

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТИКИ ТА ІНФОРМАТИКИ**

ЕЛЕКТРОННИЙ НАВЧАЛЬНО-НАОЧНИЙ ПОСІБНИК

**СХЕМОКОНСПЕКТ ЛЕКЦІЙ
з навчальної дисципліни
«АРХІТЕКТУРА СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ»
для студентів всіх форм навчання освітнього ступеня «Бакалавр»
галузі знань 12 Інформаційні технології**

Дрогобич, 2025

Схемоконспект лекцій з навчальної дисципліни «Архітектура систем захисту інформації» для студентів всіх форм навчання освітнього ступеня «Бакалавр» галузі знань 12 Інформаційні технології : електронний навчально-наочний посібник / уклад. Я.Ю. Дорогий, Т.В. Алтухова – Дрогобич : ДонНТУ, 2025. – 689 с.

Навчальна дисципліна «Архітектура систем захисту інформації» є актуальною і затребуваною в контексті підготовки сучасних фахівців у галузі інформаційних технологій та кібербезпеки та з огляду на формування когнітивних, афективних та моторних компетентностей в контексті вивчення та розуміння принципів організації та побудови комплексних систем захисту інформації (КСЗІ).

Пропонований студентам для опанування схемоконспект лекцій з цієї дисципліни має за мету забезпечити їм певну допомогу під час вивчення ними ключових положень базових тем курсу. Схематична форма конспекту акцентує увагу студентів на закріпленні основних фахових знань, формуванні відповідних умінь і в цілому отриманні ними кваліфікаційних компетентностей.

Укладачі: _____ Я. Ю. Дорогий, професор, д. т. н., в.о. зав. кафедри ПМІ, Т.В. Алтухова, доцент, к.т.н., доцент кафедри ПМІ

Рецензент: _____ В. В. Цуркан, доцент, к. т. н., доцент спеціальної кафедри №5 ІСЗІ КПІ ім. Ігоря Сікорського,

Відповідальний за випуск: Я. Ю. Дорогий, професор, д. т. н., в.о. зав. каф. ПМІ

Затверджено навчально-методичним відділом ДонНТУ, протокол № 4 від 25.02.2025 р.

Розглянуто на засіданні кафедри прикладної математики і інформатики, протокол № 2 від 21.02.2025 р.



ЗМІСТ

3

ВСТУП		6
Тема 1.	Нормативно-правове забезпечення сфери захисту інформації.	
	Лекція 1. Вступ до дисципліни. Загальні концептуальні положення інформаційної безпеки. Нормативно-правове забезпечення захисту інформації.	7
Тема 2.	Моделі порушника та загроз для інформації в ІТС.	
	Лекція 2. Вразливості інформаційної безпеки в ІКС та інструменти/методи їх пошуку/аналізу/захисту.	53
	Лекція 3. Складання моделі порушника безпеки інформації в ІТС.	167
	Лекція 4. Складання моделі загроз для інформації в ІТС.	206
Тема 3.	Політика безпеки ІТС.	
	Лекція 5. Розробка політики безпеки інформації в ІТС. Складання Плану захисту інформації в ІТС.	236
Тема 4.	Комплексна система захисту інформації. Загальні положення.	
	Лекція 6. Загальні поняття комплексних систем захисту інформації. Типова архітектура КЗСІ.	273



	Лекція 7. Етапи створення та вимоги до формування комплексних систем захисту інформації (КСЗІ).	333
Тема 5.	Проектування КСЗІ.	
	Лекція 8. Формування завдання та варіанту побудови архітектури ПСЗІ. Основні вимоги до КЗЗ від несанкціонованого доступу (НСД).	382
	Лекція 9. Технічне завдання на створення КСЗІ. Проектування КСЗІ в ІТС.	408
Тема 6.	Введення в дію КСЗІ.	
	Лекція 10. Введення КСЗІ в дію та оцінка захищеності інформації.	426
	Лекція 11. Попередні випробування та дослідна експлуатація КСЗІ.	454
Тема 7.	Державна експертиза КСЗІ.	
	Лекція 12. Державна експертиза КСЗІ в ІТС.	484
Тема 8.	Супровід КСЗІ.	
	Лекція 13. Супровід КСЗІ в ІТС.	528



Тема 9.	Системи захисту інформації для різних автоматизованих систем.	
	Лекція 14. Побудова і структура гарантій реалізації послуг безпеки та вимоги щодо захисту інформації від НСД в автоматизованих системах (АС) класу 1.	580
	Лекція 15. Особливості захисту секретної інформації в АС класу 1.	611
	Лекція 16. КЗЗ від НСД, що мають експертні висновки.	642
	СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ ДЛЯ САМОПІДГОТОВКИ	687

У сучасних умовах розвитку інформаційних технологій, коли технологічний прогрес постійно набирає обертів, безпека інформації стає надзвичайно важливою сферою. Особливо в Україні, де прискорений цифровий розвиток та умови воєнної агресії вимагають відповідних заходів для забезпечення захисту інформації від різноманітних загроз. Курс "Архітектура систем захисту інформації" спрямований на розуміння та впровадження інтегрованих систем безпеки, спеціально адаптованих до реалій національного інформаційного простору та законодавства України.

Зосереджуючись на архітектурних аспектах захисту, цей курс дозволяє студентам здобути глибокі знання та практичні навички у сфері розробки та впровадження комплексних заходів безпеки. Він враховує технічні та стратегічні аспекти захисту інформації, адаптовані до динаміки сучасних загроз, що є особливо актуальним для української державної інформаційної інфраструктури.

Проходження курсу дозволить студентам освоїти сучасні методи та стратегії захисту інформаційних систем від широкого спектру загроз, інтегрувати їх в комплексні системи захисту інформації, оцінити отримані результати.

Лабораторні роботи не лише сприятимуть розвитку навичок проектування, але й допоможуть у впровадженні комплексних систем захисту інформації, враховуючи особливості нормативно-правового регулювання даної сфери в Україні.

Донецький національний технічний університет



Тема 1. Нормативно-правове забезпечення сфери захисту інформації.

Лекція 1. Вступ до дисципліни. Загальні концептуальні положення інформаційної безпеки. Нормативно-правове забезпечення захисту інформації

Предмет: АСЗІ

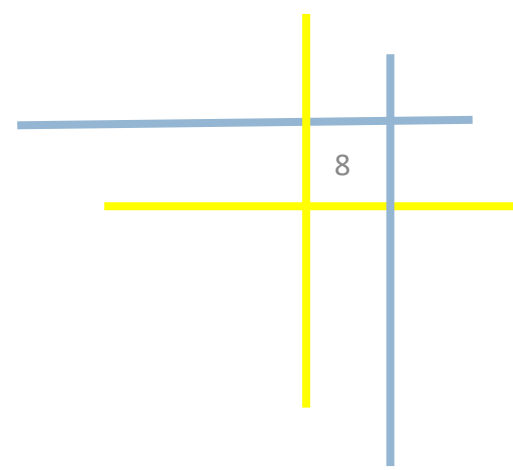
Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання



- ☐ Мета курсу
- ☐ Структура курсу
- ☐ РСО з дисципліни
- ☐ Системи захисту інформації
- ☐ Модель безпеки інформації, загрози
- ☐ Правовий захист інформації, основні НПА



Мета курсу

9

- ❑ Метою викладання навчальної дисципліни є формування системи теоретичних знань і практичних навичок з основ теорії, методів і засобів розробки архітектури комплексних систем захисту інформації.



Структура курсу

- ☐ 16 лекцій, 12 семінар-тестів
- ☐ 13 лабораторних робіт
- ☐ Іспит



РСО з дисципліни

- ☐ 13 лабораторних робіт оцінюються в 40 балів
- ☐ 12 семінар-тестів оцінюються в 60 балів
- ☐ Якщо все здано **вчасно**, то виставляється оцінка за іспит **автоматом**
- ☐ Якщо **не вчасно**, студент здає іспит у вигляді **екзаменаційного тесту на 100 питань**.



Системи захисту інформації



Інформація

- ❑ Інформація – це відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх представлення.
 - Інформація може мати різну форму (дані, закладені в комп'ютерах, кресленнях, пам'ятних записках, досьє, формулах, діаграмах, моделях продукції, дисертаціях, судових документах тощо).
 - Інформація має споживачів, що потребують її, і тому має певні споживчі якості, а також має і своїх володарів або виробників.
- ❑ З точки зору споживача, якість використовуваної інформації дозволяє отримувати додатковий економічний або моральний ефект.
- ❑ З точки зору власника – збереження в таємниці комерційно-важливої інформації дозволяє успішно конкурувати на ринку виробництва, збуту товарів і послуг. Це природньо вимагає певних дій, спрямованих на захист конфіденційної інформації.



Інформаційна безпека

□ **Інформаційна безпека** – це стан захищеності інформаційних ресурсів організації і підтримувальної інфраструктури від зовнішніх і внутрішніх загроз, які можуть завдати неприйняттого збитку суб'єктам інформаційних відношень.



Система захисту інформації (СЗІ)

□ **Система захисту інформації (СЗІ)** – це організована сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.



Концептуальні положення СЗІ

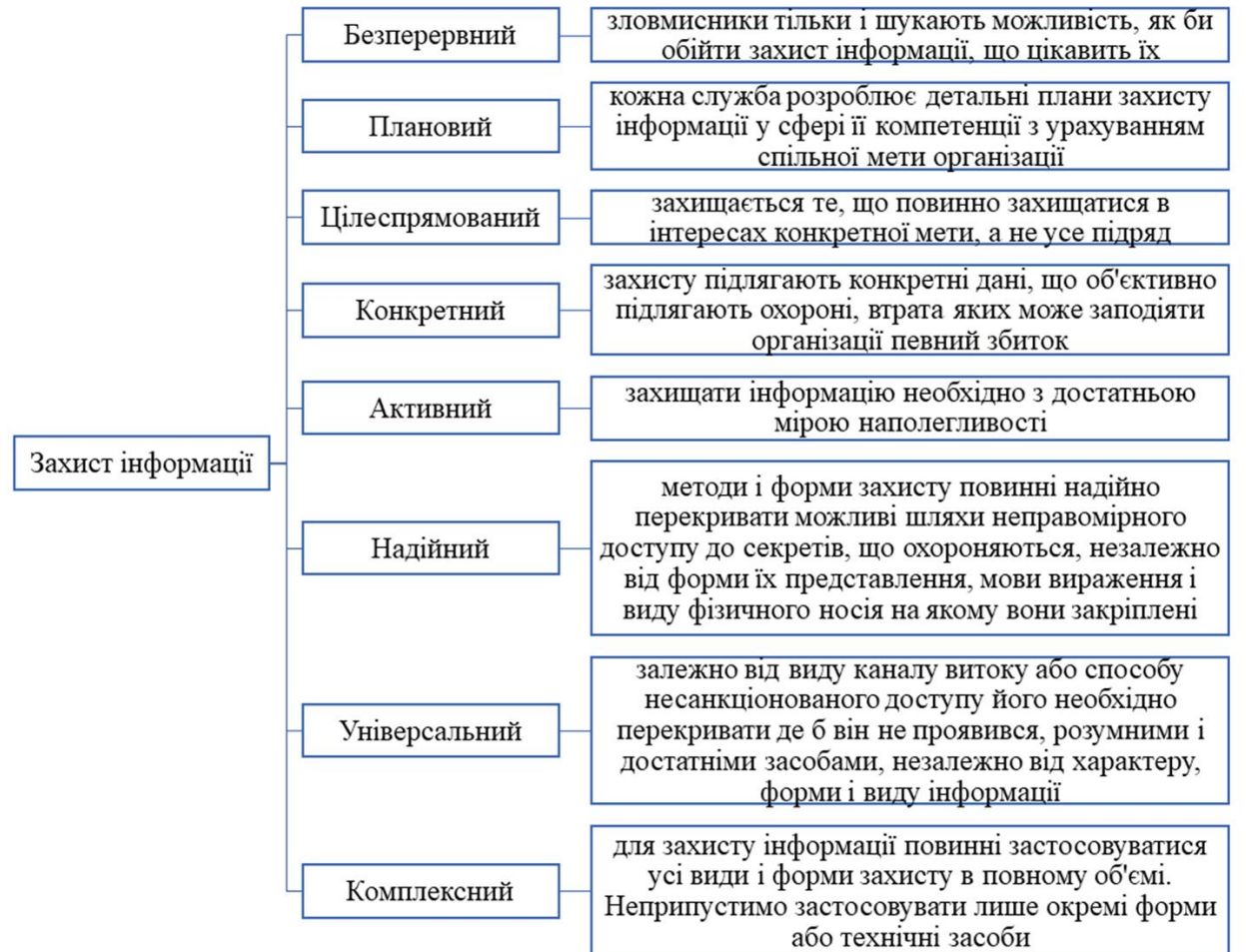
□ Основні концептуальні положення системи захисту інформації:

- **Забезпечення безпеки інформації не може бути одноразовим актом.** Це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення і розвитку системи захисту, безперервному контролю її стану, виявленні її вузьких і слабких місць і протиправних дій.
- Безпека інформації може бути забезпечена лише при комплексному використанні усього арсеналу наявних засобів захисту в усіх структурних елементах організації і на усіх етапах технологічного циклу обробки інформації.



Комплексний характер СЗІ

□ **Комплексний характер захисту** виникає з того, що **захист** – це специфічне явище, що є складною системою нерозривно взаємозв'язаних і взаємозалежних процесів, кожен з яких у свою чергу має безліч різних сторін, які взаємно обумовлюють один одного, властивостей, тенденцій.





Умови СЗІ

□ Для забезпечення виконання вимог безпеки СЗІ повинна задовольнятися певними умовами:

- охоплювати увесь технологічний комплекс інформаційної діяльності;
- бути різноманітною по використанню засобів, багаторівневою з ієрархічною послідовністю доступу;
- бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;
- бути нестандартною, різноманітною (при вибиранні засобів захисту не можна розраховувати на непоінформованість зловмисників відносно її можливостей);
- бути простою для технічного обслуговування і зручною для експлуатації користувачами;
- бути надійною (поломки технічних засобів є причиною появи неконтрольованих каналів витоку інформації);
- бути комплексною, мати цілісність, яка означає, що жодна її частина не може бути вилучена без збитку для усієї системи.



Вимоги до систем безпеки інформації

□ До системи безпеки інформації пред'являються також певні **ВИМОГИ**:

- чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
- надання користувачеві мінімальних повноважень, необхідних йому для виконання дорученої роботи;
- зведення до мінімуму числа засобів захисту, загальних для декількох користувачів;
- облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;
- забезпечення оцінки ступені конфіденційності інформації;
- забезпечення контролю цілісності засобів захисту і негайне реагування на їх вихід з ладу.



Види забезпечення СЗІ

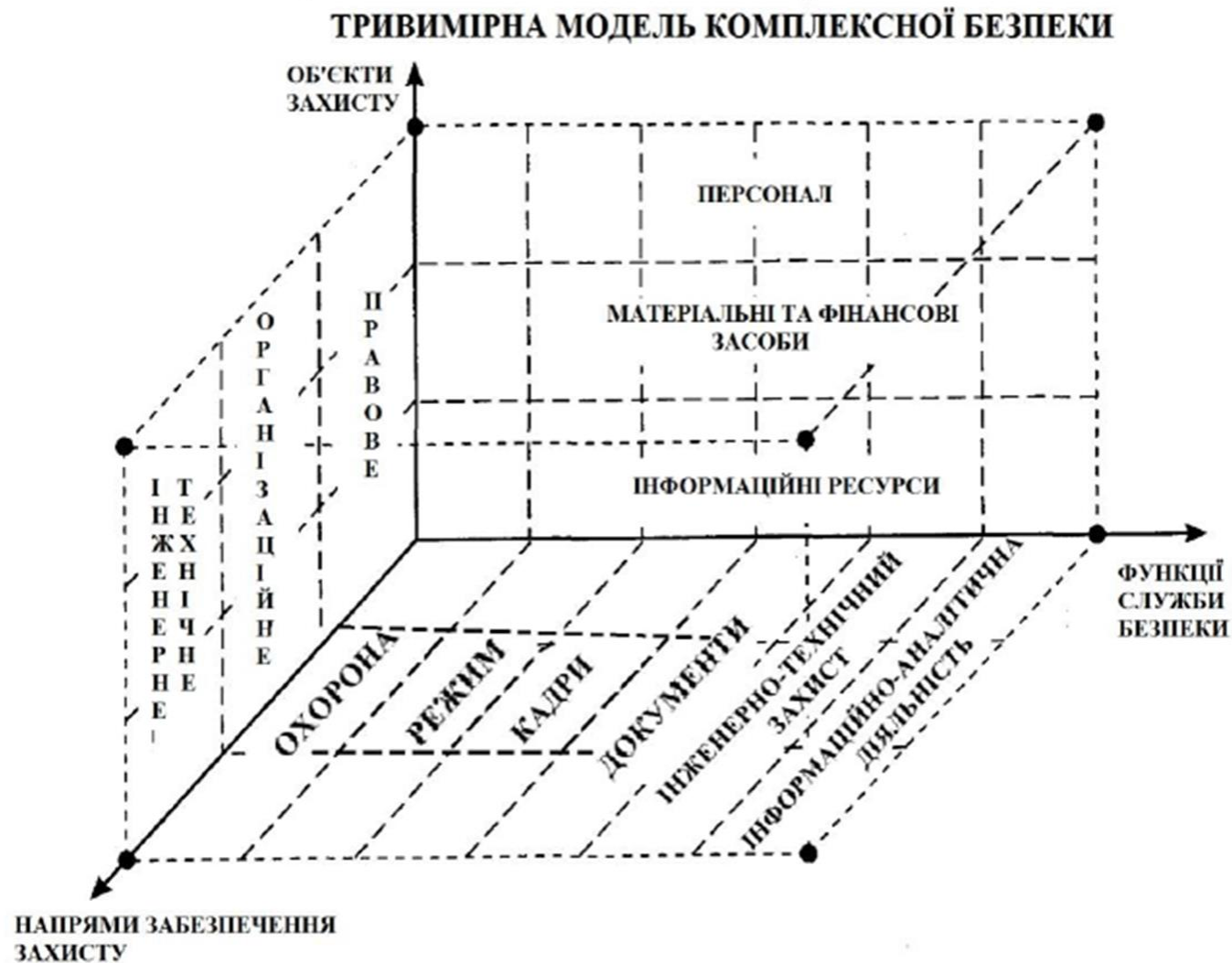
□ СЗІ повинна мати власне забезпечення, спираючись на яке вона виконуватиме свою цільову функцію.

Види забезпечення СЗІ

Правове	нормативні документи, положення, інструкції, вимоги яких є обов'язковими у рамках сфери їх дії
Організаційне	реалізація захисту інформації здійснюється певними структурними одиницями (режимно-секретна служба, служба режиму, служба охорони, служба ТЗІ та ін.), якими треба керувати
Апаратне	використання технічних засобів як для захисту інформації, так і для забезпечення діяльності СЗІ
Інформаційне	відомості, дані, показники, параметри, які лежать в основі рішення завдань, що забезпечують функціонування СЗІ
Програмне	інформаційні, облікові, статистичні і розрахункові програми, що забезпечують оцінку наявності і небезпеки різних каналів витоку і шляхів НСД до джерел інформації, що захищається
Математичне	використання математичних методів для різних розрахунків, пов'язаних з оцінкою небезпеки дій порушників, зон і норм необхідного захисту
Лінгвістичне	спеціальні мовні засоби спілкування фахівців і користувачів у сфері захисту інформації
Нормативно-методичне	норми і регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації, різного роду методики, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах жорстких вимог захисту інформації



Тривимірна модель комплексної безпеки





Вихідні дані для побудови СЗІ

□ Для побудови СЗІ потрібно:

- визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації і цілі, а також інші умови і дії, що порушують безпеку;
- розглянути заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку.

□ Для аналізу такого значного набору джерел, об'єктів і дій доцільно використовувати методи моделювання, при яких формується як би «заступник» реальних ситуацій.



Модель безпеки інформації, загрози



Концептуальна модель безпеки інформації





Загрози конфіденційної інформації

- ❑ Концепція безпеки є основним правовим документом, який визначає захищеність організації від внутрішніх і зовнішніх загроз.
- ❑ **Загрози конфіденційної інформації** – це потенційні або реально можливі дії по відношенню до інформаційних ресурсів, що призводять до неправомірного оволодіння відомостями, які охороняються. Такими діями є:
 - ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;
 - модифікація інформації в кримінальних цілях як часткова або значна зміна складу і змісту відомостей;
 - руйнування (знищення) інформації як акт вандалізму з метою прямого нанесення матеріального збитку.



Загрози інформації





Класифікація загроз





Дії, які призводять до неправомірного оволодіння інформації з обмеженим доступом (ІзОД)

- Відношення об'єкта (організація) і суб'єкта (конкурент, зловмисник) в інформаційному процесі з протилежними інтересами можна розглядати з позиції активності в діях, що призводять до оволодіння ІзОД. В цьому випадку можливі такі ситуації:
- власник не приймає ніяких заходів до збереження ІзОД, що дозволяє зловмисникові легко отримати ті відомості, що цікавлять його;
 - власник інформації строго дотримується заходів інформаційної безпеки, тоді зловмисникові доводиться докладати значних зусиль до здійснення доступу до відомостей, що охороняються, використовуючи для цього усю сукупність способів несанкціонованого проникнення: легальне або нелегальне, заходове або без заходове;
 - проміжна ситуація – це виток інформації технічними каналами, при якій власник ще не знає про це, а зловмисник без особливих зусиль може їх використовувати у своїх інтересах



Незаконне оволодіння ІзОД

□ Дії, які призводять до незаконного оволодіння ІзОД:

- **розголошення** – умисні або необережні дії осіб, яким відповідні відомості були довірені в установленому порядку, що привели до ознайомлення з ними осіб, не допущених до них.
- **витік** – безконтрольний вихід ІзОД за межі організації або кола осіб, яким вона була довірена.
- **несанкціонований доступ** – протиправне умисне оволодіння ІзОД особою, яка не має права доступу до відомостей, що охороняються.



Правовий захист інформації, основні НПА



Правовий захист інформації

- ❑ **Правовий захист інформації** – це спеціальні правові акти, правила, процедури та заходи, які забезпечують захист інформації на правовій основі.
- ❑ Правовий захист інформації як ресурсу признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними та відомчими актами.



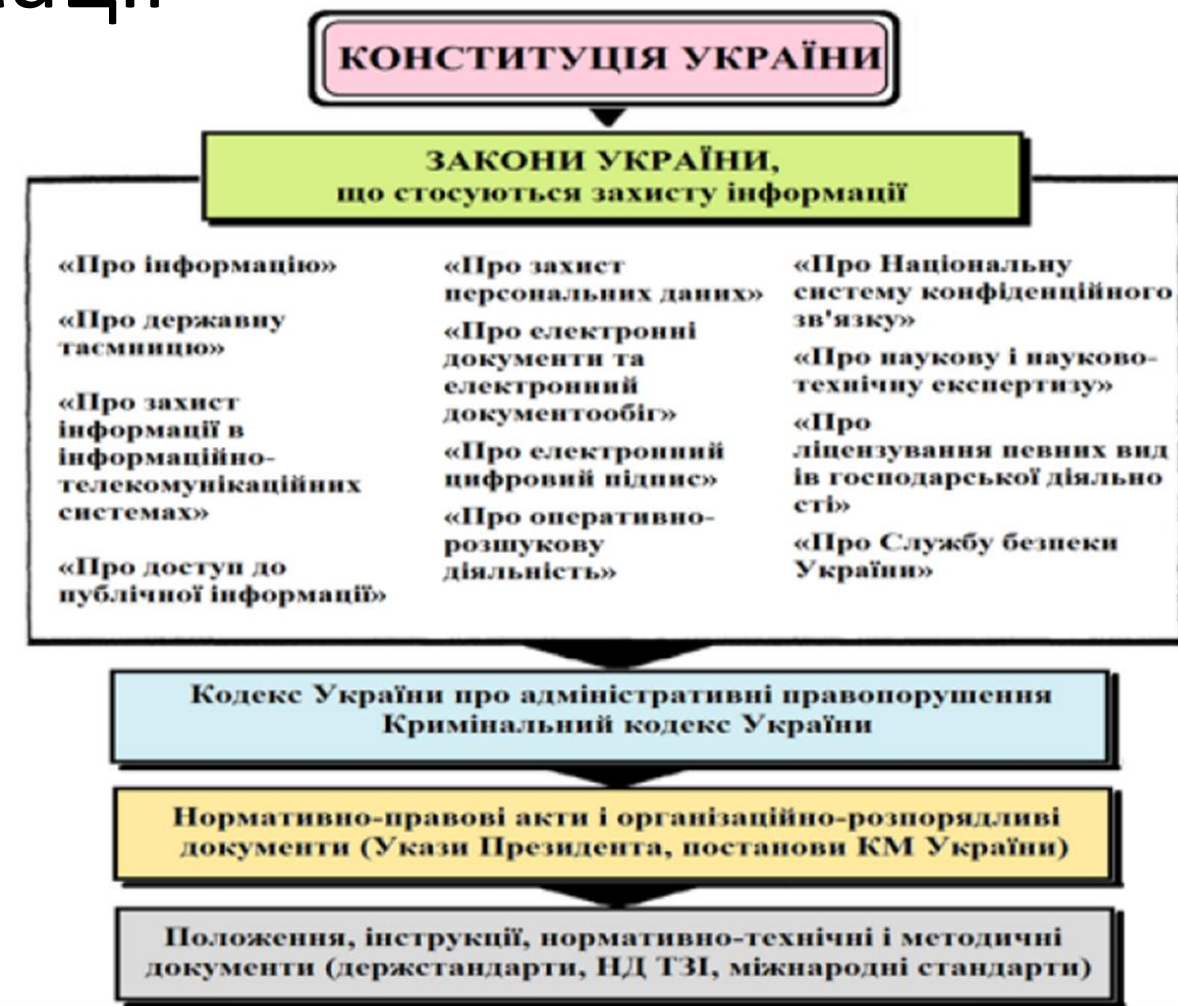
Система нормативно-правових документів в Україні, що регламентують питання захисту інформації





Структура законодавства України в області захисту інформації

- ❑ Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства із захисту інформації, його складу і змісту, співвідношення його з усією системою законів і правових актів України.





Основні НПА

- ❑ **Конституція України** (Відомості Верховної Ради України, 1996, № 30, ст. 141): «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» (ст. 17).
- ❑ **Закон України «Про інформацію»** (Відомості Верховної Ради України, 1992, № 48, ст. 650) регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.



Основні напрями державної інформаційної політики

□ Основні напрями державної інформаційної політики (ст. 3):

- забезпечення доступу кожного до інформації;
- забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;
- забезпечення інформаційної безпеки України;
- забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;
- сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору;
- створення умов для формування в Україні інформаційного суспільства;
- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
- створення інформаційних систем і мереж інформації, розвиток електронного урядування.



Суб'єкт та об'єкт інформаційних відносин

36

❑ Суб'єкти інформаційних відносин (ст. 4)):

- фізичні особи;
- юридичні особи;
- об'єднання громадян;
- суб'єкти владних повноважень.

❑ Об'єкт інформаційних відносин – **інформація** (ст. 4).



Класифікація інформації за порядком доступу

37





ЗУ «Про державну таємницю»

❑ **Закон України «Про державну таємницю»** (Відомості Верховної Ради України, 1994, № 16, ст. 93) регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

❑ Сфери, у яких інформація може бути віднесена до державної таємниці (ст.8):

- оборони;
- зовнішніх відносин;
- економіки, науки і техніки;
- державної безпеки та охорони правопорядку.



Організаційно-правові засади щодо охорони державної таємниці

□ Основні організаційно-правові заходи щодо охорони державної таємниці (ст. 18):

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;
- дозвільний порядок провадження діяльності, пов'язаної з державною таємницею (ДТ);
- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;
- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до ДТ, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;
- режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з ДТ;
- спеціальний порядок допуску та доступу громадян до ДТ;
- технічний та криптографічний захисти секретної інформації.



ЗУ «Про основи національної безпеки України»

40

□ Закон України «Про основи національної безпеки України»

(Відомості Верховної Ради України, 2003, № 39, ст. 351)

визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.



Загрози національним інтересам та безпеці України в інформаційній сфері

□ Загрози національним інтересам і національній безпеці України в інформаційній сфері (ст. 7):

- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.



Основні напрямки держполітики нацбезпеки в інформаційній сфері

□ Основні напрями державної політики з питань національної безпеки в інформаційній сфері (ст. 8):

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.



ЗУ «Про захист інформації в інформаційно-комунікаційних системах»

□ Закон України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України, 1994, № 31, ст. 286) регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.



Об'єкти та суб'єкти захисту в ІТС



□ Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю (ст. 8).



ЗУ «Про ліцензування видів господарської діяльності»

□ Закон України «Про ліцензування видів господарської діяльності» (Відомості Верховної Ради України, 2015, № 23, ст. 158) визначає види господарської діяльності, що підлягають ліцензуванню, порядок їх ліцензування, встановлює державний контроль у сфері ліцензування, відповідальність суб'єктів господарювання та органів ліцензування за порушення законодавства у сфері ліцензування.



Кодекси

46

- ❑ **Кодекс України про адміністративні правопорушення** (Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст. 1122).
- ❑ **Кримінальний кодекс України** (Відомості Верховної Ради України, 2001, № 25-26, ст. 131).



Укази президента

- ❑ **Указ Президента України «Про Положення про технічний захист інформації в Україні»** (від 27 вересня 1999 р. № 1229/99). Положення визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства.
- ❑ **Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні»** (від 22 травня 1998 р. № 505/98). Положення визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає (може завдати) шкоди державі, суспільству або особі.



Постанови Уряду

48

❑ **Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні»** (від 8 жовтня 1997 р. № 1126). Концепція визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами. Технічний захист інформації (ТЗІ) є складовою частиною забезпечення національної безпеки України.



Національні стандарти України

49

- ☐ **ДБН А.2.2-2-96** Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва
- ☐ **ДСТУ 3396 0-96** Технічний захист інформації. Основні положення.
- ☐ **ДСТУ 3396 1-96** Технічний захист інформації. Порядок проведення робіт.
- ☐ **ДСТУ 3396.2-97** Технічний захист інформації. Терміни та визначення.
- ☐ **ДСТУ 4145-2002** Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка



Міжнародні стандарти, прийняті в Україні як національні₁

- ❑ **ДСТУ ISO/IEC 9798-4:2015** Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 4. Механізми, що використовують криптографічну перевірочну функцію (ISO/IEC 9798-4:1999, Cor 1:2009, Cor 2:2012, IDT) (budstandart.com)
- ❑ **ДСТУ ISO/IEC 10118-1:2018** Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення (ISO/IEC 10118-1:2016, IDT) (budstandart.com)
- ❑ **ДСТУ ISO/IEC TR 13335-1:2003** Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції й моделі безпеки IT (ISO/IEC TR 13335-1:1996, IDT) (budstandart.com)



Міжнародні стандарти, прийняті в Україні як національні₂

- ❑ **ДСТУ ISO/IEC TR 13335-4:2005** Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту (ISO/IEC TR 13335-4:2000, IDT) (budstandart.com)
- ❑ **ДСТУ ISO/IEC 14888-2:2015** Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел (ISO/IEC 14888-2:2008, IDT) (budstandart.com)
- ❑ **ДСТУ ISO/IEC 15946-1:2006**. Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 1. Загальні положення (ISO/IEC 15946-1:2002, IDT) (budstandart.ua)



Міжнародні стандарти, прийняті в Україні як національні₃

- ❑ **ДСТУ ISO/IEC 18014-1:2006** Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Частина 1. Основні положення (ISO/IEC 18014-1:2002, IDT) (budstandart.ua)
- ❑ **ДСТУ ISO/IEC 27001:2015** Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) (budstandart.com)

Донецький національний технічний університет



Тема 2. Моделі порушника та загроз для інформації в ІТС.

Лекція 2. Вразливості інформаційної безпеки в ІКС та інструменти/методи їх пошуку/аналізу/захисту.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

54

- ☐ Мета лекції
- ☐ Спільноти з безпеки та сертифікація
- ☐ Політики безпеки мережі
- ☐ Інструменти, платформи та служби безпеки
- ☐ Запобігання поширеним мережевим атакам
- ☐ Механізм захисту Cisco Network Foundation
- ☐ Мережеві пристрої
- ☐ Бездротовий зв'язок
- ☐ Топології мережі
- ☐ Пристрої безпеки
- ☐ Послуги безпеки



Мета лекції

Метою лекції є ознайомлення з наступними лекційними питаннями:

- Спільноти з безпеки та сертифікація
- Політики безпеки мережі (домени безпеки, бізнес-політики, політики безпеки, політики BYOD)
- Інструменти, платформи та служби безпеки (цибуля безпеки, артишок безпеки)
- Запобігання поширеним мережевим атакам
- Механізм захисту Cisco Network Foundation (захист площин контролю, управління та даних)
- Мережеві пристрої (маршрутизатор, комутатор, протоколи)
- Бездротовий зв'язок
- Топології мережі
- Пристрої безпеки
- Послуги безпеки



Спільноти з безпеки та сертифікація



Професіонали з мережевої безпеки

- ❑ Фахівці з мережевої безпеки несуть відповідальність за підтримання надійності даних для організації та забезпечення цілісності та конфіденційності інформації.
- ❑ Посадові ролі спеціаліста з безпеки на підприємстві включають головного спеціаліста з інформації (CIO), головного спеціаліста з інформаційної безпеки (CISO), менеджера з безпеки (SecOps), головного спеціаліста з безпеки (CSO), менеджера з безпеки та інженера з безпеки мережі. Незалежно від посади, професіонали мережевої безпеки повинні завжди бути на крок попереду хакерів та повинні:
 - постійно вдосконалювати свої навички, щоб бути в курсі останніх загроз
 - відвідувати навчання та семінари
 - Бути підписаними на стрічки загроз у реальному часі
 - щодня переглядати веб-сайти безпеки
 - бути знайомі з організаціями мережевої безпеки. Ці організації часто мають найновішу інформацію про загрози та вразливості



Спільноти мережевого аналізу₁

Організація	Опис
SANS	Ресурси SysAdmin, Audit, Network, Security (SANS) Institute здебільшого безкоштовні за запитом і включають: • Internet Storm Center - популярна система раннього попередження в Інтернеті • NewsBites, щотижневий дайджест статей про комп'ютерну безпеку. • @RISK, щотижневий дайджест нещодавно виявлених векторів атак, вразливостей із активними експлойтами та пояснень того, як працювали останні атаки • Мигаючі сповіщення безпеки • Читальний зал - понад 1200 нагороджених оригінальних наукових робіт. • SANS також розробляє курси безпеки.
Mitre	Корпорація Mitre підтримує список поширених вразливостей (CVE), які використовують відомі організації безпеки.



Спільноти мережевого аналізу₂

Організація	Опис
FIRST	Форум груп реагування на інциденти та безпеки (FIRST) — це організація безпеки, яка об'єднує різні групи реагування на інциденти комп'ютерної безпеки від урядових, комерційних і освітніх організацій для сприяння співпраці та координації обміну інформацією, запобігання інцидентам і швидкого реагування.
SecurityNews Wire	Портал новин безпеки, який збирає останні останні, що стосуються сповіщень, експлойтів і вразливостей.
(ISC) ²	Міжнародний консорціум із сертифікації безпеки інформаційних систем (ISC ²) надає освітні продукти та послуги з кар'єрного росту, не пов'язані з постачальниками, понад 75 000 професіоналів у понад 135 країнах.
CIS	Центр безпеки в Інтернеті (CIS) є центром запобігання кіберзагрозам, захисту, реагування та відновлення для державних, місцевих, плеємінних і територіальних (SLTT) урядів через Міждержавний центр обміну та аналізу інформації (MS-ISAC). MS-ISAC пропонує цілодобові попередження та рекомендації щодо кіберзагроз, ідентифікацію вразливостей, пом'якшення та реагування на інциденти.



Сертифікати безпеки мережі

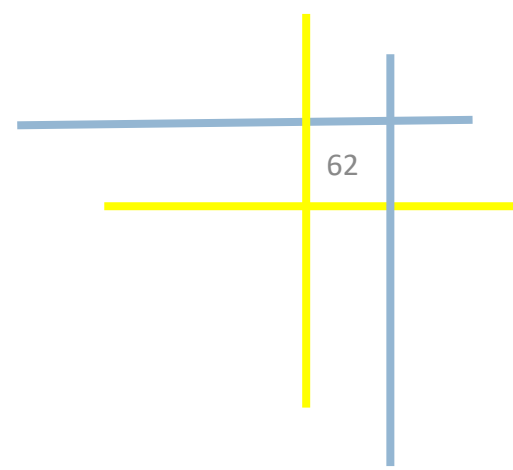
- ❑ Сертифікати для спеціалістів із мережевої безпеки пропонують такі організації:
 - Глобальна сертифікація гарантії інформації (GIAC)
 - Міжнародний консорціум сертифікації безпеки інформаційних систем (ISC) 2
 - Асоціація аудиту та контролю інформаційних систем (ISACA)
 - Міжнародна рада консультантів з електронної комерції (EC-Council)
 - Сертифіковані спеціалісти з бездротових мереж (CWNP)
- ❑ Cisco замінила сертифікацію Cisco Certified Network Associate Security (210-260 IINS) на нову сертифікацію безпеки CCNP. CCNP Security складається з базового іспиту CCNP у поєднанні з іспитом на концентрацію безпеки Cisco Certified Specialist:
 - 300-710 SNCF – Network Security Firepower
 - 300-715 SISE – Впровадження та налаштування Cisco Identity Services Engine
 - 300-720 SESA – Захист електронної пошти за допомогою Cisco Email Security Appliance
 - 300-725 SWSA – Захист Інтернету за допомогою Cisco Web Security Appliance
 - 300-730 SVPN – Впровадження безпечних рішень за допомогою віртуальних приватних мереж
 - 300-735 SAUTO – Автоматизація та програмування рішень безпеки Cisco



Безпека зв'язку: CIA

- ❑ Інформаційна безпека займається захистом інформації та інформаційних систем від несанкціонованого доступу, використання, розголошення, порушення, модифікації або знищення. Тріада CIA служить концептуальною основою для цієї галузі.
- ❑ Тріада CIA складається з трьох компонентів інформаційної безпеки:
 - Конфіденційність – доступ до конфіденційної інформації мають лише авторизовані особи, організації або процеси.
 - Цілісність – стосується захисту даних від несанкціонованої зміни.
 - Доступність – авторизовані користувачі повинні мати безперервний доступ до мережевих ресурсів і даних, які їм потрібні.





Політики безпеки мережі



Домени безпеки мережі₁

□ Міжнародна організація стандартизації (ISO)/Міжнародна електротехнічна комісія (IEC) визначає 14 domenів безпеки мережі

Домен безпеки мережі	Опис
Політика інформаційної безпеки	Призначена для забезпечення створення, перегляду та підтримки політик безпеки.
Організація інформаційної безпеки	Модель управління, розроблена організацією з інформаційної безпеки. Вона визначає відповідальність за завдання інформаційної безпеки в організації.
Безпека людських ресурсів	Стосується обов'язків щодо безпеки, пов'язаної з приєднанням співробітників до організації, переміщенням і виходом із неї.
Управління активами	Стосується того, як організації створюють перелік і схему класифікації інформаційних активів.
Управління доступом	Описує обмеження прав доступу до мереж, систем, програм, функцій і даних.
Криптографія	Стосується шифрування даних і управління конфіденційною інформацією для захисту конфіденційності, цілісності та доступності даних.
Фізична та екологічна безпека	Описує захист фізичних комп'ютерних засобів і обладнання в організації.



Домени безпеки мережі₂

Домен безпеки мережі	Опис
Безпека операцій	Описує керування технічними засобами безпеки в системах і мережах, включаючи захист від зловмисного програмного забезпечення, резервне копіювання даних, реєстрацію та моніторинг, керування вразливістю та перевірку. Цей домен також стосується цілісності програмного забезпечення, яке використовується в бізнес-операціях.
Безпека зв'язку	Стосується безпеки даних, які передаються в мережах як всередині організації, так і між організацією та третіми сторонами, такими як клієнти чи постачальники.
Придбання, розробка та обслуговування системи	Гарантує, що безпека інформації залишається центральною проблемою в процесах організації протягом усього життєвого циклу, як у приватних, так і в публічних мережах.
Відносини з постачальниками	Стосується специфікації договірних угод, які захищають інформаційні та технологічні активи організації, доступ до яких мають треті сторони, які надають товари та послуги організації.
Управління інцидентами інформаційної безпеки	Описує, як передбачити порушення інформаційної безпеки та реагувати на них.



