобах захисту, викликана помилками або недосконалістю в процедурах, проєкті, реалізації, яка може бути використана для проникнення в ІКС;
- загроза, реалізація якої можлива за допомогою використання вразливості;
- збиток, який оцінюється з урахуванням витрат на відновлення ІКС після можливого інциденту інформаційної безпеки.

Процес аналізу ризиків включає:

- оцінку можливих втрат через успішно проведених атак на ІКС;
- оцінку вірогідності виявлення вразливостей системи, що впливає на оцінку можливих втрат;
- вибір оптимальних за витратами заходів і засобів захисту, які скорочують ризик до прийнятного рівня.

З метою підвищення ефективності аналізу ризиків він проводиться по різних напрямках для:

- об'єктів ІКС;
- процесів, процедур і програм обробки інформації;
- каналів зв'язку;
- побічних електромагнітних випромінювань і наведень;
- механізмів керування системою захисту.

Керування ризиками – це процес, що складається в послідовному виконанні з 3-х основних етапів:

- визначення ризиків в незахищеній ІКС;
- застосування засобів захисту для скорочення ризиків;
- оцінка залишкових ризиків.

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 уточнюються допустимі залишкові ризики та витрати на заходи, пов'язані з захистом інформації.

На даний час процес керування ризиками описує стандарт ДСТУ ISO/IEC 27005:2023 «Інформаційна технологія. Методи забезпечення безпеки. Керування ризиками інформаційної безпеки».

Згідно вимог цього стандарту на етапі планування складається з 4-х кроків (рис. 2):

- 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, щоб застосувати ефективні заходи захисту таким чином, щоб залишковий ризик в ІКС став прийнятний. Мінімізація ризику складається з трьох частин: визначення тих областей, де ризик неприпустимо великий; вибору найбільш ефективних засобів захисту; оцінювання заходів захисту і визначення, чи прийнятний залишковий ризик в ІКС. Дамо коротку характеристику кроків керування ризиком.

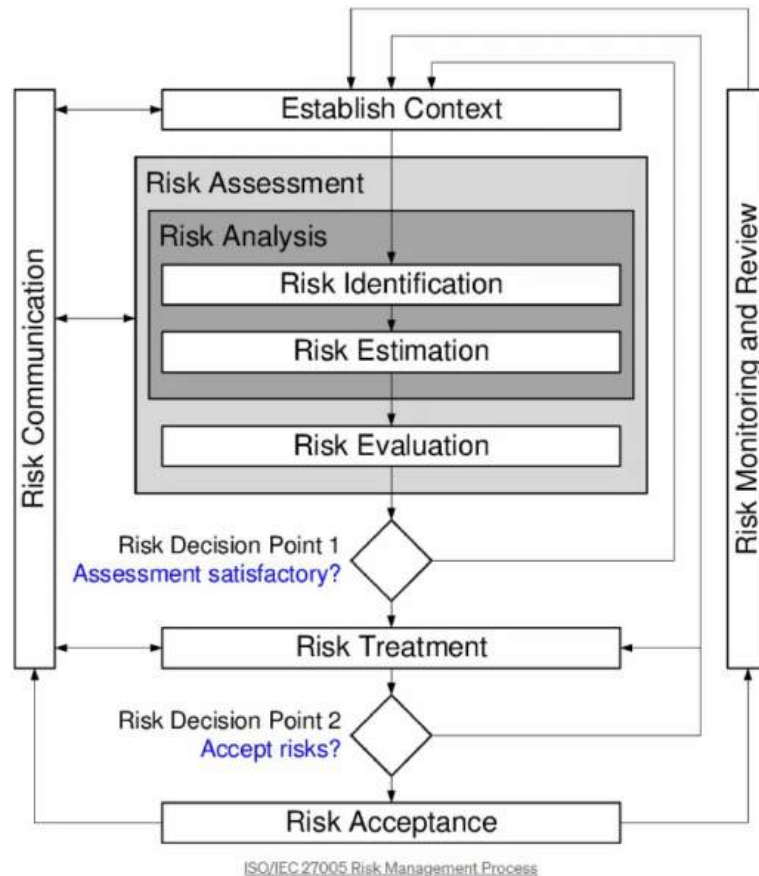


Рисунок 2 – Процес менеджменту ризику інформаційної безпеки

3. Вибір варіанту побудови КСЗІ.

Після завершення аналізу всіх можливих ризиків необхідно здійснити вибір варіанту побудови КСЗІ в залежності від ступеня обмеження доступу до інформації, яка обробляється в ІКС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника ІКС. Можливі такі варіанти:

- досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в ІКС;
- досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технологію її обробки в ІКС;
- досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технологію її обробки в ІКС.

Після цього необхідно здійснити первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів. На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм «ефективність/вартість»),

вибирається найбільш оптимальна серед них і первинна оцінка уточнюється. Якщо залишковий ризик перевищує гранично допустимий, вносяться відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконуються повторно до одержання прийняттого результату.

На підставі визначених завдань і функцій ІКС, результатів аналізу її середовищ функціонування, моделей загроз і порушників та результатів аналізу ризиків визначаються компоненти ІКС (наприклад, ЛОМ, спеціалізований АРМ, Інтернет-вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в ІКС.

Визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, обмеження щодо середовищ функціонування ІКС та використання її ресурсів для реалізації завдань захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до застосування в ІКС (окремих її підсистемах, компонентах) організаційних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

Для ІКС формується перелік необхідних функціональних послуг захисту (ФПЗ) від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг. Визначені вимоги складають профіль захищеності інформації в ІКС або її компоненті.

ФПЗ є ієрархічними в тому розумінні, що їх реалізація забезпечує зростаючу захищеність від загроз відповідного типу (конфіденційності - К, цілісності - Ц і доступності - 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.

Кожна послуга є набором функцій, які дозволяють протистояти певній множині загроз. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, хоча й не є точними підмножинами один одного. Рівні починаються з першого й зростають до певного значення, унікального для кожного виду послуг.

4. Оформлення звіту за результатами проведеної роботи.

Останній етап формування завдання на створення КСЗІ завершується оформленням «Звіту за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ», який затверджується керівником організації- власника (розпорядника) ІКС.

Звіт повинен містити 2 розділи:

- формалізований або неформалізований опис результатів аналізу

ризиків, пов'язаних з реалізацією загроз для інформації в ІКС;
- формулювання, з урахуванням результатів виконаного аналізу ризиків, завдань на створення КСЗІ в ІКС.

2 етап - Розробка політики безпеки інформації в ІКС.

Мета реалізації політики безпеки. Основною метою реалізації політики безпеки є забезпечення ефективного функціонування компанії, для чого необхідно забезпечити захист оброблюваної на підприємстві інформації від несанкціонованого доступу. Політика безпеки має на меті розробку та впровадження правил та норм внутрішнього режиму праці на підприємстві, режиму доступу та допуску до важливих об'єктів, їх охорона, середовище розміщень.

Опис політики безпеки інформації в ІКС здійснюється згідно вимог додатку «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) ІКС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ.

Під політикою безпеки інформації слід розуміти набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо АС, окремого її компонента, послуги захисту, що реалізується системою і т. ін. Політика безпеки інформації в АС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи.

Політика (з урахуванням результатів обстеження середовищ функціонування ІКС) визначає інформаційні ресурси ІКС, що потребують захисту. Мають бути сформульовані основні загрози для інформації з різними характеристиками відповідно до встановленого законодавством правового режиму та режиму доступу, компонентів обчислювальної системи, персоналу та вимоги щодо захисту від цих загроз.

Перераховуються основні рішення з протидії всім суттєвим загрозам, правила, які регламентують використання захищених технологій обробки інформації в ІКС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій.

Як складові частини загальної політики повинні бути наведені політики забезпечення конфіденційності, цілісності та доступності оброблюваної інформації, а також політика забезпечення спостережності та керованості ІКС.

Під час розробки політики повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. Як складові частини загальної політики мають існувати політики забезпечення конфіденційності,

цілісності, доступності оброблюваної інформації та спостережності ІКС.