Домени безпеки мережі₃

Домен безпеки мережі	Опис
Управління безперервністю бізнесу	Описує захист, обслуговування та відновлення критично важливих бізнес-процесів і систем.
Відповідність	Описує процес забезпечення відповідності політикам, стандартам і нормам інформаційної безпеки.



Бізнес-політики₁

□ Бізнес політика – це керівні принципи, розроблені організацією для керування її діями. Політики визначають стандарти коректної поведінки для бізнесу та його співробітників. У мережі політика визначає дії, які дозволені в мережі. Це встановлює базову лінію прийнятного використання. Якщо в мережі виявлено поведінку, яка порушує бізнес-політику, можливо, це симптом того, що стався злом безпеки.

Політика	Опис
Політика компанії	• Ці політики встановлюють правила поведінки та відповідальність як працівників, так і роботодавців. • Політики захищають права працівників, а також бізнес інтереси роботодавців. • Залежно від потреб організації, різні політики та процедури встановлюють правила щодо поведінки працівників, відвідуваності, дрес-коду, конфіденційності та інших сфер, пов'язаних із умовами найму.
Політика щодо працівників	• Ці політики створюються та підтримуються персоналом відділу кадрів, щоб визначити зарплату співробітників, графік оплати праці, винагороди працівникам, графік роботи, відпустки тощо. • Їх часто надають новим співробітникам для ознайомлення та підпису.



Бізнес-політики₂

Політика	Опис
Політики безпеки	• Ці політики визначають набір цілей безпеки для компанії, визначають правила поведінки для користувачів і адміністраторів і визначають системні вимоги. • Ці цілі, правила та вимоги разом забезпечують безпеку мережі та комп'ютерних систем в організації. • Подібно до плану забезпечення безперервності, політика безпеки — це документ, що постійно розвивається і базується на змінах у ландшафті загроз, уразливостях і вимогах бізнесу та співробітників.



Політики безпеки

- ❑ Політики безпеки використовуються для інформування користувачів, персоналу та менеджерів про вимоги організації щодо захисту технологій та інформаційних активів. Політика безпеки також визначає механізми, необхідні для задоволення вимог безпеки, і забезпечує базову лінію для отримання, налаштування та аудиту комп'ютерних систем і мереж на відповідність. Політики, які можуть бути включені в політику безпеки:

Політика	Опис
Політика ідентифікації та автентифікації	Визначає уповноважених осіб, які можуть мати доступ до мережевих ресурсів і процедур перевірки особи.
Політика паролів	Гарантує, що паролі відповідають мінімальним вимогам і регулярно змінюються.
Політика прийнятного використання (AUP)	Визначає мережеві програми та способи використання, прийнятні для організації. Вона також може визначати наслідки порушення цієї політики.
Політика віддаленого доступу	Визначає, як віддалені користувачі можуть отримати доступ до мережі та що доступно через віддалене підключення.
Політика обслуговування мережі	Визначає операційні системи мережевих пристроїв і процедури оновлення застосунків кінцевих користувачів.
Процедури врегулювання інцидентів	Описує, як обробляються інциденти безпеки.



Політики BYOD

- ❑ Багато організацій тепер також повинні підтримувати Bring Your Own Device (BYOD). Це дозволяє співробітникам використовувати власні мобільні пристрої для доступу до систем компанії, програмного забезпечення, мереж або інформації. Це може призвести до підвищення ризику інформаційної безпеки, оскільки BYOD може призвести до витоку даних і збільшення відповідальності для організації. Найкращі практики безпеки BYOD, які допоможуть пом'якшити вразливості BYOD:

Найкраща практика	Опис
Доступ захищений паролем	Використовуйте унікальні паролі для кожного пристрою та облікового запису.
Ручне керування бездротовим підключенням	Вимкніть Wi-Fi і Bluetooth, коли вони не використовуються. Підключайтеся лише до надійних мереж.
Оновлення	Завжди оновлюйте ОС пристрою та інше програмне забезпечення. Оновлене програмне забезпечення часто містить виправлення безпеки для захисту від останніх загроз або експлойтів.
Резервне копіювання даних	Увімкніть резервне копіювання пристрою на випадок його втрати або викрадення.
Увімкнути «Знайти мій пристрій»	Підпишіться на службу пошуку пристроїв із функцією віддаленого стирання.
Антивірусне програмне забезпечення	Використовуйте антивірусне програмне забезпечення для затверджених пристроїв BYOD.
Програмне забезпечення для керування мобільними пристроями (MDM).	Програмне забезпечення MDM дозволяє IT-групам впроваджувати параметри безпеки та конфігурації програмного забезпечення на всіх пристроях, які підключаються до мереж компанії.



Відповідність нормам і стандартам

- ❑ Існують також зовнішні правила безпеки мережі. Фахівці з мережевої безпеки повинні бути знайомі із законами та кодексами етики, які є обов'язковими для фахівців з безпеки інформаційних систем (INFOSEC).
- ❑ Багато організацій мають повноваження розробляти та впроваджувати політику безпеки. Правила відповідності визначають, які організації несуть відповідальність за надання та відповідальність у разі їх невиконання. Правила відповідності, яких зобов'язана дотримуватися організація, залежать від типу організації та даних, які організація обробляє.



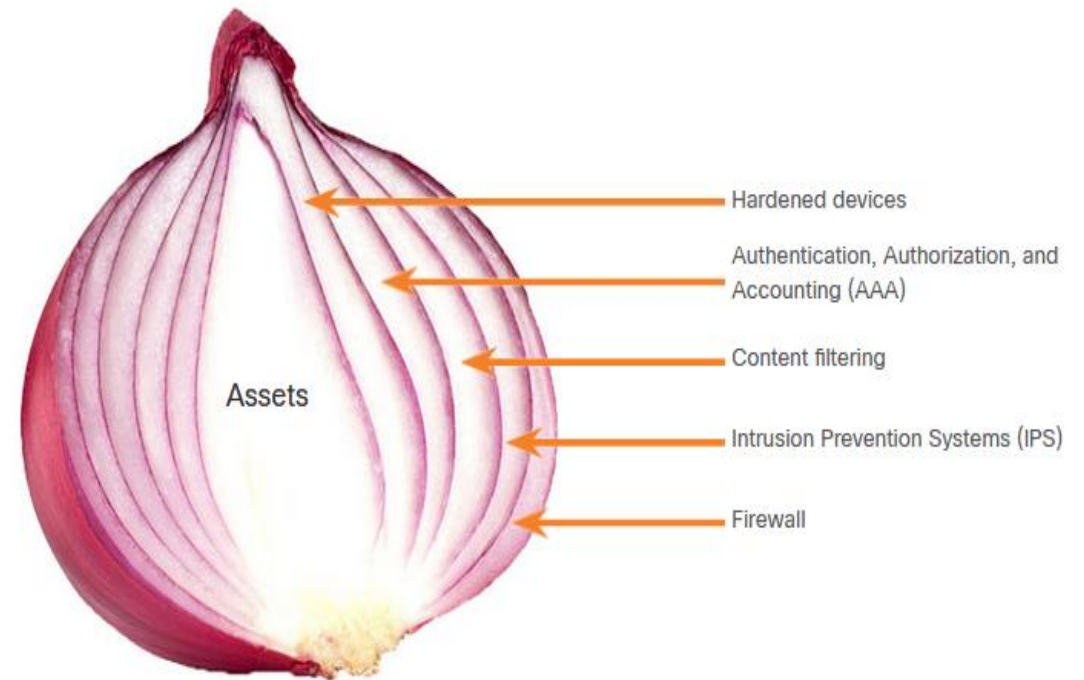
Інструменти, платформи та служби безпеки



Цибуля безпеки (The Security Onion) та артишок безпеки (The Security Artichoke)₁

❑ Загальна аналогія, яка використовується для опису підходу до поглибленого захисту, називається «цибуля безпеки». Зловмисник мав би шар за шаром знімати захист мережі, подібно до чищення цибулі. Лише після проникнення на кожен рівень зловмисник досягне цільових даних або системи.

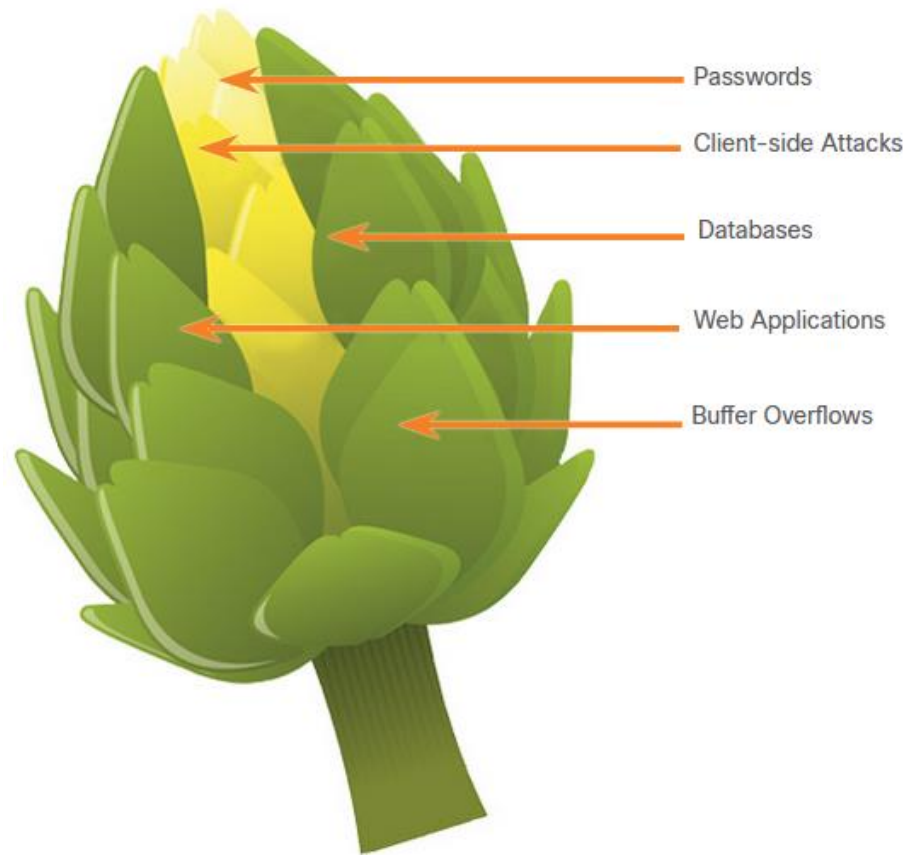
❑ Цибуля безпеки, описана на цьому слайді є способом візуалізації поглибленого захисту. Не слід плутати з пакетом інструментів безпеки мережі Security Onion.





Цибуля безпеки (The Security Onion) та артишок безпеки (The Security Artichoke)₂

- ❑ Зміна ландшафту мереж, еволюція мереж без кордонів, замінила попередню аналогію на «артишок безпеки», що є вигідним для зловмисників, оскільки їм більше не потрібно знімати кожен шар. Їм потрібно лише видалити певні «листя артишоку». Зловмисник знімає броню по периметру, щоб дістатися до «серця» підприємства.





Інструменти тестування безпеки₁

- ❑ Етичне хакерство передбачає використання різних типів інструментів для тестування мережі та кінцевих пристроїв для підтвердження безпеки мережі. Тестування на проникнення використовує хакерські методи та інструменти для оцінки надійності заходів безпеки мережі. Співробітники служби кібербезпеки також повинні знати, як використовувати ці інструменти під час проведення тестів на проникнення в мережу.

Категорії інструментів	Опис
Зломщики паролів	Паролі є найбільш вразливою загрозою безпеці. Інструменти злому паролів часто називають інструментами відновлення пароля і їх можна використовувати для злому або відновлення пароля. Це досягається або видаленням початкового пароля після обходу шифрування даних, або прямим виявленням пароля. Зломщики паролів постійно вгадують пароль, щоб отримати доступ до системи. Приклади інструментів для злому паролів включають John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack і Medusa.
Засоби бездротового злому	Бездротові мережі більш сприйнятливі до загроз безпеці мережі. Інструменти бездротового злому використовуються для навмисного злому бездротової мережі з метою виявлення вразливостей безпеки. Приклади бездротових хакерських інструментів включають Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep і NetStumbler.



Інструменти тестування безпеки₂

Категорії інструментів	Опис
Інструменти сканування та злому мережі	Інструменти сканування мережі використовуються для перевірки мережевих пристроїв, серверів і хостів на наявність відкритих портів TCP або UDP. Приклади інструментів сканування включають Nmap, SuperScan, Angry IP Scanner і NetScanTools.
Інструменти для виготовлення пакетів	Інструменти створення пакетів використовуються для перевірки надійності брандмауера за допомогою спеціально створених підроблених пакетів. Прикладами таких інструментів є Hping, Scapy, Socat, Yersinia, Netcat, Nping і Nemesis.
Сніфери пакетів	Інструменти аналізатора пакетів використовуються для захоплення та аналізу пакетів у традиційних локальних мережах Ethernet або WLAN. Інструменти включають Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy і SSLstrip.
Детектори руткітів	Детектор руткітів — це засіб перевірки цілісності каталогів і файлів, який використовується білими капелюхами для виявлення встановлених руткітів. Приклади інструментів включають AIDE, Netfilter і PF: OpenBSD Packet Filter.
Фазери для пошуку вразливостей	Фазери — це інструменти, які використовують суб'єкти загроз, коли намагаються виявити вразливі місця безпеки комп'ютерної системи. Приклади фазерів включають Skipfish, Wapiti та W3af.
Криміналістичні інструменти	Білі хакери використовують криміналістичні інструменти, щоб знайти будь-які сліди доказів, які існують у певній комп'ютерній системі. Приклади інструментів включають Sleuth Kit, Helix, Maltego та Encase.



Інструменти тестування безпеки₃

Категорії інструментів	Опис
Налагоджувачі	Інструменти налагодження використовуються чорними капелюхами для зворотного проектування бінарних файлів під час написання експлойтів. Вони також використовуються білими капелюхами під час аналізу шкідливих програм. Інструменти налагодження включають GDB, WinDbg, IDA Pro та Immunity Debugger .
Злом операційних систем	Операційні системи для злому — це спеціально розроблені операційні системи з попередньо завантаженими інструментами та технологіями, оптимізованими для злому. Прикладами спеціально розроблених хакерських операційних систем є Kali Linux, SELinux, Knoppix, Parrot OS і BackBox Linux .
Засоби шифрування	Ці інструменти захищають вміст даних організації під час їх зберігання або передачі. Інструменти шифрування використовують схеми алгоритмів для шифрування даних, щоб запобігти несанкціонованому доступу до даних. Прикладами таких інструментів є VeraCrypt, CipherShed, Open SSH, OpenSSL, OpenVPN і Stunnel .
Інструменти експлуатації вразливостей	Ці інструменти визначають, чи є віддалений хост вразливим до атаки на безпеку. Приклади інструментів для використання вразливостей включають Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit і Netsparker .
Сканери вразливостей	Ці інструменти сканують мережу або систему, щоб визначити відкриті порти. Їх також можна використовувати для пошуку відомих уразливостей і сканування віртуальних машин, пристроїв BYOD і клієнтських баз даних. Прикладами таких інструментів є Nipper, Securia PSI, Core Impact, Nessus, SAINT і Open VAS .



Платформа безпеки даних₁

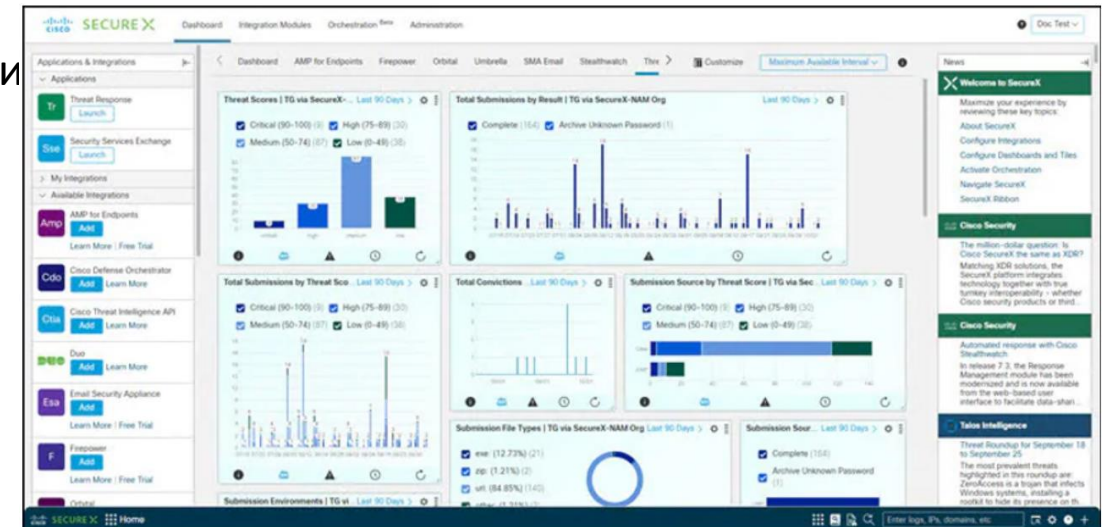
- ❑ Платформа безпеки даних (DSP) — це інтегроване рішення безпеки, яке поєднує традиційно незалежні інструменти в набір інструментів, створених для спільної роботи. Інструменти безпеки, які захищають і контролюють мережі, часто виготовляються різними постачальниками. Може бути важко інтегрувати ці інструменти таким чином, щоб можна було досягти єдиного погляду на безпеку мережі.
- ❑ Одним з таких DSP є платформа Helix від FireEye. FireEye Helix — це хмарна платформа безпеки, яка дозволяє організаціям інтегрувати багато функцій безпеки в єдину платформу. Helix забезпечує керування подіями, аналітику мережевої поведінки, розширене виявлення загроз і оркестрування безпеки інцидентів, автоматизацію та реагування (SOAR) для реагування на загрози в міру їх виявлення.





Платформа безпеки даних₂

- ❑ Іншим інтегрованим DSP є Cisco SecureX. Портфоліо Cisco Secure складається з широкого набору технологій, які функціонують як команда, забезпечуючи взаємодію з інфраструктурою безпеки, включаючи технології сторонніх розробників. Це призводить до єдиної видимості, автоматизації та міцнішого захисту.
- ❑ Платформа Cisco SecureX працює з різноманітними продуктами, які разом захищають мережу, користувачів і кінцеві точки, межі хмари та програми.
- ❑ Функціональність SecureX вбудована у великий і різноманітний портфель продуктів безпеки Cisco, включаючи брандмауери наступного покоління, VPN, мережеву аналітику, систему ідентифікації, розширений захист від зловмисного програмного забезпечення (AMP) і багато інших систем, які працюють для захисту всіх аспектів мережі.
- ❑ SecureX також інтегрує низку інструментів безпеки сторонніх виробників.



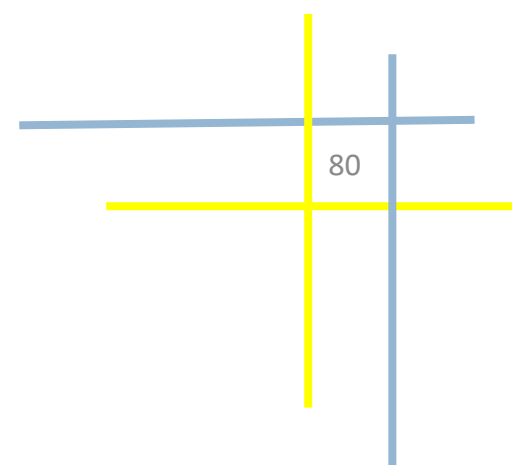


Служби безпеки

79

- ❑ Служби аналізу загроз і безпеки дозволяють обмінюватися інформацією про загрози, наприклад про вразливості, індикатори компрометації (IOC) і методи пом'якшення. У міру появи загроз служби аналізу загроз створюють і розповсюджують правила брандмауера та IOC на пристрої, які підписалися на службу.
- ❑ Однією з таких служб є Cisco Talos Threat Intelligence Group. Talos є однією з найбільших у світі груп розвідки комерційних загроз. Мета Talos — допомогти захистити корпоративних користувачів, дані та інфраструктуру від активних зловмисників. Команда Talos збирає інформацію про активні, існуючі та нові загрози. Тоді Talos надає своїм передплатникам комплексний захист від цих атак і шкідливих програм.
- ❑ Продукти Cisco Security можуть використовувати аналіз загроз Talos у режимі реального часу, щоб забезпечити швидкі та ефективні рішення безпеки.





Запобігання поширеним мережевим атакам



Захист мережі

□ Для захисту мережі від атак потрібні постійна пильність і постійне навчання. Нижче наведено найкращі методи захисту мережі:

- Розробіть письмову політику безпеки для компанії.
- Розкажіть співробітникам про ризики соціальної інженерії та розробіть стратегії перевірки особи по телефону, електронною поштою чи особисто.
- Контролюйте фізичний доступ до систем.
- Використовуйте надійні паролі та часто змінюйте їх.
- Шифруйте та захищайте конфіденційні дані паролем.
- Впроваджуйте апаратне та програмне забезпечення безпеки, наприклад брандмауери, IPS, пристрої віртуальної приватної мережі (VPN), антивірусне програмне забезпечення та фільтрацію вмісту.
- Регулярно створюйте резервні копії та тестуйте резервні копії файлів.
- Вимкніть непотрібні служби та порти.
- Слідкуйте за актуальністю патчів, встановлюючи їх щотижня або щодня, якщо можливо, щоб запобігти переповненню буфера та атакам підвищення привілеїв.
- Виконуйте аудит безпеки, щоб перевірити мережу.



Пом'якшення атак шкідливих програм

- ☐ Зловмисне програмне забезпечення, зокрема віруси, хробаки та троянські програми, може спричинити серйозні проблеми в мережах і кінцевих пристроях. У мережевих адміністраторів є кілька засобів пом'якшення цих атак.
- ☐ Антивірусне програмне забезпечення допомагає запобігти зараженню хостів і поширенню шкідливого коду. Кілька компаній, які створюють антивірусне програмне забезпечення, наприклад Symantec, McAfee та Trend Micro. Антивірусні продукти мають параметри автоматизації оновлення, щоб нові визначення вірусів і нові оновлення програмного забезпечення можна було завантажувати автоматично або на вимогу. Ця практика є найважливішою вимогою для захисту мережі від вірусів і має бути формалізована в політиці безпеки мережі.
- ☐ Ці продукти встановлюються на комп'ютерах і серверах для виявлення та знищення вірусів. Однак вони не перешкоджають проникненню вірусів у мережу. Ще один спосіб пом'якшити загрози зловмисного програмного забезпечення – взагалі запобігти потраплянню файлів шкідливого програмного забезпечення в мережу.
- ☐ Пристрої безпеки на периметрі мережі можуть ідентифікувати відомі файли зловмисного програмного забезпечення на основі їх індикаторів компрометації. Файли можна видалити з вхідного потоку даних, перш ніж вони спричинять інцидент.



Пом'якшення атак від хробаків

❑ Хробаки більше мережеві, ніж віруси. Захист від хробаків вимагає старанності та координації з боку спеціалістів із мережевої безпеки. Реакцію на атаку хробаків можна розділити на чотири етапи: стримування, щеплення, карантин і лікування.

Фаза	Відповідь
1. Стимування	Етап стримування передбачає обмеження розповсюдження хробакової інфекції на вже уражені ділянки мережі. Це вимагає розділення та сегментації мережі, щоб уповільнити або зупинити хробака та запобігти націлюванню та інфікуванню інших систем на заражених хостах. Стимування вимагає використання як вихідних, так і вхідних ACL на маршрутизаторах і брандмауерах у контрольних точках мережі.
2. Щеплення	Фаза інокуляції проходить паралельно або після фази стримування. Під час фази щеплення всі неінфіковані системи виправляються відповідним патчем постачальника. Процес щеплення ще більше позбавляє хробака доступних цілей.
3. Карантин	Етап карантину включає відстеження та ідентифікацію заражених машин у закритих зонах, а також їх відключення, блокування або видалення. Це відповідно ізолює ці системи для фази лікування.
4. Лікування	Етап лікування передбачає активну дезінфекцію заражених систем. Це може включати припинення процесу хробака, видалення змінених файлів або системних налаштувань, які ввів хробак, і виправлення вразливості, яку хробак використовував для використання системи. Крім того, у більш серйозних випадках може знадобитися перевстановити систему, щоб переконатися, що хробак і його побічні продукти видалені.



Пом'якшення розвідувальних атак

- ❑ Розвідувальні атаки, як правило, є попередниками інших атак, спрямованих на отримання несанкціонованого доступу до мережі або порушення роботи мережі. Ви можете виявити, коли триває розвідувальна атака, отримуючи сповіщення від попередньо налаштованих сигналів тривоги. Ці сигнали тривоги спрацьовують, коли перевищуються певні параметри, наприклад кількість запитів ICMP за секунду. Розвідувальні атаки можна пом'якшити декількома способами, зокрема:
 - Впровадження автентифікації для забезпечення належного доступу.
 - Використання шифрування, щоб зробити атаки аналізатора пакетів марними.
 - Використання засобів захисту від сніфера для виявлення атак сніфера пакетів.
 - Впровадження комутованої інфраструктури.
 - Використання брандмауера та IPS.
- ❑ Неможливо пом'якшити сканування портів. Використання IPS і брандмауера може обмежити інформацію, яку можна виявити за допомогою сканера портів.
- ❑ Перевірку Ping можна зупинити, якщо на периферійних маршрутизаторах вимкнено відлуння ICMP і відлуння-відповідь; однак, коли ці служби вимкнено, також втрачається можливість діагностики мережі.



Пом'якшення атак доступу

- ❑ Для пом'якшення атак доступу доступно кілька методів, зокрема надійний захист паролем, принцип мінімальної довіри, криптографія та застосування патчів операційної системи та програм. Дивовижна кількість атак на доступ здійснюється за допомогою простого вгадування пароля або атаки на паролі за допомогою словника. Щоб захиститися від цього, створіть і застосуйте політику надійної автентифікації, яка включає:
 - Використання надійних паролів. Надійні паролі містять принаймні вісім символів і містять великі та малі літери, цифри та спеціальні символи.
 - Налаштування вимкнення облікових записів після певної кількості невдалих входів у систему. Ця практика допомагає запобігти безперервним спробам ввести пароль.
- ❑ Використовуйте шифрування для віддаленого доступу до мережі та трафіку протоколу маршрутизації, щоб зменшити ймовірність атак типу "людина посередині".
- ❑ Розкажіть співробітникам про ризики соціальної інженерії та розробіть стратегії перевірки особи по телефону, електронною поштою чи особисто.
- ❑ Багатофакторна автентифікація (MFA) має стати стандартом.



Пом'якшення атак DoS

- ❑ Однією з перших ознак DoS-атаки є велика кількість скарг користувачів на недоступність ресурсів або надзвичайно низьку продуктивність мережі.
- ❑ Графік використання мережі, що показує незвичайну активність, може свідчити про атаку DoS. Щоб мінімізувати кількість атак, пакет програмного забезпечення моніторингу використання мережі повинен бути запущений постійно.
- ❑ Історично багато DoS-атак відбувалися з підроблених адрес. Маршрутизатори та комутатори Cisco підтримують багато технологій захисту від спуфінгу, таких як безпека портів, стеження за протоколом динамічної конфігурації хоста (DHCP), IP Source Guard, перевірка протоколу динамічного визначення адрес (ARP) і списки контролю доступу (ACL).



Механізм захисту Cisco Network Foundation

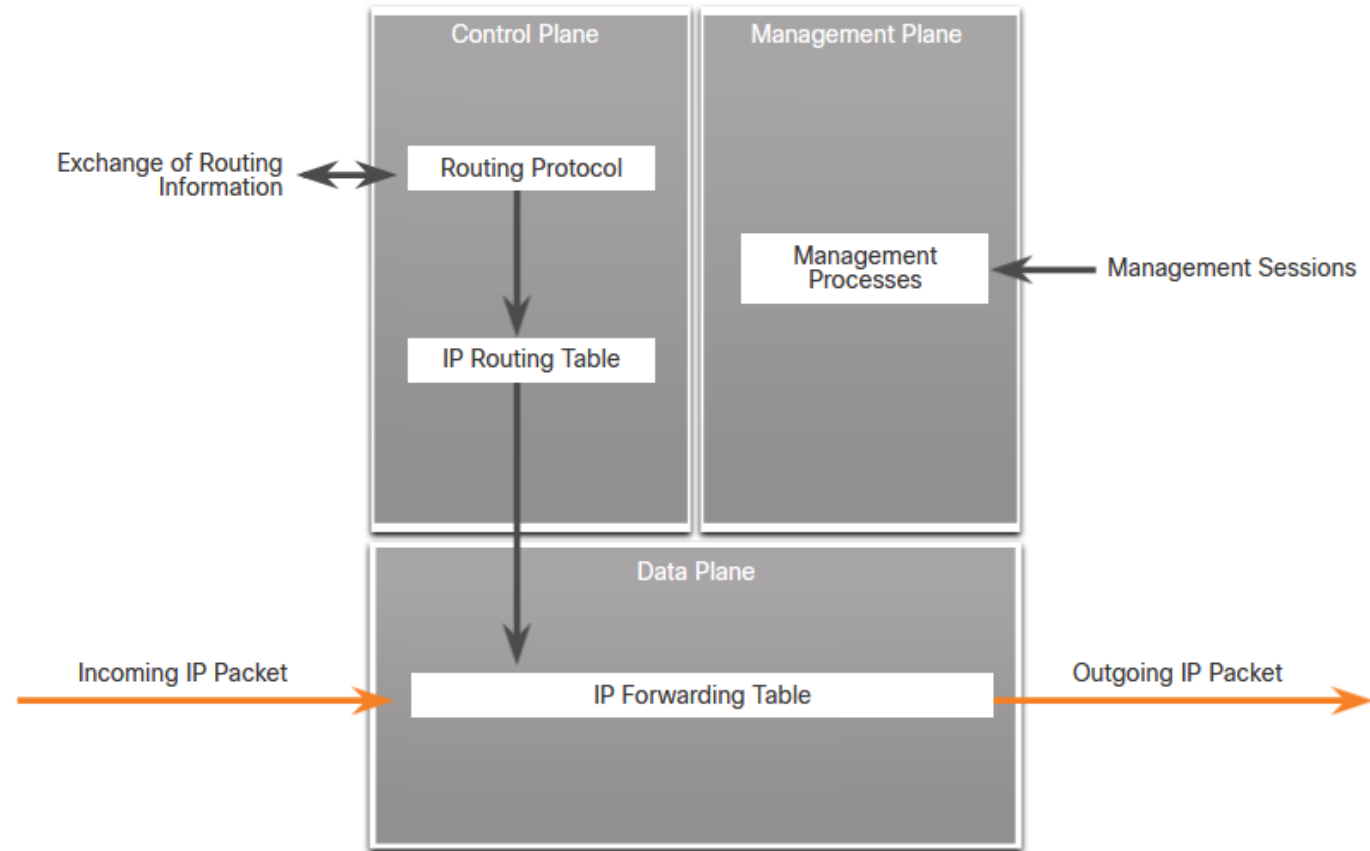


NFP Framework

88

❑ Фреймворк Cisco Network Foundation Protection (NFP) надає вичерпні рекомендації щодо захисту мережевої інфраструктури. Ці вказівки є основою для безперервного надання послуг. NFP логічно розділяє маршрутизатори і комутатори на три функціональні області:

- **Площина контролю (control plane)** – відповідає за правильну маршрутизацію даних.
- **Площина керування (management plane)** – відповідає за керування елементами мережі.
- **Площина даних (data plane)** – відповідає за пересилання даних.





Забезпечення безпеки площини контролю

89

- ❑ Трафік площини контролю складається з пакетів, згенерованих пристроєм, необхідних для роботи самої мережі. Безпеку площини контролю можна реалізувати за допомогою таких функцій:
 - Автентифікація протоколу маршрутизації. Автентифікація протоколу маршрутизації або автентифікація сусідів запобігає прийняттю маршрутизатором шахрайських оновлень маршрутизації.
 - Control Plane Policing (CoPP) – CoPP — це функція Cisco IOS, яка дозволяє користувачам контролювати потік трафіку, який обробляється процесором маршрутизації мережевого пристрою.
 - AutoSecure – функція, яка може заблокувати функції площини контролю та служби і функції рівня пересилання маршрутизатора.
- ❑ CoPP розроблено для запобігання перевантаженню процесора маршрутизації непотрібним трафіком. Функція CoPP розглядає площину контролю як окрему сутність із власними вхідними (input) і вихідними (output) портами. Набір правил можна встановити та пов'язати з портами входу та виходу площини контролю.



Захист площини управління

- ❑ Трафік площини управління генерується або мережевими пристроями, або станціями керування мережею за допомогою процесів і протоколів, таких як Telnet, SSH і TFTP тощо. Площина управління є дуже привабливою мішенню для хакерів.
- ❑ Безпеку рівня управління можна реалізувати за допомогою таких функцій:
 - Політика входу та пароля – обмежує доступність пристрою.
 - Юридичне сповіщення (банер) – відображає повідомлення юридичного характеру.
 - Забезпечення конфіденційності даних – захист конфіденційних даних, що зберігаються локально, від перегляду чи копіювання. Використовує протоколи керування з надійною автентифікацією для пом'якшення атак на конфіденційність, спрямованих на розкриття паролів і конфігурацій пристрою.
 - Контроль доступу на основі ролей (RBAC) – гарантує, що доступ надається лише автентифікованим користувачам, групам і службам.
 - Авторизація дій - обмежує дії та перегляди, дозволені певним користувачем, групою чи службою.
 - Звітування про доступ до керування – ввімкнення журналів та облікових записів для всіх видів доступу.



Захист площини даних

- ❑ Трафік площини даних складається здебільшого з пакетів користувачів, які пересилаються через маршрутизатор. Безпеку рівня даних можна реалізувати за допомогою ACL, механізмів захисту від підробки та функцій безпеки рівня 2. ACL використовуються для захисту площини даних різними способами:
 - Блокування небажаного трафіку або користувачів
 - Зменшення ймовірності DoS
 - Пом'якшення атак спуфінгу
 - Забезпечення контролю пропускнуої здатності
 - Класифікація трафіку для захисту площин управління та контролю
- ❑ Комутатори Cisco Catalyst можуть використовувати інтегровані функції для захисту інфраструктури рівня 2. У комутатори Cisco Catalyst інтегровані такі інструменти безпеки рівня 2:
 - Безпека порту (port security)
 - Відстеження DHCP
 - Динамічна перевірка ARP (DAI)
 - IP Source Guard

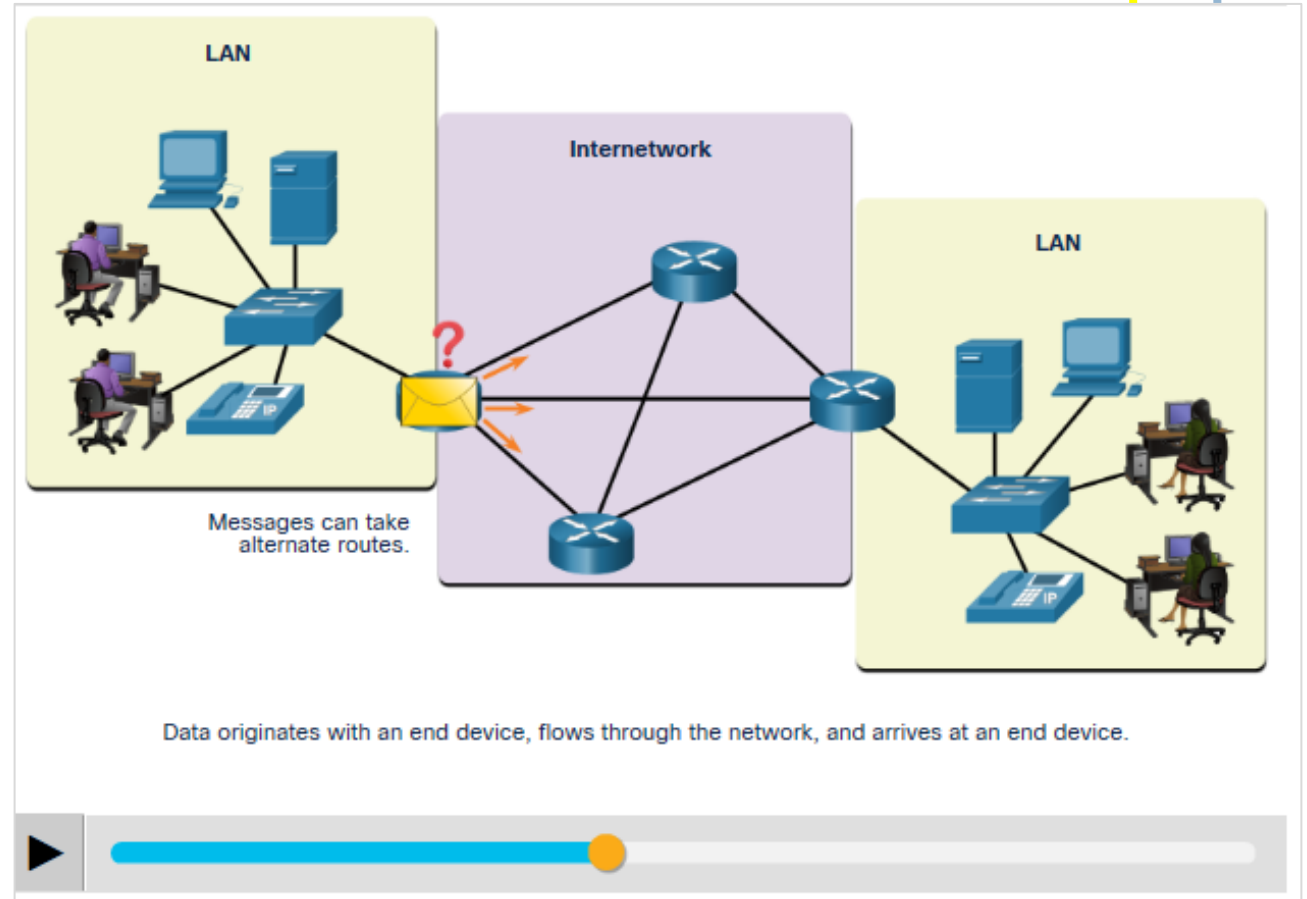


Мережеві пристрої



Кінцеві пристрої

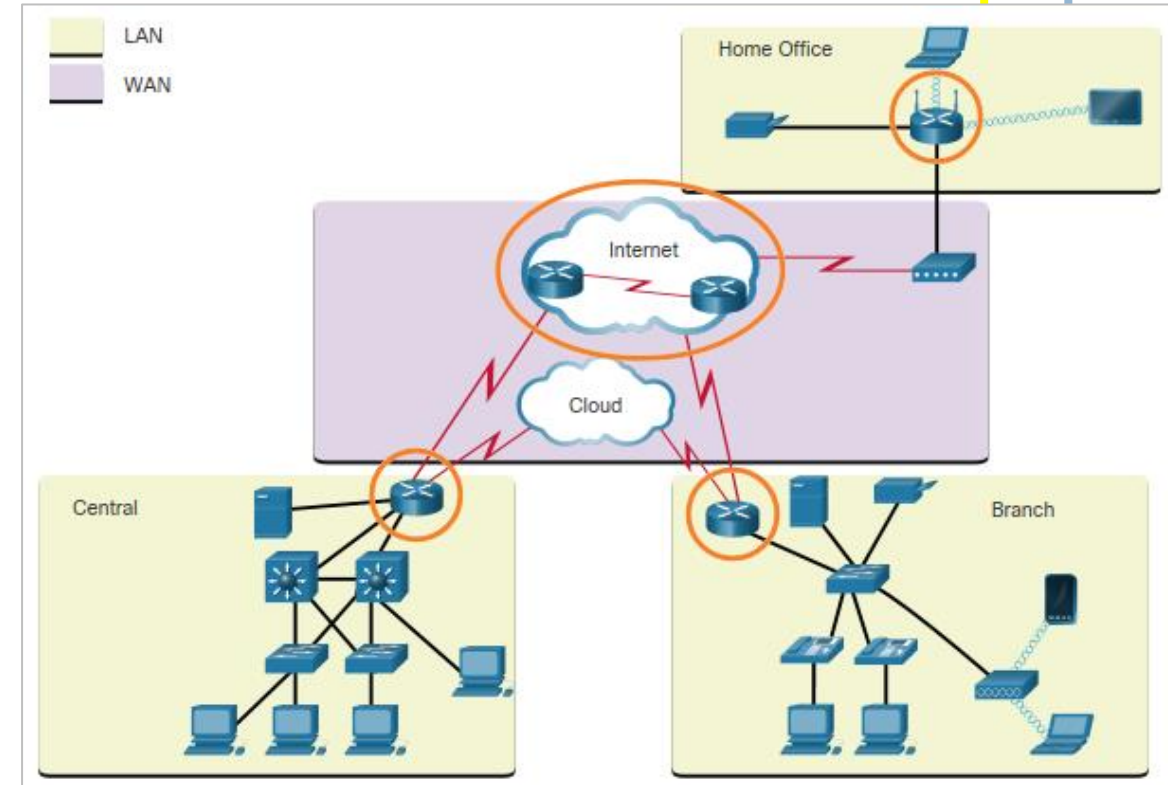
- ❑ Найвідомішими мережевими пристроями є кінцеві пристрої. Кінцевий пристрій є джерелом або одержувачем повідомлення, що передається через мережу.
- ❑ Щоб відрізнити один кінцевий пристрій від іншого, кожен кінцевий пристрій у мережі має адресу.
- ❑ Коли кінцевий пристрій ініціює зв'язок, він використовує адресу кінцевого пристрою призначення, щоб указати, куди доставити повідомлення.
- ❑ Дані надходять із кінцевого пристрою, проходять через мережу та надходять на кінцевий пристрій.





Маршрутизатори₁

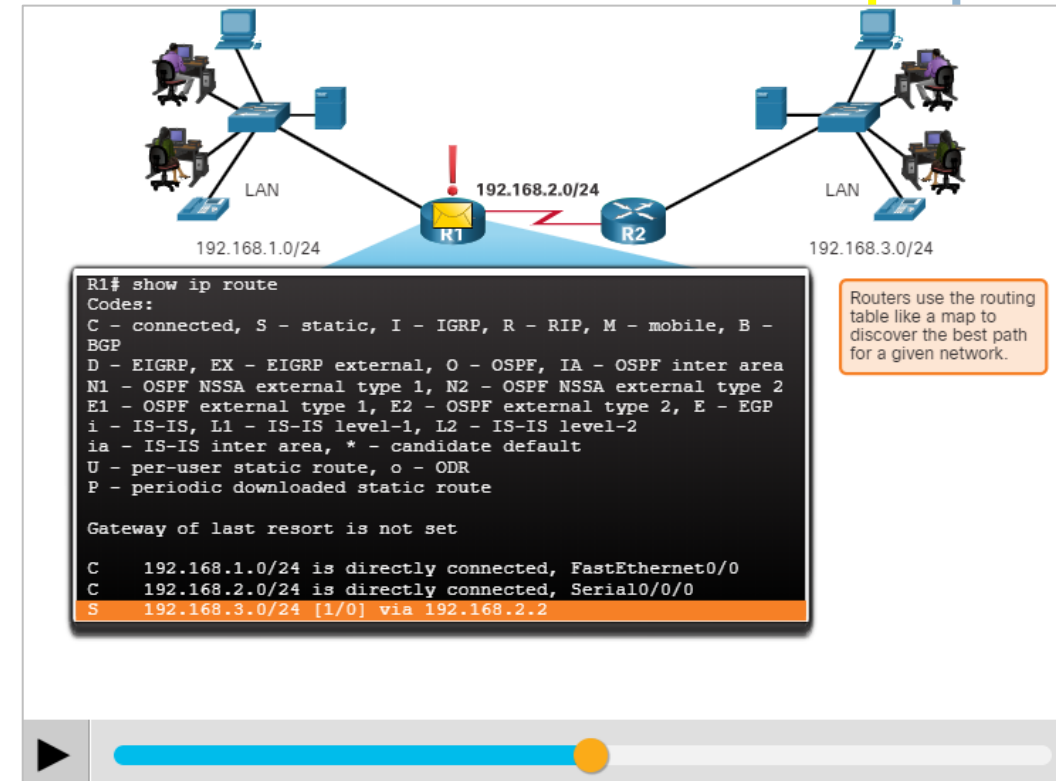
- ❑ Маршрутизатори — це пристрої, які працюють на мережевому рівні OSI (рівень 3).
- ❑ Як показано на слайді, маршрутизатори використовуються для з'єднання віддалених сайтів. Вони використовують процес маршрутизації для пересилання пакетів даних між мережами.
- ❑ Процес маршрутизації використовує таблиці мережевої маршрутизації, протоколи та алгоритми для визначення найбільш ефективного шляху для пересилання IP-пакету.
- ❑ Маршрутизатори збирають інформацію про маршрути та інформують інші маршрутизатори про зміни в мережі.





Маршрутизатори₂

- ❑ Щоб виконати визначення шляху, кожен маршрутизатор створює та підтримує таблицю маршрутизації, яка є базою даних відомих мереж і способів їх досягнення.
- ❑ Таблиця маршрутизації може бути створена вручну та містити статичні маршрути або може бути побудована за допомогою протоколу динамічної маршрутизації.
- ❑ Пересилання пакетів здійснюється за допомогою функції комутації.
- ❑ Комутація — це процес, який використовується маршрутизатором для прийняття пакета на одному інтерфейсі та пересилання його з іншого інтерфейсу.
- ❑ Основною метою функції комутації є інкапсуляція пакетів у відповідний тип кадру каналу даних для вихідного каналу даних.





Маршрутизатори₃

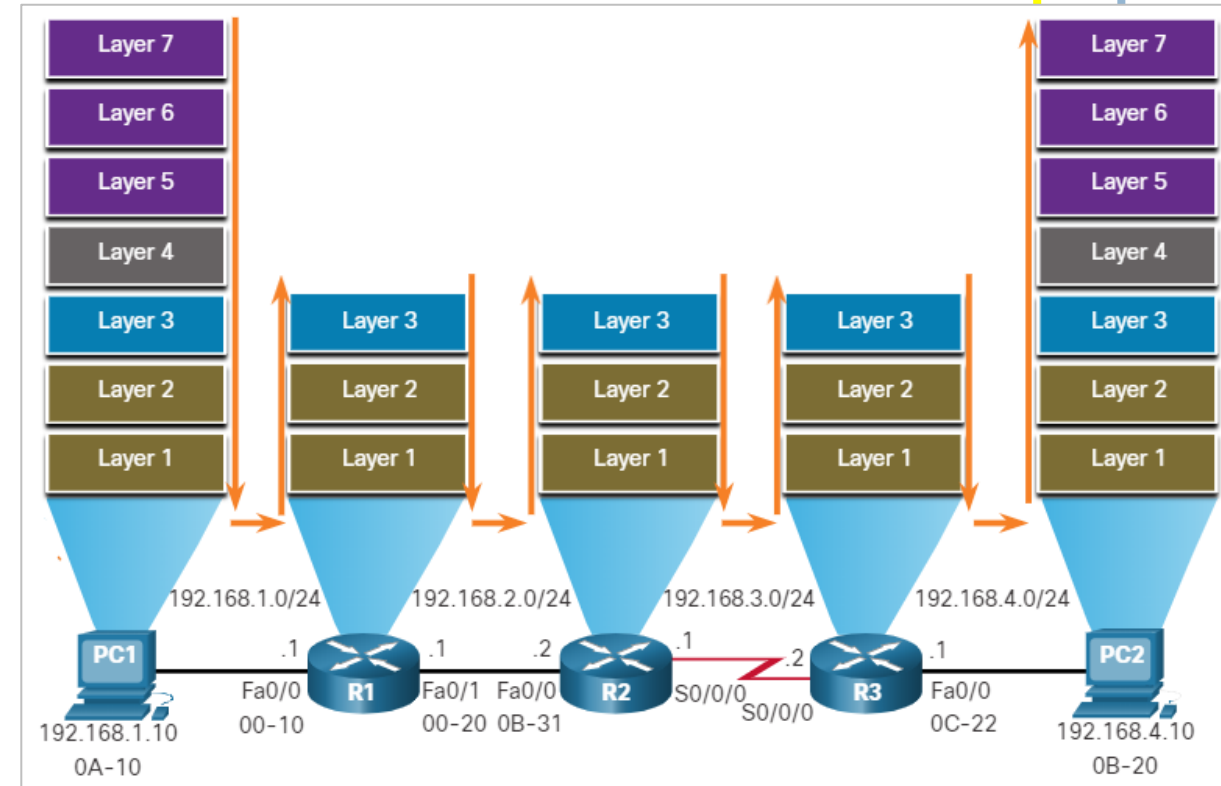
- ❑ Після того як маршрутизатор визначив вихідний інтерфейс за допомогою визначення шляху, маршрутизатор повинен інкапсулювати пакет у кадр каналу даних вихідного інтерфейсу.
- ❑ Коли пакет, отриманий з однієї мережі та призначений для іншої мережі, маршрутизатор виконує такі три основні кроки:
 - Він деінкапсулює заголовок кадру рівня 2 і трейлер, щоб відкрити пакет рівня 3.
 - Він перевіряє IP-адресу призначення IP-пакета, щоб знайти найкращий шлях у таблиці маршрутизації.
 - Якщо маршрутизатор знаходить шлях до місця призначення, він інкапсулює пакет рівня 3 у новий кадр рівня 2 і пересилає цей кадр через інтерфейс виходу.



Маршрутизатори₄

Інкапсуляція та деінкапсуляція пакетів

- ❑ Як показано на слайді, пристрої мають адреси IPv4 рівня 3, тоді як інтерфейси Ethernet мають адреси каналів передачі даних рівня 2. MAC-адреси скорочені для спрощення ілюстрації.
- ❑ Коли пакет переміщується від пристрою-джерела до пристрою кінцевого призначення, IP-адреси рівня 3 не змінюються, оскільки PDU рівня 3 не змінюється.
- ❑ Адреси каналів передачі даних рівня 2 змінюються на кожному маршрутизаторі на шляху до місця призначення, оскільки пакет деінкапсулюється та повторно інкапсулюється в новому кадрі рівня 2.

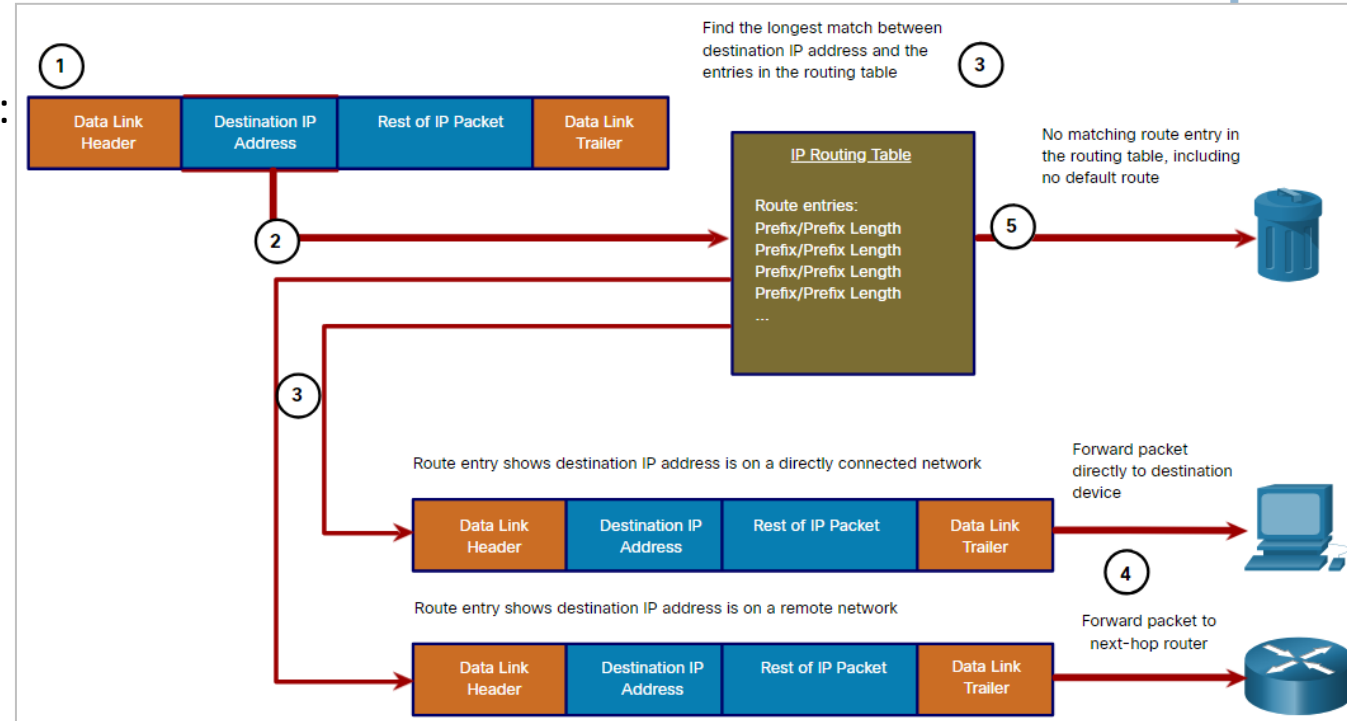




Процес прийняття рішення про пересилання пакетів₁

Тепер маршрутизатор повинен визначити, як інкапсулювати пакет і переслати його через правильний вихідний інтерфейс. Наступні кроки описують процес пересилання пакетів, показаний на слайді:

1. Кадр каналу передачі даних з інкапсульованим IP-пакетом надходить на вхідний інтерфейс.
2. Маршрутизатор перевіряє IP-адресу призначення в заголовку пакета та звертається до своєї таблиці IP-маршрутизації.
3. Маршрутизатор знаходить найдовший відповідний префікс у таблиці маршрутизації.
4. Маршрутизатор інкапсулює пакет у кадр каналу передачі даних і пересилає його через вихідний інтерфейс. Місцем призначення може бути пристрій, підключений до мережі, або наступний маршрутизатор.
5. Якщо відповідного запису маршруту немає, пакет відкидається.





Процес прийняття рішення про пересилання пакетів₂

Три дії, які маршрутизатор може виконати з пакетом після визначення найкращого шляху:

- Пересилає пакет на пристрій у мережі з прямим підключенням
- Пересилає пакет на наступний маршрутизатор
- Відкидає пакет - немає відповідності в таблиці маршрутизації

Пересилає пакет на пристрій у мережі з прямим підключенням

- Якщо запис маршруту вказує на те, що вихідний інтерфейс є мережею з прямим підключенням, це означає, що IP-адреса призначення пакета належить пристрою в мережі з прямим підключенням.
 - Пакет можна пересилати безпосередньо на пристрій призначення, кінцевий пристрій у локальній мережі Ethernet, що означає, що пакет має бути інкапсульований у фрейм Ethernet.
- ☐ Щоб інкапсулювати пакет у фрейм Ethernet, маршрутизатор повинен визначити MAC-адресу призначення, пов'язану з IP-адресою призначення пакета.



Процес прийняття рішення про пересилання пакетів₃

Процес залежить від того, чи є пакет пакетом IPv4 чи IPv6.

Пакет IPv4:

- Маршрутизатор перевіряє свою таблицю ARP на наявність IPv4-адреси призначення та пов'язаної MAC-адреси Ethernet.
- Якщо відповідності немає, маршрутизатор надсилає ARP-запит, а пристрій призначення поверне ARP-відповідь зі своєю MAC-адресою.
- Маршрутизатор тепер може пересилати пакет IPv4 у кадрі Ethernet із правильною MAC-адресою призначення.

Пакет IPv6:

- Маршрутизатор перевіряє свій сусідній кеш на IPv6-адресу призначення та пов'язану MAC-адресу Ethernet.
- Якщо відповідності немає, маршрутизатор надсилає повідомлення ICMPv6 Neighbor Solicitation (NS), а пристрій призначення поверне повідомлення ICMPv6 Neighbor Advertisement (NA) із своєю MAC-адресою.
- Маршрутизатор тепер може пересилати пакет IPv6 у кадрі Ethernet із правильною MAC-адресою призначення.



Процес прийняття рішення про пересилання пакетів₄

Пересилає пакет на наступний маршрутизатор

- Якщо запис маршруту вказує, що IP-адреса призначення знаходиться у віддаленій мережі, це означає, що IP-адреса призначення пакета належить пристрою в мережі, який не підключено напямую.
- Таким чином, пакет має бути перенаправлений на інший маршрутизатор, зокрема, на наступний маршрутизатор. Адреса наступного переходу вказується у записі маршруту.
- Якщо маршрутизатор пересилання та маршрутизатор наступного переходу знаходяться в мережі Ethernet, подібний процес (ARP та ICMPv6 Neighbor Discovery) відбудеться для визначення MAC-адреси призначення пакета. Різниця полягає в тому, що маршрутизатор шукатиме IP-адресу наступного маршрутизатора в таблиці ARP або сусідньому кеші замість IP-адреси призначення.

Відкидає пакет - немає відповідності в таблиці маршрутизації

- Якщо IP-адреса призначення та префікс у таблиці маршрутизації не збігаються, а також якщо немає маршруту за замовчуванням, пакет буде відкинуто.



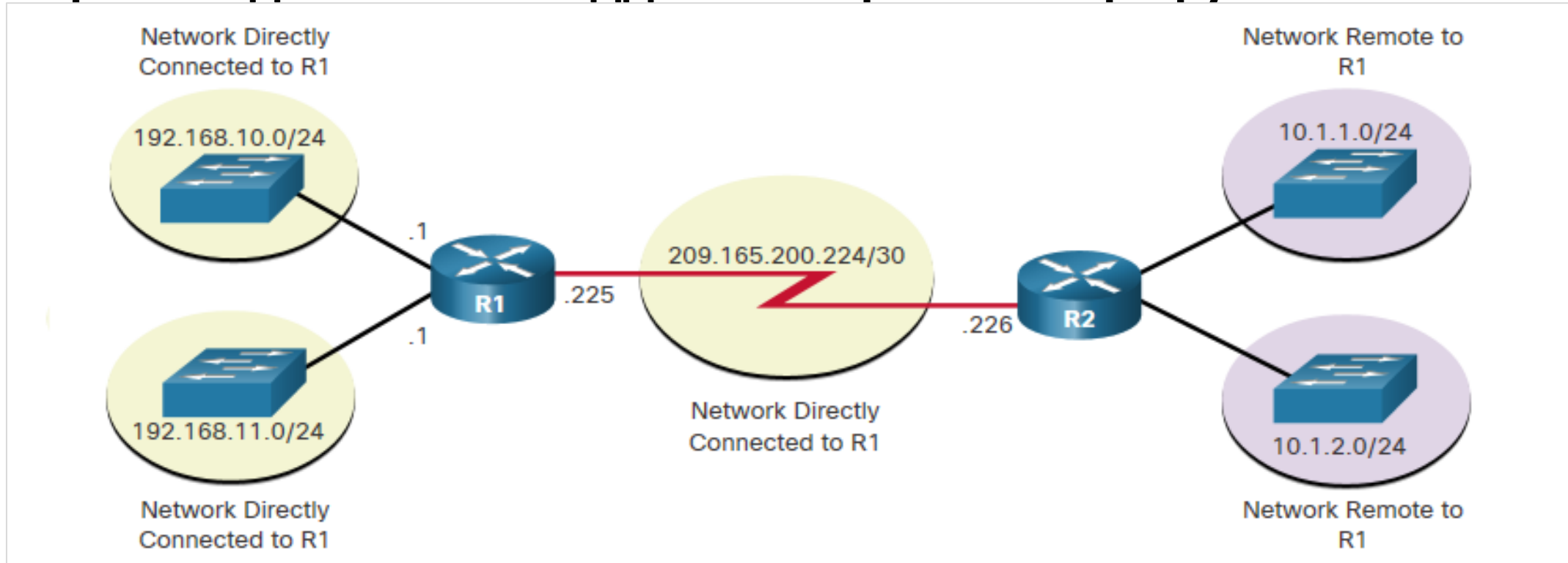
Інформація про маршрутизацію₁

- ❑ Таблиця маршрутизації зберігає таку інформацію:
 - Прямо підключені маршрути – ці маршрути надходять від активних інтерфейсів маршрутизатора. Маршрутизатори додають маршрут безпосереднього підключення, коли інтерфейс налаштовано з IP-адресою та активовано.
 - Віддалені маршрути - це віддалені мережі, підключені до інших маршрутизаторів.
- ❑ Таблиця маршрутизації – це файл даних в оперативній пам'яті, який використовується для зберігання інформації про маршрути безпосередньо підключених і віддалених мереж.
- ❑ Таблиця маршрутизації містить асоціації мережі або наступного переходу. Ці асоціації повідомляють маршрутизатору, що певний пункт призначення може бути оптимально досягнутий шляхом відправлення пакету на певний маршрутизатор, який представляє наступний стрибок (hop) на шляху до кінцевого пункту призначення.
- ❑ Асоціація наступного переходу також може бути вихідним або вихідним інтерфейсом до наступного пункту призначення.



Інформація про маршрутизацію₂

Прямо підключені та віддалені мережеві маршрути





Інформація про маршрутизацію₃

- ❑ Записи мережі призначення в таблицю маршрутизації можна додати кількома способами:
 - **Інтерфейси локального маршруту** – додаються, коли інтерфейс налаштований і активний. Цей запис відображається лише в IOS 15 або новішій версії для маршрутів IPv4, а також у всіх випусках IOS для маршрутів IPv6.
 - **Прямо підключені інтерфейси** – додаються до таблиці маршрутизації, коли інтерфейс налаштований і активний.
 - **Статичні маршрути** – додаються, коли маршрут налаштовано вручну та активний інтерфейс виходу.
 - **Протокол динамічної маршрутизації** – додаються, коли протоколи маршрутизації, які динамічно дізнаються про мережу, такі як EIGRP або OSPF, реалізують та ідентифікують мережі.
- ❑ Протоколи динамічної маршрутизації обмінюються інформацією про доступність мережі між маршрутизаторами та динамічно адаптуються до змін мережі.



Інформація про маршрутизацію₄

- ☐ Одним із перших протоколів динамічної маршрутизації був RIP. RIPv1 був випущений у 1988 році.
- ☐ Щоб задовольнити потреби великих мереж, було розроблено два розширені протоколи маршрутизації Open Shortest Path First (OSPF) і Intermediate System-to-Intermediate System (IS-IS).
- ☐ Cisco розробила протоколи внутрішньодоменої маршрутизації (IGRP) і розширений IGRP (EIGRP), які також добре масштабуються у великих мережах.
- ☐ Протокол BGP (Border Gateway Protocol) тепер використовується між постачальниками послуг Інтернету (ISP) та їхніми більшими приватними клієнтами для обміну інформацією про маршрутизацію.

☐ Наступна таблиця класифікує протоколи:

Протокол	Внутрішньодоменова маршрутизація		Міждоменова маршрутизація
	Дистанційно-векторні протоколи	Протоколи маршрутизації за станом каналу зв'язку	Шляхо-векторний протокол
RIP, RIPng	RIP, RIPng	RIP, RIPng	RIP, RIPng

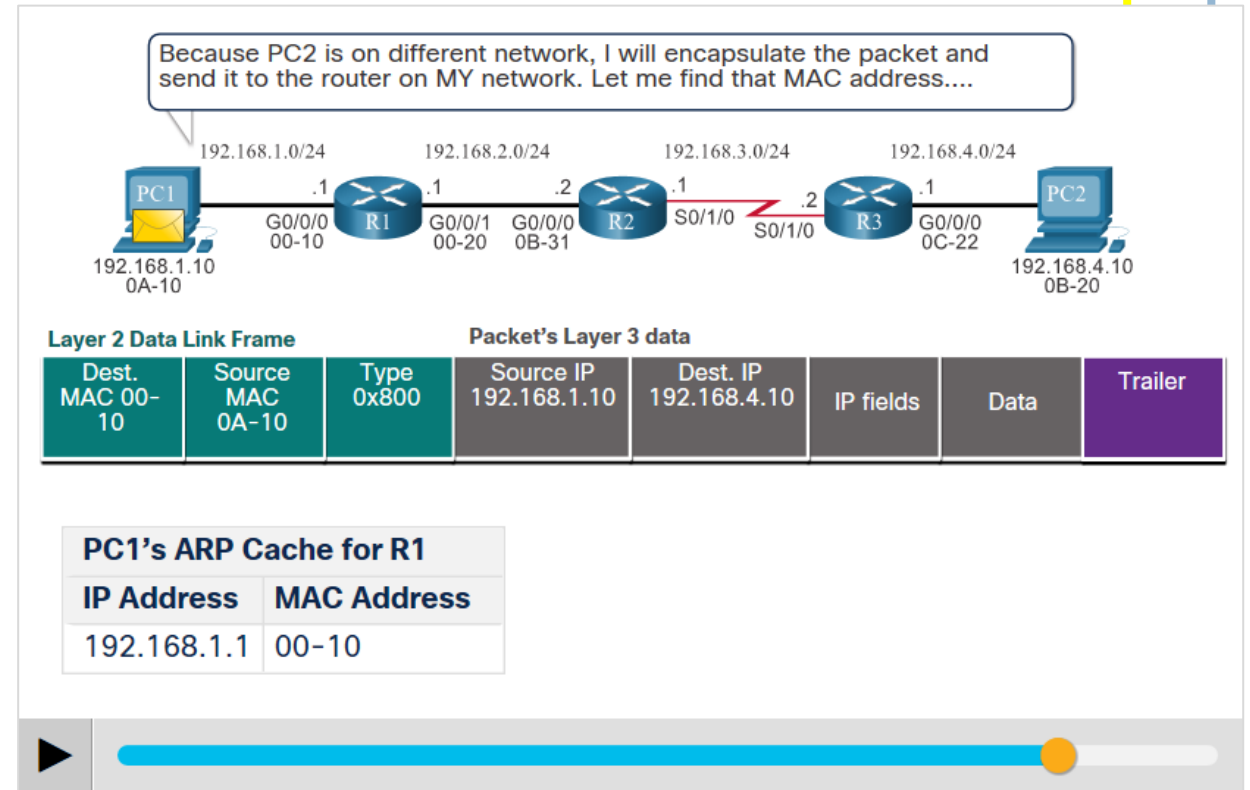


Наскрізне пересилання пакетів₁

□ Основною відповідальністю функції пересилання пакетів є інкапсуляція пакетів у відповідний тип кадру каналу даних для вихідного інтерфейсу. Процес пересилання пакетів описаний у наступному прикладі.

□ ПК1 надсилає пакет до ПК2

- На рисунку PC1 надсилає пакет PC2.
- Зауважте, що якщо запис ARP не існує в таблиці ARP для шлюзу за замовчуванням 192.168.1.1, PC1 надсилає запит ARP.
- Потім маршрутизатор R1 повертає відповідь ARP.

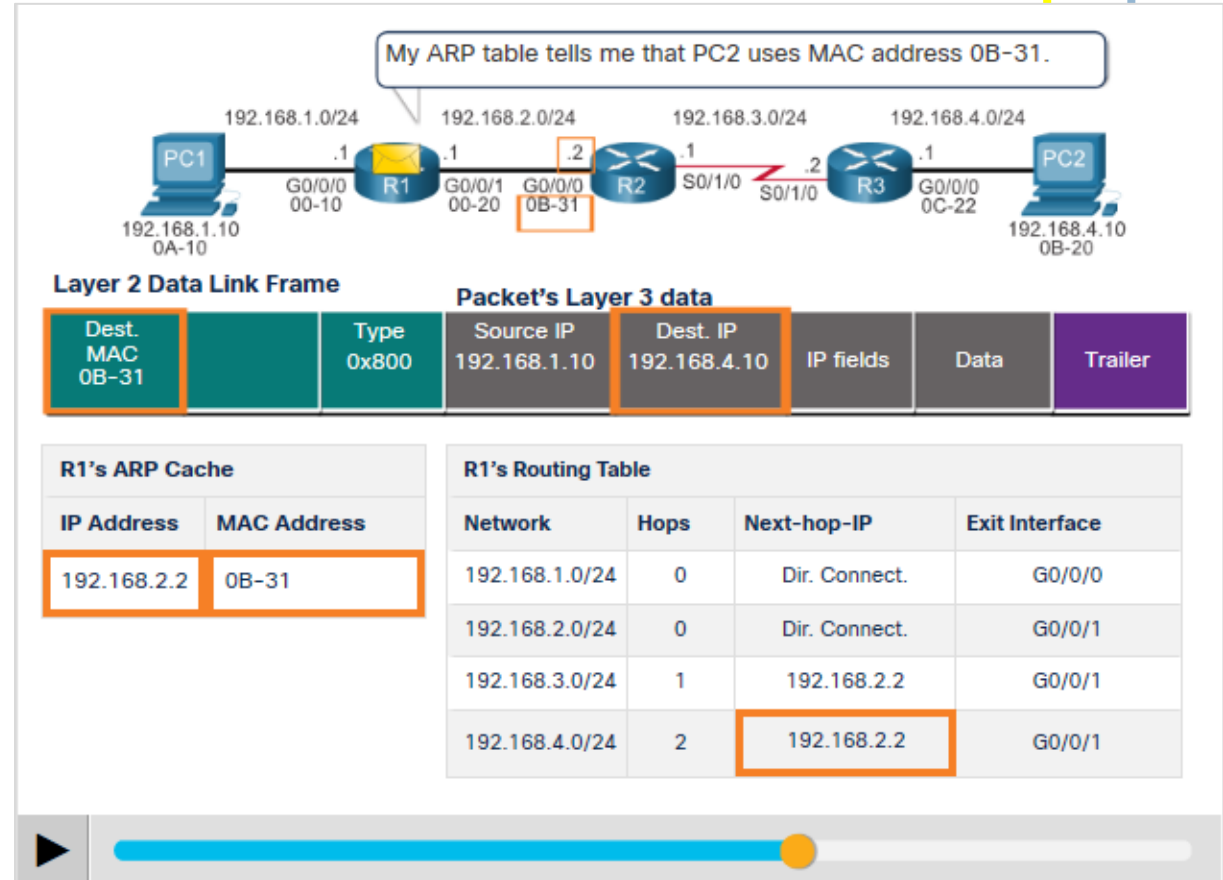




Наскрізне пересилання пакетів₂

R1 пересилає пакет до ПК2

- Тепер R1 пересилає пакет до ПК2.
- Оскільки інтерфейс виходу знаходиться в мережі Ethernet, R1 має визначити IPv4-адресу наступного стрибка з MAC-адресою призначення за допомогою своєї таблиці ARP.
- Якщо запис ARP не існує в таблиці ARP для інтерфейсу наступного переходу 192.168.2.2, R1 надсилає запит ARP.
- Потім R2 повертає відповідь ARP.

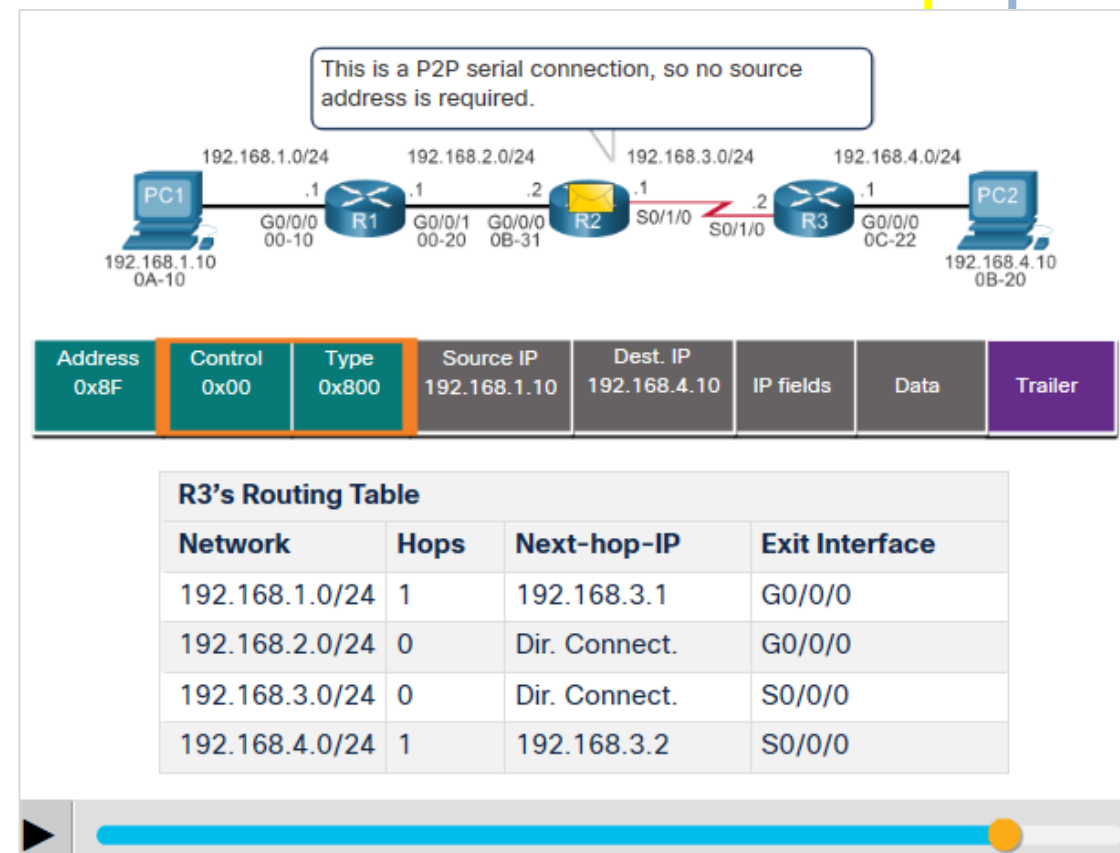




Наскрізне пересилання пакетів₃

R2 пересилає пакет до R3

- Тепер R2 пересилає пакет до R3.
- Оскільки інтерфейс виходу не є мережею Ethernet, R2 не потрібно розпізнавати IPv4-адресу наступного переходу з MAC-адресою призначення.
- Коли інтерфейс є послідовним з'єднанням «точка-точка» (P2P), маршрутизатор інкапсулює пакет IPv4 у відповідний формат кадру каналу даних, який використовується інтерфейсом виходу.
- Оскільки на послідовних інтерфейсах немає MAC-адрес, R2 встановлює адресу призначення каналу передачі даних на еквівалент широкомовної передачі.

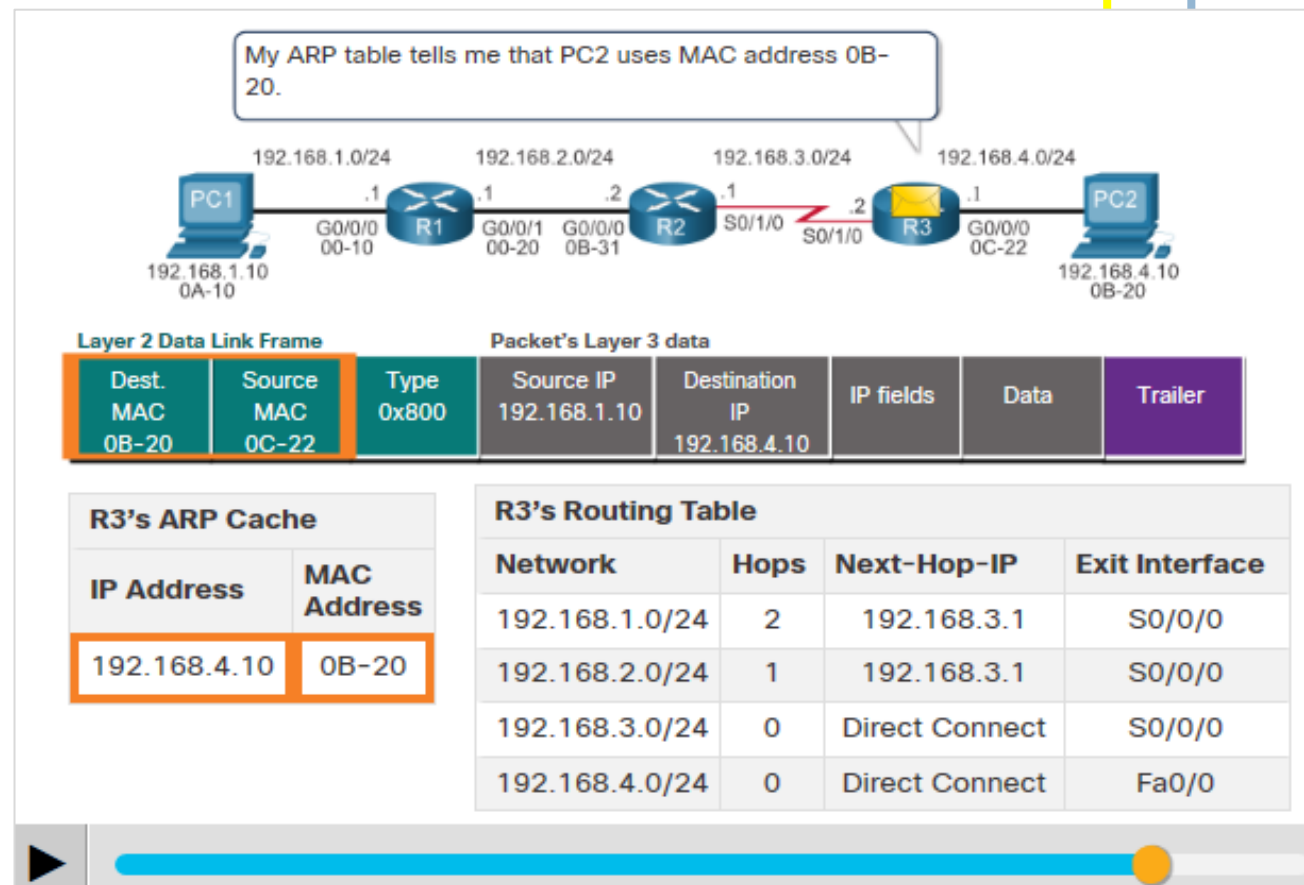




Наскрізне пересилання пакетів₄

R3 пересилає пакет до ПК2

- Тепер R3 пересилає пакет до ПК2.
- Оскільки IPv4-адреса призначення знаходиться в мережі Ethernet, підключеної безпосередньо, R3 має визначити IPv4-адресу призначення пакета з пов'язаною з ним MAC-адресою.
- Якщо запису немає в таблиці ARP, R3 надсилає запит ARP зі свого інтерфейсу FastEthernet 0/0.
- Після цього PC2 повертає ARP-відповідь зі своєю MAC-адресою.

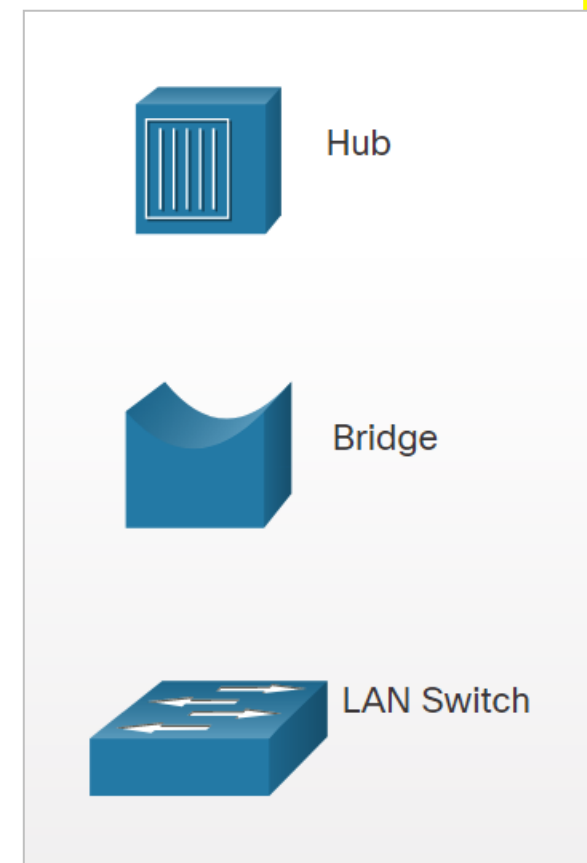




Концентратори, мости, комутатори LAN

110

- ☐ Піктограми топології концентраторів, мостів і комутаторів локальної мережі показано на рисунку.
- ☐ Концентратор Ethernet діє як багатопортовий повторювач, який отримує вхідний електричний сигнал (дані) через порт. Потім він негайно пересилає відновлений сигнал на всі інші порти. Концентратори використовують обробку фізичного рівня для пересилання даних.
- ☐ Мости мають два інтерфейси та з'єднують концентратори, щоб розділити мережу на кілька колізійних доменів. Кожен домен колізій може мати лише одного відправника одночасно.
- ☐ Комутатори LAN — це багатопортові мости, які з'єднують пристрої в топологію «зірка». Комутатори також сегментують локальну мережу на окремі домени колізій, по одному для кожного порту комутатора. Комутатор приймає рішення про переадресацію на основі MAC-адрес Ethernet.





Операція перемикання₁

- ☐ Комутатори використовують MAC-адреси для спрямування мережевого зв'язку через комутатор до відповідного порту та до місця призначення.
- ☐ Комутатор складається з інтегральних схем і супровідного програмного забезпечення, яке контролює шляхи передачі даних через комутатор.
- ☐ Щоб комутатор знав порт для передачі кадру, він повинен спочатку дізнатися про пристрої, які існують на кожному порту. Коли комутатор вивчає зв'язок між портами та пристроями, він створює таблицю, яка називається таблицею MAC-адрес, або таблицею пам'яті з адресацією вмісту (CAM), яка є особливим типом пам'яті, що використовується у програмах високошвидкісного пошуку.
- ☐ Комутатори локальної мережі визначають, як обробляти вхідні кадри даних, зберігаючи таблицю MAC-адрес.
- ☐ Комутатор використовує інформацію в таблиці MAC-адрес для надсилання кадрів, призначених для певного пристрою, через порт, до якого підключений пристрій.