Політика має бути розроблена таким чином, що б вона не потребувала частоті модифікації (потреба частоті зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика повинна стосуватись:

- інформації (рівня критичності ресурсів ІКС),
- взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту),
- області застосування (яких складових компонентів ІКС політика безпеки стосується, а яких - ні).

Політика повинна передбачати використання всіх заходів захисту інформації:

- правові та морально-етичні норми,
- організаційні (адміністративні),
- фізичні, технічні (апаратні і програмні) заходи,
- правила та порядок застосування в ІКС кожного заходу.

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;
- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки повинна поширюватись на такі об'єкти захисту:

- відомості (незалежно від виду їхнього представлення), віднесені до інформації з обмеженим доступом (ІзОД) або інших видів інформації, що підлягають захисту, обробка яких здійснюється в АС і які можуть знаходитись на паперових, магнітних, оптичних та інших носіях;

- інформаційні масиви та бази даних, програмне забезпечення, інші інформаційні ресурси;

- обладнання АС та інші матеріальні ресурси, включаючи технічні засоби та системи, не задіяні в обробці ІзОД, але знаходяться у контрольованій зоні, носії інформації, процеси і технології її обробки. Технічні області, в яких необхідно захищати інформаційне та програмне забезпечення - робоча станція, комунікаційні канали (фізична мережа) та комутаційне обладнання, сервери, засоби друку

та буферизації для утворення твердих копій, накопичувачі інформації;

- засоби та системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту;
- користувачів (персонал) АС, власників інформації та АС, а також їхні права.

Політика повинна визначити вимоги до заходів, методів та засобів захисту, вихідними даними для чого є:

- завдання і функції ІКС;
- результати аналізу середовищ функціонування ІКС;
- модель загроз і модель порушників;
- результати аналізу ризиків.

На підставі цих даних визначаються компоненти ІКС (наприклад, окрема ЛОМ, спеціалізований АРМ, Інтернет- вузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в ІКС.

Для кожного компонента та (або) ІКС в цілому формується перелік необхідних функціональних послуг захисту від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг (згідно з НД ТЗІ 2.5-004 та НД ТЗІ 2.5-005). Визначені вимоги будуть складати ФПЗ ІКС або її компоненти.

Для кожного компонента та (або) ІКС в цілому у разі обробки таємної інформації визначаються загальні підходи та вимоги з захисту інформації від витоків технічними каналами.

На наступному кроці визначаються механізми безпеки, що реалізують функціональні послуги безпеки, здійснюється вибір технічних засобів захисту інформації від витоків технічними каналами.

Політика повинна доказово давати гарантії того, що:

- в ІКС забезпечується адекватність рівня захисту інформації рівню її критичності;
- реалізація заходів захисту інформації є рентабельною;
- в будь-якому середовищі функціонування ІКС забезпечується оцінюваність і перевіряємість захищеності інформації;
- забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів ІКС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування ІКС;
- персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;
- всі критичні з точки зору безпеки інформації технології (функції) ІКС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;

- враховані вимоги всіх документів, які регламентують порядок захисту інформації в ІКС, та забезпечується їхнє суворе дотримання.

Документальне оформлення політики безпеки. Результати робіт з розроблення політики безпеки оформлюються у вигляді окремих документів або розділів одного документа, в якому викладена політика безпеки інформації в ІКС. Структурно до політики безпеки (документів, що її складають) повинні входити такі розділи:

- загальний, у якому визначається відношення керівництва ІКС до проблеми безпеки інформації;

- організаційний, у якому наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їхніх функцій, викладаються підходи, що застосовуються до персоналу (опис посад з точки зору безпеки інформації, організація навчання та перепідготовки персоналу, порядок реагування на порушення режиму безпеки тощо);

- класифікаційний, де визначаються матеріальні та інформаційні ресурси, які є у наявності в ІКС, та необхідний рівень їхнього захисту;

- розділ, у якому визначаються правила розмежування доступу (ПРД) користувачів та процесів до інформаційних ресурсів ІКС;

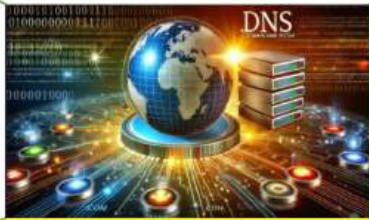
- розділ, у якому визначається підхід щодо керування робочими станціями, серверами, мережевим обладнанням тощо;

- розділ, у якому висвітлюються питання фізичного захисту;

- розділ, де викладено порядок розробки та супроводження ІКС, модернізації апаратного та програмного забезпечення;

- розділ, який регламентує порядок проведення відновлювальних робіт і забезпечення неперервного функціонування ІКС;

- юридичний розділ, у якому приводиться підтвердження відповідності політики безпеки законодавству України.



Тема 6

Розробка технічного завдання на створення КСЗІ. Розробка проекту КСЗІ

3 етап - Розробка технічного завдання на створення КСЗІ.

Технічне завдання (ТЗ) на створення КСЗІ в ІКС розробляється згідно вимог НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення КСЗІ в АС.

Технічне завдання на створення КСЗІ в АС (ТЗ на КСЗІ) є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі.

Технічне завдання на КСЗІ розробляється у разі необхідності розробки або модернізації КСЗІ існуючої (що функціонує) АС. В разі розробки КСЗІ в процесі проектування АС допускається оформлення вимог з захисту інформації в АС у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ на АС або розділу загального ТЗ на АС.

Технічне завдання на КСЗІ повинно розроблятися з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу АС.

В технічному завданні на КСЗІ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброблення в обчислювальній системі АС. Додатково треба викласти вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою АС у доповнення до комплексу програмно-технічних засобів захисту інформації.

Перелік вимог з захисту інформації, які включаються в ТЗ на КСЗІ, може бути для кожної конкретної АС як розширений, так і скорочений відносно рекомендованого в даному документі переліку в рамках діючих законодавчих і нормативних документів.

Вимоги повинні передбачати розроблення та використання сучасних ефективних засобів і методів захисту, які дають можливість забезпечити виконання цих вимог з найменшими матеріальними затратами.

Технічне завдання на КСЗІ є одним із обов'язкових засадничих документів під час проведення експертизи АС на відповідність вимогам захищеності інформації.

Приклад побудови технічного завдання на створення комплексної системи захисту інформації в АС, який спрямований на надання методичної допомоги власникам АС, наведено в доповненні.

Порядок розроблення технічного завдання.

Вихідними даними для розроблення ТЗ на КСЗІ є ***функціональний профіль захищеності КС від НСД і вимоги до захищеності інформації від витоку технічними каналами.***

Функціональний профіль захищеності інформації в конкретній АС може бути визначений в результаті проведення аналізу загроз та оцінки ризиків або обраний на підставі класу АС відповідно до НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

Вимоги до захисту інформації від витоку технічними каналами визначаються на підставі нормативних документів з технічного захисту інформації, якими встановлено норми захищеності інформації від витоку технічними каналами та порядок виконання відповідних робіт.

В технічному завданні повинно бути наведено обґрунтування вибору функціонального профілю захищеності і вимог до показників захищеності інформації від витоку технічними каналами.

Перелік основних робіт етапу формування ТЗ такий:

- класифікація та опис ресурсів АС (ОС, засобів зв'язку і комунікацій, інформації, її категорій, виду подання, місця зберігання, технології обробки тощо, обслуговуючого персоналу і користувачів, території і приміщень і т. ін.);
- розробка інформаційної моделі для існуючої АС, тобто опис (формальний або неформальний) інформаційних потоків АС, інтерфейсів між користувачем і АС і т. ін.;
- визначення переліку загроз і можливих каналів витоку інформації;
- експертна оцінка очікуваних втрат у разі здійснення загроз;
- визначення послуг безпеки, які треба реалізувати;
- обґрунтування необхідності проведення спец перевірок і спец досліджень ЗОТ та інших технічних засобів, а також спеціального обладнання приміщень;
- визначення вимог до організаційних, фізичних та інших заходів захисту, що реалізуються у доповнення до комплексу програмно-технічних засобів захисту;
- визначення вимог до метрологічного забезпечення робіт;
- визначення переліку макетів, що розробляються, і технологічних стендів;
- оцінка вартості і ефективності обраних засобів;
- прийняття остаточного рішення про склад КСЗІ.