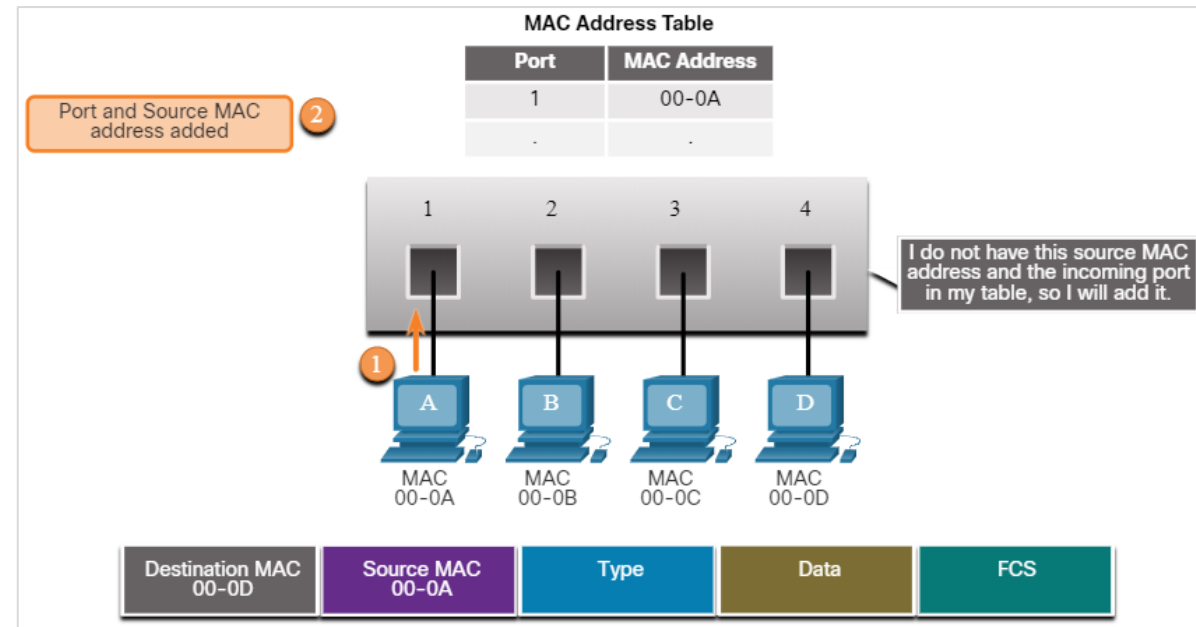


Операція перемикання₂

Наступний двоетапний процес виконується для кожного кадру Ethernet, який входить до комутатора.

Вивчення – перевірка MAC-адреси джерела

- Кожен кадр, який надходить на комутатор, перевіряється на наявність нової інформації про MAC-адресу шляхом вивчення MAC-адреси джерела кадру та номера порту, через який кадр потрапив на комутатор.
- Якщо MAC-адреса джерела відсутня в таблиці, вона додається до таблиці MAC-адрес разом із номером вхідного порту.
- Якщо MAC-адреса джерела існує в таблиці, комутатор оновлює таймер оновлення для цього запису. За замовчуванням більшість комутаторів Ethernet зберігають запис у таблиці протягом п'яти хвилин.



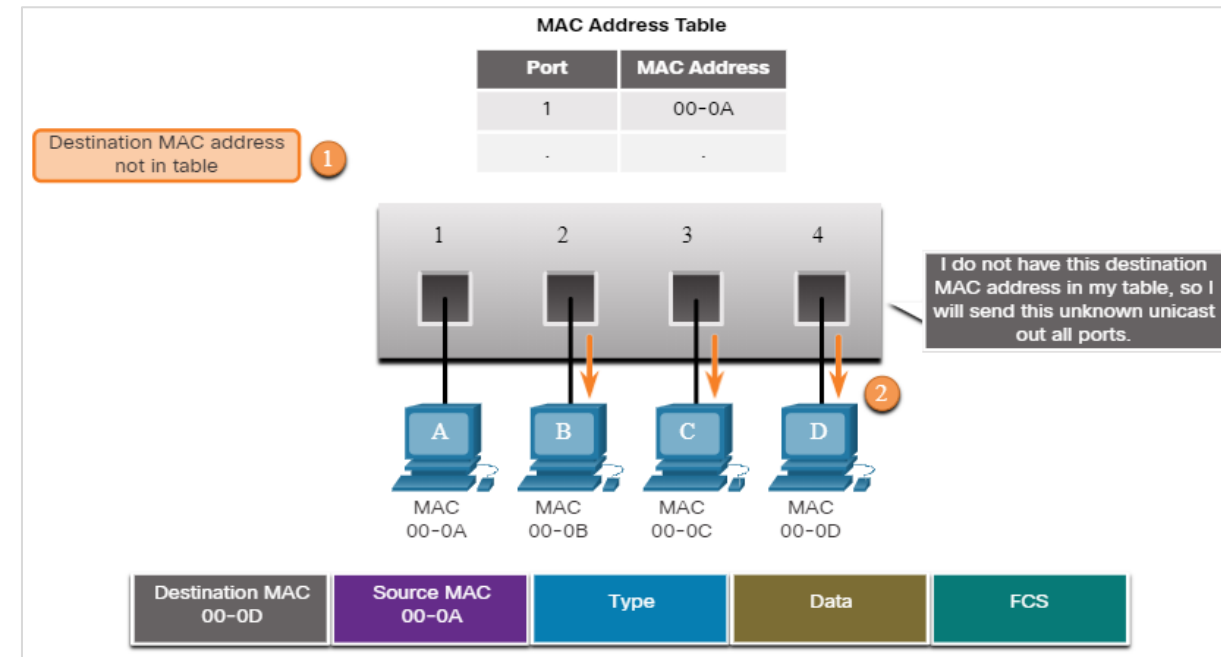
Примітка. Якщо MAC-адреса джерела існує в таблиці, але на іншому порту, комутатор розглядає це як новий запис. Запис замінюється на ту саму MAC-адресу, але з більш актуальним номером порту.



Операція перемикання₃

Пересилання – перевірка MAC-адреси призначення

- Якщо MAC-адреса призначення є одноадресною адресою, комутатор шукатиме відповідність між MAC-адресою призначення кадру та записом у його таблиці MAC-адрес.
- Якщо MAC-адреса призначення вказана в таблиці, кадр пересилається на вказаний порт.
- Якщо MAC-адреса призначення відсутня в таблиці, комутатор перешле кадр на всі порти, крім вхідного. Це називається невідомою одноадресною передачею.



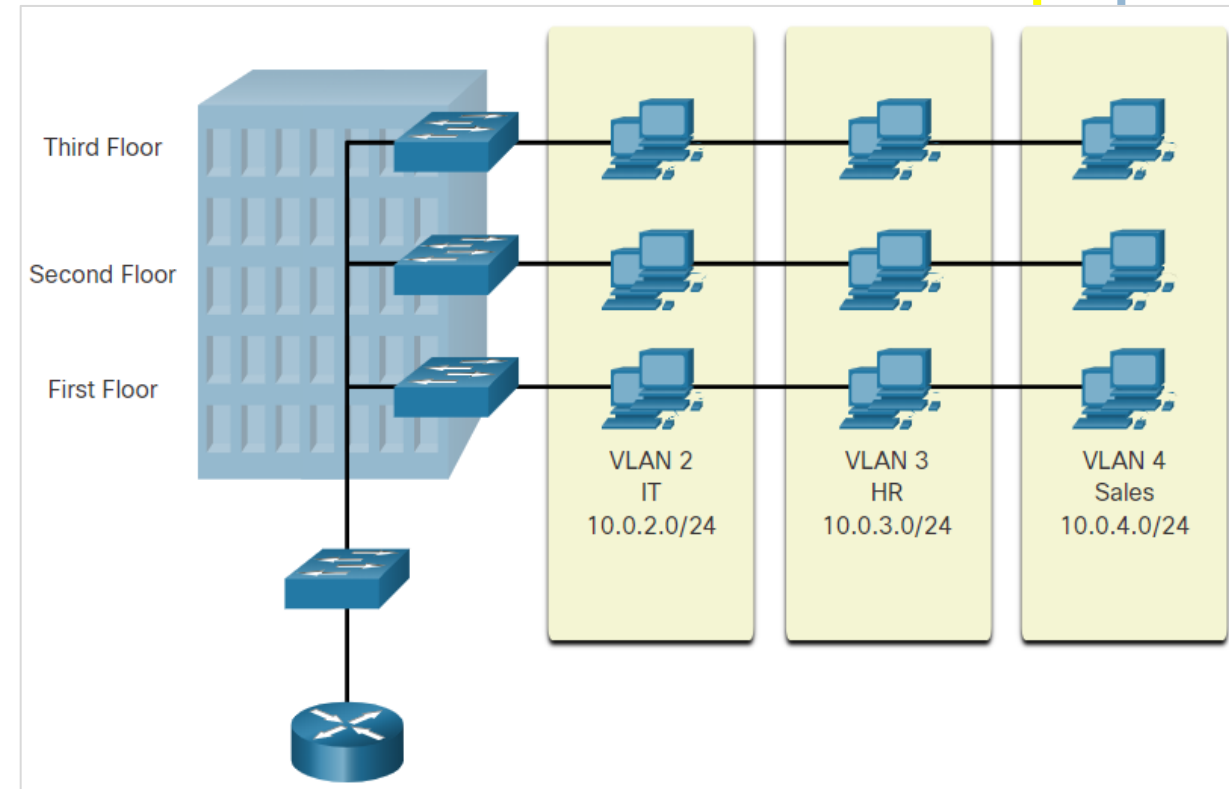
Примітка. Якщо MAC-адреса призначення є широкомовною або багатоадресною, кадр також розповсюджується на всі порти, крім вхідного.



VLAN

114

- ☐ VLAN надають можливість групувати пристрої в локальній мережі.
- ☐ VLAN забезпечує сегментацію та організаційну гнучкість у комутаційній міжмережі.
- ☐ VLAN дозволяє адміністратору сегментувати мережі на основі таких факторів, як функція, команда проекту або програма, незалежно від фізичного розташування користувача чи пристрою.
- ☐ VLAN створює логічний широкомовний домен, який може охоплювати кілька фізичних сегментів локальної мережі.
- ☐ VLAN запобігає користувачам різних VLAN стежити за трафіком один одного.





STP

- ☐ Протокол охоплюючого дерева використовується для підтримки одного незацикленого шляху в мережі рівня 2 у будь-який час.
- ☐ Петлі та повторювані кадри мають серйозні наслідки для комутованої мережі. STP було розроблено для вирішення цих проблем.
- ☐ Він забезпечує наявність одного логічного шляху між усіма пунктами призначення в мережі, блокуючи надлишкові шляхи.
- ☐ Порт вважається заблокованим, якщо дані користувача не можуть увійти або вийти з цього порту. Це не включає кадри блоку даних протоколу мосту (BPDU), які використовуються STP для запобігання циклам.
- ☐ Якщо шлях коли-небудь знадобиться для компенсації збою мережевого кабелю або комутатора, STP перераховує шляхи та розблокує необхідні порти для активації резервного шляху.



Багаторівнева комутація₁

Багаторівневі комутатори (комутатори рівня 3) виконують комутацію рівня 2, а також пересилають кадри на основі інформації рівнів 3 і 4.

Усі багаторівневі комутатори Cisco Catalyst підтримують такі типи інтерфейсів рівня 3:

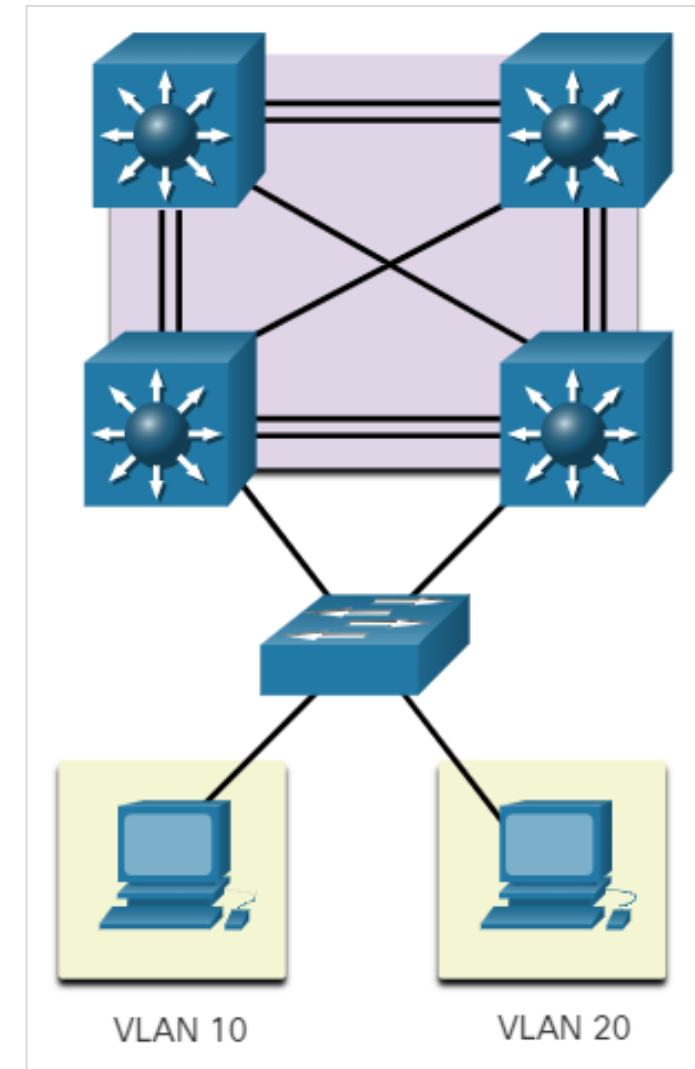
- **Маршрутизований порт** – чистий інтерфейс рівня 3, подібний до фізичного інтерфейсу на маршрутизаторі Cisco IOS.
- **Віртуальний інтерфейс комутатора (SVI)** – віртуальний інтерфейс VLAN для маршрутизації між VLAN. Іншими словами, SVI — це інтерфейси VLAN з віртуальною маршрутизацією.



Багаторівнева комутація₂

Маршрутизовані порти

- Маршрутизований порт — це фізичний порт, який діє подібно до інтерфейсу на маршрутизаторі.
- На відміну від порту доступу, маршрутизований порт не пов'язаний з конкретною VLAN. Він поводить себе як звичайний інтерфейс маршрутизатора.
- Крім того, оскільки функції рівня 2 було видалено, протоколи рівня 2, такі як STP, не функціонують на маршрутизованому інтерфейсі.
- Деякі протоколи, такі як LACP і EtherChannel, функціонують на рівні 3. На відміну від маршрутизаторів Cisco IOS, маршрутизовані порти комутатора Cisco IOS не підтримують підінтерфейси.

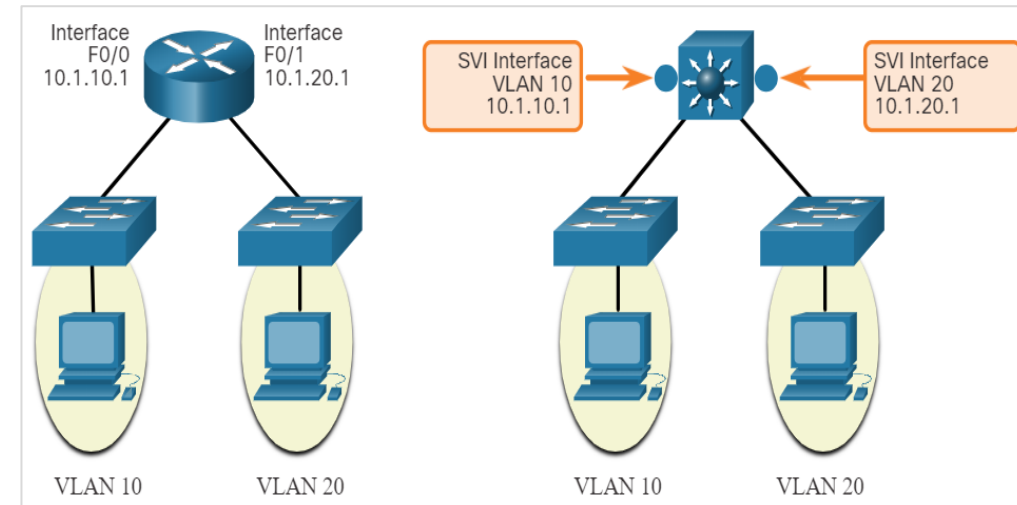




Багаторівнева комутація₃

SVI

- SVI — це віртуальний інтерфейс, налаштований у багаторівневому комутаторі. На відміну від базових комутаторів рівня 2, багаторівневий комутатор може мати кілька SVI. SVI можна створити для будь-якої VLAN, яка існує на комутаторі.
- SVI вважається віртуальним, оскільки немає фізичного порту виділеного для інтерфейсу. Він може виконувати ті самі функції для VLAN, що й інтерфейс маршрутизатора, і його можна налаштувати майже так само, як інтерфейс маршрутизатора.
- SVI для VLAN забезпечує обробку рівня 3 для пакетів до або з усіх портів комутатора, пов'язаних із цією VLAN.





Бездротовий зв'язок



WLAN vs Wired LAN₁

- ❑ WLAN використовують радіочастоти (RF) замість кабелів на фізичному рівні та підрівні MAC канального рівня.
- ❑ IEEE прийняв портфель стандартів архітектури комп'ютерних мереж 802 LAN/MAN, який включає дві домінуючі робочі групи: 802.3 Ethernet, який визначив Ethernet для дротових локальних мереж, і 802.11, який визначив Ethernet для WLAN.
- ❑ WLAN також відрізняються від дротових локальних мереж наступним чином:
 - WLAN підключають клієнтів до мережі через бездротову точку доступу (AP) або бездротовий маршрутизатор замість комутатора Ethernet.
 - Мережі WLAN підключають мобільні пристрої, які часто живляться від батареї, на відміну від підключених пристроїв локальної мережі. Бездротові мережеві карти, як правило, скорочують час роботи акумулятора мобільного пристрою.
 - Мережі WLAN підтримують хости, які претендують на доступ до радіочастотного середовища (смуги частот).
 - WLAN використовує інший формат кадру, ніж дротові локальні мережі Ethernet. WLAN вимагає додаткової інформації в заголовку рівня 2 кадру.
 - Бездротові мережі викликають більше проблем із конфіденційністю, оскільки радіочастоти можуть виходити за межі приміщення.



WLAN vs Wired LAN₂

Різниця між WLAN і дротовою локальною мережею наведена в наступній таблиці.

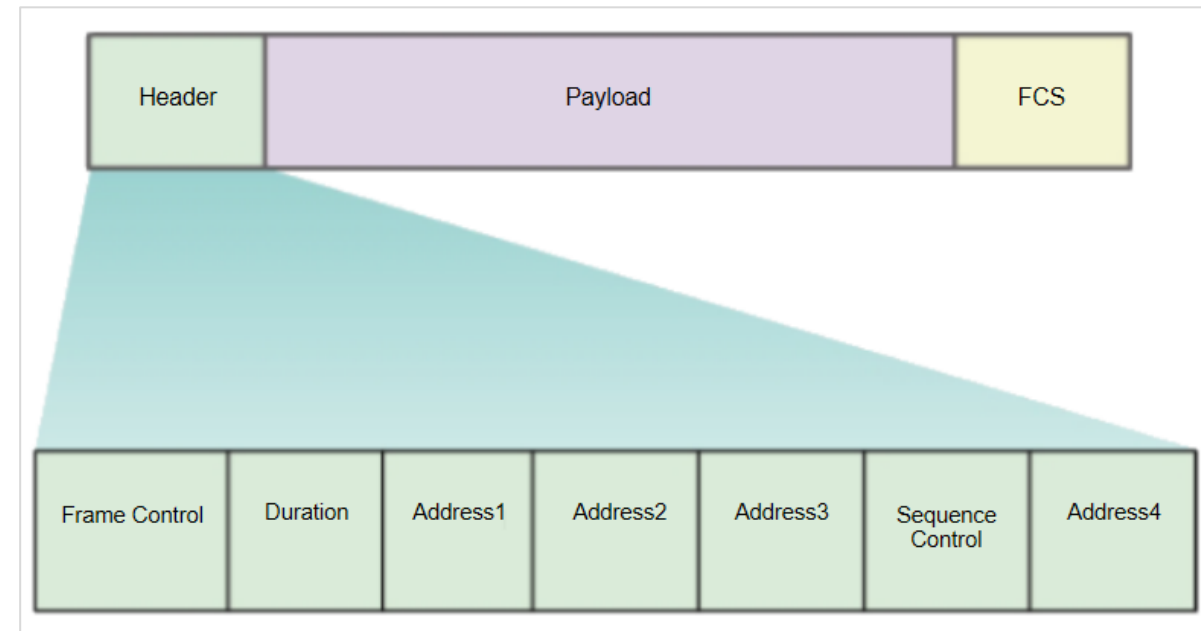
Характеристи ка	Бездротова локальна мережа 802.11	Дротові локальні мережі Ethernet 802.3
Фізичний рівень	Радіочастота (РЧ)	Фізичні кабелі
Доступ до медіа	Уникнення колізій	Виявлення колізій
Доступність	Усі, хто має бездротовий мережевий адаптер у зоні дії точки доступу	Потрібне фізичне кабельне підключення
Перешкоди сигналу	Так	Мінімальний



Структура кадру 802.11₁

□ Усі бездротові кадри 802.11 містять такі поля:

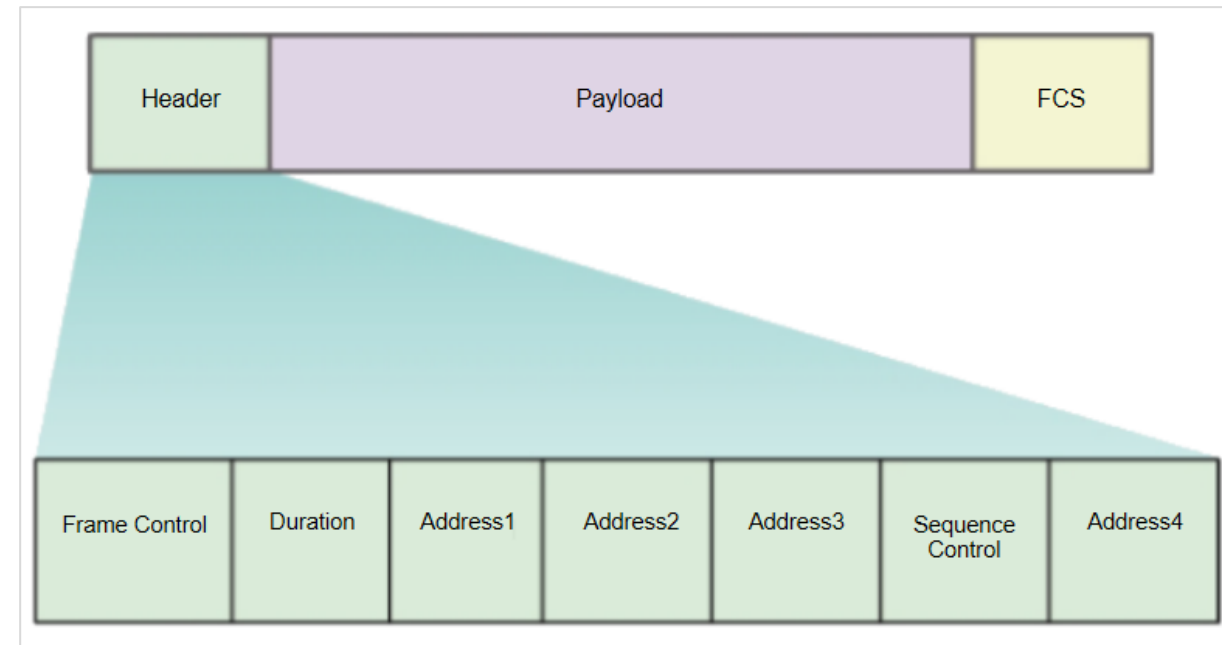
- **Frame Control** – визначає тип бездротового кадру та містить підполя для версії протоколу, типу кадру, типу адреси, керування живленням і параметрів безпеки.
- **Duration** – використовується для вказівки тривалості, що залишилася, необхідної для отримання наступної передачі кадру.
- **Address1** – містить MAC-адресу приймаючого бездротового пристрою або точки доступу.
- **Address2** – містить MAC-адресу бездротового пристрою або точки доступу, що передає дані.





Структура кадру 802.11₂

- ❑ **Address3** – містить MAC-адресу пункту призначення, наприклад інтерфейс маршрутизатора з підключеною точкою доступу.
- ❑ **Sequence control** – містить інформацію для керування послідовністю та фрагментованими кадрами.
- ❑ **Address4** – зазвичай відсутня, оскільки використовується лише в режимі ad hoc.
- ❑ **Payload** – містить дані для передачі.
- ❑ **FCS** – використовується для контролю помилок рівня 2.





CSMA/CA₁

- ☐ WLAN — це напівдуплексні конфігурації спільного медіа.
- ☐ Напівдуплекс означає, що тільки один клієнт може передавати або приймати в будь-який момент.
- ☐ Спільний медіа означає, що всі бездротові клієнти можуть передавати та приймати на одному радіоканалі.
- ☐ Це створює проблему, оскільки бездротовий клієнт не чує під час надсилання, що унеможлиблює виявлення конфлікту.
- ☐ Щоб вирішити цю проблему, мережі WLAN використовують метод множинного доступу з визначенням несучої з уникненням колізій (CSMA/CA), щоб визначити, як і коли надсилати дані в мережі.



CSMA/CA₂

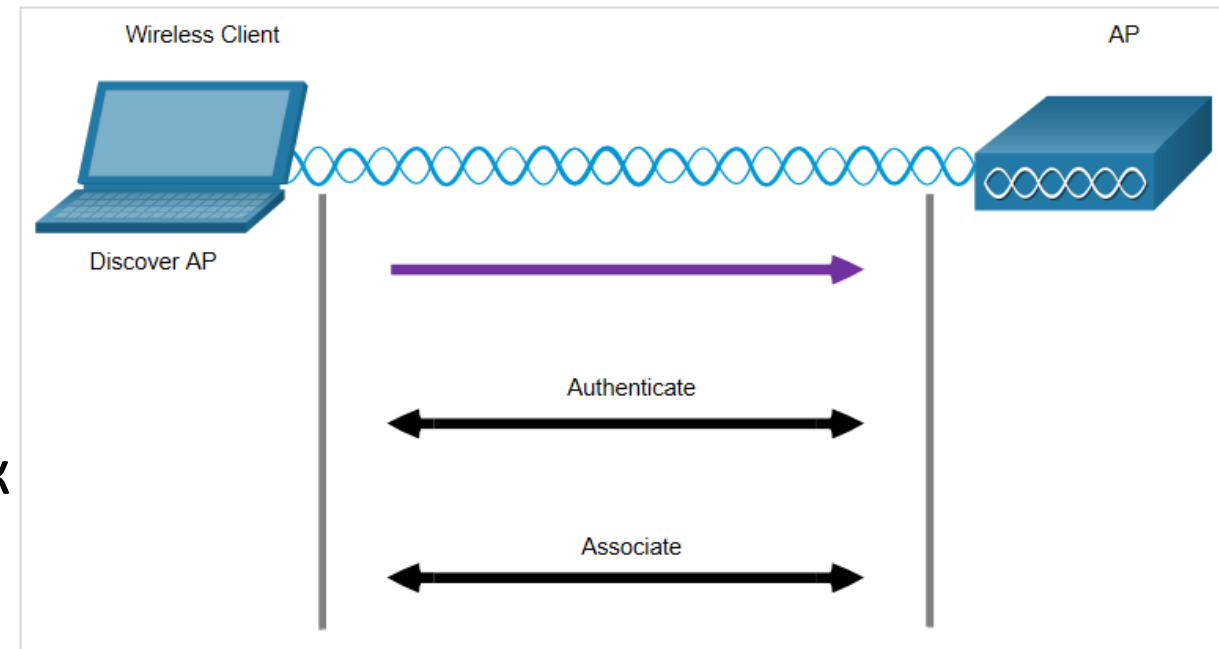
Бездротовий клієнт робить наступне:

- ☐ Прослуховує канал, щоб перевірити, чи він неактивний. Канал ще називають несучим.
- ☐ Надсилає повідомлення Ready To Send (RTS) до точки доступу для запиту виділеного доступу до мережі.
- ☐ Отримує повідомлення Clear To Send (CTS) від AP, що надає доступ для надсилання.
- ☐ Якщо бездротовий клієнт не отримує повідомлення CTS, він чекає довільний проміжок часу перед перезапуском процесу.
- ☐ Після отримання CTS він передає дані.
- ☐ Усі передачі підтверджуються.



Бездротовий клієнт і асоціація з AP₁

- ❑ Щоб бездротові пристрої могли обмінюватися даними через мережу, вони повинні спочатку зв'язатися з точкою доступу або бездротовим маршрутизатором.
- ❑ Важливою частиною процесу 802.11 є виявлення WLAN і подальше підключення до неї.
- ❑ Бездротові пристрої виконують наступний триетапний процес, як показано на рисунку:
 - Пошук бездротової точки доступу
 - Автентифікація з AP
 - Асоціація з AP





Бездротовий клієнт і асоціація з AP₂

Щоб мати успішне з'єднання, бездротовий клієнт і точка доступу повинні узгодити певні параметри. Параметри потрібно налаштувати на точці доступу, а потім на клієнті. Налаштовані параметри бездротового зв'язку включають:

- ☐ SSID – ім'я SSID відображається в списку доступних бездротових мереж клієнта.
- ☐ Пароль – потрібний від бездротового клієнта для автентифікації в точці доступу.
- ☐ Режим мережі – стосується стандартів WLAN 802.11a/b/g/n/ac/ad.
- ☐ Режим безпеки – стосується налаштувань параметрів безпеки, таких як WEP, WPA або WPA2. Завжди вмикайте найвищий підтримуваний рівень безпеки.
- ☐ Параметри каналу – діапазони частот, які використовуються для передачі бездротових даних.

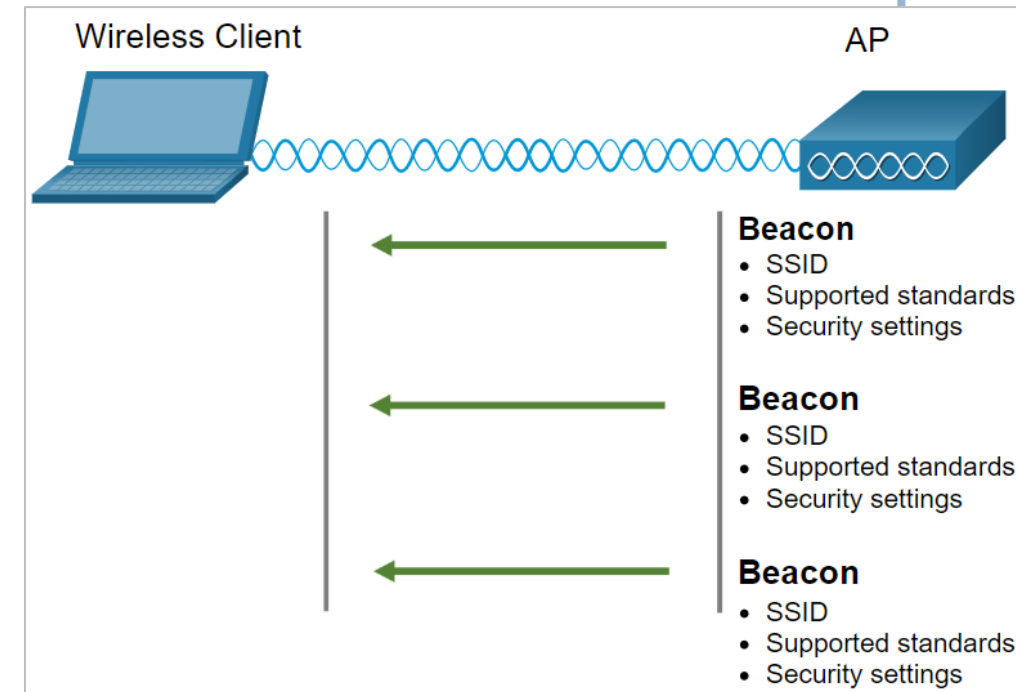


Пасивний і активний режим виявлення точки доступу₁

Бездротові пристрої повинні виявити точку доступу або бездротовий маршрутизатор і підключитися до нього. Бездротові клієнти підключаються до точки доступу за допомогою процесу сканування (зондування), наприклад пасивного та активного.

Пасивний режим

- ☐ У цьому режимі точка доступу відкрито рекламує свою послугу, періодично надсилаючи кадри широкомовного маяка, що містять SSID, підтримувані стандарти та налаштування безпеки.
- ☐ Основна мета маяка — дозволити бездротовим клієнтам дізнатися, які мережі та точки доступу доступні в певній області.
- ☐ Це дозволяє бездротовим клієнтам вибирати, яку мережу та точку доступу використовувати.

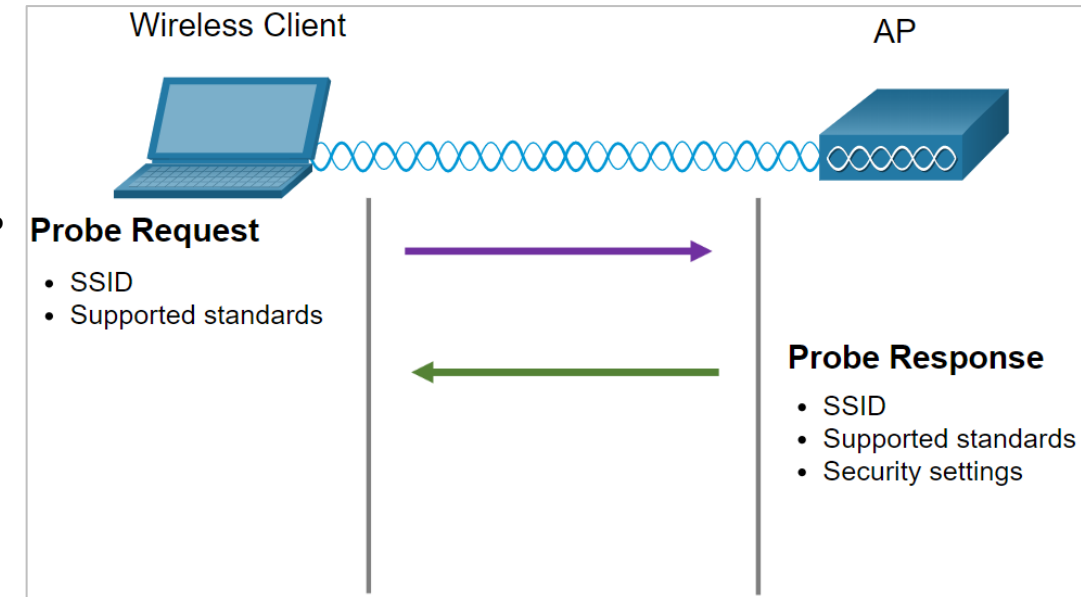




Пасивний і активний режим виявлення точки доступу₂

Активний режим

- ☐ У цьому режимі бездротові клієнти повинні знати назву SSID.
- ☐ Бездротовий клієнт ініціює процес, транслюючи кадр тестового запиту на кількох каналах, що включає назву SSID і підтримувані стандарти.
- ☐ Точки доступу, налаштовані за допомогою SSID, надішлють тестову відповідь, яка містить SSID, підтримувані стандарти та налаштування безпеки.
- ☐ Активний режим може знадобитися, якщо точку доступу налаштовано так, щоб не транслювати кадри маяка.
- ☐ Бездротовий клієнт може також надіслати запит на зондування без назви SSID, щоб виявити найближчі мережі WLAN. Точки доступу, налаштовані на трансляцію кадрів маяка, відповідатимуть бездротовому клієнту відповіддю на тестування та нададуть ім'я SSID.





Бездротові пристрої - AP, LWAP і WLC₁

- ❑ Загальною реалізацією бездротових даних є можливість бездротового підключення пристроїв через локальну мережу.
- ❑ Загалом для бездротової локальної мережі потрібні бездротові точки доступу та клієнти, які мають бездротові мережеві карти.
- ❑ Бездротові маршрутизатори для дому та малого бізнесу об'єднують функції маршрутизатора, комутатора та точки доступу в одному пристрої, як показано на слайді.
- ❑ У невеликих мережах бездротовий маршрутизатор може бути єдиною точкою доступу, оскільки бездротове покриття вимагає лише невеликої території.
- ❑ У великих мережах може бути багато точок доступу.





Бездротові пристрої - AP, LWAP і WLC₂

- ☐ Усі функції контролю та управління точками доступу в мережі можуть бути централізовані в контролері бездротової локальної мережі (WLC).
- ☐ При використанні WLC точки доступу більше не працюють автономно, а замість цього діють як полегшені точки доступу (LWAP).
- ☐ LWAP лише пересилає дані між бездротовою локальною мережею та WLC.
- ☐ Усі функції керування, такі як визначення SSID та автентифікація, виконуються на централізованому WLC, а не на кожній окремій AP.
- ☐ Основною перевагою централізації функцій керування AP у WLC є спрощена конфігурація та моніторинг численних точок доступу.