Вимоги з захисту інформації визначаються замовником, погоджуються з розробником АС і виконавцем робіт по створенню КСЗІ в АС. У випадках, передбачених Положенням про технічний захист інформації в Україні, ТЗ на КСЗІ погоджується Адміністрацією Державної служби спеціального зв'язку та захисту інформації.

Зміст технічного завдання.

ТЗ на КСЗІ в загальному випадку повинно містити такі основні підрозділи:

- *загальні відомості;*
- *мета і призначення комплексної системи захисту інформації;*
- *загальна характеристика автоматизованої системи та умов її функціонування;*
- *вимоги до комплексної системи захисту інформації;*
- *вимоги до складу проектної та експлуатаційної документації;*
- *етапи виконання робіт;*
- *порядок внесення змін і доповнень до технічного завдання;*
- *порядок проведення випробувань комплексної системи захисту інформації.*

Загальні відомості.

В підрозділі зазначають:

- повне найменування КСЗІ та її умовне позначення;
- шифр теми і реквізити договору;
- найменування підприємств-розробників і замовника (користувача) КСЗІ та їх реквізити;
- перелік документів, на підставі яких створюється КСЗІ, ким і коли затверджені ці документи;
- планові терміни початку і закінчення роботи із створення КСЗІ;
- відомості про джерела і порядок фінансування робіт;
- порядок оформлення і подання замовнику результатів робіт із створення КСЗІ, з виготовлення і налагодження окремих засобів (технічних, програмних, інформаційних) і програмно-технічних (програмно-методичних) комплексів системи.

Мета і призначення комплексної системи захисту інформації.

Вказується мета розробки КСЗІ в АС, функціональне призначення і особливості застосування. Необхідно зазначати, на підставі яких нормативно-правових актів, інших нормативних документів регламентується порядок захисту інформації в АС.

Загальна характеристика автоматизованої системи і умов її функціонування.

В підрозділі рекомендується зазначити такі моменти, які впливають на безпеку інформації під час її оброблення в АС та на загальні вимоги до реалізації СЗІ:

- загальну структурну схему і склад ОС АС (перелік і склад устаткування, технічних і програмних засобів, їх зв'язки, особливості конфігурації і архітектури, особливості підключення до локальних або глобальних мереж тощо);

- технічні характеристики каналів зв'язку (пропускна спроможність, типи кабельних ліній, види зв'язку з віддаленими сегментами АС і користувачами і т. ін.);

- характеристики інформації, що обробляється (категорії інформації, вищий гриф секретності і т. ін.);

- характеристики персоналу (кількість користувачів і категорій користувачів, форми допуску тощо);

- характеристики фізичного середовища (наявність категоризованих приміщень, територіальне розміщення компонентів АС, їх фізичні параметри, вплив на них чинників навколишнього середовища, захищеність від засобів технічної розвідки і т.п.);

- загальну технічну характеристику АС (обсяги основних інформаційних масивів і потоків, швидкість обміну інформацією і продуктивність системи під час розв'язання функціональних завдань, тривалість процедури підготовки АС до роботи після подачі живлення на її компоненти, тривалість процедури відновлення працездатності після збоїв, наявність засобів підвищення надійності і живучості і т. ін.);

- особливості функціонування АС (надання машинного часу або устаткування в оренду стороннім організаціям, цілодобовий режим роботи без відключення живлення тощо);

- особливості реалізованих або припустимих заходів організаційних, фізичних та інших заходів захисту (режимні заходи в приміщеннях і на території, охорона, сигналізація, протипожежна охорона і т. ін.);

- інші чинники, що впливають на безпеку оброблюваної інформації;

- потенційні загрози інформації (способи здійснення НСД, можливі технічні канали витоку інформації і умови їх формування, стихійні лиха і т. ін.), а також можливі наслідки їх реалізації;

- клас АС згідно з НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу".

Крім того, треба описати функціонуючі в складі АС (для існуючої АС) засоби захисту, а також засоби захисту, реалізовані в компонентах, які планується використовувати для побудови АС. При цьому треба враховувати, що функції захисту, які реалізуються

засобами імпортного виробництва, не мають зв'язаного з ними рівня гарантій. Використання таких засобів у складі КСЗІ можливе тільки за наявності експертного висновку, зареєстрованого Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

В підрозділі не вказуються ті характеристики і умови функціонування АС, опис яких є в ТЗ на АС або в інших документах. Даються тільки посилання на розділи цих документів.

Вимоги до комплексної системи захисту інформації.

1. Вимоги до комплексної системи захисту інформації в АС в частині захисту від несанкціонованого доступу.

Вимоги до комплексної системи захисту інформації в АС в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004 "Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу" (Критерії). Згідно з цим документом в процесі оцінки захищеності КС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

Має бути вказаний функціональний профіль захищеності, який передбачається реалізувати. Профіль може бути або вибраний із профілів, описаних в НД ТЗІ 2.5-005-99, або визначений як упорядкована сукупність рівнів послуг згідно з вимогами зазначеного документа. Повинен бути вказаний рівень гарантій, що передбачається досягти.

Опису послуг має передувати опис політики безпеки інформації, яку повинен реалізувати комплекс засобів захисту ОС АС. Опис політики безпеки має включати в себе опис:

- об'єктів (елементів ресурсів) ОС;
- принципів керування доступом користувачів до інформації (довірче і/або адміністративне керування доступом);
- правил розмежування інформаційних потоків;
- правил маркірування носіїв інформації;
- основних атрибутів доступу користувачів, процесів і пасивних об'єктів;
- правил розмежування доступу користувачів і процесів до пасивних об'єктів;
- правил адміністрування КЗЗ і реєстрації дій користувачів;
- інші загальні моменти політики безпеки, які вважає за потрібне описати розробник ТЗ.

Вимоги до послуг безпеки мають бути викладені і згруповані в тому порядку і стилі, в якому вони подані в Критеріях. В розділі мають бути викладені вимоги до реалізації послуг забезпечення:

- конфіденційності;

- цілісності;
- доступності;
- спостереженості.

Для кожної включеної до розділу послуги відповідно до Критеріїв має бути визначений рівень послуги, який передбачається реалізувати. Має бути описана політика даної послуги: визначення об'єктів, до яких застосовується дана послуга, і правил (в тому числі, що застосовуються за умовчужанням), відповідно до яких повинні функціонувати механізми, що реалізують послугу. Відповідно до особливостей розроблюваної АС мають бути конкретизовані всі вимоги, що викладені в Критеріях для відповідного рівня кожної послуги.

У разі, якщо передбачається реалізувати послуги безпеки, які не зазначені в Критеріях, їх також необхідно описати, дотримуючись, по можливості, стилю, прийнятого для опису інших послуг.

Вимоги до гарантій також мають бути викладені і згруповані в тому порядку і стилі, як вони подані в Критеріях. Це передбачає включення вимог до:

- архітектури КЗЗ (додатково до загальних вимог до архітектури на даному етапі бажано визначити основні модулі (підсистеми), з яких повинен складатися КЗЗ);
- середовища розробки (організації процесу розробки і системи керування конфігурацією);
- гарантій проектування (етапності розробки і проектної документації);
- середовища функціонування;
- експлуатаційної документації;
- випробувань комплексу засобів захисту.

Всі вимоги повинні відповідати належному рівню гарантій.

Оскільки деякі з вимог гарантій стосуються розроблюваної системи в цілому, а не тільки КЗЗ, то в даному розділі допускається дати посилання на інші підрозділи ТЗ. Зокрема, вимоги до етапності розробки і складу документації мають бути визначені в розділах "Вимоги до складу проектної та експлуатаційної документації" та "Етапи виконання робіт". Крім того, допускаються посилання на інші документи, що розробляються на більш пізніх етапах.