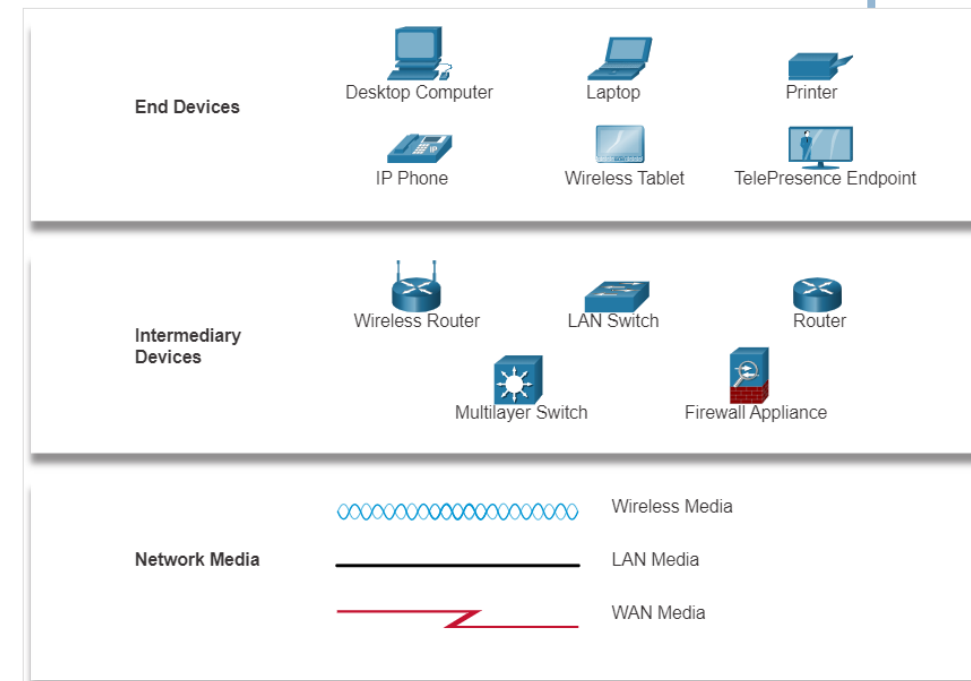
Топології мережі



Представлення мереж

- ❑ Діаграми мережі, які часто називають діаграмами топології, використовують символи для представлення різних пристроїв і з'єднань у мережі.
- ❑ Важливі терміни, які слід знати, включають:
 - Карта мережевого інтерфейсу (NIC)
 - Фізичний порт
 - Інтерфейс

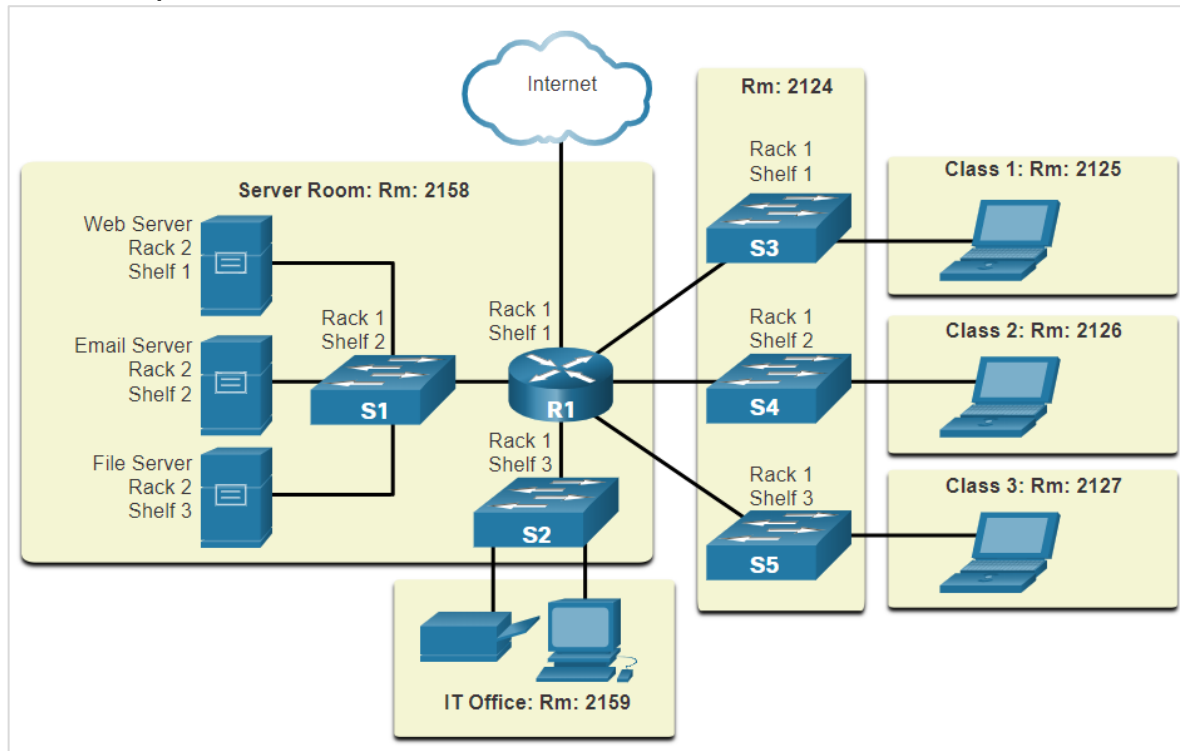
***Примітка.** Терміни порт та інтерфейс часто використовуються як синоніми.*



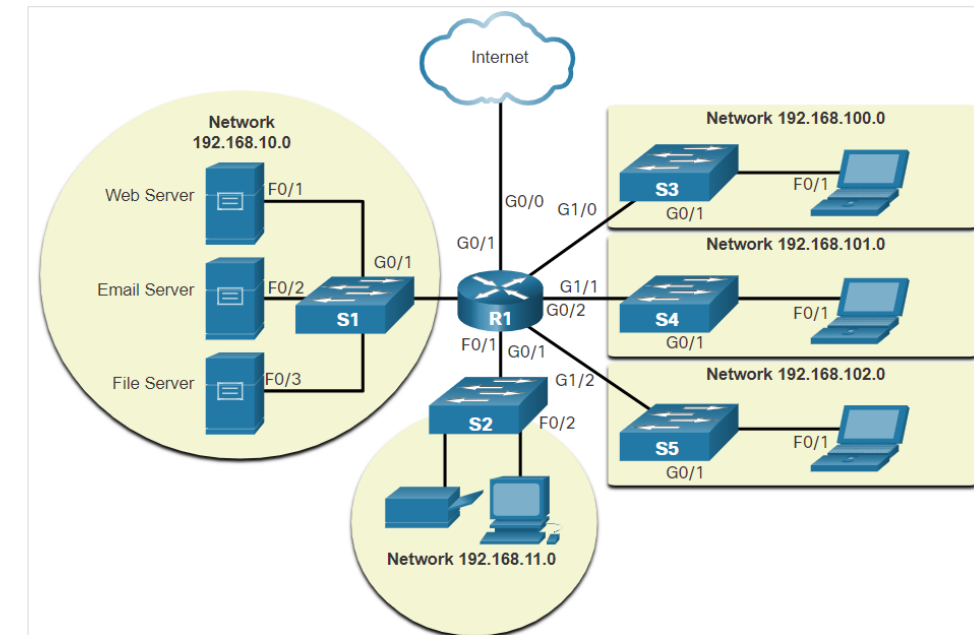


Топологічні діаграми

Фізичні топології ілюструють фізичне розташування проміжних пристроїв і кабельної інсталяції.



Логічні топології ілюструють пристрої, порти та схему адресації мережі.





Розміри мереж

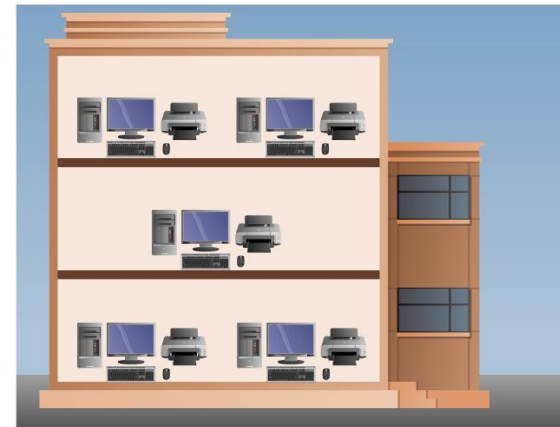
- Невеликі домашні мережі – з'єднують кілька комп'ютерів один з одним та з Інтернетом.
- Малий і домашній офіси (SOHO) – дозволяє комп'ютеру вдома, в офісі чи віддаленому офісі підключатися до корпоративної мережі або отримувати доступ до централізованих спільних ресурсів.
- Середні та великі – можуть мати багато місць із сотнями чи тисячами взаємопов'язаних комп'ютерів.
- Всесвітні мережі – об'єднують сотні мільйонів комп'ютерів по всьому світу – наприклад, Інтернет.



Малий офіс



SOHO



Середня/велика



Всесвітня



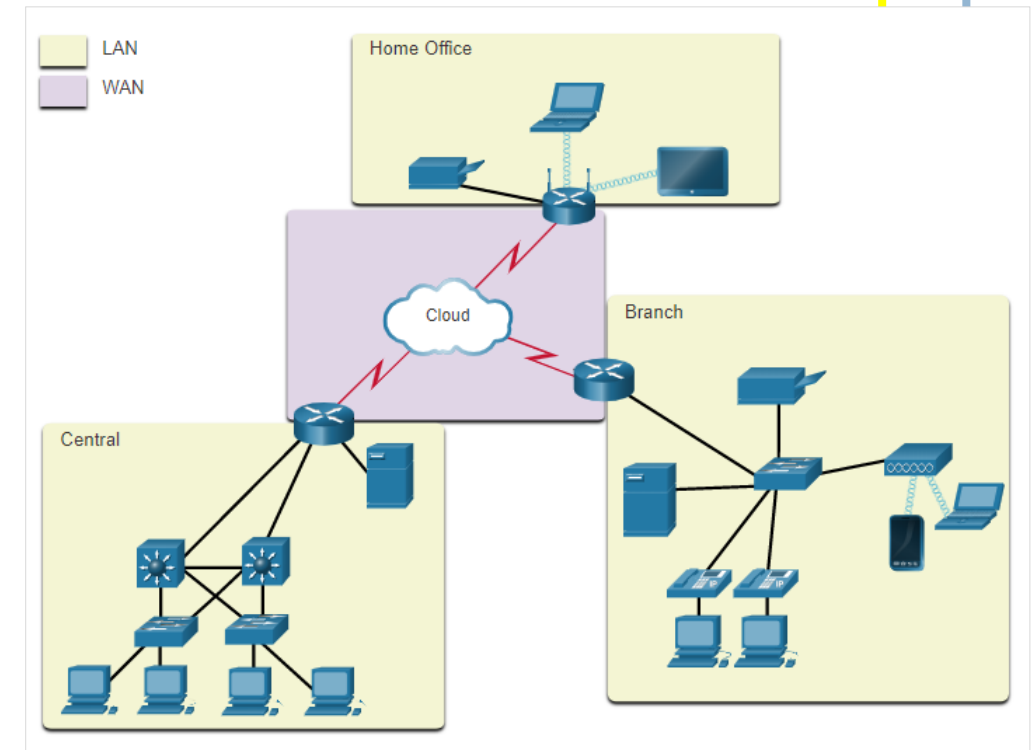
LAN і WAN₁

❑ Мережеві інфраструктури значно відрізняються з точки зору:

- розміру охопленої території
- кількості підключених користувачів
- кількості і виду доступних послуг
- зони відповідальності

❑ Два найпоширеніші типи мережевих інфраструктур:

- локальні мережі (LAN)
- глобальні мережі (WAN)

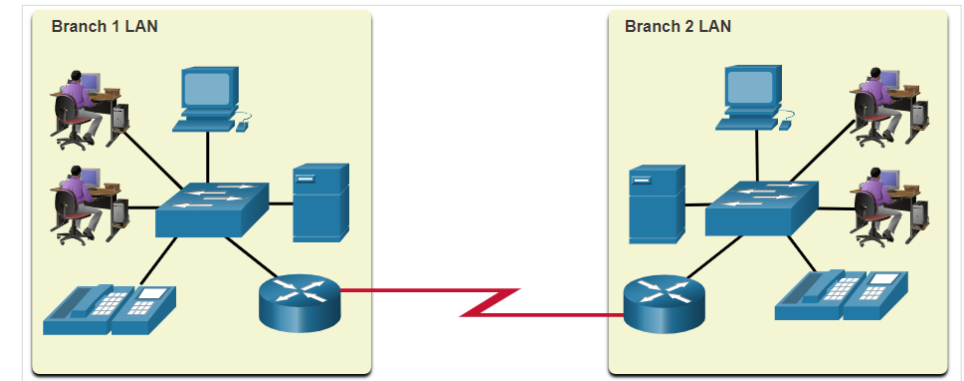
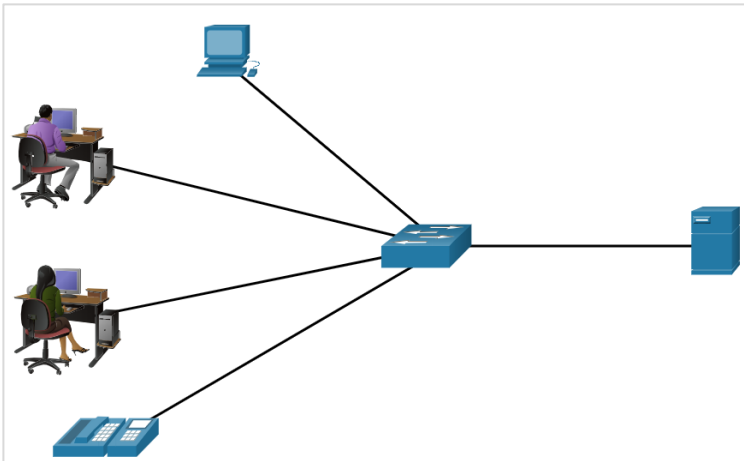


Локальні мережі, підключені до WAN



LAN і WAN₂

□ Локальна мережа – це мережева інфраструктура, яка охоплює невелику географічну область.

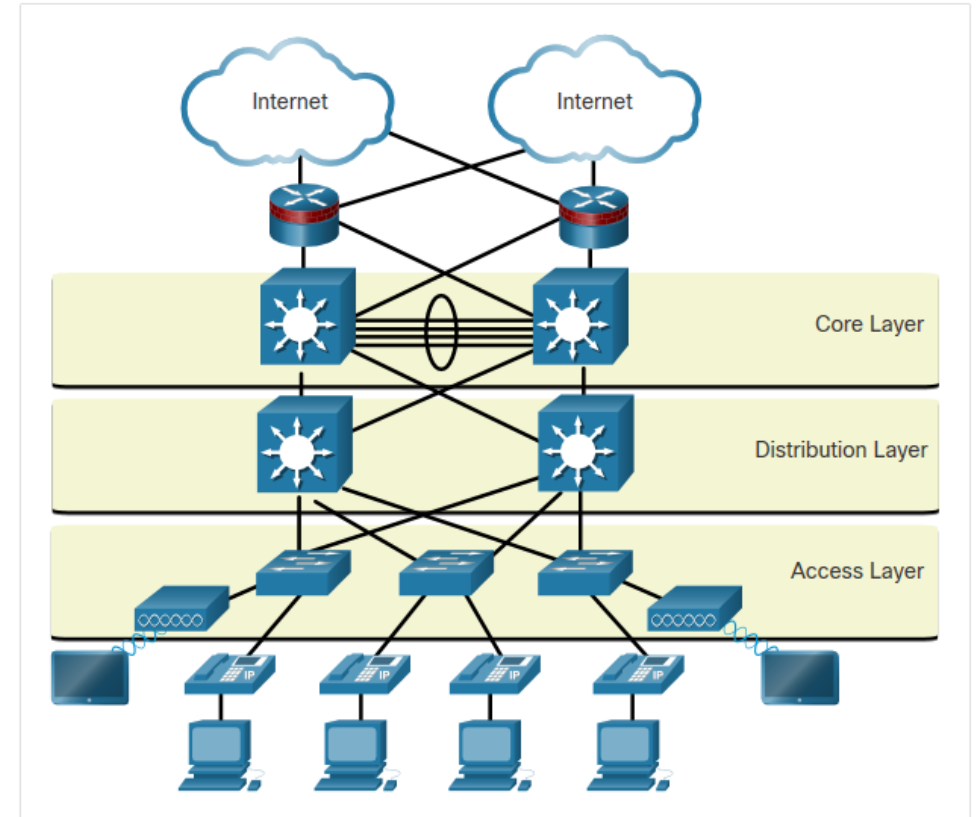


LAN	WAN
З'єднує кінцеві пристрої в обмеженій зоні.	З'єднує локальні мережі в широких географічних зонах.
Керується окремою організацією або особою.	Зазвичай адмініструється кількома постачальниками послуг.
Забезпечує високошвидкісну смугу пропускання для внутрішніх кінцевих пристроїв і проміжних пристроїв.	Зазвичай забезпечує повільніші з'єднання між локальними мережами.



Трирівнева модель проектування мережі₁

- ❑ Кампусна дротова локальна мережа використовує ієрархічну модель для поділу топології мережі на модульні групи або рівні.
- ❑ Ієрархічна структура локальної мережі включає три рівні:
 - **Доступу** – надає кінцевим точкам і користувачам прямий доступ до мережі.
 - **Розподілу** – агрегує рівні доступу та забезпечує підключення до служб.
 - **Ядро** - забезпечує підключення між рівнями розподілу для великих локальних середовищ.

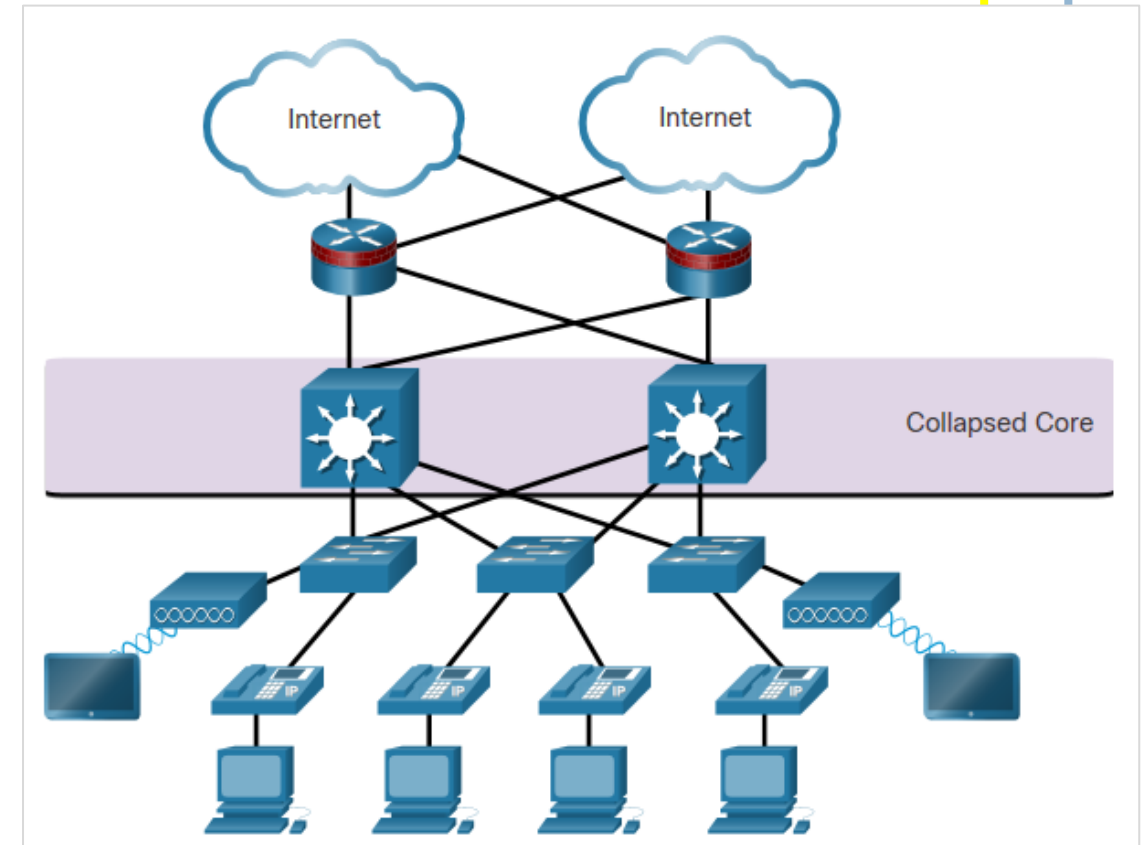


Ієрархічна модель проектування



Трирівнева модель проектування мережі₂

- ❑ Хоча ієрархічна модель має три рівні, деякі менші корпоративні мережі можуть реалізовувати дворівневу ієрархічну структуру.
- ❑ У цій дворівневій ієрархічній структурі рівні ядра і розподілу згортаються в один, таким чином зменшуючи вартість і складність.



Згорнуте ядро



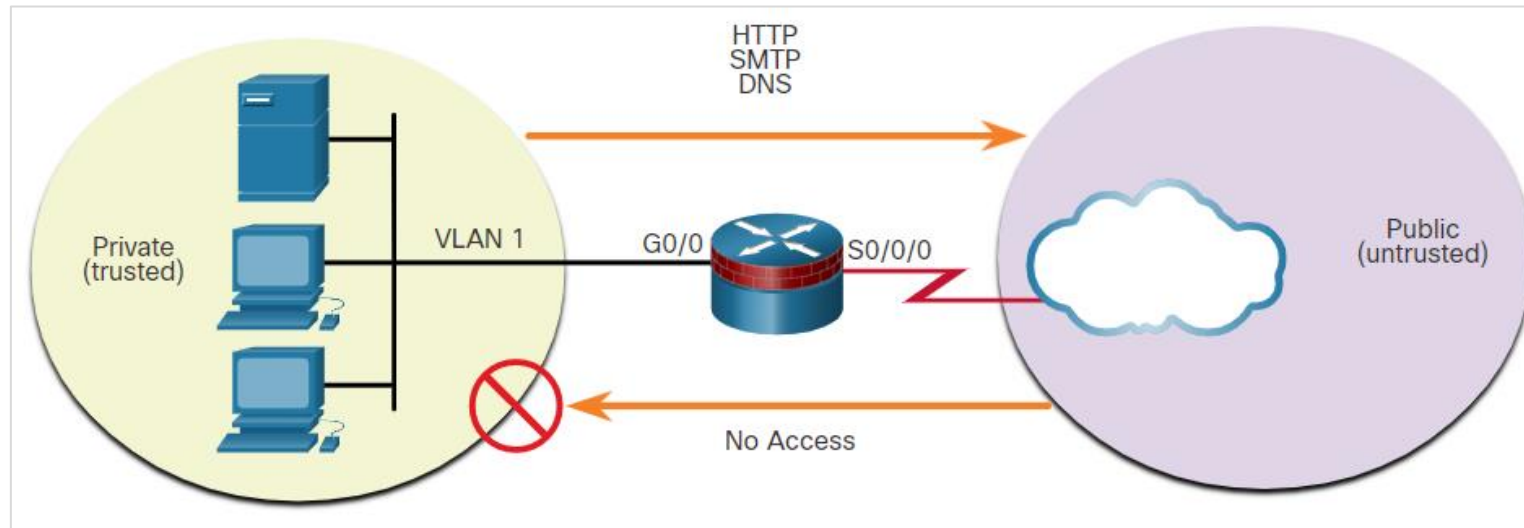
Загальні архітектури безпеки₁

Дизайн брандмауера в першу чергу стосується інтерфейсів пристроїв, які дозволяють або забороняють трафік на основі джерела, призначення та типу трафіку.

Три дизайни брандмауера:

☐ Громадський і приватний

- Загальнодоступна мережа (або зовнішня мережа) є ненадійною, а приватна мережа (або внутрішня мережа) є надійною.

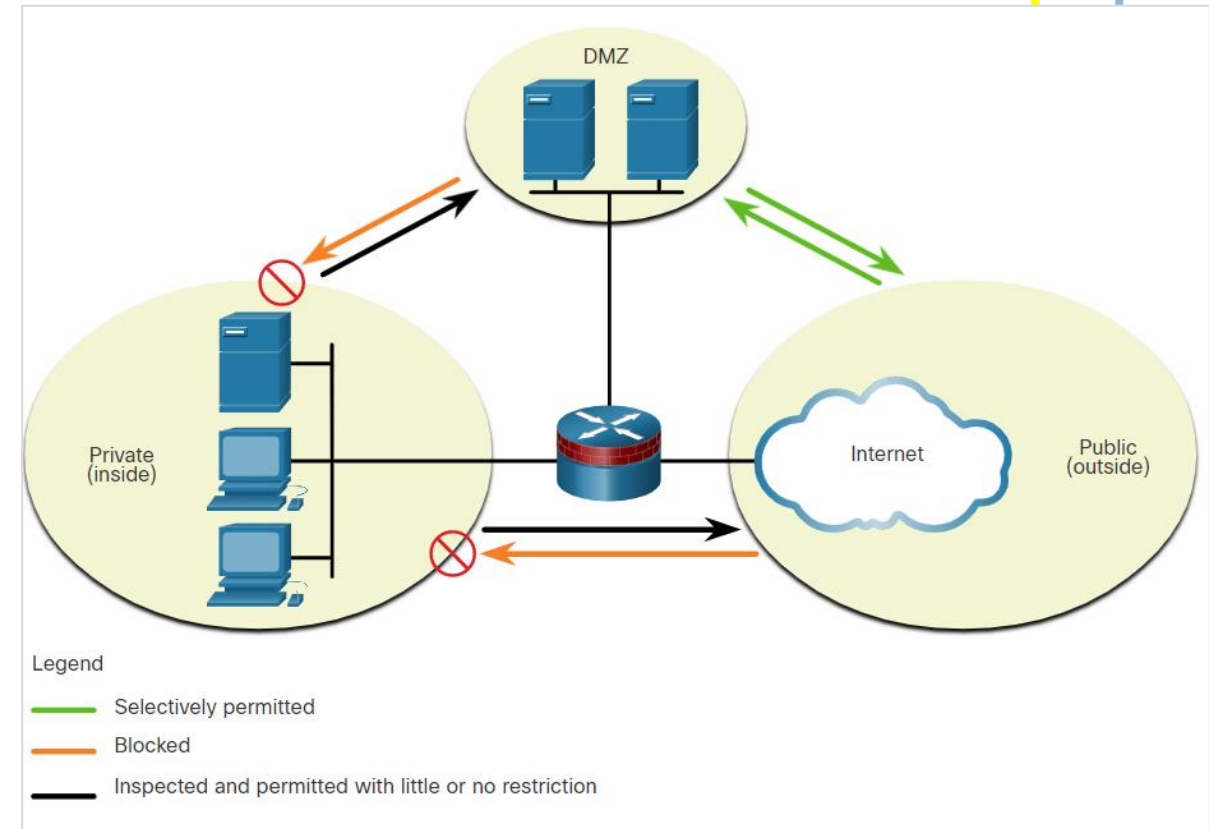




Загальні архітектури безпеки₂

□ Демілітаризована зона (DMZ)

- Конструкція брандмауера, де зазвичай є:
 - внутрішній інтерфейс, підключений до приватної мережі
 - зовнішній інтерфейс, підключений до загальнодоступної мережі
 - інтерфейс DMZ

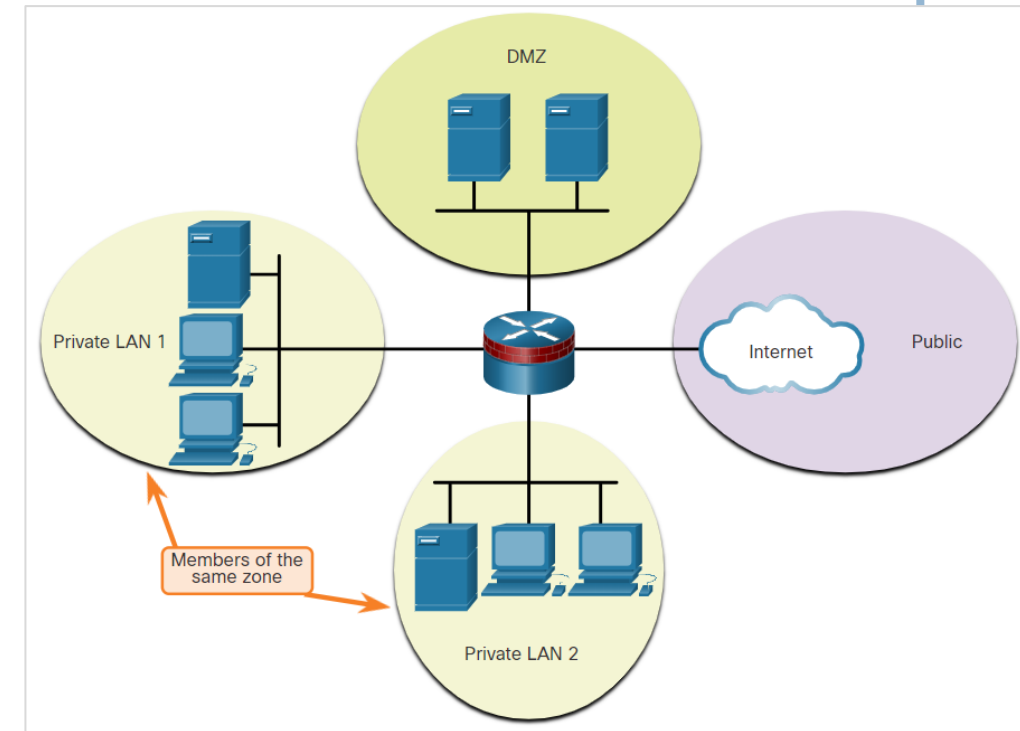




Загальні архітектури безпеки₃

❑ Брандмауери з зональною політикою (ZPF)

- ZPF використовують концепцію зон, щоб забезпечити додаткову гнучкість.
- Зона — це група з одного або кількох інтерфейсів, які мають схожі функції чи можливості.
- Зони допомагають указати, де слід застосовувати правило чи політику брандмауера Cisco IOS.





Пристрої безпеки

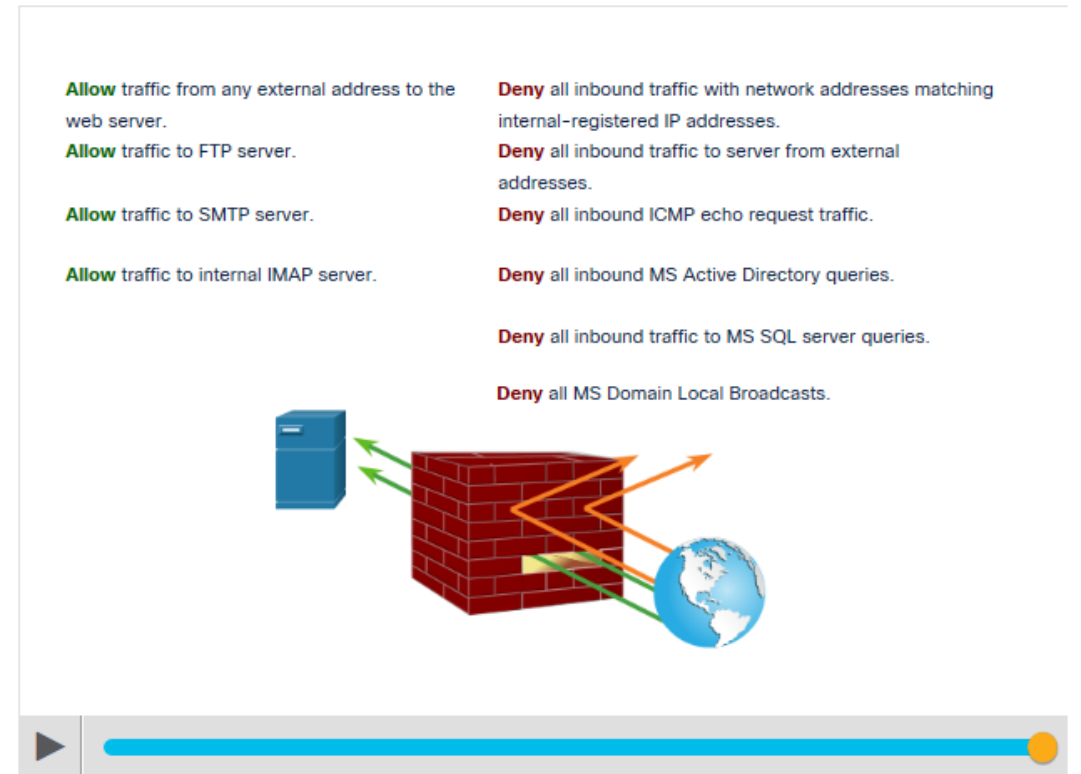


Брандмауери₁

Брандмауер — це система або група систем, яка забезпечує дотримання політики контролю доступу між мережами.

Загальні властивості брандмауера:

- ☐ Стійкість до мережевих атак
- ☐ Єдина транзитна точка між внутрішніми корпоративними мережами та зовнішніми мережами, оскільки весь трафік проходить через брандмауер
- ☐ Забезпечує виконання політики контролю доступу





Брандмауери₂

Нижче наведено переваги та обмеження брандмауерів.

Переваги брандмауера	Обмеження брандмауера
Запобігає доступу недовірених користувачів до конфіденційних хостів, ресурсів і програм.	Неправильно налаштований брандмауер може мати серйозні наслідки для мережі, наприклад стати єдиною точкою збою.
Дезінфікує потік трафіку, що запобігає використанню недоліків протоколу.	Дані з багатьох програм неможливо безпечно передати через брандмауери.
Блокує шкідливі дані з серверів і клієнтів.	Користувачі можуть завчасно шукати шляхи обходу брандмауера, щоб отримати заблокований матеріал, що наражає мережу на потенційну атаку.
Зменшує складність керування безпекою.	Продуктивність мережі може сповільнитися.
	Неавторизований трафік можна тунелювати або приховувати як законний трафік через брандмауер.

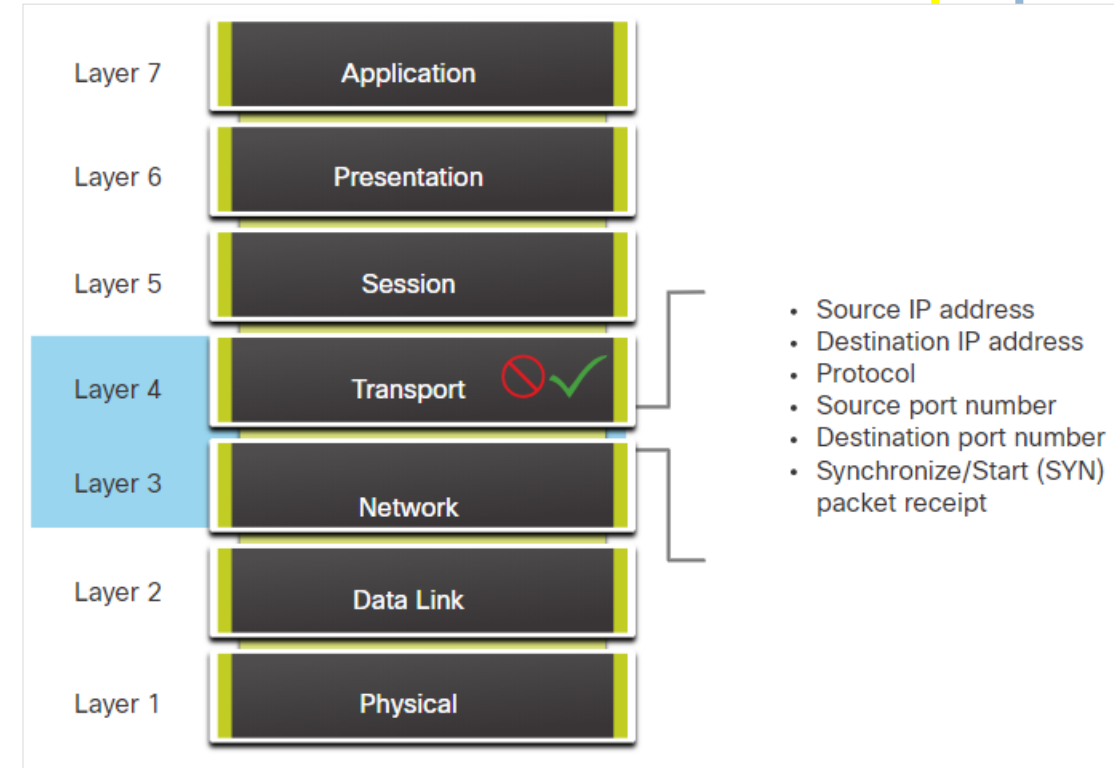


Типи брендмауерів₁

Різні типи брендмауерів:

□ Брендмауер із фільтрацією пакетів (без стану)

- брендмауери фільтрації пакетів є частиною брендмауера маршрутизатора, який дозволяє або забороняє трафік на основі інформації рівнів 3 і 4
- це брендмауери без стану, які використовують простий пошук у таблиці політик і який фільтрує трафік на основі певних критеріїв

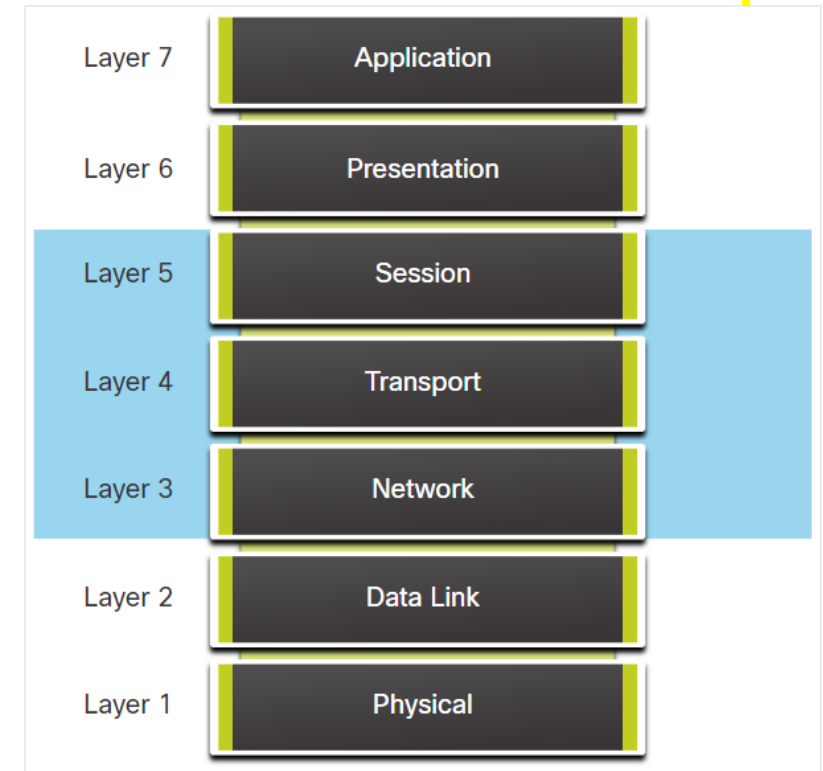




Типи брандмауерів₂

□ Брандмауери з контролем стану

- брандмауери з підтримкою стану є найбільш універсальними та найпоширенішими технологіями брандмауерів, які використовуються
- ці брандмауери забезпечують фільтрацію пакетів за допомогою інформації про з'єднання, яка зберігається в таблиці стану

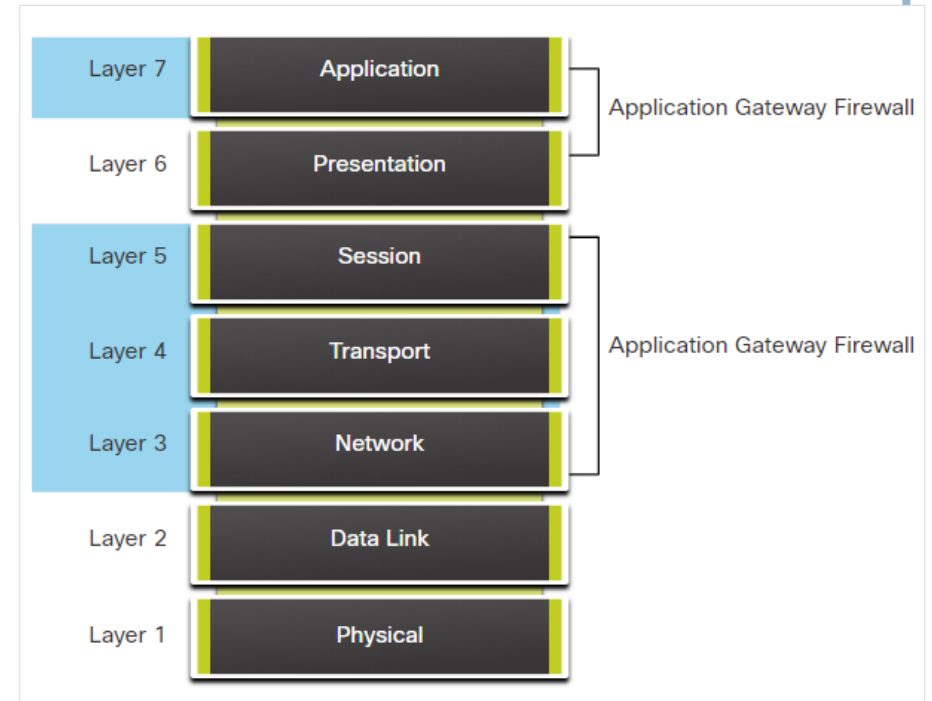




Типи брандмауерів₃

□ Брандмауер шлюзу програм (брандмауер проксі)

- брандмауер шлюзу програм фільтрує інформацію на рівнях 3, 4, 5 і 7 еталонної моделі OSI
- більша частина контролю та фільтрації брандмауера виконується програмним забезпеченням





Типи брандмауерів₄

□ Брандмауери нового покоління (NGFW)

- NGFW виходить за межі брандмауерів із збереженням стану, надаючи:
 - вбудовану систему запобігання вторгненням
 - обізнаність і контроль програм з метою визначення та блокування ризикованих програм
 - оновлення шляхів з метою включення майбутніх каналів інформації
 - методи вирішення нових загроз безпеці





Типи брендмауерів₅

□ Інші методи впровадження брендмауерів включають:

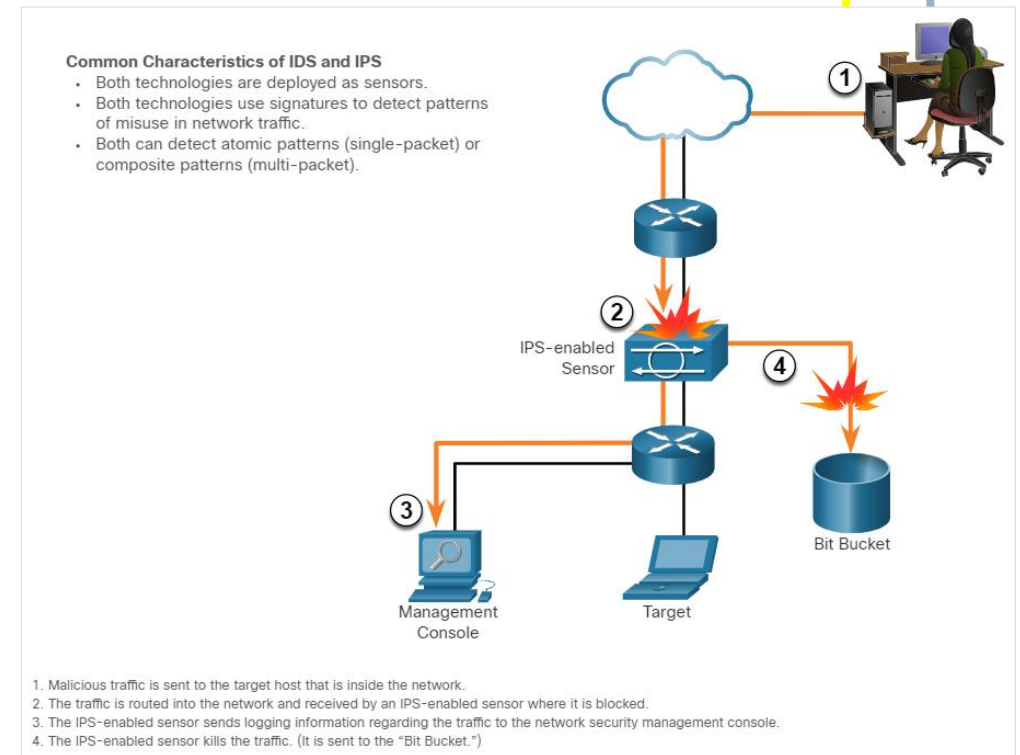
- Брендмауер на основі хоста (серверний і персональний) — комп'ютер або сервер із запущеним на ньому програмним забезпеченням брендмауера.
- Прозорий брендмауер - фільтрує IP-трафік між парою мостових інтерфейсів.
- Гібридний брендмауер - комбінація різних типів брендмауера.



Пристрої запобігання та виявлення вторгнень

151

- ❑ Зміна парадигми мережевої архітектури необхідна для захисту від атак, що швидко розвиваються. Такий підхід має включати економічно ефективні та профілактичні системи, такі як:
 - системи виявлення вторгнень (IDS)
 - системи запобігання вторгненням (IPS)
- ❑ Архітектура мережі інтегрує ці рішення в точки входу та виходу мережі.
- ❑ На слайді показано, як пристрій IPS обробляє шкідливий трафік.





Переваги та недоліки IDS та IPS

❑ У таблиці наведено переваги та недоліки IDS та IPS:

Рішення	Переваги	Недоліки
IDS	- Немає впливу на мережу (затримка, jitter) - Немає впливу на мережу, якщо є збій сенсора - Немає впливу на мережу, якщо є перевантаження сенсора	- Дія відповіді не може зупинити тригерні пакети - Для відповідних дій потрібна правильна настройка - Більш вразливий до методів обходу безпеки мережі
IPS	- Зупиняє тригерні пакети - Може використовувати методи нормалізації потоку	- Проблеми з сенсором можуть вплинути на мережевий трафік - Перевантаження сенсора впливає на мережу - Певний вплив на мережу (затримка, jitter)

Розгортання:

- Технології IPS і IDS можуть доповнювати одна одну.
- Рішення про те, яку реалізацію використовувати, ґрунтується на цілях безпеки організації, які зазначено в її політиці безпеки мережі.



Типи IPS₁

Існує два основних типи IPS:

- IPS на основі хоста
- мережевий IPS

❑ IPS на основі хоста (HIPS)

HIPS — це програмне забезпечення, встановлене на хості для моніторингу й аналізу підозрілої активності

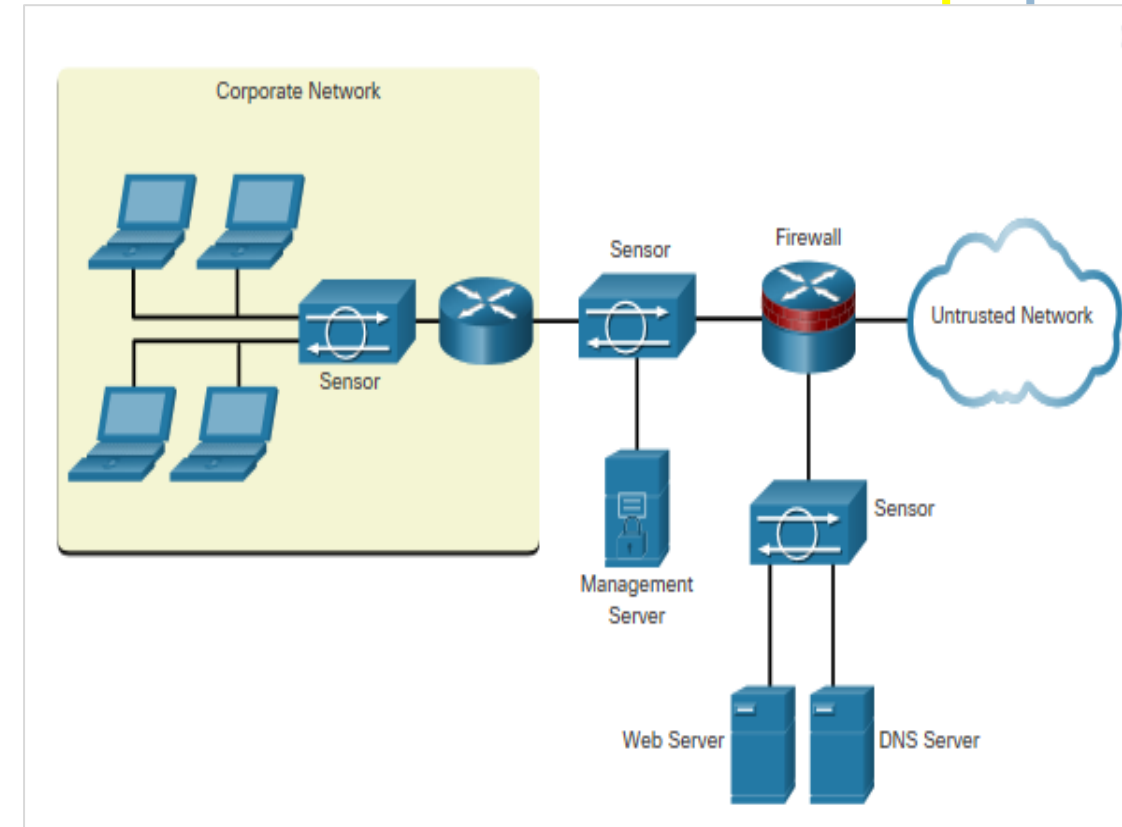
Переваги	Недоліки
• Забезпечує захист, характерний для операційної системи хоста • Забезпечує захист на рівні операційної системи та програм • Захищає хост після розшифрування повідомлення	• Залежить від операційної системи • Має бути встановлено на всіх хостах



Типи IPS₂

☐ Мережевий IPS

- Мережевий IPS реалізується за допомогою виділеного або невиділеного пристрою IPS.
- Рішення IDS/IPS на основі хоста інтегровані з мережевою реалізацією IPS для забезпечення надійної архітектури безпеки.
- Сенсори виявляють зловмисну та несанкціоновану активність у режимі реального часу та можуть вжити необхідних заходів.





Спеціалізовані засоби безпеки

□ Кілька прикладів спеціалізованих засобів безпеки:

Розширений захист від шкідливих програм Cisco (AMP)	Cisco Web Security Appliance (WSA)	Cisco Email Security Appliance (ESA)
Удосконалене рішення для аналізу шкідливих програм і захисту корпоративного рівня	Захищений веб-шлюз, який поєднує провідні засоби захисту, щоб допомогти організаціям вирішити зростаючі проблеми безпеки та контролю веб-трафіку	ESA/ Cisco Cloud Email Security допомагає пом'якшити наслідки загрози від електронної пошти, а ESA захищає критично важливі системи електронної пошти
Забезпечує комплексний захист організацій від шкідливих програм до, під час і після атаки	Захищає мережу, автоматично блокуючи ризиковані сайти та перевіряючи невідомі сайти, перш ніж дозволити користувачам отримати до них доступ	Постійно оновлюється за допомогою каналів у реальному часі від Cisco Talos, який виявляє та корелює загрози за допомогою всесвітньої системи моніторингу бази даних
		Особливості: глобальна розвідка про загрози, блокування спаму, розширений захист від шкідливих програм, контроль вихідних повідомлень

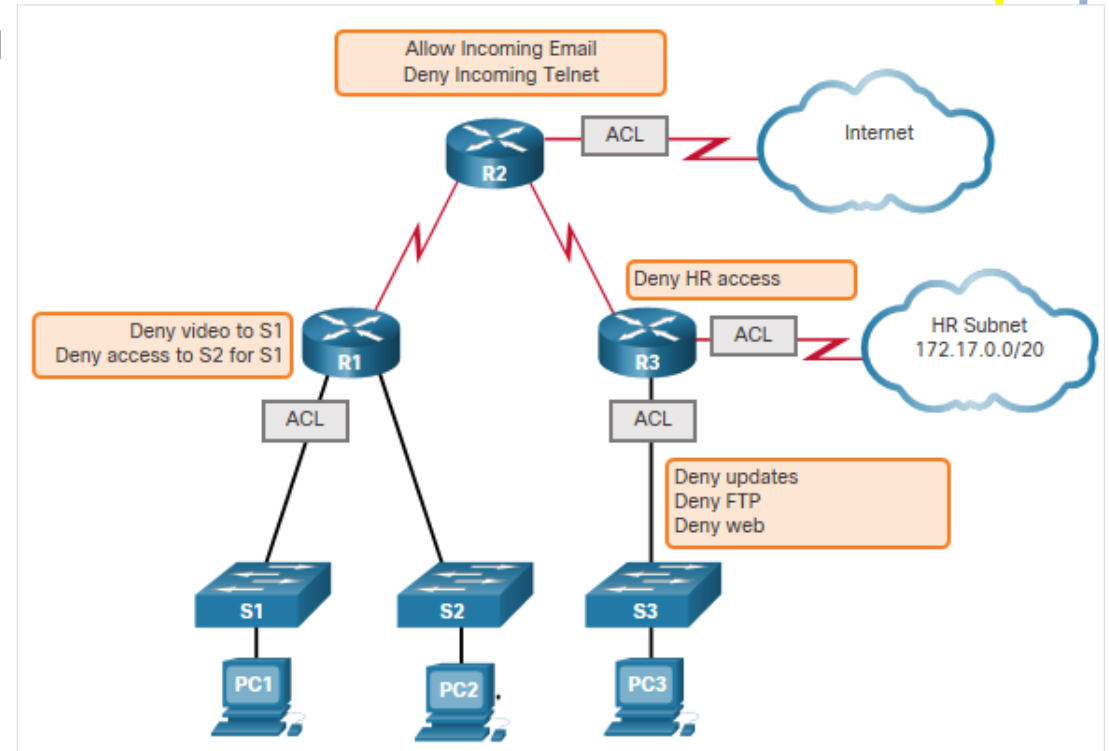


Послуги безпеки



Контроль трафіку за допомогою ACL

- ❑ Список керування доступом (ACL) — це серія команд, які контролюють, чи пристрій пересилає або скидає пакети на основі інформації, знайденої в заголовку пакета.
- ❑ Після налаштування списки керування доступом виконують такі завдання:
 - обмежують мережевий трафік, щоб підвищити продуктивність мережі
 - забезпечують контроль руху транспорту
 - забезпечують базовий рівень безпеки для доступу до мережі
 - фільтрують трафік за типом трафіку
 - екранують хости щодо заборони або дозволу доступу до мережевих служб



Приклад топології зі списками ACL, застосованими до маршрутизаторів R1, R2 і R3.



ACL: важливі функції

Є два типи ACL Cisco IPv4:

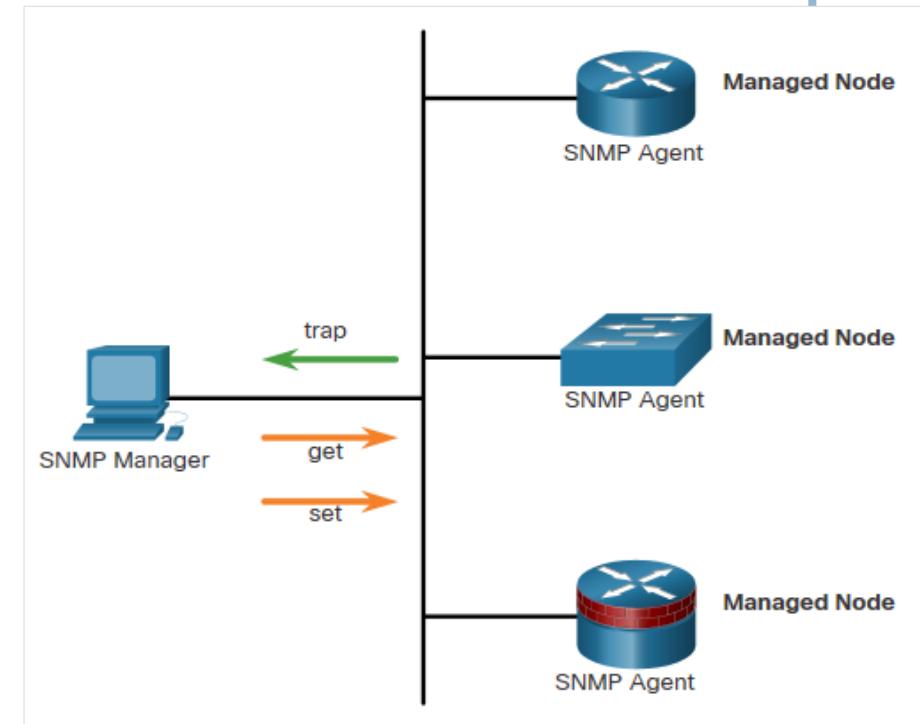
- ☐ **Стандартний ACL** – використовується для дозволу або заборони трафіку лише з вихідних адрес IPv4.
- ☐ **Extended ACL** – фільтрує пакети IPv4 на основі кількох атрибутів, які включають:
 - Тип протоколу
 - Адреса джерела IPv4
 - IPv4-адреса призначення
 - Вихідні порти TCP або UDP
 - Порти призначення TCP або UDP
 - Додаткова інформація про тип протоколу для більш точного контролю
- ☐ Стандартні та розширені списки керування доступом можна створити за допомогою номера або імені для ідентифікації списку керування доступом та його списку операторів.



SNMP

159

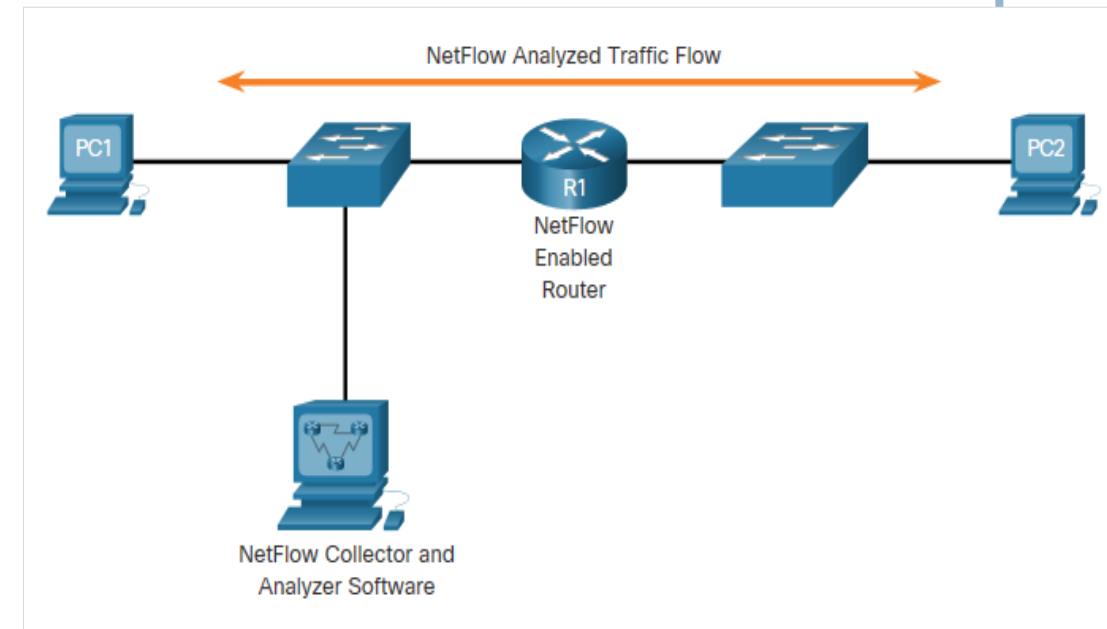
- ❑ Простий протокол керування мережею (SNMP) — це протокол прикладного рівня, який забезпечує формат повідомлення для зв'язку між менеджерами та агентами.
- ❑ Дозволяє мережевим адміністраторам виконувати такі дії:
 - Керувати кінцевими пристроями, такими як сервери, робочі станції, маршрутизатори, комутатори та пристрої безпеки в IP-мережі.
 - Відстежувати та керувати продуктивністю мережі.
 - Знаходити і вирішувати проблеми з мережею.
 - Планувати розвиток мережі.
- ❑ Система SNMP складається з двох елементів:
 - **Менеджер SNMP:** запускає програмне забезпечення для керування SNMP.
 - **Агенти SNMP:** вузли, які контролюються та керуються.





NetFlow

- ❑ NetFlow — це технологія Cisco IOS, яка забезпечує статистику пакетів, що проходять через маршрутизатор Cisco або багаторівневий комутатор.
- ❑ NetFlow надає дані для:
 - моніторингу мережі та безпеки,
 - мережевого планування,
 - аналізу трафіку, включаючи виявлення вузьких місць мережі,
 - обліку IP для виставлення рахунків.
- ❑ NetFlow може контролювати підключення програми, відстежувати кількість байтів і пакетів для окремого потоку програми.
- ❑ Потім він надсилає статистику на зовнішній сервер, який називається збирачем NetFlow.

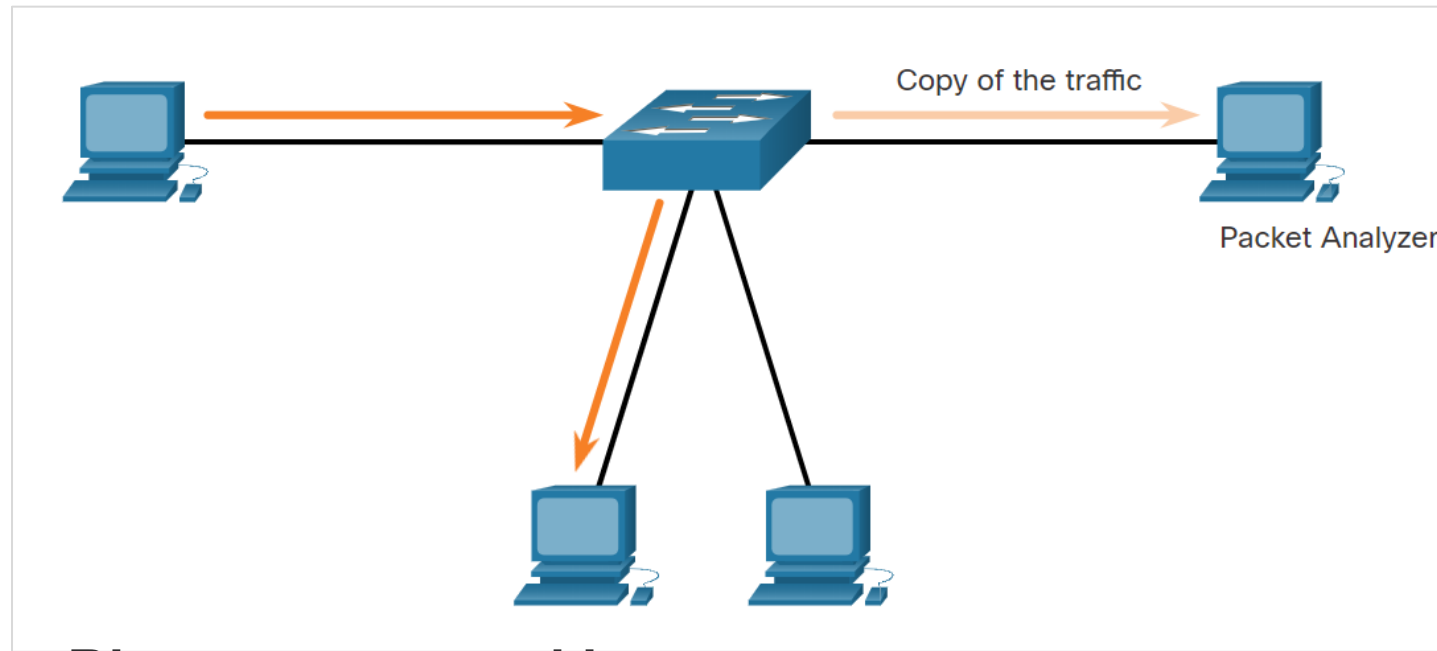


ПК 1 підключається до ПК 2 за допомогою HTTPS



Віддзеркалення портів

Віддзеркалення портів — це функція, яка дозволяє комутатору створювати дублікат трафіку, що проходить через комутатор, а потім надсилати його через порт із підключеним мережевим монітором.



Відстеження трафіку за допомогою комутатора



Сервери Syslog

- ❑ Найпоширенішим методом доступу до системних повідомлень є використання протоколу під назвою syslog.
- ❑ Протокол Syslog дозволяє мережевим пристроям надсилати свої системні повідомлення через мережу на сервери syslog.
- ❑ Він надає три основні функції:
 - Можливість збору інформації журналу для моніторингу та усунення несправностей
 - Можливість вибрати тип записаної інформації журналу
 - Можливість вказувати призначення захоплених повідомлень системного журналу

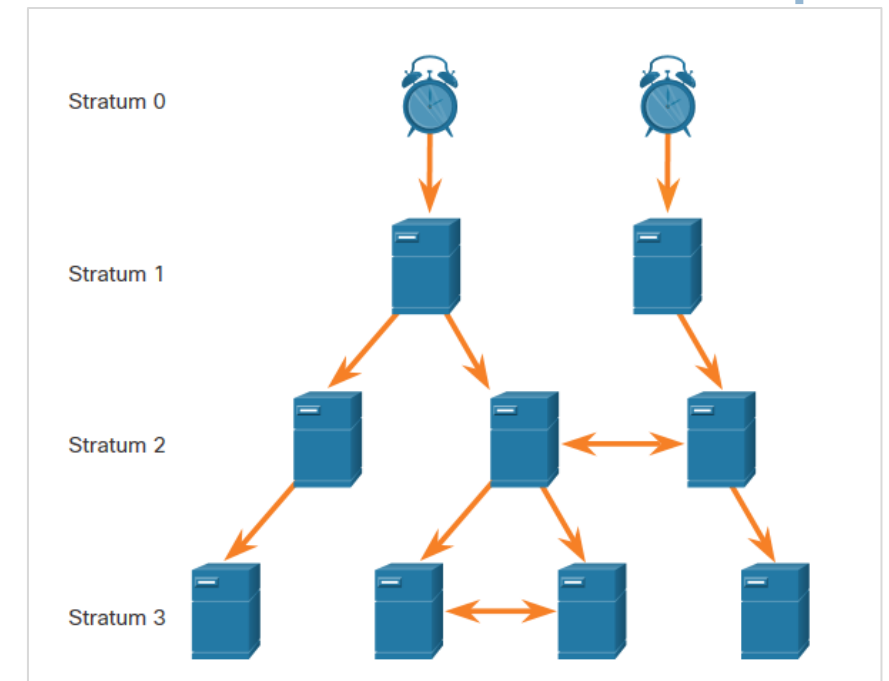




NTP

163

- ❑ Важливо синхронізувати час на всіх пристроях у мережі. Параметри дати й часу на мережевому пристрої можна встановити одним із двох способів:
 - Ручне налаштування дати та часу
 - Налаштування мережевого протоколу часу (NTP)
- ❑ Мережі NTP використовують ієрархічну систему джерел часу, де кожний рівень у цій системі називається стратумом. NTP-сервери розташовані на трьох основних рівнях-стратумах:
 - **Рівень 0:** NTP-мережа отримує час з авторитетних джерел часу.
 - **Рівень 1:** пристрої безпосередньо підключені до авторитетних джерел часу.
 - **Рівень 2 і нижчі рівні:** пристрої рівня 2, такі як NTP-клієнти, синхронізують свій час за допомогою пакетів NTP із серверами рівня 1.



Рівні стратумів NTP



Сервери AAA₁

□ У наведеній нижче таблиці перераховано три незалежні функції безпеки, які забезпечуються архітектурною структурою AAA.

Функції	Опис
Аутентифікація	• Користувачі та адміністратори повинні довести, що вони ті, за кого себе видають. • Автентифікація може бути встановлена за допомогою комбінацій імені користувача та пароля, питань виклику та відповіді, карток жетонів та інших методів. • Аутентифікація AAA забезпечує централізований спосіб контролю доступу до мережі.
Авторизація	• Після аутентифікації користувача служби авторизації визначають, до яких ресурсів користувач може отримати доступ і які операції йому дозволено виконувати. • Приклад: «Користувач «студент» може отримати доступ до хост-сервера XYZ лише за допомогою SSH».
Облік	• Облік фіксує те, що робить користувач, у тому числі доступ до нього, кількість часу доступу до ресурсу та будь-які внесені зміни. • Облік відстежує, як використовуються ресурси мережі. • Приклад: «Користувач «студент» отримав доступ до хост-сервера XYZ за допомогою SSH протягом 15 хвилин».



Сервери AAA₂

❑ У наведеній нижче таблиці вказано різницю між протоколами Terminal Access Controller Access-Control System Plus (TACACS+) і Remote Authentication Dial-In User Service (RADIUS).

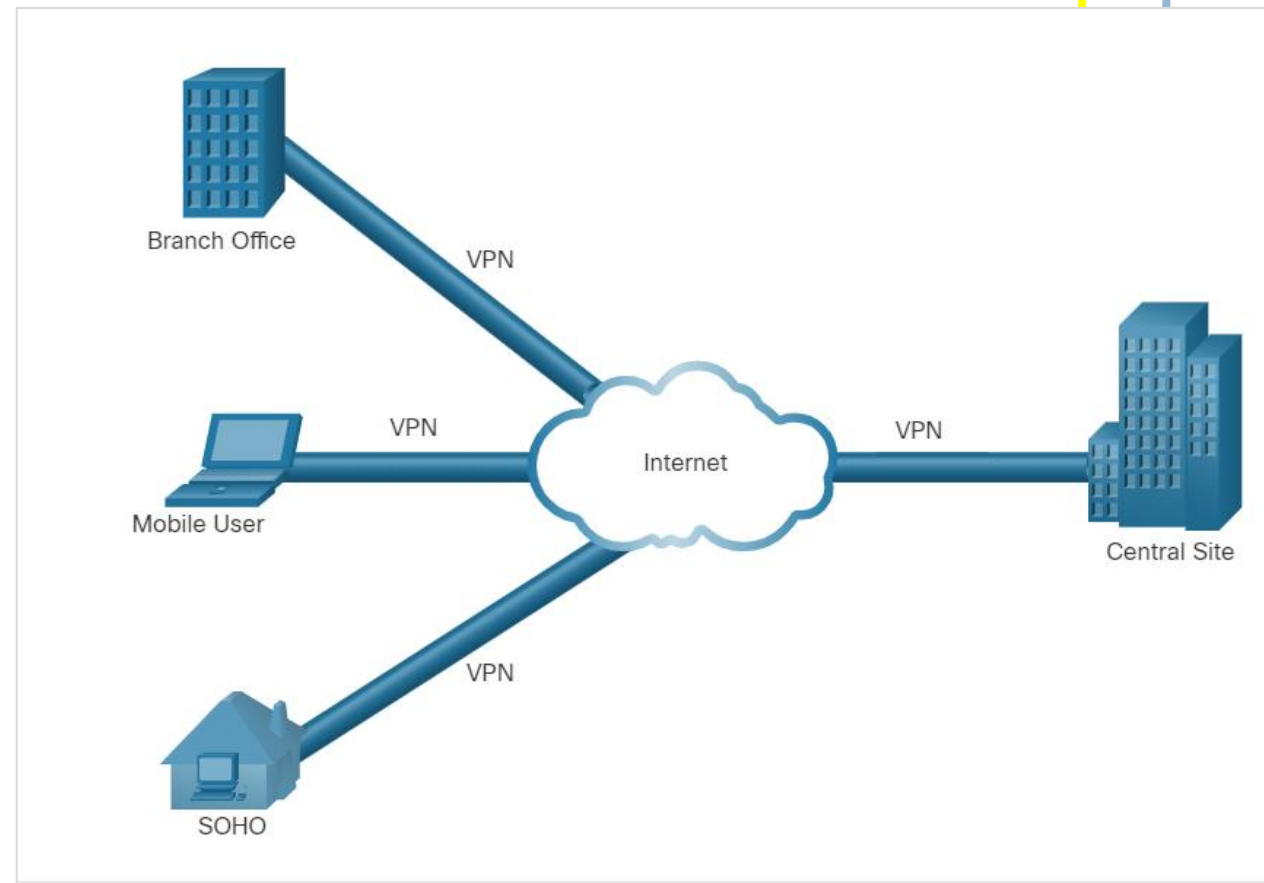
	TACACS+	Radius
❑ Функціональність	Розділяє AAA відповідно до архітектури AAA	Поєднує автентифікацію та авторизацію, але розділяє облік
Стандартний	В основному підтримується Cisco	Стандарт Open/RFC
Транспорт	TCP	UDP
Протокол CHAP	Двонаправлений виклик і відповідь, що використовуються в протоколі автентифікації виклику рукостискання (CHAP)	Односпрямований виклик і відповідь від сервера безпеки RADIUS до клієнта RADIUS
Конфіденційність	Весь пакет зашифрований	Пароль зашифрований
Налаштування	Забезпечує авторизацію команд маршрутизатора для кожного користувача чи групи	Немає можливості авторизувати команди маршрутизатора для кожного користувача чи групи
Облік	Обмежений	Екстенсивний



VPN

166

- ❑ VPN — це приватна мережа, яка створюється через загальнодоступну мережу (зазвичай Інтернет).
- ❑ VPN використовує віртуальні з'єднання, що направляються через Інтернет від організації до віддаленого сайту.
- ❑ VPN — це комунікаційне середовище, доступ до якого суворо контролюється, щоб дозволити однорангові з'єднання в межах визначеної спільноти інтересів.
- ❑ Конфіденційність досягається шляхом шифрування трафіку в межах VPN.
- ❑ Коротше кажучи, VPN з'єднує дві кінцеві точки через загальнодоступну мережу, формуючи логічне з'єднання, яке можна встановити на рівні 2 або 3.



Віртуальна приватна мережа

Донецький національний технічний університет



Тема 2. Моделі порушника та загроз для інформації в ІТС.

Лекція 3. Складання моделі порушника безпеки інформації в ІТС.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

168

- ☐ Безпека мережі та вектори атак
- ☐ Загроза, вразливість, ризик, суб'єкт загроз
- ☐ Класифікація порушників
- ☐ Модель порушника



Безпека мережі та вектори атак



Мережі є цілями

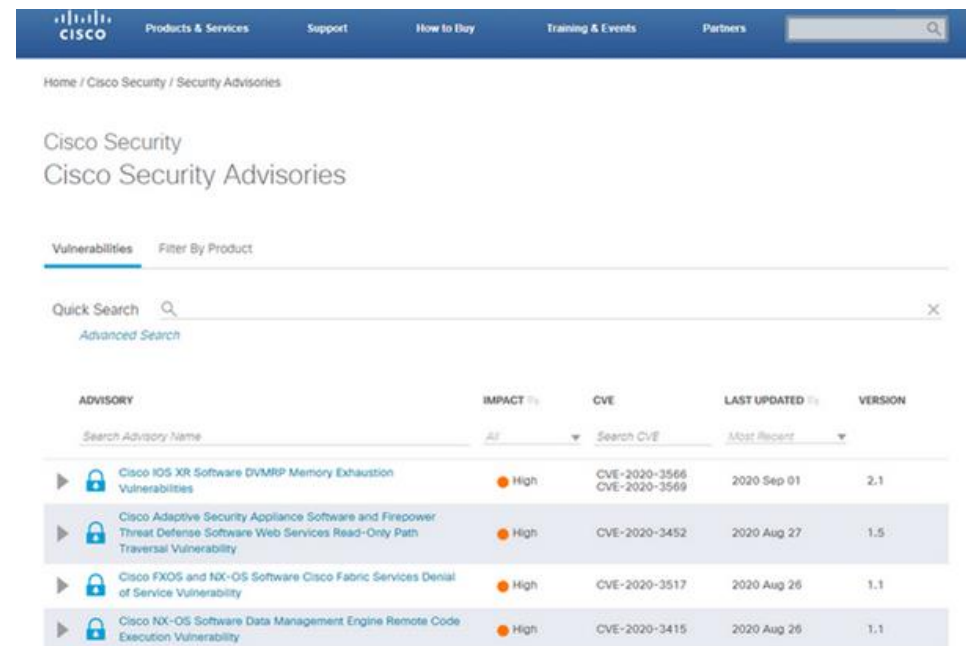
- ☐ Мережі регулярно піддаються атакам.
- ☐ Kaspersky підтримує інтерактивне відображення поточних мережеских атак Cyberthreat Real-Time Map. Дані про атаку надходять із продуктів мережевої безпеки Kaspersky, які розгорнуті по всьому світу.





Необхідність безпеки мережі

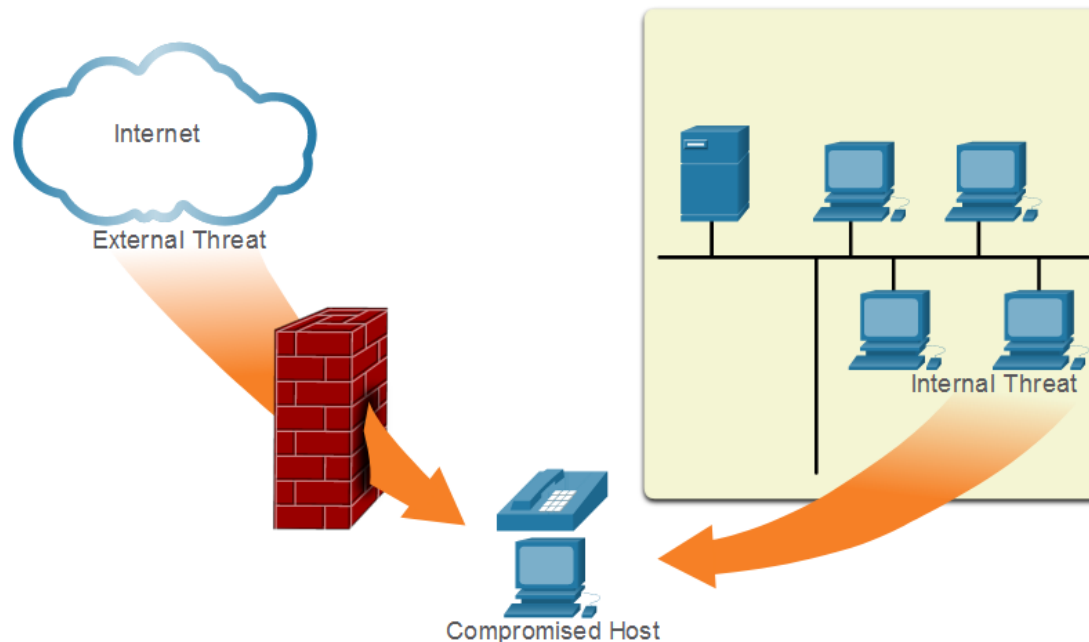
- ❑ Порушення безпеки мережі можуть обвалити електронну комерцію, спричинити втрату бізнес-даних, загрожувати конфіденційності людей і поставити під загрозу цілісність інформації.
- ❑ Веб-сайт Cisco Talos Intelligence Group надає комплексну інформацію про безпеку та аналіз загроз. Група реагування на інциденти безпеки продуктів Cisco (PSIRT) відповідає за розслідування й усунення потенційних уразливостей у продуктах Cisco.





Вектори мережевих атак

- ❑ Вектор атаки – це шлях, яким порушник може отримати доступ до сервера, хосту чи мережі. Вектори атак походять з внутрішньої чи зовнішньої корпоративної мережі. Зловмисники можуть націлитися на мережу через Інтернет з метою порушення роботи мережі та створити атаку на відмову в обслуговуванні (DoS).





Втрата даних

Термін	Визначення
Електронна пошта/Соціальні мережі	Найпоширенішим вектором втрати даних є програмне забезпечення для обміну миттєвими повідомленнями та сайти соціальних мереж. Наприклад, перехоплені електронні листи або миттєві повідомлення можуть бути захоплені та розкрита конфіденційна інформація.
Незашифровані пристрої	Викрадений корпоративний ноутбук зазвичай містить конфіденційні організаційні дані. Якщо дані не зберігаються за допомогою алгоритму шифрування, злодій може отримати цінні конфіденційні дані.
Хмарні пристрої зберігання	Збереження даних у хмарі має багато потенційних переваг. Однак конфіденційні дані можуть бути втрачені, якщо доступ до хмари буде скомпрометовано через слабкі налаштування безпеки.
Знімний носій	Один із ризиків полягає в тому, що працівник може здійснити несанкціоноване перенесення даних на USB-накопичувач. Інший ризик полягає в тому, що USB-накопичувач із цінними корпоративними даними може бути втрачено.
Роздрукована копія	Від конфіденційних даних слід ретельно позбуватися. Наприклад, конфіденційні дані слід видаляти, коли вони більше не потрібні. Інакше злодій може отримати викинуті звіти та отримати цінну інформацію.
Неналежний контроль доступу	Паролі – це перша лінія захисту. Викрадені або зламані слабкі паролі можуть надати зловмиснику легкий доступ до даних.



Захоплені люди

- ❑ Хакери можуть створювати відкриті «шахрайські» бездротові точки доступу, видаючи себе за справжню бездротову мережу.
- ❑ Шахрайські бездротові точки доступу також відомі як точки доступу «злих близнюків».





Захоплені компанії

- ❑ Співробітників організації часто спокушають відкрити посилання, які встановлюють програми-вимагачі на комп'ютери співробітників.
- ❑ Це програмне забезпечення-вимагач після встановлення починає процес збору та шифрування корпоративних даних.
- ❑ Метою зловмисників є фінансова вигода, оскільки вони утримують дані компанії з метою отримання викупу.





Таргетовані країни

- ❑ Деякі з сучасних зловмисних програм є настільки складними та дорогими для створення, що експерти з безпеки вважають, що лише держава чи група країн може мати вплив і фінансування для їх створення.
- ❑ Таке зловмисне програмне забезпечення може бути спрямоване для атаки на критичну інфраструктуру країни, як-от систему водопостачання або електромережі.
- ❑ Одною з таких шкідливих програм був хробак Stuxnet, який заразив USB-накопичувачі та проник в операційні системи Windows. Потім він був спрямований на програмне забезпечення Step 7, розроблене Siemens для програмування логічних контролерів (PLC).





Загроза, вразливість, ризик, суб'єкт загроз



Загроза, вразливість і ризик₁

- ❑ Зловмисники хочуть отримати доступ до наших активів, таких як дані та інша інтелектуальна власність





Загроза, вразливість і ризик₂

ТЕРМІН	ПОЯСНЕННЯ
Загроза	Потенційна небезпека для такого активу, як дані або сама мережа.
Вразливість	Слабке місце в системі або її дизайні, яке може бути використано загрозою.
Поверхня атаки	Поверхня атаки — це загальна сума вразливостей у певній системі, доступних для зловмисника. Поверхня атаки описує різні точки, де зловмисник може проникнути в систему та де він може отримати дані з системи.
Експлойт	Механізм, який використовується для використання вразливості для компрометації активу. Експлойти можуть бути віддаленими або локальними. Віддалений експлойт — це той, який працює через мережу без попереднього доступу до цільової системи. У локальному експлойті зловмисник має певний тип доступу користувача або адміністратора до кінцевої системи. Це не обов'язково означає, що зловмисник має фізичний доступ до кінцевої системи.
Ризик	Ймовірність того, що певна загроза використає певну вразливість активу та призведе до небажаних наслідків.



Загроза, вразливість і ризик_з

□ Управління ризиками – це процес, який збалансовує операційні витрати на забезпечення захисних заходів з вигодами, досягнутими від захисту активу.

Стратегія управління ризиками	Пояснення
Прийняття ризику	Коли вартість варіантів управління ризиком перевищує вартість ризику, ризик приймається, і жодних дій не вживається.
Уникнення ризику	Це означає уникнення будь-якого ризику шляхом виключення діяльності, що призведе до втрати будь-яких переваг від діяльності.
Зниження ризику	Це найбільш часто використовувана стратегія зниження ризику. Ця стратегія вимагає ретельної оцінки вартості збитків, стратегії пом'якшення наслідків та вигод, отриманих від операції або діяльності, яка піддається ризику.
Передача ризику	Частина або весь ризик передається добровільній третій стороні, наприклад страховій компанії.



Загроза, вразливість і ризик₄

☐ Загальні умови безпеки мережі:

- Протидія – дії, вжиті для захисту активів шляхом пом'якшення загрози або зменшення ризику.
- Вплив – потенційна шкода організації, спричинена загрозою

☐ Локальний експлойт вимагає внутрішнього доступу до мережі, наприклад користувача з обліковим записом у мережі.