2 Вимоги до комплексної системи захисту інформації в АС в частині захисту від витоків інформації технічними каналами.

Мають бути сформульовані загальні вимоги до об'єктів (компонентів АС), що захищаються, визначені засоби захисту і засоби їх використання (наприклад, реалізація вимог до захищеності повинна досягатись без застосування екранування приміщень, активні засоби мають застосовуватись тільки для захисту інформації головного сервера АС і т. ін.).

Наводиться перелік нормативних і методичних документів, відповідно до яких повинні проводитись роботи щодо захисту інформації від витоку технічними каналами.

Мають бути вказані вимоги до розмірів зони безпеки інформації.

Мають бути вказані необхідні величини показників захищеності, що враховують реальну заводську обстановку на об'єкті електронної обчислювальної техніки. Основними показниками є:

- відношення величин електричної і магнітної складових напруженості поля побічних електромагнітних випромінювань до рівня завод на об'єкті ЕОТ;

- відношення величини напруженості інформативного сигналу в провідних комунікаціях на межі зони безпеки інформації до рівня завод на об'єкті ЕОТ;

- величина нерівномірності струму, який споживається по мережі електроживлення;

- коефіцієнт екранування засобів обчислювальної техніки, в тому числі від впливу зовнішніх ЕМВ.

Гранично допустимі значення основних показників є нормованими величинами і визначаються за відповідними методиками.

Відношення розрахованих (вимірених) значень основних показників до гранично допустимих (нормованих) значень визначають необхідні умови захисту інформації.

Мають бути вказані вимоги щодо застосування способів, методів і засобів досягнення необхідних показників захищеності. Рекомендується застосування таких способів, методів і засобів:

- а) системо- і схемотехнічних методів:

- обмеження використання інтерфейсів з передачею сигналів у вигляді послідовного коду і в режимі багатократних повторень;

- використання мультиплексних режимів обробки інформації, а також ЗОТ і системного забезпечення, що базуються на багаторозрядних платформах, інтерфейсів з передачею сигналів у вигляді багаторозрядного паралельного коду;

- використання раціональних способів монтажу, за яких забезпечується мінімальна довжина електричних зв'язків і комунікацій;

- використання ЗОТ і технічних засобів, до складу яких входять стійкі до самозбудження схеми, розв'язувальні і фільтрувальні елементи, комплектуючі з низькими рівнями ЕМВ;

- використання мережевих фільтрів для блокування витоку ІзОД мережами електроживлення, а також лінійних (високочастотних) фільтрів для блокування витоку ІзОД лініями зв'язку;

- використання ЗОТ і технічних засобів у захисному виконанні;

б) засобів просторового і лінійного "зашумлення";
в) засобів локального або загального екранування;
г) засобів оптимального розміщення ЗОТ і технічних засобів з метою мінімізації зони, в межах якої граничне відношення сигнал/шум не перевищує встановлених норм.

Мають бути вказані вимоги до проведення спецдосліджень ЗОТ і технічних засобів, мета яких – пряме вимірювання показників ЕМВ.

Мають бути вказані вимоги до проведення спецперевірки ЗОТ, мета якої – виявлення та вилучення (блокування) спеціальних електронних (закладних) пристроїв.

Вимоги до складу проектної та експлуатаційної документації.

В цьому розділі слід навести перелік проектної та експлуатаційної документації, що розробляється в процесі створення КСЗІ в АС.

Склад обов'язкової проектної і експлуатаційної документації визначається вимогами нормативних документів, відповідно до яких проводиться розробка (зокрема, вимогами Критеріїв для відповідного рівня гарантій). Повний перелік необхідної документації визначається розробником КСЗІ і погоджується із замовником.

Етапи виконання робіт.

Процес створення КСЗІ доцільно поділяти на три основні етапи: попередній, проектування і розробки КСЗІ, проведення випробувань і передачі в експлуатацію КСЗІ. Кожний з етапів допускається поділяти на окремі підетапи.

До переліку робіт етапу проектування і розробки КСЗІ включаються роботи з вибору і модернізації штатних засобів захисту ПЗ і апаратури, що використовуються, архітектури ЗОТ, стандартних інтерфейсів і протоколів обміну, а також з розробки додаткового ПЗ і апаратної частини засобів захисту.

Етап випробувань і передачі в експлуатацію КСЗІ містить роботи, пов'язані з забезпеченням організації та проведення випробувань, включаючи, в разі необхідності, розробку спеціальної апаратури, ПЗ і відповідної документації.

Всі основні роботи кожного етапу відображаються в календарному плані, де зазначаються терміни проведення робіт за окремими етапами, види звітності і форми подання результатів замовнику.

Порядок внесення змін і доповнень до технічного завдання.

Зміни затвердженого ТЗ на створення КСЗІ в АС, необхідність внесення яких виявлена в процесі виконання робіт, оформляються окремим доповненням, яке погоджується і затверджується в тому ж порядку і на тому ж рівні, що і основний документ.

Доповнення до ТЗ на створення КСЗІ в АС складається з вступної

частини і змінюваних підрозділів. У вступній частині зазначається причина випуску доповнення. В змінюваних підрозділах наводяться номери та зміст змінюваних, нових або пунктів, що скасовуються.

Порядок проведення випробувань комплексної системи захисту інформації.

Для кожного виду випробувань (попередніх, державних, сертифікаційних та ін.) комплексної системи (підсистеми, компонента) захисту виконавець розробляє "Програму і методику випробувань комплексної системи (підсистеми, компонента) захисту інформації в АС", яка затверджується в установленому порядку. Терміни подання проекту Програми, його розгляду і затвердження погоджуються з замовником.

Для проведення випробувань замовником призначається комісія, склад якої погоджується з розробником КСЗІ.

Випробування проводяться з використанням умовної інформації (що не є ІзОД).

Наводиться необхідне для проведення випробувань забезпечення (необхідна нормативна, методична та інша документація, програмні та технічні засоби, метрологічне, спеціальне та інше обладнання, створення інших умов для проведення випробувань), сторона, що його надає, порядок усунення зауважень і т.ін.

Наводиться перелік документів, якими завершуються випробування (етапи випробувань): акт приймання, сертифікат (атестат, експертний висновок) відповідності встановленим критеріям, наказ про введення в експлуатацію тощо..

Погодження Технічного завдання.

Після того, як ТЗ на створення КСЗІ в ІКС розроблене, воно має бути погоджено з органами Держспецзв'язку згідно вимог статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»:

43) погодження проектів (завдань) створення та розвитку інформаційно-комунікаційних систем, систем спеціального зв'язку, систем електронного документообігу (в частині захисту інформації), в яких оброблятимуться державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, організація проведення їх експертної оцінки;

49) погодження та здійснення контролю за виконанням технічних завдань на проектування, будівництво і реконструкцію особливо важливих об'єктів і на розроблення зразків військової та спеціальної техніки в частині протидії технічним розвідкам;

4 етап - Розробка проекту КСЗІ.

Проект КСЗІ розробляється на підставі та у відповідності до погодженого та затвердженого «Технічного завдання на створення КСЗІ в ІКС» (ТЗ) згідно вимог розділу 6.4 «Розробка проекту КСЗІ» НД ТЗІ 3.7-003-2023.

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 ІКС: ескізний, технічний і робочий проект. Дозволяється вилучати етап ескізний проект, а також поєднувати етапи технічного і робочого проектів в один етап техноробочий проект.

Для всіх стадій розробки проекту КСЗІ склад документації визначається ТЗ на КСЗІ та НД ТЗІ 2.5-004-99. Додатково розробляється документація на програмні та технічні засоби.

Ескізний проект КСЗІ.

На цьому етапі 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.

Визначаються: функції КСЗІ в цілому та функції її окремих складових частин; склад комплексів ТЗІ від витоку технічними каналами та спеціальних впливів; склад заходів протидії технічним розвідкам, організаційних, правових та інших заходів захисту; склад КЗЗ; 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 етап ескізного проекту, у такому випадку документація ескізного проекту не розробляється.

Технічний проект КСЗІ.

Виконується розробка: загальних проектних рішень, необхідних для реалізації вимог ТЗ; рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів), алгоритмів функціонування та умов використання засобів захисту; рішень щодо архітектури КЗЗ та механізмів реалізації, визначених функціональним профілем послуг безпеки інформації.

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 розроблення, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ. Зміст та стиль документації повинні бути достатніми для забезпечення реалізації вимог ТЗ; рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів); рішень щодо архітектури та складу КЗЗ (у тому числі щодо засобів антивірусного захисту, засобів виявлення та попередження про мережеві вторгнення тощо); рішень щодо механізмів реалізації ФПБ, визначених у наведеному в ТЗ ФПЗ; рішень щодо алгоритмів, порядку та умов функціонування засобів захисту інформації, які використовуються у складі КЗЗ для реалізації певних функцій захисту.

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 розроблення 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 КСЗІ.

На цьому етапі здійснюється розроблення, 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 пусканалагоджувальних робіт і тестування підсистем та засобів КСЗІ.

У разі обробки в ІКС секретної інформації до складу робочої документації на комплекси ТЗІ від витоків технічними каналами повинні входити схеми розміщення засобів ІКС, 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 ІКС та іншими технічними засобами, що знаходяться у приміщеннях, де розташоване обладнання ІКС, та у суміжних приміщеннях (засоби зв'язку, системи та засоби кондиціонування, сигналізації, електроосвітлення тощо). Зазначені умови розміщення та мінімально

допустимі відстані беруться з експлуатаційної документації, яка супроводжує сертифіковані засоби ІКС.

До складу робочої документації на КЗЗ повинні входити описи процедур інсталяції та ініціалізації комплексу, налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІКС, контролю за діями користувачів, формування та актуалізації баз даних захисту, а також контролю цілісності програмного забезпечення та баз даних захисту.

Експлуатаційна документація включає опис порядку функціонування КСЗІ та настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом і користувачами, порядку супроводження КСЗІ впродовж життєвого циклу ІКС.

Дозволяється поєднувати етапи технічного та робочого проектів ***в один етап техно-робочого проекту КСЗІ.***

Згідно вимог вище зазначених стандартів техно-робочий проект КСЗІ повинен містити такі документи:

- 1) відомість проекту;
- 2) відомість виробів, що закуповуються;
- 3) пояснювальна записка до проекту;
- 4) опис завдань і функцій КСЗІ;
- 5) опис інформаційного забезпечення КСЗІ;
- 6) опис комплексу технічних засобів;
- 7) опис програмного забезпечення КСЗІ;
- 8) опис комплексу засобів захисту від НСД;
- 9) опис алгоритмів реалізації ФПБ;
- 10) опис організаційної структури;
- 11) відомість устаткування та матеріалів;
- 12) кошторисний розрахунок створення КСЗІ;
- 13) проектна оцінка надійності КСЗІ.

Для службового користування
(по заповненню)
Прим. № _____

(повна назва органу)

ЗАТВЕРДЖУЮ
Керівник органу

« _____ » _____ 202_ р.
мп

Автоматизована система класу «І» для обробки конфіденційної інформації,
що є власністю держави, в _____

(структурний підрозділ та назва органу)

(_____)

(скорочена назва автоматизованої системи)

(ЛОЗА-І)

Комплексна система захисту інформації

Технічне завдання

ПОГОДЖЕНО

Керівник підрозділу захисту
інформації

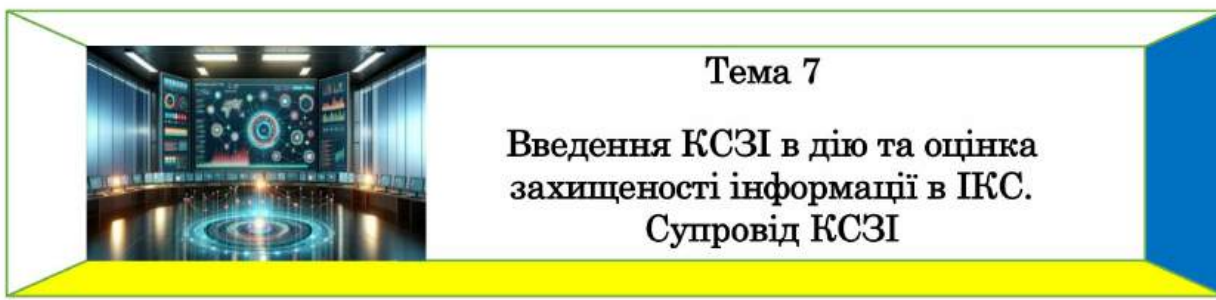
« _____ » _____ 202_ р.

ПОГОДЖЕНО

« _____ » _____ 202_ р.

ЗМІСТ

1. ЗАГАЛЬНІ ВІДОМОСТІ	
2. ПРИЗНАЧЕННЯ ТА МЕТА СТВОРЕННЯ КСЗІ	
3. ЗАГАЛЬНА ХАРАКТЕРИСТИКА АС ТА УМОВ ЇЇ ФУНКЦІОНУВАННЯ	
3.1. Характеристика обчислювальної системи	
3.2. Характеристика фізичного середовища	
3.3. Характеристика користувачів	
3.4. Характеристика інформації, що обробляється в АС	
3.5. Характеристика технології обробки інформації	
3.6. Можливі загрози інформації	
4. ВИМОГИ ДО КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ	
4.1. Організаційне забезпечення захисту	
4.2. Вимоги до комплексної системи захисту інформації у частині захисту від несанкціонованого доступу	
4.2.1. Політика безпеки інформації	
4.2.1.1. Об'єкти доступу	
4.2.1.2. Принципи керування доступом	
4.2.1.3. Правила розмежування інформаційних потоків	
4.2.1.4. Атрибути доступу об'єктів доступу	
4.2.1.5. Атрибути доступу користувачів	
4.2.1.6. Види доступу	
4.2.1.7. Правила розмежування доступу	
4.2.1.8. Правила адміністрування КЗЗ	
4.2.1.9. Реєстрація дій користувачів	
4.2.1.10. Правила маркування носіїв	
4.2.2. Вимоги до послуг безпеки	
4.2.2.1. Адміністративна конфіденційність	
4.2.2.2. Повторне використання об'єктів	
4.2.2.3. Адміністративна цілісність	
4.2.2.4. Гаряча заміна	
4.2.2.5. Відновлення після збоїв	
4.2.2.6. Реєстрація	
4.2.2.7. Ідентифікація і автентифікація	
4.2.2.8. Достовірний канал	
4.2.2.9. Розподіл обов'язків	
4.2.2.10. Цілісність комплексу засобів захисту	
4.2.2.11. Самотестування	
4.2.2.12. Керованість КЗЗ	
4.2.3. Вимоги до гарантій реалізації	
5. ВИМОГИ ДО СКЛАДУ ПРОЕКТНОЇ ТА ЕКСПЛУАТАЦІЙНОЇ ДОКУМЕНТАЦІЇ	
6. ЕТАПИ ВИКОНАННЯ РОБІТ	
7. ПОРЯДОК ВНЕСЕННЯ ЗМІН І ДОПОВНЕНЬ ДО ТЕХНІЧНОГО ЗАВДАННЯ	
8. ПОРЯДОК ПРОВЕДЕННЯ ВИПРОБУВАНЬ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ	
ПЕРЕЛІК СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ	



5 етап - Введення КСЗІ в дію та оцінка захищеності інформації в ІКС

5.1. Підготовка КСЗІ до введення в дію

5.2. Навчання користувачів

5.3. Комплектування КСЗІ

5.4. Будівельно-монтажні роботи

5.5. Пуско-налагоджувальні роботи

5.6. Попередні випробування КСЗІ

5.7. Дослідна експлуатація КСЗІ

5.8. Державна експертиза КСЗІ

5.1. Підготовка КСЗІ до введення в дію:

- проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІКС;

- 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, що входять до Плану захисту (за виключенням тих, для розробки яких необхідні результати наступних етапів робіт).