☐ Для використання вразливості цієї мережі не потрібен обліковий запис у мережі.



Хакер₁

□ «Хакер» — це загальний термін, який використовується для опису загрози. Хакер має різні значення:

- Розумний програміст, здатний розробляти нові програми та вносити зміни в код існуючих програм, щоб зробити їх ефективнішими.
- Мережевий фахівець, який використовує складні навички програмування з метою забезпечення невразливості мережі до атак.
- Особа, яка запускає програми для запобігання або пошкодження даних на серверах.

□ Типи хакерів:

- Хакери **White Hat**
- Хакери **Gray Hat**
- Хакери **Black Hat**



Хакер₂

183

❑ Хакери **White Hat**:

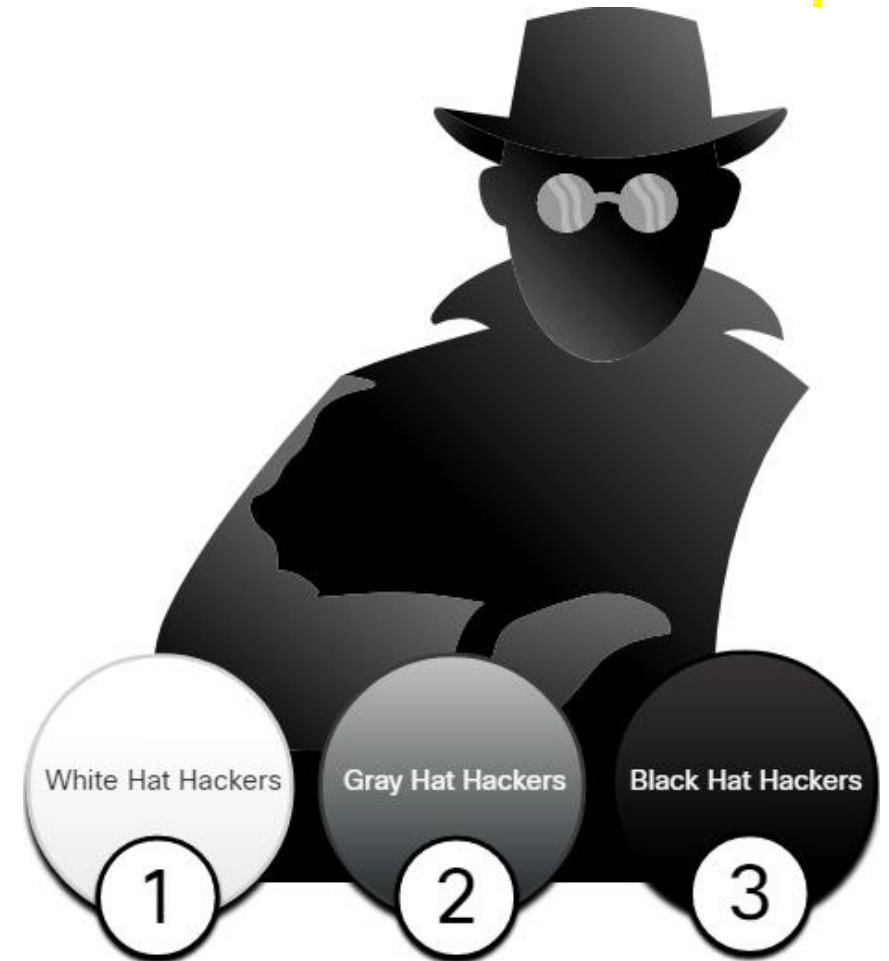
- Хакери «білого капелюха» — це етичні хакери, які використовують свої навички програмування в добрих, етичних і законних цілях.

❑ Хакери **Gray Hat**:

- Хакери сірого капелюха — це особи, які скоюють злочини та неетичні дії, але не заради особистої вигоди чи завдання шкоди.

❑ Хакери **Black Hat**:

- Хакери «чорних капелюхів» — це неетичні злочинці, які порушують безпеку комп'ютера та мережі заради особистої вигоди.
- Термін **«ЗЛОВМИСНИК»** використовується, коли йдеться про осіб або групи, яких можна класифікувати як сірих або чорних хакерів.





Зловмисники₁

184

❑ Зловмисники (суб'єкти загроз) — це окремі особи або групи осіб, які здійснюють кібератаки. Вони включають, але не обмежуються:

- Любителі
- Хактивісти
- Організовані злочинні групи
- Групи, які фінансуються державою
- Терористичні групи

❑ Кібератаки — це навмисні зловмисні дії, спрямовані на негативний вплив щодо іншої особи чи організації.





Зловмисники₂



❑ Любителі

- Вони також відомі як сценарні діти (**Script kiddies**), і вони мають незначні навички або взагалі не мають.
- Вони часто використовують наявні інструменти або інструкції, знайдені в Інтернет для здійснення атак.
- Навіть якщо вони використовують базові інструменти, результати все ще можуть бути були руйнівним.



❑ Хактивісти

- Це хакери, які публічно протестують проти різноманітних політичних і соціальних ідей.
- Вони публікують статті та відео, викладають конфіденційну інформацію та порушують роботу веб-сервісів за допомогою нелегітимного трафіку через DDoS-атаки.



❑ Фінансова вигода

- Значна частина хакерської діяльності, яка постійно загрожує нашій безпеці, мотивована фінансовою вигодою.
- Кіберзлочинці хочуть отримати доступ до банківських рахунків, особистих даних і всього іншого, що вони можуть використовувати для отримання грошових потоків.



❑ Комерційні таємниці та глобальна політика

- Часом окремі держави атакують інші країни або втручаються в їхню внутрішню політику.
- Часто вони можуть бути зацікавлені у використанні кіберпростору для промислового шпигунства.
- Крадіжка інтелектуальної власності може дати країні значну перевагу.



ЗЛОВМИСНИКИ₃

□ Типи суб'єктів загрози:

- **Script kiddies** – підлітки або недосвідчені особи, які запускають існуючі сценарії, інструменти та експлойти, щоб завдати шкоди, але зазвичай не з метою отримання прибутку.
- **Брокери вразливостей** – хакери «сірий капелюх», які намагаються виявити експлойти та повідомити про них постачальникам за призи чи винагороди.
- **Хактивісти** – хакери «сірий капелюх», які збираються і протестують проти різних політичних і соціальних ідей.
- **Кіберзлочинці** - хакери «чорний капелюх», які є самозайнятими або працюють на великі організації, що займаються кіберзлочинністю.
- **Спонсоровані державою хакери.** Спонсоровані державою хакери є зловмисниками, які викрадають державні секрети, збирають розвідувальні дані та саботують мережі іноземних урядів, терористичних груп і корпорацій.



Кіберзлочинці

- ☐ Кіберзлочинці - це зловмисники, які мотивовані заробляти гроші будь-якими необхідними засобами.
- ☐ Інколи кіберзлочинці працюють самостійно або фінансуються та спонсоруються злочинними організаціями.
- ☐ Щороку вони крадуть мільярди доларів у споживачів і компаній.
- ☐ Вони працюють у підпільній економіці та купують і продають особисту інформацію та інтелектуальну власність, яку вони викрадають у жертв.
- ☐ Вони орієнтовані на малий бізнес і споживачів, а також на великі підприємства та галузі.





Класифікація порушників



Мотиви порушень

- ☐ Можна виділити три основних мотиви порушень:
безвідповідальність, самоствердження та корисливий інтерес.
- ☐ При порушеннях, викликаних **безвідповідальністю**, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості.
- ☐ Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру заради **самоствердження** або у власних очах, або в очах колег.
- ☐ Порушення безпеки ІТС може бути викликано **корисливим інтересом користувача** ІТС. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для несанкціонованого доступу до інформації в ІТС.



Класифікація порушників₁

□ 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.



Класифікація порушників₂

❑ Потенціальних внутрішніх порушників можна розділити на:

- допоміжний персонал об'єкту, що допущений на об'єкт, але не допущений до життєво важливого центру ІТС;
- основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);
- співробітників служби безпеки, які часто формально не допущені до життєво важливого центру ІТС, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

❑ Серед внутрішніх порушників можна виділити такі **категорії персоналу**:

- користувачі (оператори) системи;
- персонал, що обслуговує технічні засоби (інженери, техніки);
- співробітники відділів розробки та супроводження програмного забезпечення (прикладні та системні програмісти);
- технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти ІТС);
- співробітники служби безпеки;
- керівники різних рівнів та посадової ієрархії.



Класифікація порушників₃

□ Усіх порушників можна класифікувати за такими ознаками:

- за рівнем знань про ІТС:
 - володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС;
 - володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування;
 - володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС;
 - знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості.
- за рівнем можливостей:
 - застосовує чисто агентурні методи отримання відомостей;
 - застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);
 - використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні носії інформації, які можуть бути тайком пронесені крізь пости охорони;
 - застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, перехоплення з каналів передачі даних, впровадження спеціальних програмних закладок).



Класифікація порушників₄

- 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.



Модель порушника



Модель порушника₁

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



Модель порушника₂

□ Модель порушника повинна визначати:

- можливі цілі порушника та їх градацію за ступенями небезпечності для ІТС та інформації, що потребує захисту;
- категорії персоналу, користувачів ІТС 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;
- можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.



Модель порушника₃

- ❑ Порушник - це фахівець вищої кваліфікації, який має повну інформацію про ІТС і засоби захисту. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.
- ❑ Під час формування моделі порушника обов'язково повинно бути визначено:
 - ймовірність реалізації загрози,
 - своєчасність виявлення,
 - відомості про порушення.



Складання моделі порушника



Приклад складання моделі порушників₁

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

Таблиця 1. Категорії порушників, визначених у моделі

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



Приклад складання моделі порушників₂

Таблиця 2. Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
M1	Безвідповідальність	1
M2	Самоствердження	2
M3	Корисливий інтерес	3
M4	Професійний обов'язок (ПЗ4)	4

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

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
K1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
K2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
K3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
K4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4



Приклад складання моделі порушників₃

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

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



Приклад складання моделі порушників₄

Таблиця 5. Специфікація моделі порушника за часом дії

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

Таблиця 6. Специфікація моделі порушника за місцем дії

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



Приклад складання моделі порушників₅

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

- **внутрішній порушник «ПВ»** - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов'язків;
- **зовнішній порушник «ПЗ4»** (агент конкурентів або закордонних спецслужб «під прикриттям») – варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.



Приклад складання моделі порушників₆

Посада	Категорія порушника	Мотив порушника	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
прибир	ПВ1	М1	К1	31	Ч4	Д1	9
	1	1	1	1	4	1	
	ПЗ4	М4	К4	34	Ч4	Д1	21
	4	4	4	4	4	1	
електр	ПВ1	М1	К1	31	Ч1	Д1	8
	1	1	1	1	3	1	
	ПЗ4	М4	К4	34	Ч1	Д1	20
	4	4	4	4	3	1	
технік	ПВ2	М1	К2	31	Ч4	Д3	12
	2	1	2	1	4	2	
	ПЗ4	М4	К4	34	Ч4	Д3	22
	4	4	4	4	4	2	
корист	ПВ3	М1	К2	31	Ч3	Д2	11
	2	1	2	1	3	2	
	ПЗ4	М4	К4	34	Ч3	Д2	21
	4	4	4	4	3	2	
адмініс	ПВ4	М1	К4	31	Ч4	Д4	17
	3	1	4	1	4	4	
	ПЗ4	М4	К4	34	Ч4	Д4	24
	4	4	4	4	4	4	
безпека	ПВ5	М1	К1	31	Ч4	Д3	14
	4	1	1	1	4	3	
	ПЗ4	М4	К4	34	Ч4	Д3	23
	4	4	4	4	4	3	



Приклад складання моделі порушників₇

□ Після зведення усіх даних в одну таблицю отримуємо таку табличну «Модель внутрішнього порушника політики безпеки інформації»:

Категорія порушника «ПВ»	Мо-тив пору-шень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливос ті за часом дії	Можливість і за місцем дії	Сума заг-роз
Служба безпеки	М1	К1	31	Ч4	Д3	14
Адмініст-ратор ІТС	М1	К4	31	Ч4	Д4	17
Користувач	М1	К2	31	Ч3	Д2	11
Технік ІТС	М1	К2	31	Ч4	Д3	12
Електрик	М1	К1	31	Ч1	Д1	8
Прибираль-ник	М1	К1	31	Ч4	Д1	9

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

Донецький національний технічний університет



Тема 2. Моделі порушника та загроз для інформації в ІТС.

Лекція 4. Складання моделі загроз для інформації в ІТС.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

207

- ☐ Загроза
- ☐ Канали витоку інформації
- ☐ Модель загроз
- ☐ Приклад складання моделі загроз



Загроза



Загроза

- ❑ 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.
- ❑ Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в ІТС в процесі її функціонування. Найбільш відомими випадковими загрозами є стихійні лиха, відмови, збої, помилки та побічні впливи.
- ❑ Сутність цих загроз (окрім стихійних лих, сутність яких незрозуміла) визначається таким чином:
 - **відмова** - порушення працездатності системи, що призводить до неможливості виконання нею основних своїх функцій;
 - **збій** - тимчасове порушення працездатності системи, наслідком чого може бути неправильне виконання у цей момент своїх функцій;
 - **помилка** - неправильне виконання системою своїх функцій, що відбувається внаслідок її специфічного стану;
 - **побічний вплив** - негативний вплив на систему, який чиниться будь-якими явищами, що відбуваються всередині системи або у зовнішньому середовищі.



Передумови загроз

- ☐ Навмисне походження загроз обумовлюється зловмисними діями людей.
- ☐ Передумови появи загроз можуть бути **об'єктивними** та **суб'єктивними**. Об'єктивні передумови можуть бути спричинені кількісною або якісною недостатністю елементів системи тощо.
- ☐ До суб'єктивних передумов відносяться різновиди людської діяльності: іноземна розвідка, промислове шпигунство, злочинні дії, неякісна робота персоналу ІТС.
- ☐ Перераховані різновиди передумов інтерпретуються таким чином:
 - **кількісна недостатність** - фізична нестача одного або декількох елементів системи, що викликає порушення технологічного процесу обробки даних і / або перевантаження наявних елементів.
 - **недосконалість конструкції (організації) елементів системи**, в силу цього можуть з'являтися можливості випадкового або навмисного негативного впливу на оброблювану або збережену інформацію.



Суб'єктивні загрози

- ❑ Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу.
- ❑ Загрози, що мають суб'єктивну природу, поділяються на **випадкові** (ненавмисні) та **навмисні**. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у **моделі загроз**, наприклад:
 - 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 (далі - ПЗ) ІТС;
 - наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);
 - помилки персоналу (користувачів) ІТС під час експлуатації;
 - навмисні дії (спроби) потенційних порушників.



Випадкові загрози₁

❑ **Випадкові загрози суб'єктивної природи** - це помилкові дії персоналу по неувважності, недбалості, незнанню тощо, але без навмисного наміру.

❑ До них відносяться:

- дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);
- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);



Випадкові загрози₂

- неумисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в ІТС 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.



Навмисні загрози1

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

□ До них відносяться:

- порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);
- порушення режимів функціонування ІТС (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 ІТС;



Навмисні загрози₂

- 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 маскуванню 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.



Канали витоку інформації



Канали витоку інформації

- ❑ Всі можливі канали витоку інформації (КВІ) класифікуються за двома критеріями:
 - наявність доступу до ІТС;
 - стан функціонування ІТС.
- ❑ За першим критерієм КВІ можуть бути розділені на такі, що:
 - не вимагають доступу, тобто дозволяють отримувати необхідну інформацію дистанційно (наприклад, шляхом візуального спостереження через вікна приміщень ІТС),
 - вимагають доступу в приміщення ІТС. У свою чергу, такі канали можуть не залишити слідів в ІТС (наприклад, візуальний перегляд зображень на екранах моніторів або документів на паперових носіях), а можуть і залишити ті чи інші сліди (наприклад, розкрадання документів або машинних носіїв інформації).
- ❑ За другим критерієм КВІ можуть бути розділені на:
 - потенційно існуючі незалежно від стану ІТС (наприклад, викрадати носії інформації можна незалежно від того, в робочому стані знаходяться засоби АС чи ні);
 - існуючі тільки в робочому стані ІТС (наприклад, побічні електромагнітні випромінювання та наведення).



Класи витоку інформації₁

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

- 1-й клас - КВІ, які проявляються безвідносно до обробки інформації без доступу до елементів ІТС (підслуховування розмов, а також провокування на розмови осіб, що мають відношення до ІТС, і використання зловмисником візуальних, оптичних та акустичних засобів);
- 2-й клас - КВІ, які проявляються у процесі обробки інформації без доступу до елементів ІТС (електромагнітні випромінювання різних пристроїв ІТС, апаратури та ліній зв'язку, паразитні наведення в ланцюгах харчування, телефонних мережах, системах теплопостачання, вентиляції тощо);



Класи витоку інформації₂

- 3-й клас - КВІ, які проявляються безвідносно до обробки інформації з доступом до елементів ІТС, але без зміни останніх (всілякі види копіювання носіїв інформації і документів, а також розкрадання виробничих відходів);
- 4-й клас - КВІ, які проявляються у процесі обробки інформації з доступом до елементів ІТС, але без зміни останніх (запам'ятовування та копіювання інформації в процесі обробки, використання програмних закладок тощо);
- 5-й клас - КВІ, які проявляються безвідносно до обробки інформації з доступом до елементів ІТС і зі зміною останніх (підміна та розкрадання носіїв інформації й апаратури, впровадження у програмне забезпечення шкідливих кодів, вірусів тощо);
- 6-й клас - КВІ, які проявляються у процесі обробки інформації з доступом до елементів ІТС і зі зміною останніх (незаконне підключення до апаратури та ліній зв'язку, а також зняття інформації з ліній живлення різних елементів ІТС).



Модель загроз



Модель загроз₁

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



Модель загроз₂

□ Модель загроз повинна визначити:

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



Модель загроз_з

- ❑ Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити її спрямованість, джерело, механізм реалізації та можливі наслідки.
- ❑ **По-перше, на порушення яких властивостей інформації або ІТС загроза спрямована:**
 - **конфіденційності** - несанкціоноване ознайомлення з інформацією;
 - **цілісності** - несанкціонована модифікація (спотворення, фальсифікація, викривлення) інформації;
 - **доступності** - порушення можливості використання ІТС або оброблюваної інформації (відмова в обслуговуванні користувача);
 - **спостереженості ІТС** - відмова в ідентифікації, автентифікації та реєстрації небезпечних дій.



Модель загроз₄

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

- персонал і користувачі;
- технічні засоби;
- моделі, алгоритми, програми;
- технологія функціонування;
- зовнішнє середовище.



Модель загроз₅

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

- шляхом підключення до апаратури та ліній зв'язку,
- маскуванню під зареєстрованого користувача,
- подолання заходів захисту з метою використання інформації або нав'язування хибної інформації,
- застосування закладних пристроїв чи програм, впровадження шкідливих кодів і вірусів.



Модель загроз₆

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



Приклад складання моделі загроз



Перелік загроз з визначенням порушень властивостей інформації та ІТС₁

№	Потенційні загрози для інформації в ІТС	Ризики для			
		К	Ц	Д	С
1. Загрози об'єктивної природи					
1.1.	Стихійні явища (пожежа, аварії)		+	+	+
1.2.	Збої та відмови системи електроживлення			+	+
1.3.	Збої та відмови обчислювальної техніки			+	+
1.4.	Збої, відмови та пошкодження носіїв інформації		+	+	
1.5.	Збої та відмови програмного забезпечення		+	+	+
2. Загрози суб'єктивної природи					
2.1	Зовнішні загрози				
2.1.1	Несанкціоноване підключення до технічних засобів	+			
2.1.2	Несанкціоноване підключення до каналів зв'язку	+			
2.1.3	Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду документів	+			
2.1.4	Несанкціоноване перехоплення інформації за рахунок витоку інформації за рахунок ПЕМВН	+			
2.1.5	Несанкціонований перегляд інформації за рахунок візуально-оптичного каналу	+			



Перелік загроз з визначенням порушень властивостей інформації та ІТС₂

№	Потенційні загрози для інформації в ІТС	Ризики для			
		К	Ц	Д	С
2.2	Порушення нормальних режимів роботи				
2.2.1	Зараження системи комп'ютерними вірусами		+	+	+
2.2.2	Втрата (розголошення) засобів розмежування доступу (паролів), магнітних носіїв інформації та резервних копій	+	+	+	
2.2.3	Несанкціоноване внесення змін у технічні засоби, програмне забезпечення, компоненти інформаційного забезпечення тощо		+	+	+
2.2.4	Використання недозволеного програмного забезпечення або модифікація компонентів програмного та інформаційного забезпечення		+	+	+
2.2.5	Пошкодження носіїв інформації			+	
2.2.6	Вхід у систему недопущених осіб (подолання систем захисту)	+	+	+	



Перелік загроз з визначенням порушень властивостей інформації та ІТС₃

№	Потенційні загрози для інформації в ІТС	Ризики для			
		К	Ц	Д	С
2.3	Помилки персоналу				
2.3.1	Помилки користувачів (впровадження і використання програм, що не є необхідними для виконання службових обов'язків; запуск програм, здатних викликати критичні зміни в системі)	+	+	+	
2.4.2	Помилки адміністраторів (неправильне конфігурування та адміністрування системи захисту, операційної системи; неправомірне відключення засобів захисту).	+	+	+	
2.3.3	Порушення технології обробки, введення та виведення інформації, роботи з МНІ (резервними копіями, еталонами та дистрибутивами)	+	+	+	
2.3.4	Недбале зберігання та облік документів, носіїв інформації, баз даних	+	+	+	
2.3.5	Отримання сторонньою особою інформації у персоналу ІТС	+			



Модель загроз з визначенням рівня ризиків та збитків₁

1. Загрози конфіденційності інформації

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



Модель загроз з визначенням рівня ризиків та збитків₂

2. Загрози цілісності інформації

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



Модель загроз з визначенням рівня ризиків та збитків₃

3. Загрози доступності інформації

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



Модель загроз з визначенням рівня ризиків та збитків₄

4. Загрози спостереженості ІТС

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



Модель загроз з розрахунком сумарного рівня ризиків та збитків

№	Види загроз	1	2	3	4	5	6	7	Сума загроз
1	Конфіденційності	5	4	5	6	5	4	4	33
2	Спостереженості	3	5	4	4	4	5	4	29
3	Доступності	4	4	4	4	4	4	3	27
4	Цілісності	4	4	4	3	4	4	3	25

Донецький національний технічний університет



Тема 3. Політика безпеки ІТС.

Лекція 5. Розробка політики безпеки інформації в ІТС.

Складання Плану захисту інформації в ІТС.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

237

- ☐ Структура політики безпеки
- ☐ Спеціалізовані політики безпеки
- ☐ Розробка політики безпеки інформації в ІТС
- ☐ Складання Плану захисту інформації в ІТС
- ☐ Приклад календарного плану



Структура політики безпеки організації



Загальні заходи безпеки

- ☐ **Політика безпеки** – формальний виклад правил, яких повинні дотримуватись користувачі при доступі до технологічних та інформаційних ресурсів.
- ☐ Політика безпеки - сукупність керівних принципів, правил, процедур та практичних прийомів у сфері безпеки, що регулюють управління, захист та розподіл цінної інформації .
- ☐ Політика може зводитись до простих правил користування або може займати сотні сторінок з деталізацією кожного аспекту правил підключення та користування мережею.
- ☐ Політика безпеки повинна забезпечити централізацію заходів щодо захисту, контролю, випробування та розвитку мережі.
- ☐ Розроблена політика безпеки буде ефективною лише в тому випадку, якщо вона підтримуватиметься і дотримуватиметься всіма користувачами мережі.

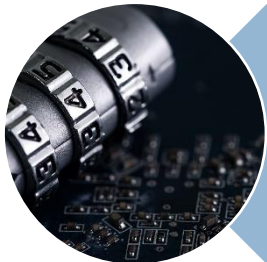


Зазвичай політика безпеки організації включає:

240



базову безпекову політику



спеціалізовані політики
безпеки



процедури безпеки



ПОНЯТТЯ

- ❑ **Огляд політики безпеки** – розкриває мету політики безпеки, описує структуру політики безпеки, детально викладає, хто і за що відповідає, встановлює процедури та передбачувані часові рамки для внесення змін. Залежно від масштабу організації, політика безпеки може містити більше або менше розділів;
- ❑ **Опис базової політики безпеки** — визначає дозволені та заборонені дії, а також необхідні засоби управління в рамках архітектури безпеки, що реалізується;
- ❑ **Посібник з архітектури безпеки** — описує реалізацію механізмів безпеки в компонентах архітектури, що використовуються в мережі організації



Спеціалізовані політики безпеки



Спеціалізовані політики безпеки

- ❑ Потенційно існують десятки спеціалізованих політик, які можуть застосовуватись більшістю організацій середнього та великого розміру.
- ❑ З урахуванням особливостей застосування спеціалізовані політики безпеки можна поділити на дві групи:
 - політики, які стосуються значної кількості користувачів;
 - політики, пов'язані із конкретними технічними областями.



До спеціалізованих політик, що зачіпають значну кількість користувачів, належать:

244

Політика
допустимого
використання

Політика
віддаленого
доступу до
ресурсів мережі

Політика захисту

Політика захисту
паролів та ін.



До спеціалізованих політик, пов'язаних з конкретними технічними областями, належать:

Політика
конфігурації
міжмережевих
екранів

Політика з
шифрування та
управління
криптоключами

Політика безпеки
віртуальних
захищених мереж
VPN

Політика з
обладнання
бездротової
мережі та ін.



Політика припустимого використання

Встановлення
стандартних
норм безпечного
використання
комп'ютерного
обладнання та
сервісів у
компанії

Мета

Встановлення
відповідних заходів
безпеки працівників
для захисту
корпоративних
ресурсів та власної
інформації



Політика допустимого використання встановлює:

Відповідальність користувачів за будь-який захист інформації, що використовується та/або зберігається на їх комп'ютерах

Правомочність користувачів читати та копіювати файли, які не є їх власними, але доступні їм

Рівень допустимого використання електронної пошти та Web -доступу



Політика віддаленого доступу₁

Встановлення стандартних норм
безпечного віддаленого з'єднання
будь-якого хоста з мережею
компанії

Мета

□ Стандартні норми покликані мінімізувати збитки компанії через можливе неавторизоване використання ресурсів компанії. До таких збитків відносяться:

- втрата інтелектуальної власності компанії,
- втрата конфіденційних даних,
- спотворення іміджу компанії,
- ушкодження критичних внутрішніх систем компанії тощо.



Політика віддаленого доступу₂

- ☐ Намічає та визначає допустимі методи віддаленого з'єднання з внутрішньою мережею.
- ☐ Суттєва у великій організації, де мережі територіально розподілені.
- ☐ Повинна охоплювати наскільки можна всі поширені методи віддаленого доступу до внутрішніх ресурсів.



Політика віддаленого доступу₃

□ Визначає:

- які методи дозволяються для віддаленого доступу;
- обмеження на дані, до яких можна отримати віддалений доступ;
- хто може мати віддалений доступ.



Правила ідентифікації та аутентифікації

- ☐ Визначає коло осіб, які мають право на доступ до ресурсів ІТС, та для опису процедур верифікації.
- ☐ Сюди відносяться фізичний доступ в комутаційні відсіки та до основних мережевих ресурсів, таким як сервера, комутатори, маршрутизатори та точки доступу.



Правила визначення паролей

- ☐ Визначають мінімальні вимоги та регулярність змін паролей, які використовуються для доступу для ресурсів підприємства.



Правила технічного обслуговування ІТС

253

- ☐ Описує процедури оновлення операційних систем мережевих пристроїв та застосунків кінцевих користувачів.



Розробка політики безпеки інформації в ІТС



Розробка політики безпеки інформації в ІТС

□ Даний етап створення КСЗІ передбачає складання наступних документів:

- політика безпеки інформації;
- план захисту інформації;
- календарний план робіт із захисту інформації.



Типи політики безпеки

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

- **Програмна політика безпеки** є політикою вищої ланки управління в організації. Об'єктом є організація в цілому, за розробку і здійснення програмної політики несе відповідальність керівництво організації. Програмна політика визначає стратегічні напрямки забезпечення інформаційної безпеки.
- **Системно-орієнтована політика** – це структура, склад, вимоги до окремих компонентів, процедур і функцій ІТС, етапу документування, які визначені вітчизняними нормативними документами.
- **Проблемно-орієнтована політика** спрямована на вирішення окремих проблем або завдань в області забезпечення інформаційної безпеки. Існує ряд областей діяльності організації, для яких необхідно розробити окремі політики:
 - фізичної безпеки,
 - керування доступом,
 - адміністрування,
 - криптозахисту,
 - антивірусного захисту,
 - інтернет-доступу тощо.



Опис політики безпеки

- ❑ Опис політики безпеки інформації в ІТС 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) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ.
- ❑ На підставі Плану захисту складається «Календарний план робіт із захисту інформації в ІТС», який містить такі заходи:
 - організаційні;
 - контрольно-профілактичні;
 - інженерно-технічні;
 - кадрові.



Організаційні заходи

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

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



Контрольні та профілактичні заходи

□ До **контрольних заходів** можуть бути віднесені:

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

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



Інженерно-технічні заходи

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



Кадрові заходи

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



Приклад календарного плану

Приклад календарного плану робіт із захисту інформації в ІТС

1. Організаційні заходи

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

2. Контрольно-профілактичні заходи

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

3. Інженерно-технічні заходи

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

4. Робота з кадрами

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



Складання плану захисту в ІТС



План захисту інформації в ІТС

☐ План захисту інформації в ІТС розробляється на підставі:

- аналізу технологій обробки інформації;
- аналізу ризиків реалізації загроз;
- політики безпеки інформації.

☐ План захисту визначає та документально закріплює:

- об'єкти захисту та завдання їх захисту;
- правила обробки інформації;
- мету побудови КСЗІ;
- заходи захисту інформації.

☐ План захисту має фіксувати на певний момент часу:

- склад ІТС;
- перелік інформації, що обробляється;
- технологію обробки інформації;
- заходи та засоби захисту інформації;
- склад необхідної документації тощо.



Склад і зміст плану захисту

- ☐ План захисту повинен регулярно переглядатися та за необхідності змінюватись. Зміни та доповнення до Плану захисту затверджуються у тому ж порядку, що і основний документ.
- ☐ Для АС, в яких обробляється інформація, що становить державну або іншу встановлену законом таємницю, службова інформація, інформація, яка належить до державних інформаційних ресурсів, або інформація, необхідність захисту якої встановлено законом, План захисту є обов'язковим документом.
- ☐ Склад і зміст Плану захисту для таких АС встановлено **«Положенням про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в АС»**, затвердженим ПКМУ № 180-98.



Розділи плану захисту

□ План захисту повинен складатись з таких розділів:

1. Завдання захисту, класифікацію, опис технології обробки службової інформації.
2. Модель загроз інформації в АС.
3. Політика (основні правила) захисту інформації в АС.
4. Перелік нормативних, розпорядчих, організаційно-технічних та інших документів, згідно з якими реалізовано захист інформації в АС.
5. Календарний план робіт із захисту інформації в АС.



План захисту для інших ІТС

- ❑ План захисту рекомендується розробляти і для всіх інших ІТС, в яких обробляється інформація, що підлягає захисту згідно з законодавством України, згідно вимог **«Правил забезпечення захисту інформації в ІТС»**, затверджених ПКМУ № 373-2006.
- ❑ План захисту повинен складатись з таких розділів:
 1. Завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації.
 2. Визначення моделі загроз для інформації в системі.
 3. Основні вимоги щодо захисту інформації та правила доступу до неї в системі.
 4. Перелік документів, згідно з якими здійснюється захист інформації в системі.
 5. Перелік і строки виконання робіт службою захисту інформації.



Склад плану захисту інших ІТС

- ☐ НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в АС» має додаток «Методичні вказівки щодо структури та змісту Плану захисту інформації в АС».
- ☐ План захисту повинен складатись з таких розділів:
 1. Завдання захисту інформації в АС.
 2. Класифікація інформації, що обробляється в АС.
 3. Опис компонентів АС та технології обробки інформації.
 4. Загрози для інформації в АС.
 5. Політика безпеки інформації в АС.
 6. Система документів з забезпечення захисту інформації в АС.

Донецький національний технічний університет



Тема 3. Комплексна система захисту інформації. Загальні положення.

Лекція 6. Загальні поняття комплексних систем захисту інформації. Типова архітектура КЗСІ

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

274

- ☐ Загальні поняття комплексних систем захисту інформації. Цілі та завдання створення КЗСІ
- ☐ Підходи до побудови КСЗІ
- ☐ Принципи створення захищених систем
- ☐ Загальні поняття архітектури КЗСІ. Класифікація. Етапи розробки
- ☐ Стратегія – як першочерговий етап архітектури КЗСІ
- ☐ Політика безпеки
- ☐ Типова архітектура комплексу засобів захисту інформації.
- ☐ Загальні вимоги до архітектури захисту інформації



Загальні поняття комплексних систем захисту інформації. Цілі та завдання створення КЗСІ



Цілі створення КСЗІ

□ **Комплексна система захисту інформації (КСЗІ)** – це сукупність організаційних та інженерних заходів, програмно-апаратних, криптографічних та інших засобів, які забезпечують захист інформації обмеженого доступу в ІТС.

□ **Цілі створення КСЗІ:**

- захист законних інтересів організації від протиправних посягань;
- недопущення:
- розкрадання фінансових і матеріально-технічних засобів;
- знищення майна і цінностей;
- розголошування, витоку і НСД до ІзОД;
- порушення роботи технічних засобів забезпечення виробничої діяльності (включаючи інформаційні технології).



Завдання створення КСЗІ

□ Завдання створення КСЗІ наступні:

- прогнозування, своєчасне виявлення і усунення загроз безпеки, причин і умов, сприяючих нанесенню збитку організації, порушенню її нормального функціонування і розвитку;
- віднесення інформації до категорії обмеженого доступу, а інших ресурсів – до різних рівнів небезпеки, що підлягають збереженню;
- створення механізму і умов оперативного реагування на загрози безпеки прояву негативних тенденцій у функціонуванні організації;
- ефективне припинення загроз персоналу і посягань на ресурси на основі правових, організаційних і інженерно-технічних заходів і засобів забезпечення безпеки;
- створення умов для максимально можливого відшкодування і локалізації збитку, послаблення негативного впливу наслідків порушення безпеки організації.



Склад КСЗІ

- Комплексна система захисту інформації включає:
- службу захисту інформації;
 - фізичну охорону об'єктів;
 - інженерно-технічні заходи;
 - комплекс засобів захисту від НСД;
 - комплекс засобів блокування технічних каналів витоку інформації;
 - комплекс засобів криптографічного захисту;
 - регламентацію дій користувачів.



Об'єкти захисту в ІТС

□ Об'єктами захисту в ІТС є:

- інформаційні ресурси обмеженого доступу та інші інформаційні ресурси, що підлягають захисту від НСД, в тому числі такі, що містять відкриту інформацію;
- процеси обробки інформації в ІТС – інформаційні технології, регламенти та процедури збирання, обробки, зберігання та передачі інформації;
- інфраструктура ІТС – системи обробки та аналізу інформації, технічні та програмні засоби її обробки, передачі та відображення, в тому числі канали інформаційного обміну та телекомунікації, системи та засоби захисту інформації, об'єкти та приміщення, в яких розміщено компоненти ІТС;
- користувачі і обслуговуючий персонал ІТС.



Захист інформації в ІТС

□ Захисту підлягає вся інформація, що може циркулювати в ІТС:

- відкрита інформація, для якої необхідно забезпечити такі властивості, як цілісність та доступність;
- ІЗОД, для якої необхідно забезпечити захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення;
- конфіденційна інформація, доступ до якої обмежено власником у відповідності до прав, наданих Законом України «Про інформацію»;
- персональні дані, доступ до яких обмежено у відповідності з Законом України «Про захист персональних даних»;
- службова інформація, доступ до якої обмежено у відповідності з Законом України «Про доступ до публічної інформації»;
- інформація, що становить державну або іншу передбачену законом таємницю, відповідно до вимог Закону України «Про державну таємницю» та інших спеціальних законів.



Суб'єкти інформаційних відносин в ІТС

□ Суб'єктами інформаційних відносин в ІТС є:

- організація як власник інформаційних ресурсів;
- структурні підрозділи організації, що забезпечують експлуатацію ІТС;
- посадові особи та співробітники структурних підрозділів організації, як користувачі ІТС у відповідності з службовими обов'язками;
- підприємства, державні органи та установи – учасники інформаційної взаємодії з ІТС;
- юридичні та фізичні особи, інформація про яких накопичується, зберігається та обробляється в ІТС;
- юридичні та фізичні особи, задіяні в процесі створення та функціонування ІТС – розробники компонентів ІТС, обслуговуючий персонал, організації, що надають послуги у сфері захисту інформації тощо.



Зацікавленість суб'єктів ІТС

□ Суб'єкти інформаційних відносин в ІТС зацікавлені в забезпеченні:

- конфіденційності інформації з обмеженим доступом;
- цілісності інформації;
- захисту від нав'язування хибної інформації;
- своєчасного доступу до необхідної інформації;
- розмежування відповідальності за порушення законних прав інших суб'єктів інформаційних відносин та встановлених правил поведінки з інформацією;
- можливості здійснення неперервного контролю та керування процесами обробки та передачі інформації.



Підходи до побудови КСЗІ



Розроблення захищених систем «з нуля»

□ У сучасних умовах застосовуються **дві технології створення КЗСІ:**

▪ **Розроблення захищених систем «з нуля»**

➤ Під час розроблення захищених систем «з нуля» всі їхні функціональні можливості та архітектурні рішення (які мають бути сертифіковані за встановленим класом вимог) закладаються на етапі проектування. Характерною рисою такого підходу є розроблення методів гарантованої реалізації встановлених вимог. У цьому випадку застосовують класичну схему проектування захищених систем:

- ✓ визначення вимог безпеки;
- ✓ розроблення моделі безпеки;
- ✓ визначення об'єктів взаємодії;
- ✓ визначення правил керування доступом;
- ✓ вибір механізмів керування доступом;
- ✓ вибір методів ідентифікації й автентифікації взаємодіючих сторін;
- ✓ визначення множини подій, що підлягають аудиту;
- ✓ реалізація системи.



Побудова «довірених» систем

- **Побудова так званих «довірених» версій шляхом модернізації наявних систем**
 - Під час побудови «довірених» версій шляхом модернізації наявних систем, як правило, додають функції шифрування, цифрового підпису, підсилюють у них керування доступом через впровадження мандатного керування, розподіляють обов'язки адміністратора системи між різними обліковими записами чи «ролями», впроваджують додаткові засоби ідентифікації й автентифікації, аудита та моніторингу.
 - Цей підхід до створення захищених систем переважає насамперед завдяки своїй економічності, яку зумовлюють менший обсяг робіт зі створення й реалізації системи та можливість збереження сумісності з наявними рішеннями. Крім того, модернізовані системи успадковують імідж систем-прототипів (створений популярністю фірм-розробників), що підвищує довіру до них і дає змогу використовувати досвід їх експлуатації й супроводження.



Принципи створення захищених систем



Принципи створення КСЗІ





Законність

- ☐ Забезпечення захисту інформації та створення КСЗІ в ІТС здійснюється відповідно до вимог чинного законодавства в сфері захисту інформації.
- ☐ Користувачі та обслуговуючий персонал ІТС повинні мати уявлення про відповідальність за неправомірне розголошення інформації з обмеженим доступом та правопорушення в області інформаційних відносин, визначену нормативно-правовими актами України.



Системність

- ❑ Системний підхід до створення КСЗІ в ІТС передбачає врахування всіх пов'язаних та взаємодіючих елементів, умов та факторів, суттєва значущих для вирішення проблеми забезпечення захисту інформації в ІТС.
- ❑ При створенні КСЗІ необхідно враховувати всі критичні та найбільш вразливі сегменти системи обробки інформації, а також характер, можливі об'єкти та напрямки атак на систему з боку порушників, шляхи проникнення в розподілені системи та НСД до інформації.
- ❑ КСЗІ повинна створюватися не лише з врахуванням всіх відомих каналів проникнення та НСД до інформації, але й з врахуванням можливості виникнення принципово нових шляхів реалізації загроз.



Комплексність

- ☐ Комплексне використання заходів та механізмів захисту ІТС передбачає узгоджене використання різнорідних засобів при створенні цілісної системи захисту, яка перекриває всі значущі канали реалізації загроз та не містить вразливих місць на стиках окремих її компонентів.
- ☐ Захист повинен будуватися ешелоновано. Зовнішній захист має забезпечуватися фізичними засобами, організаційними та правовими заходами.
- ☐ Одними з найбільш стійких до атак повинні бути механізми захисту, реалізовані на рівні операційних систем ПЕОМ, оскільки саме ОС керує використанням ресурсів комп'ютерної системи.
- ☐ Прикладний рівень захисту, який враховує особливості предметної області, забезпечує внутрішню межу захисту.