Створення СЗІ та розробка Плану захисту здійснюються згідно з НД ТЗІ 1.4-001-2000.

5.2. Навчання користувачів

Проводиться навчання користувачів ІКС 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 правил політики безпеки інформації, експлуатації засобів захисту інформації тощо, проводиться перевірка їх умінь користуватися впровадженими технологіями захисту інформації і реєстрація результатів навчання.

5.3. Комплектування КСЗІ

Забезпечується отримання продукції (засобів захисту інформації, матеріалів, обладнання та іншого) від постачальників та співвиконавців робіт. Приймається рішення щодо підготовки до

проведення оцінки на відповідність вимогам НД ТЗІ засобів захисту, які на момент проектування КСЗІ не мали відповідного сертифіката або експертного висновку, а також щодо порядку проведення такої оцінки під час державної експертизи КСЗІ.

5.4. Будівельно-монтажні роботи

Роботи цього етапу виконуються під час переобладнання існуючих або при будівництві нових спеціалізованих споруд (приміщень), призначених для розміщення технічних засобів ІКС та персоналу, сховищ матеріальних носіїв інформації.

При проведенні будівельно-монтажних робіт враховуються вимоги технічного завдання на створення КСЗІ в ІКС. Будівельні роботи проводяться силами організації-власника ІКС або будівельно-монтажних організацій згідно з проектною документацією на будівництво, яка розробляється проектною організацією відповідно до вимог ДБН 2.2-3-2012.

Після завершення будівельних робіт **створюється комісія з прийняття робіт**, до складу якої входять представники організації-замовника будівельних робіт, проектної та будівельно-монтажної організацій. За результатами роботи комісії складається за довільною формою **акт приймання робіт** з оцінкою їх відповідності вимогам ТЗІ, який затверджується керівником організації-замовника будівництва.

5.5. Пуско-налагоджувальні роботи

Метою пусконалагоджувальних робіт є:

- монтаж обладнання і атестація комплексу технічного захисту інформації від витoku технічними каналами;
- встановлення і налагодження КЗЗ;
- перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії.

Монтаж ОТЗ ІКС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту. Якщо до складу КСЗІ входять ОТЗ, які не мають сертифіката або експертного висновку про відповідність вимогам з ТЗІ, визначаються мінімально допустимі відстані між цими засобами та ДТЗ за результатами їх спеціальних досліджень.

У разі неможливості дотримання вимог з розміщення ОТЗ або наявності підстав щодо можливого порушення умов їх постачання оцінка монтажних робіт ОТЗ має бути підтверджена результатами контрольних інструментальних вимірювань рівня ПЕМВН.

Спеціальні дослідження та інструментальні вимірювання рівня ПЕМВН виконуються підрозділом ТЗІ організації-власника ІКС або іншими суб'єктами господарювання за умови наявності ліцензії чи дозволу на проведення відповідного виду робіт. За результатами робіт складається акт, де зазначаються:

категорії приміщень, де розташоване обладнання ІКС, межі контрольованих зон для приміщень, перелік ОТЗ, ДТЗ і комунікацій (із зазначенням найменування, типу, заводського номера), що знаходяться у цих приміщеннях, оцінка відповідності проведення монтажних робіт вимогам експлуатаційних документів на засоби та НД ТЗІ 3.6-003-2016, пропозиції щодо застосування додаткових заходів захисту, впровадження яких є необхідним у разі неможливості під час виконання монтажних робіт дотримання окремих вимог із розміщення ОТЗ. Акт затверджується керівником організації - власника ІКС.

Упроваджуються додаткові заходи захисту, необхідність впровадження яких зафіксована в акті, відповідно до порядку проведення робіт етапу та відповідне коригування проектної, робочої, експлуатаційної документації. Оцінка повноти та якості виконання робіт з ТЗІ в приміщеннях проводиться шляхом атестації впровадженого комплексу ТЗІ від виток технічними каналами, за результатами якої реєструється **Акт атестації комплексу технічного захисту інформації**.

Проводяться інсталяція, ініціалізація та перевірка працездатності КЗЗ згідно з документацією робочого проекту. Інсталяція та ініціалізація КЗЗ, який має експертний висновок про відповідність вимогам НД ТЗІ, здійснюються в порядку, визначеному в експлуатаційній документації на цей комплекс. Під час інсталяції мають бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІКС, контролю за діями користувачів, а також контролю цілісності програмного забезпечення та бази даних захисту КЗЗ.

До бази даних захисту вносяться відомості про користувачів ІКС, встановлюються їх повноваження щодо доступу до захищених об'єктів КС, їх створення, модифікації, архівування, знищення, експорту/імпорту із системи та інші дані.

5.6. Попередні випробування КСЗІ

Метою попередніх випробувань є перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію. Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

Попередні випробування проводяться згідно з **програмою та методиками випробувань**. Програму й методики випробувань готує розробник КСЗІ, а узгоджує замовник ІКС. Програма та методики випробувань, протоколи випробувань розробляються та оформлюються згідно з вимогами РД 50-34.698.

Попередні випробування організовує замовник ІКС, а проводить розробник КСЗІ спільно із замовником. Для проведення попередніх випробувань замовником ІКС створюється комісія. Головою комісії призначається представник замовника.

Результати попередніх випробувань оформлюються **протоколом випробувань**, де міститься висновок щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідних заходів з їх усунення, і рекомендовані терміни виконання цих робіт. Після усунення недоліків у випадку їх наявності та коригування проєктної, робочої, експлуатаційної документації КСЗІ оформлюється акт про приймання КСЗІ у дослідну експлуатацію.

5.7. Дослідна експлуатація КСЗІ

Під час дослідної експлуатації КСЗІ:

- відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІКС та автоматизованого контролю за діями користувачів;

- співробітники СЗІ та користувачі ІКС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

- здійснюється (у разі потреби) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КСЗІ;

- здійснюється (у разі потреби) коригування робочої та експлуатаційної документації.

За результатами робіт за довільною формою складається акт про завершення дослідної експлуатації, який містить висновок щодо можливості (неможливості) подання КСЗІ на державну експертизу.

5.8. Державна експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом приймальних випробувань ІКС і проводиться з метою визначення відповідності КСЗІ технічному завданню, вимогам НД із захисту інформації та визначення можливості введення КСЗІ в складі ІКС в експлуатацію.

Державна експертиза КСЗІ в ІКС проводиться згідно з **Положенням про державну експертизу у сфері технічного захисту інформації**, затвердженим наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087.

Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо через якісь причини усунути недоліки в ході експертизи неможливо, це оформлюється актом, до якого вноситься перелік необхідних доробок та рекомендації щодо їх виконання. Після завершення передбачених актом робіт проводиться повторна експертиза.

Для інтегрованих ІКС може проводитися державна експертиза кожної складової частини (модуля) КСЗІ окремо.

Державна експертиза КСЗІ інтегрованої ІКС 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 ІКС в цілому, оформлюються з урахуванням відповідних документів на складові частини КСЗІ. Якщо інтегрована КСЗІ має у своєму складі типові модулі, які створювалися за єдиним ТЗ, то експертиза таких модулів КСЗІ виконується в два етапи: на першому проводиться в повному обсязі експертиза одного обраного типового модуля, а на другому - проводиться перевірка відповідності умов експлуатації типовим на кожному конкретному об'єкті для всіх модулів КСЗІ цього типу.

Введення до складу діючої КСЗІ нового (оціненого) модуля здійснюється без проведення повторної експертизи всієї КСЗІ. Проводиться оцінювання взаємодії нового модуля зі складовими частинами КСЗІ, які вже знаходяться в експлуатації. Допускається розпочинати і проводити державну експертизу КСЗІ паралельно з роботами етапів проектування. У першу чергу такий порядок рекомендується застосовувати для складних з точки зору архітектури, складу та обсягів робіт КСЗІ. При цьому експертами послідовно проводиться оцінка технічних та організаційних рішень на всіх етапах робіт. Це дає змогу оперативно усувати недоліки проектування та коротити час проведення державної експертизи, яка може бути в основному завершена до етапу приймальних випробувань ІКС.

6 етап - Супроводження КСЗІ.

Виконуються роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійного і післягарантійного технічного обслуговування засобів захисту інформації.

Весь період функціонування КСЗІ забезпечується її супроводом, під час якого персоналом ІКС виконуються такі роботи щодо:

- організаційного забезпечення працездатності ІКС;
- керування КСЗІ згідно Плану захисту та експлуатаційної документації на КСЗІ;
- гарантійного та післягарантійного технічного обслуговування засобів КСЗІ;
- вдосконалення та модернізації КСЗІ, відповідного оновлення документів КСЗІ.

Всі заходи супроводу та модернізації КСЗІ вносяться до Календарного плану робіт із захисту інформації в ІКС, який щорічно поновлюється.

Виконання Календарного плану забезпечується Службою захисту інформації (СЗІ) в ІКС, 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 ІКС, 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 ІКС (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 ІКС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;
- підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в ІКС, впровадження нових технологій захисту і модернізації КСЗІ;
- організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІКС або КСЗІ;
- участь в роботах з модернізації ІКС - узгодженні пропозицій з введення до складу ІКС 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 ІКС (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 ІКС і типові правила, встановлені для персоналу і користувачів ІКС;
- негайне втручання в процес роботи ІКС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;

- регулярне подання звітів керівництву організації про виконання користувачами ІКС вимог щодо захисту інформації;

- аналіз відомостей щодо засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів для організації;

- розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу ІКС;

- участь в організації і проведенні навчання користувачів і персоналу ІКС 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 ІКС 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 згідно вимог НД ТЗІ входять (приклади):

- інструкції щодо забезпечення правил оброблення ІзОД в ІКС;
- інструкції співробітників СЗІ, персоналу та користувачів ІКС;
- 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 ІКС;
- порядок обліку і супроводження архівів та ротації носіїв інформації;

- інструкція про порядок оперативного відновлення функціонування ІКС;

- інструкція про організацію контролю за функціонуванням КСЗІ;

- інструкція про порядок розробки, впровадження та модернізації ПЗ ІКС;

- інструкція про порядок проведення ремонтних робіт.
- правила видачі, вилучення та обліку персональних ідентифікаторів;
- правила управління паролями в ІКС;
- правила класифікації та класифікатор інформації і користувачів ІКС;
- формуляр (паспорт) ІКС;
- 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 зазначених реєстраційних журналів можна розглядати такі:

- обліку користувачів ІКС;
- обліку роботи користувачів ІКС;
- обліку захищених інформаційних ресурсів ІКС;
- реєстрації проведених робіт з технічного обслуговування, ремонту, модернізації;
- реєстрації перевірок складу програмних засобів ІКС;
- реєстрації позаштатних ситуацій у роботі ІКС.

У випадку, якщо в ІКС передбачається оброблення ІзОД, заводяться журнал обліку матеріальних носіїв ІзОД та журнал обліку сховищ, де носії зберігаються.

Якщо в ІКС передбачається оброблення службової інформації, під час функціонування ІКС використовуються такі журнали, форми, акти, замовлення, реєстраційно-контрольна картка та правила ведення яких встановлені типова інструкція **«Про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію»**, затвердженою постановою Кабінету Міністрів України від 19 жовтня 2016 р. № 736:

- обліку документів та видань з грифом «Для службового користування»;
- обліку машинних носіїв інформації з грифом «Для службового користування».

Якщо в ІКС передбачається оброблення таємною інформацією, під час функціонування ІКС використовуються правила встановлені **«Порядок організації та забезпечення режиму секретності»**, затвердженим постановою Кабінету Міністрів України від 18.12.2013 № 939. Цей порядок є ключовим інструментом, що забезпечує охорону державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин та безпеки. Основні положення:

- Функції PCO. Створення режимно-секретних підрозділів (PCO) є обов'язковим для підприємств, що працюють з таємною інформацією, підпорядковуються вони безпосередньо керівнику.

- Режим секретності. Сукупність заходів, що виключають доступ до таємної інформації осіб, які не мають допуску, або у випадках, не передбачених законом.

- Документальне забезпечення. Суворий облік секретної кореспонденції, документів, журналів та видань. Доступ до документів здійснюється лише за наявності допуску та доступу відповідної форми.

Адміністратор безпеки під час супроводу КСЗІ зобов'язаний:

- контролювати встановлення ПЗ, його працездатність та оновлення, конфігурування політики безпеки ІКС;

- забезпечувати конфігурування КЗЗ, ПЗ для захисту інформації, налагодження антивірусного ПЗ та елементів ІКС, які мають вбудовані функції захисту;

- забезпечувати надійне функціонування КЗЗ і ПЗ для захисту інформації, антивірусного ПЗ та контролювати його працездатність;

- встановлювати в ІКС 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 ІКС;

- відновлювати роботу засобів захисту у разі їх збоїв або виходу з ладу;

- брати участь у впровадженні заходів захисту інформації в ІКС та здійснювати контроль умов використання ІКС відповідно до експлуатаційної документації та вимог приписів на експлуатацію об'єктів ІКС;

- здійснювати адміністрування в частині захисту інформації та оновлення баз даних захисту ІКС;

- забезпечувати проведення технічного обслуговування та контролю за функціонуванням засобів захисту інформації;

- здійснювати опечатування вузлів, блоків, усіх портів ІКС та щоденний контроль за його станом;

- проводити поточний контроль за забезпеченням режиму обробки та захисту інформації в ІКС згідно затвердженої інструкції;

- проводити інструктаж та навчання персоналу з питань дотримання вимог забезпечення режиму обробки та захисту інформації в ІКС;

- здійснювати контроль за роботою користувачів та виконанням ними вимог щодо захисту інформації шляхом періодичних спостережень за діями користувачів під час роботи в ІКС (вибірково);

- здійснювати контроль за проведенням робіт з ремонту та заміни технічних засобів ІКС або комплексу ТЗІ;

- вносити пропозиції та брати участь у проектуванні, створенні та дослідній експлуатації КСЗІ в ІКС;

- доповідати керівнику СЗІ про всі виявлені порушення режиму обробки та захисту інформації в ІКС.

Системний адміністратор під час супроводу КСЗІ зобов'язаний:

- встановлювати та налаштовувати ОС та необхідне для роботи апаратне й програмне забезпечення (АПЗ);

- встановлювати на ІКС сертифіковане антивірусне програмне забезпечення (ПЗ) та оновлювати його бази даних, після чого перевіряти ІКС на наявність комп'ютерних вірусів;

- підтримувати робочий стан ОС і АПЗ ІКС та контролювати їх працездатність;

- навчати користувачів роботі на ІКС і формуванню її інформаційного фонду;

- зберігати еталони ПЗ та резервні копії інформаційних фондів ІКС для відновлення її роботи після аварійних ушкоджень або ураження комп'ютерними вірусами;

- вести та оновлювати фонд дозволеного до використання ПЗ ІКС, щорічно проводити його інвентаризацію;

- щомісячно контролювати копіювання інформаційних фондів ІКС на зареєстровані зовнішні носії інформації згідно затвердженої інструкції;

- оперативно відновлювати працездатність ІКС при збоях і виході з ладу ОС і АПЗ ІКС згідно затвердженої інструкції;

- брати участь у проведенні інвентаризації ІКС;

- здійснювати контроль за проведенням ремонту та монтажу устаткування ІКС фахівцями сторонніх організацій;

- виявляти помилки користувачів та проводити їх інструктаж;

- готувати пропозиції з модернізації та придбання ІКС, АПЗ, розвитку автоматизації обробки даних;

- готувати пропозиції до планів роботи підрозділів стосовно заходів із забезпечення надійного та безперебійного функціонування ІКС;

- інформувати керівника СЗІ про випадки порушень правил експлуатації ІКС та обробки інформації.

Користувач під час супроводу КСЗІ зобов'язаний:

- використовувати надані інформацію ідентифікації та автентифікації (пароль) виключно для роботи з ІКС;

- 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 ІКС резервне копіювання на з'ємні носії інформації, яка важлива для забезпечення службової діяльності установи;

- спільно з адміністратором ІКС визначати «папки» (файли) зі службовою інформацією, розпорядником якої є користувач, для встановлення аудиту прав доступу;

- негайно інформувати адміністратора про відхилення в нормальній роботі ІКС, системного та прикладного ПЗ, виходу із ладу або нестійкого функціонування технічних засобів ІКС, а також порушення цілісності або невідповідності печаток (пломб) вузлів та блоків, портів введення-виведення інформації технічних засобів ІКС.

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 ІКС, 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 ІКС», 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 ІКС.

Під час планових та позапланових перевірок перевіряються такі питання:

- дотримання користувачами ІКС встановлених вимог щодо забезпечення режиму обробки та захисту ІзОД;

- комплектація ІКС згідно з Формуляром;
- наявність та дотримання вимог приписів на експлуатацію об'єктів ІКС;
- виконання заходів щодо забезпечення захисту ІзОД від НСД на відповідність вимогам технічної та експлуатаційної документації, згідно з якими здійснюється експлуатація ІКС;
- відповідність ступеня обмеження доступу інформації, яка обробляється з використанням ІКС, наданій категорії об'єкта ІКС;
- 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 ІКС 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.

Повсякденний контроль за забезпеченням режиму під час обробки інформації в ІКС здійснюється СЗІ. Порядок його проведення та усунення виявлених недоліків або порушень вимог НД ТЗІ та інших нормативно-правових актів у сфері захисту інформації визначається 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 ІКС 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 з метою забезпечення органів державної влади, органів місцевого самоврядування, утворених відповідно до законів України військових формувань, підприємств, установ та організацій державної форми власності антивірусними оновленнями для антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації.

Поняття, що використовуються у цьому Порядку:

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

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 ІКС без відома користувача, й направлена на деструктивну дію;

антивірусний програмний засіб (АВПЗ) - програмне забезпечення, яке призначене для захисту об'єктів/ресурсів ІКС від ушкодження комп'ютерними вірусами;

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

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 (стаття 9):

- не менше ніж раз на день отримують антивірусні оновлення АВПЗ за допомогою веб-серверу ЦАЗІ (www.cazi.dsszzi.gov.ua);

(Інструкція користувача https://cazi.gov.ua/assets/files/cazi_instructions_01.09.2023.pdf)

- інсталиють отримані за допомогою веб-серверу ЦАЗІ (www.cazi.dsszzi.gov.ua) 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 надають до Адміністрації Держспецв'язку відомості щодо кожного користувача у паперовому вигляді за формою "Реєстраційна інформація для доступу до ресурсів веб-серверу Центру антивірусного захисту інформації" (рис. 1).

Крім того, всі міністерства, інші центральні органи виконавчої влади, обласні державні адміністрації, а також підприємства, установи та організації, що належать до сфери їх управління, (державні органи) подають відомості про створені ІКС, згідно вимог «Положення про Реєстр інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем державних органів, а також підприємств, установ і організацій, що належать до сфери їх управління», затвердженого постановою КМУ від 03.08.2005 № 688.

Це Положення визначає порядок функціонування Реєстру інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем державних органів, а також підприємств, установ і організацій, що належать до сфери їх управління, до якого

вносяться відомості про інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи державних органів, а також підприємств, установ і організацій, що належать до сфери їх управління (системи), які є розподіленими багатомашинними багатокористувачевими комплексами з передачею даних через незахищене середовище.

Інформація про систему подається до Реєстру створювачами реєстрової інформації:

*один раз на рік станом на 1 січня - до 1 лютого поточного року;
за результатами виконання перших етапів стадій життєвого циклу системи - проектування, промислової експлуатації, виведення з промислової експлуатації системи - протягом 30 днів з дня завершення етапу.*

РЕЄСТРАЦІЙНА ІНФОРМАЦІЯ
для доступу до ресурсів веб-серверу Центру антивірусного захисту
інформації

Призначення поля	Значення
Повна назва установи	
Прізвище, ім'я, по батькові користувача	
Посада користувача	
Назва та версія антивірусного програмног засобу	
Перелік IP-адрес для доступу до ресурсів веб-серверу Центру антивірусного захисту інформації	
Телефон користувача	
Адреса електронної пошти користувача	
Ім'я користувача*	

Рисунок 1 – Реєстраційна інформація для доступу до ресурсів веб-серверу Центру антивірусного захисту інформації

Особливості побудови КСЗІ з використанням базових профілів безпеки. Роботи з побудови КСЗІ можуть проводитися з використанням базових профілів безпеки, затверджених Адміністрацією Держспецзв'язку, для відповідного виду інформації, що обробляється в ІКС. Побудова КСЗІ ІКС з використанням базових профілів проводиться відповідно до НД ТЗІ 3.6-004-21.

Оцінка КСЗІ ІКС, яка побудована з використанням базових профілів безпеки, здійснюється під час проведення державної експертизи відповідно до НД ТЗІ 2.3-025-21.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Закон України «Про критичну інфраструктуру»
2. Закон України «Про інформацію»
3. Закон України «Про доступ до публічної інформації»
4. Закон України «Про державну таємницю»
5. Закон України «Про захист персональних даних»
6. Закон України «Про захист інформації в інформаційно-комунікаційних системах»
7. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури»
8. Постанова Кабінету Міністрів України від 22 липня 2022 р. № 821 «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури»
9. Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1174 «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури»
10. Постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1175 «Деякі питання подання інформації у сфері захисту критичної інфраструктури»
11. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури»
12. Концепція технічного захисту інформації в Україні
13. Наказ Адміністрації Держспецзв'язку від 15.01.2021 № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури»
14. ДСТУ ISO/IEC 27005:2023 «Інформаційна технологія. Методи забезпечення безпеки. Керування ризиками інформаційної безпеки»
15. ДСТУ ISO/IEC 15408-1:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель» (ISO/IEC 15408-1:2022, IDT) ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ (ISO/IEC 18045:2008, IDT)
16. ДСТУ ISO/IEC 15408-1:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель» (ISO/IEC 15408-1:2009, IDT)
17. ДСТУ ISO/IEC 15408-2:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги» (ISO/IEC 15408-2:2008, IDT)
18. ДСТУ ISO/IEC 15408-3:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки» (ISO/IEC 15408-3:2008, IDT)

19. НД ТЗІ 1.1-003-99 Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу
20. НД ТЗІ 2.5-004-99 Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу
21. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
22. НД ТЗІ 3.7-001-99 Методичні вказівки з розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
23. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
24. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу
25. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
26. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу
27. 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
28. НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах
29. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі
30. НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці
31. НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації
32. НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем
33. НД ТЗІ 3.6-008-21 Порядок моніторингу безпеки інформаційних систем

34. НД ТЗІ 3.6-007-21 Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

35. НД ТЗІ 2.3-025-24 Т1 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

36. НД ТЗІ 2.3-025-24 Т2 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

37. НД ТЗІ 2.3-025-24 Т3 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

38. НД ТЗІ 2.6-004-21 Порядок авторизації безпеки інформаційних систем

39. НД ТЗІ 2.7-009-2009 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

40. НД ТЗІ 2.7-010-2009 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

41. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 93 «Положення про державну експертизу в сфері технічного захисту інформації»

42. Наказ Адміністрації Держспецзв'язку від 26.03.2007 № 45 «Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ»

43. Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 93 «Положенням про державну експертизу у сфері технічного захисту інформації»

44. Типова інструкція «Про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» затвердженою постановою Кабінету Міністрів України від 19 жовтня 2016 р. № 736

45. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»