Неперервність

- ❑ Захист інформації – неперервний цілеспрямований процес, який передбачає здійснення відповідних заходів на всіх етапах життєвого циклу ІТС, починаючи з ранніх стадій проектування системи.
- ❑ Більшості технічних засобів захисту для ефективного виконання своїх функцій необхідна постійна адміністративна підтримка – своєчасна зміна та забезпечення коректного режиму зберігання та застосування ідентифікаторів, паролів, ключів шифрування, призначення повноважень тощо.
- ❑ Перерви в роботі засобів захисту можуть бути використані зловмисниками для аналізу методів та засобів, що використовуються для забезпечення захисту інформаційних ресурсів ІТС, для встановлення спеціальних програмних та апаратних закладних пристроїв та інших засобів подолання системи захисту після відновлення її функціонування.



Своєчасність

- ❑ Процеси визначення задач комплексного захисту ІТС та реалізації заходів забезпечення захисту інформації починають здійснюватися на ранніх стадіях розробки ІТС.
- ❑ Створення КСЗІ повинне проводитись паралельно з розробкою та розвитком самої автоматизованої системи, ресурси якої підлягають захисту. Це дозволить врахувати вимоги щодо забезпечення захисту інформації вже на стадіях проектування архітектури ІТС та створити більш ефективно захищену систему як з точки зору витрат ресурсів, так і стійкості.



Неперервність вдосконалення

- ❑ Заходи та засоби захисту інформації, організаційні та технічні рішення, кадровий склад повинен постійно вдосконалюватися з врахуванням змін в методах та засобах перехоплення інформації, нормативних вимог з забезпечення захисту інформації, досягнутого вітчизняного та зарубіжного досвіду.



Достатність

- ❑ Рівень витрат на забезпечення захисту інформації в ІТС повинен відповідати цінності інформаційних ресурсів та величині можливих збитків від їх розголошення, втрати, витоку, руйнування та спотворення.



Персональна відповідальність

- ❑ Передбачає покладання відповідальності за забезпечення захисту інформації та системи її обробки на кожного співробітника організації в межах його повноважень.
- ❑ Розподіл прав та обов'язків співробітників повинен здійснюватися таким чином, щоб у випадку будь-якого порушення множина винних була чітко відома та мінімальна.



Мінімізація повноважень

- ☐ Означає надання користувачам мінімальних прав доступу.
- ☐ Доступ до інформаційних ресурсів ІТС повинен надаватися виключно в тому випадку та об'ємі, якщо це необхідно співробітнику організації для виконання його функціональних обов'язків.



Гнучкість системи захисту

- ☐ Прийняті заходи та встановлені засоби захисту, особливо в початковий період їх експлуатації, можуть забезпечити як надмірний, так і недостатній рівень захисту.
- ☐ Для забезпечення можливості варіювання рівнем захищеності, засоби захисту повинні мати необхідну гнучкість.
- ☐ Особливо важливою дана властивість є в тих випадках, коли встановлення засобів захисту необхідно здійснити на систему, що вже експлуатується, без порушення процесу її нормального функціонування.
- ☐ Крім того, зовнішні умови та вимоги з часом змінюються. В таких ситуаціях властивість гнучкості КСЗІ звільняє власників ІТС від необхідності прийняття кардинальних заходів щодо повної заміни засобів захисту на нові.



Простота застосування засобів захисту

- ☐ Механізми захисту інформації в ІТС повинні бути інтуїтивно зрозумілими та простими у використанні.
- ☐ Застосування засобів захисту не повинне бути пов'язане з спеціальними знаннями або з виконанням дій, що потребують додаткових навичок при звичайній роботі зареєстрованих за встановленим порядком користувачів.



Обґрунтованість та технічна реалізованість

- ❑ Інформаційні технології, технічні та програмні засоби, засоби та заходи захисту інформації в ІТС повинні бути реалізовані на сучасному рівні розвитку науки та техніки, обґрунтовані з точки зору досягнення заданого рівня захищеності інформаційних ресурсів та повинні відповідати встановленим нормам та вимогам з забезпечення захисту інформації.



Спеціалізація та професіоналізм

- ❑ Передбачає залучення до розробки засобів та реалізації заходів захисту інформації в ІТС спеціалізованих організацій, які найбільш підготовлені до конкретного виду діяльності з забезпечення захисту інформаційних ресурсів, мають досвід практичної роботи та ліцензію на провадження господарської діяльності з надання послуг у галузі захисту інформації, видану Держспецзв'язку.
- ❑ Реалізація організаційних заходів та налаштування засобів захисту повинні здійснюватися професійно підготовленими спеціалістами організації.



Обов'язковість контролю

- ☐ Спроби порушення встановлених правил забезпечення захисту інформації в ІТС повинні бути обов'язково та своєчасно виявлені та припинені.
- ☐ Контроль за діяльністю будь-якого користувача, кожного засобу захисту та відносно будь-якого об'єкта захисту має здійснюватися на основі застосування засобів оперативного контролю і реєстрації та повинен охоплювати як несанкціоновані, так і санкціоновані дії користувачів.



Загальні поняття архітектури КЗСІ. Класифікація. Етапи розробки



Архітектура системи

- ❑ **Архітектури системи** – це опис організації системи в термінах компонентів, їх взаємозв'язків між собою і з довкіллям, принципи управління їх розробкою і розвитком.
- ❑ Архітектуру ІС можна описати як концепцію, що визначає модель, структуру, виконувані функції та взаємозв'язок компонентів.



Компоненти ІС

□ Компоненти ІС поділяються на три основні функціональні групи:

- **компонент подання** (взаємодія з користувачами) – все, що пов'язано з взаємодією з користувачем: натискання кнопок, рух миші, отрисовка зображення, висновок результатів пошуку і т.д.
- **прикладний компонент або бізнес-логіка** – правила, алгоритми реакції програми на дії користувача або на внутрішні події, правила обробки даних.
- **компонент управління ресурсами** – зберігання, вибір, модифікація і видалення даних, пов'язаних з розв'язуваною додатком прикладною задачею

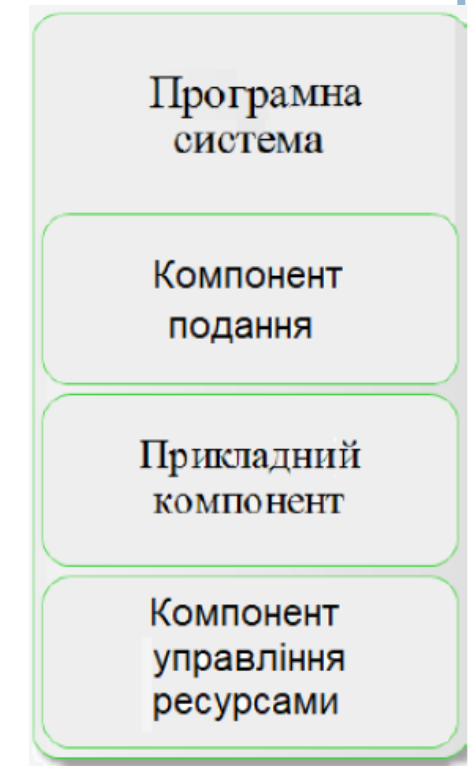


Рис. 1 Компоненти програмної системи



Архітектура системи безпеки інформації

- ❑ **Архітектура системи безпеки інформації** – це сукупність технічних засобів захисту та організаційних заходів, спрямованих на протидію актуальним ІБ-загрозам та на зниження ІБ-ризиків для захисту активів компанії.
- ❑ Архітектура залежить від моделі ризиків та від організаційної структури підприємства. Завдання побудови оптимальної системи вирішується на основі досягнення поставленої мети та відмови від надмірності.
- ❑ Архітектура безпеки інформаційних систем спирається на дві складові:
 - архітектура ІБ загалом;
 - організаційна структура підприємства.



Класифікація архітектур СІБ

□ **Вендор** — це фізична чи юридична особа, яка просуває та постачає товари під власним брендом.





Базові принципи оптимальної архітектури КСЗІ

□ Оптимальна архітектура КЗСІ має відповідати декільком базовим принципам:

- Втілювати у собі концепцію багатоешелонованого захисту (Defense in depth). Обмежившись установкою міжмережевого екрана, ви не вирішите всіх проблем ІБ.
- Мати можливості для розширення та зростання, горизонтального та вертикального масштабування. Побудована система повинна відповідати зростаючим потребам бізнесу на проміжок часу, що закладається.
- Бути простий в експлуатації та діагностиці. Вам не доведеться поспішати вночі до ЦОДу при втраті доступу до централізованої системи управління, щоб негайно відновити працездатність додатків, порушену через неправильно налаштоване правило.
- Мати змогу інтеграції з усіма необхідними інфраструктурними системами компанії. Якщо ви використовуєте службу каталогів AD (Active Directory) під час аутентифікації адміністраторів у всіх системах, засіб захисту повинен також інтегруватися з AD.
- Реально підвищувати рівень безпеки. Можна встановити всі можливі засоби захисту, але при неправильно збудованій архітектурі або неправильному налаштуванні цих засобів, інформаційна безпека все одно залишиться на колишньому рівні.



Етапи розробки архітектури КСЗІ

- ☐ Перший етап розробки архітектури має на увазі визначення цільової установки захисту. Визначити цінності, процеси, дані, програми які потрібно захищати.
- ☐ Другий етап проводить огляд злочинних дій, які можуть бути потенційно вчинені стосовно об'єкта захисту. Потрібно визначити рівень загрози інформаційній безпеці.
- ☐ Третій етап показує аналіз обстановки, умов, процесів та вже встановлених засобів захисту.



Стратегія – як першочерговий етап архітектури СІБ



Стратегія захисту інформації₁

- ☐ В основі системи захисту інформації має бути **стратегія захисту інформації**, що є послідовністю етапів досягнення цілей і використання ресурси.
- ☐ Три групи ресурсів – людські, фінансові та тимчасові – мають бути скоординовані.
- ☐ Тому розробку стратегії не можна доручати окремим департаментам, вона має контролюватись на рівні керівництва компанії. Саме воно визначає, що є максимальним пріоритетом – короткий час створення системи або мінімізація ресурсів, що витрачаються.



Стратегія захисту інформації₂

□ Стратегія описує бажані елементи архітектури, які мають забезпечити її функціонування:

1. **Інформація.** Вказуються інформаційні масиви та види надання даних, серед них – текстові, відео- та аудіофайли, усна інформація, дані на паперових носіях. У цьому розділі визначаються ступінь важливості даних, рівень їхнього захисту.
2. **Інфраструктура.** Цей підрозділ документа визначає матеріальні об'єкти, де є дані, що підлягають захисту. Це комп'ютери, матеріальні носії, периферійні пристрої, місця знаходження документованої інформації, наприклад реєстратура в поліклініці, де знаходяться медичні картки пацієнтів, що містять персональні дані.
3. **Інформаційні системи,** які містять конфіденційні дані: ERP-, CRM-, SCM-, SCADA-системи, білінгові програми, бізнес-додатки, програми бухгалтерського обліку.



Стратегія захисту інформації₃

4. Інформаційна безпека. У розділі описується, які завдання безпеки вирішуються і які засоби, програмні рішення, наприклад DLP-системи, будуть використані, передбачається інсталяція готового програмного продукту або розробка власного рішення.

5. Служба інформаційної безпеки. Тут описується структура підрозділу, який відповідає за підтримання елементів архітектури безпеки інформаційних систем, його завдання та функціональні обов'язки, методи оцінки ключових показників ефективності.



Політика безпеки



Адекватна політика безпеки₁

- ☐ **Адекватна політика безпеки** – це така політика безпеки яка забезпечує захист від визначеної множини загроз із достатнім ступенів надійності.
- ☐ Вибір і підтримка адекватної політики безпеки – одна з найважливіших задач адміністратора ІС.
- ☐ Не слід вважати адекватною політику безпеки, яка забезпечує максимальний рівень захисту. Як правило, високий рівень захисту системи обмежує її функціональність і ускладнює роботу користувачів.



Адекватна політика безпеки₂

- ☐ Єдиної адекватної політики безпеки на всі існуючі випадки немає й бути не може.
- ☐ Адекватна політика безпеки визначається задачами тієї інформаційної системи, яка побудована із застосуванням конкретної ІС, а також діючими загрозами безпеці інформації у конкретній ІКС. Одна й та сама серверна інформаційна система може забезпечувати функціонування веб-сервера, сервера баз даних і сервера електронного документообігу, а одна й та сама клієнтська ІС — домашнього комп'ютера і робочої станції у корпоративному середовищі. В усіх цих випадках загрози інформації та задачі захисту різні.
- ☐ Адекватна політика безпеки може також залежати від версії застосованої ІС, її конфігурації, встановленого прикладного ПЗ.



Основні етапи визначення адекватної політики безпеки₁

- ❑ **Аналіз загроз.** Вивчаються можливі загрози безпеці конкретного екземпляра ІС. Будується модель загроз. Визначаються ймовірності реалізації окремих загроз і можливі втрати у випадках їх реалізації. Оцінюються ризики. Визначаються пріоритети у захисті від конкретних загроз.



Основні етапи визначення адекватної політики безпеки₂

- ❑ **Формування вимог до політики безпеки.** На цьому етапі визначаються засоби і методи захисту від кожної окремої загрози. Водночас проводиться аналіз можливих побічних ефектів застосування обраних засобів і методів захисту. Як правило, неминучим є компроміс між вадами захисту від певних загроз і ускладненням роботи користувачів у системі.
- ❑ Результатом проведених на цьому етапі робіт є формування набору вимог до реалізації політики безпеки у вигляді переліку методів і засобів захисту, які мають бути реалізованими.



Основні етапи визначення адекватної політики безпеки₃

- ❑ **Формальне визначення політики безпеки.** На цьому етапі здійснюється чітке визначення засобів, які реалізовуватимуть сформульовані на попередньому етапі вимоги. Зокрема, з'ясовується, чи можливе виконання зазначених вимог лише штатними засобами ІС, чи потрібно встановлювати спеціальне ПЗ.
- ❑ Формулюються вимоги до конфігурації ІС, що реалізують функції захисту, якщо такі встановлено. Результатом робіт на цьому етапі є детальний перелік конфігураційних налаштувань інформаційних систем.
- ❑ Мають бути передбачені різні нештатні ситуації та відповідні налаштування ІС у разі виникнення таких ситуацій.



Основні етапи визначення адекватної політики безпеки₄

- ❑ **Втілення політики безпеки.** На цьому етапі виконуються налаштування ІС, які реалізують функції захисту відповідно до формалізованої політики безпеки, розробленої на попередньому етапі.
- ❑ **Підтримка і корекція політики безпеки.** На цьому етапі здійснюється ретельний контроль за дотриманням формальної політики безпеки, який передбачає перевірку налаштувань засобів захисту, що входять до складу ІС.

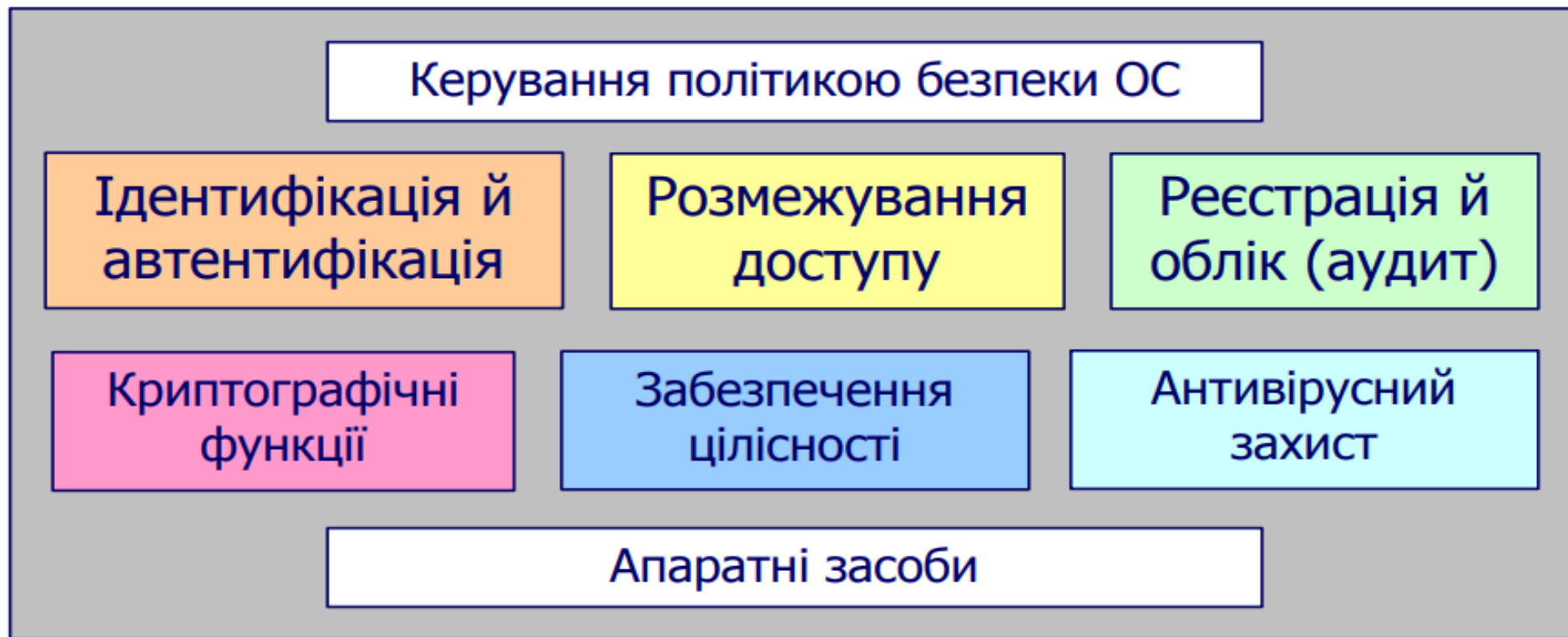


Типова архітектура комплексу засобів захисту інформації



Типова архітектура СІБ₁

- ❑ Структура будь-якої підсистеми СІБ загалом відповідає структурі типової підсистеми захисту.



Типова архітектура СІБ



Типова архітектура СІБ₂

□ Структура підсистеми КЗСІ містить наступні компоненти:

1. Розмежування доступу

- Кожному користувачеві надається доступ лише до тих захищених об'єктів, доступ до яких дозволений йому політикою безпеки
- Ця підсистема безпосередньо реалізовує політику безпеки.

2. Ідентифікація й автентифікація

- Жодний користувач не може розпочати роботу в середовищі захищеної ІС, не надавши системі свого ідентифікатора і не підтвердивши справжність наданого ідентифікатора за допомогою додаткової інформації, що автентифікує цього користувача.



Типова архітектура СІБ_з

3. Аудит

- у захищеній ІС здійснюється реєстрація всіх подій, що є потенційно небезпечними;
- підсистема аудиту здійснює захист журналів, в яких відбувається реєстрація, від НСД;
- також ця підсистема може надавати засоби для аналізу журналів і відстеження джерел тих чи інших подій.

4. Керування політикою безпеки

- захищена ІС повинна надавати інтерфейси, які дозволяють адміністраторам ефективно вирішувати завдання з підтримання адекватної політики безпеки;
- обов'язково надаються інтерфейси для налаштування підсистем розмежування доступу, ідентифікації й автентифікації, аудиту.



Типова архітектура СІБ₄

5. Криптографічні функції

- криптографічні функції застосовуються для захисту конфіденційності і цілісності інформації, для автентифікації і забезпечення неможливості відмовлення від авторства;
- криптографічні функції можуть використовуватись в якості самостійних засобів захисту, або в якості допоміжних механізмів в інших засобах.

6. Забезпечення цілісності

- будь-яка сучасна ІС надає додаткові засоби для захисту цілісності даних не лише від НСД, але й від випадкових помилок, а також від аварій і збоїв системи (В першу чергу це стосується даних у файлових системах);
- такі засоби реалізують можливості відкату, а також автоматизацію процесу створення резервних копій і відновлення з них.



Типова архітектура СІБ₅

7. Антивірусний захист

- як правило, під підсистемою антивірусного захисту розуміють сукупність програм, які надають можливість виявляти і знешкоджувати відомі шкідливі програми, які відносяться як до вірусів (у широкому розумінні – включаючи троянських коней, мережевих хробаків, шпигунські програми), так і до засобів здійснення атак;
- без антивірусного захисту в наш час неможливо підтримувати ІС у безпечному стані, особливо якщо вона встановлена на комп'ютері, що підключений до мережі;
- як правило, антивірусні засоби не входять до складу ІС, а постачаються окремо.

8. Апаратні засоби

- КЗЗ ІС спирається на функції захисту, реалізовані в апаратних засобах – процесорі і системній платі.



Особливості архітектури КЗЗ ІС

- ☐ КЗЗ ІС практично завжди є сукупністю значної кількості програмних модулів (частина модулів КЗЗ виконується у режимі ядра, а частина – у режимі користувача, тобто як прикладні програми)
- ☐ В деяких ІС, де використовується більша кількість рівнів привілеїв процесів (кілець захисту), будується ієрархія засобів захисту
- ☐ В сучасних ІС КЗЗ чітко виділяються в архітектурі системи
- ☐ Зустрічаються такі ІС, в яких підсистеми і окремі компоненти КЗЗ розпорошені по всій системі
- ☐ Як правило, підсистема захисту дозволяє додавати додаткові модулі, які реалізують підсилені функції захисту, для чого передбачаються відповідні інтерфейси.



Загальні вимоги до архітектури захисту інформації



Вимоги до КСЗІ

- ❑ Комплексна система захисту інформації у своїй загальній структурі може бути позначена як організований набір всіх механізмів, які передбачені на об'єкті обробки даних для вирішення певних завдань захисту.
- ❑ Введення поняття КСЗІ пояснюється тим, що всі ресурси, що виділяються для захисту даних, об'єднуються в одну цілісну систему, яка є функціонально самостійною підсистемою будь-якого об'єкта обробки даних.
- ❑ Важливою концептуальною вимогою до КСЗІ є адаптованість, можливість пристосування системи під зміну структури підприємства та ін.
- ❑ Крім концептуальної вимоги до СЗІ, є ще ряд конкретних вимог:
 - **функціональні:** реалізує рішення, які потрібні для вирішення завдань по ЗІ, щоб входили до рамок вимог щодо захисту, щодо політики безпеки;
 - **ергономічні:** зручність для співробітників; мінімальні перешкоди для співробітників;
 - **технічні:** оптимізація архітектури; комплексна реалізація механізмів захисту;
 - **організаційні:** простота реалізації; структурованість усіх елементів захисту.



Принципи працюючої КСЗІ₁

□ На сьогоднішній день працююча КСЗІ має низку загальнометодологічних принципів:

- **Концептуальна єдність** - означає, що технологія, архітектура та інші елементи повинні розглядатися та реалізовуватися у суворому визначенні з головними аспектами концепції захисту інформації
- **Адекватність вимогам** — пояснює, що КСЗІ має реалізовуватись у суворій відповідності до написаних вимог до захисту, які у свою чергу визначаються категорією захищеності об'єкта.



Принципи працюючої КСЗІ₂

- **Гнучкість (адаптованість)** - системи захисту означає те, що при зміні структури об'єкта функції системи захисту будуть також ефективні. Функціональна самостійність визначає, що КСЗІ бути самостійною самореалізуючою системою обробки даних та при реалізації функцій захисту не повинна залежати від інших підсистем.
- **Зручність використання** — означає, що КСЗІ не має бути тягарем для користувачів та співробітників, які безпосередньо контактують з об'єктами захисту.



Принципи працюючої КСЗІ₃

- **Мінімалізація наданих прав** означає, що кожному співробітнику інформаційної системи мають видаватися лише ті права на доступ до ресурсів, які йому необхідні за службовими обов'язками.
- **Повнота контролю** пояснює, що всі дії автоматизованих функцій на даних, що захищаються, повинні контролюватись КСЗІ, а результати контролю повинні фіксуватися.
- **Активність реагування** пояснює, що КСЗІ має бути чутливою до всіх спроб несанкціонованого доступу.



Принципи працюючої КСЗІ₄

- **Економічність КСЗІ** визначає, що витрати мають бути мінімальними за максимально реалізованої системи захисту інформації КСЗІ є функціональною підсистемою об'єкта інформатизації.
- **Функціональна побудова** підсистеми визначає організовану зібрану функціонально розмежовану КСЗІ елементів.

Донецький національний технічний університет



Тема 3. Комплексна система захисту інформації. Загальні положення.

Лекція 7. Етапи створення та вимоги до формування комплексних систем захисту інформації (КСЗІ).

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

334

- ☐ Етапи створення КСЗІ в ІТС (інформаційно-телекомунікаційна система)
- ☐ Формування вимог до КСЗІ



Етапи створення КСЗІ в ІТС (інформаційно- телекомунікаційна система)



НД ТЗІ 3.7-003-2005₁

- ❑ Основний керівний документ щодо створення КСЗІ в ІТС – це НД ТЗІ 3.7 - 003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»
- ❑ Він визначає порядок прийняття рішень щодо складу КСЗІ в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.



НД ТЗІ 3.7-003-2005₂

- ❑ НД ТЗІ призначений для суб'єктів інформаційних відносин (власників або розпорядників ІТС, користувачів), діяльність яких пов'язана з обробкою інформації, що підлягає захисту, розробників КСЗІ в ІТС, для постачальників компонентів ІТС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам ТЗІ.
- ❑ Встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством.
- ❑ Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.



Порядок створення КСЗІ₁

- ☐ **Порядок створення КСЗІ в ІТС є єдиним незалежно від того, створюється КСЗІ в ІТС, яка проектується, чи в діючій ІТС, якщо виникла необхідність забезпечення захисту інформації або модернізації вже створеної КСЗІ.**
- ☐ **Процес створення КСЗІ полягає у здійсненні комплексу взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.**



Порядок створення КСЗІ₂

- ❑ Порядок створення КСЗІ в ІТС розглядається цим НД як сукупність впорядкованих у часі, взаємопов'язаних, об'єднаних в окремі етапи робіт, виконання яких необхідне й достатнє для КСЗІ, що створюється.
- ❑ Створення КСЗІ повинно виконуватись у комплексі із заходами, щодо забезпечення режиму секретності, протидії технічним розвідкам, а також з режимними заходами щодо охорони інформації з обмеженим доступом, яка не є державною таємницею.



Склад КСЗІ

- ❑ До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:
 - витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;
 - несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо;
 - спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.
- ❑ Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом та умовами експлуатації ІТС.



Створення КТЗІ

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



Створення КЗЗ

- ☐ Створення комплексу засобів захисту від несанкціонованого доступу (далі – КЗЗ) здійснюється в усіх ІТС, де обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації.
- ☐ Рішення щодо необхідності вжиття заходів захисту від спеціальних впливів на інформацію приймається власником інформації в кожному випадку окремо.
- ☐ Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження діяльності у сфері захисту інформації.
- ☐ Після прийняття рішення про необхідність створення КСЗІ в ІТС для організації цих робіт створюється Служба захисту інформації (далі - СЗІ) в ІТС.



Етап 1. Формування вимог

1. Формування вимог до КСЗІ в ІТС

1.1. Обґрунтування необхідності створення КСЗІ і призначення СЗІ:

- наказ про порядок проведення робіт зі створення КСЗІ;
- наказ про створення СЗІ;
- положення про СЗІ;
- перелік інформації, що підлягає обробленню в ІТС та потребує захисту.

1.2. Категоріювання ІТС:

- наказ про призначення комісії з категоріювання;
- акт категоріювання;

1.3. Обстеження середовищ функціонування ІТС:

- наказ про призначення комісії з обстеження
- акт обстеження
- формуляр ІТС

1.4. Опис моделі порушника політики безпеки інформації: модель порушника

1.5. Опис моделі загроз для інформації: модель загроз

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



Етап 2. Розробка політики безпеки

2. Розробка політики безпеки інформації в ІТС

2.1. Вибір варіанту КСЗІ

2.2. Складання політики безпеки

2.3. Складання плану захисту

2.4. Складання календарного плану робіт із захисту інформації



Етап 3. Розробка ТЗ на КСЗІ

3. Розробка Технічного завдання на створення КСЗІ:

- складання технічного завдання та погодження його з органами Держспецзв'язку.



Етап 4. Проектування КСЗІ

4. Проектування КСЗІ:

- складання документів ескізного проекту КСЗІ;
- складання документів технічного проекту КСЗІ;
- складання документів робочого проекту КСЗІ.



Етап 5. Введення КСЗІ в дію₁

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

5.1. Підготовка КСЗІ до введення в дію:

- інструкція про порядок введення в експлуатацію КСЗІ;

5.2. Навчання користувачів:

- інструкція адміністратора безпеки в ІТС;
- інструкція системного адміністратора ІТС;
- інструкція користувача ІТС;
- правила управління паролями в ІТС;
- правила видачі, вилучення та обміну персональних ідентифікаторів, інших атрибутів розмежування доступу в ІТС;

5.3. Комплектування КСЗІ

5.4. Будівельно-монтажні роботи:

- наказ про призначення комісії з приймання робіт;
- акт приймання робіт;



Етап 5. Введення КСЗІ в дію₂

5.5. Пуско-налагоджувальні роботи:

- акт інсталяції та налагоджування АВПЗ і КЗЗ від НСД;
- акт оцінки відповідності проведених робіт вимогам експлуатаційних документів;

5.6. Попередні випробування КСЗІ:

- наказ про створення комісії з проведення випробувань;
- програма та методика попередніх випробувань;
- протокол про проведення попередніх випробувань;
- акт про приймання КСЗІ у дослідну експлуатацію;

5.7. Дослідна експлуатація КСЗІ:

- наказ про введення ІТС в дослідну експлуатацію;
- акт про завершення дослідної експлуатації;
- акт про завершення робіт зі створення КСЗІ;

5.8. Державна експертиза КСЗІ:

- заявка на проведення державної експертиза КСЗІ;
- експертний висновок щодо відповідності КСЗІ вимогам НД ТЗІ;
- атестат відповідності КСЗІ вимогам НД ТЗІ;
- наказ про дозвіл на обробку в ІТС інформації, яка підлягає захисту.



Етап 6. Супровід КСЗІ

6. На даному етапі розробляються:

- наказ про порядок забезпечення захисту інформації в ІТС;
- інструкція щодо забезпечення правил обробки ІзОД в ІТС;
- інструкція з антивірусного захисту інформації в ІТС;
- інструкція про порядок використання засобів КЗІ в ІТС;
- інструкція про порядок обліку та використання машинних носіїв інформації;
- інструкція з правил управління паролями в ІТС;
- інструкція про порядок створення і зберігання резервних копій інформаційних ресурсів ІТС;
- інструкція про порядок проведення контролю режиму обробки та захисту інформації в ІТС;
- інструкція про порядок супроводу та модернізації КСЗІ в ІТС;
- інструкція про порядок.



Формування вимог до КСЗІ



Заходи з формування вимог до КСЗІ

□ Формування вимог до КСЗІ в ІТС - складається з таких заходів:

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



Вихідні дані щодо КСЗІ

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

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;
- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;
- оцінки можливих переваг (фінансово-економічних, соціальних тощо) експлуатації ІТС у разі створення КСЗІ.



Класи КСЗІ₁

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



Класи КСЗІ₁

❑ **Клас «1»** - одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності.

❑ **Особливості такого класу:**

- в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється;
- технічні засоби (носії інформації і засоби У/В) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження і У/В всієї інформації.

❑ *Приклад – автономна ПЕОМ, доступ до якої контролюється з використанням організаційних заходів.*



Класи КСЗІ₂

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



Класи КСЗІ₃

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



Рішення про створення КСЗІ

- На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ, після чого відповідальний за ТЗІ організації-власника (розпорядника) ІТС готує для керівника організації 3 накази:
- 1) про створення Служби захисту інформації в ІТС (далі - СЗІ), порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000 «Типове положення про СЗІ в АС»;
 - 2) про призначення комісії з категоріювання ІТС, завдання та повноваження якої визначено в НД ТЗІ 1.6-005-2013 «Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»;
 - 3) про призначення комісії з обстеження середовищ функціонування ІТС, завдання та повноваження якої визначено в ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт».



Склад СЗІ

□ До складу СЗІ, який визначається наказом, повинні призначатися фахівці 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 складається з таких спеціалістів (за рівнем ієрархії):

- системний адміністратор ІТС;
- мережевий адміністратор ІТС;
- адміністратор безпеки інформації в ІТС;
- адміністратор КСЗІ в ІТС.



Положення про СЗІ₁

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



Положення про СЗІ₂

- ☐ В залежності від конкретних завдань і умов функціонування СЗІ дозволяється, у разі необхідності, поєднувати окремі розділи в один, вводити нові розділи або вилучати розділи, що не є актуальними.
- ☐ До Положення у вигляді додатків можуть включатися нормативні документи, таблиці, схеми, графіки, необхідні для визначення заходів захисту інформації, плани об'єктів захисту з вказанням робочих місць та встановлених на них технічних засобів передачі, прийому, зберігання, обробки інформації, що підлягає захисту, та інші документи.
- ☐ Положення має бути погоджене з юрисконсультом та керівниками підрозділів (служби безпеки, РСО, підрозділу ТЗІ) організації.
- ☐ Зміни суттєвого характеру вносяться до Положення на підставі наказу керівника організації (підрозділу, до якого структурно входить СЗІ).



Категоріювання ІТС

- ☐ Об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься ІзОД, підлягають обов'язковому категоріюванню. Об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься тільки відкрита інформація, категоріюванню не підлягають.
- ☐ **Об'єктами категоріювання** є об'єкти інформаційної діяльності (далі - ОІД), в тому числі об'єкти електронно-обчислювальної техніки (далі - ЕОТ) ІТС.
- ☐ **ОІД** - це інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами ІзОД.
- ☐ **Категоріювання ІТС здійснюється** комісією організації-власника (розпорядника) ІТС для визначення необхідного рівня захисту інформації, що обробляється на об'єктах ЕОТ ІТС. Категоріювання здійснюється за ознакою ступеня обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.



Категорії об'єктів

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

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



Види категоріювань

- ☐ Категоріювання ОІД четвертої категорії здійснюється згідно вимог НД ТЗІ 1.6-005-2013 «Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці».
- ☐ Категоріювання може бути первинним, черговим або позачерговим.
 - **Первинне** категоріювання здійснюється у разі створення ІТС, де буде оброблятися ІзОД.
 - **Чергове** - не рідше ніж один раз на 5 років.
 - **Позачергове** - у разі зміни ознаки, за якою була встановлена категорія ІТС.
- ☐ Комісія з категоріювання визначає ступень обмеження доступу до інформації, яка оброблятиметься в ІТС, та з урахуванням цього ступеня встановлює категорію ІТС. Встановлена категорія зазначається в Акті категоріювання ІТС, який складається комісією за результатами її роботи.
- ☐ Акт категоріювання є чинним протягом 5 років з моменту проведення категоріювання, якщо не змінилась ознака, за якою була встановлена категорія об'єкта.



Акт про категоріювання

□ В акті зазначається:

1. Підстава для категоріювання (рішення про створення КСЗІ, закінчення терміну дії акта категоріювання, зміна ознаки, за якою була встановлена категорія, та реквізити наказу про призначення комісії з категоріювання).
 2. Вид категоріювання: первинне, чергове, позачергове (у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання, та реквізити акту, яким було встановлено цю категорію).
 3. В ІТС здійснюється обробка ІзОД.
 4. Ступінь обмеження доступу до ІзОД, що обробляється в ІТС (передбачена законом таємниця; службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, інша конфіденційна інформація, вимога щодо захисту якої встановлена законом).
 5. Встановлена комісією категорія.
- ІТС, яким комісія встановила відповідну категорію, вносяться до «Переліку категорійованих об'єктів», який ведеться власником (розпорядником, користувачем) ОІД.



Обстеження середовищ функціонування ІТС₁

- ❑ **Метою обстеження** є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.
- ❑ Під час проведення обстеження ІТС необхідно вивчити такі середовища:
 - обчислювальне;
 - інформаційне;
 - користувацьке;
 - фізичне (у разі обробки інформації, що становить державну таємницю).



Обстеження середовищ функціонування ІТС₂

□ При обстеженні обчислювального середовища ІТС повинні бути проаналізовані й описані:

- обладнання - ЕОМ та їхні складові частини (процесори, монітори, термінали, робочі станції та ін.), периферійні пристрої;
- програмне забезпечення - вихідні, завантажувальні модулі, утиліти, СКБД, операційні системи та інші системні програми, діагностичні і тестові програми тощо;
- види і характеристики каналів зв'язку;
- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного, можливі обмеження щодо використання засобів тощо.



Обстеження середовищ функціонування ІТС₃

- ❑ Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням тощо.
- ❑ Повинні бути зафіксовані всі активні і пасивні об'єкти, які беруть участь у технологічному процесі обробки і тим чи іншим чином впливають на безпеку інформації. Для кожного активного об'єкту ІТС має бути визначено перелік пасивних об'єктів, які з ним взаємодіють.
- ❑ Окрім компонентів ІТС, необхідно дати опис технології обробки інформації в ІТС, що потребує захисту, тобто способів і методів застосування засобів обчислювальної техніки під час виконання функцій збору, зберігання, обробки, передачі і використання даних, або алгоритмів окремих процедур.



Обстеження середовищ функціонування ІТС₄

- ❑ При цьому рекомендується розробити структурну схему інформаційних потоків в ІТС, яка б відображала інформаційну взаємодію між основними компонентами ІТС (завданнями, об'єктами) з прив'язкою до кожного елемента схеми категорій інформації та визначених політикою безпеки рівнів доступу до неї.
- ❑ Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.



Обстеження середовищ функціонування ІТС₄

- ❑ При цьому рекомендується розробити структурну схему інформаційних потоків в ІТС, яка б відображала інформаційну взаємодію між основними компонентами ІТС (завданнями, об'єктами) з прив'язкою до кожного елемента схеми категорій інформації та визначених політикою безпеки рівнів доступу до неї.
- ❑ Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.



Обстеження середовищ функціонування ІТС₅

- ❑ При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС. Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, за типом їхнього представлення в ІТС, визначені й описані види її представлення в ІТС. Класифікація є підставою для визначення власником (розпорядником) інформації або ІТС методів і способів захисту кожного окремого виду інформації.
- ❑ За режимом доступу інформація в АС має бути поділена на відкриту та з обмеженим доступом. Відкриту інформацію слід поділити на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.



Обстеження середовищ функціонування ІТС₆

- ❑ 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.



Обстеження середовищ функціонування ІТС₇

- ❑ Конфіденційна інформація може мати велику цінність для її власника, втрата або передача якої іншим особам може завдати організації (власнику) значних збитків. З метою встановлення правил розмежування доступу до конфіденційної інформації необхідно класифікувати її, поділивши на декілька категорій за ступенем цінності (критерії розподілу можуть бути визначені під час оцінки ризиків).
- ❑ Для встановлення правил взаємодії активних і пасивних об'єктів ІТС інформація повинна бути класифікована за типом її представлення в ІТС (для кожної з визначених категорій встановлюються типи пасивних об'єктів комп'ютерної системи, якими вона може бути представлена). Для кожного виду інформації і типу об'єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи ІТС (спостережність), яким вони повинні задовольняти.



Обстеження середовищ функціонування ІТС₈

- Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС.
- **Для кожного структурного елемента схеми інформаційних потоків** фіксуються склад інформаційних об'єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.



Обстеження середовищ функціонування ІТС₉

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



Обстеження середовищ функціонування ІТС₁₀

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

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



Обстеження середовищ функціонування ІТС₁₁

□ При обстеженні користувацького середовища здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;
- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;
- повноважень користувачів щодо управління КСЗІ;
- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС.



Обстеження середовищ функціонування ІТС₁₂

- **За результатами обстеження вище зазначених середовищ складається «Формуляр ІТС», який оформлюється як окремий документ і складається з таких розділів:**
- загальні відомості про ІТС;
 - склад технічних засобів ІТС;
 - склад програмного забезпечення;
 - відомості про програмно-апаратний КЗЗ від НСД;
 - відомості про впровадження, випробування та приймання в експлуатацію;
 - посадові особи, відповідальні за технічне обслуговування;
 - посадові особи, відповідальні за забезпечення захисту інформації;
 - реєстрація проведених робіт (технічне обслуговування, ремонт, модернізація тощо);
 - відмітки про проведення перевірок КСЗІ;
 - перелік технічних та експлуатаційних документів КСЗІ.



Обстеження середовищ функціонування ІТС₁₃

- ☐ У разі обробки в ІТС інформації, що становить **державну таємницю**, обов'язково здійснюється також обстеження фізичного середовища, під час якого аналізується взаємне розміщення засобів обробки інформації ІТС на ОІД, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів.
- ☐ Порядок проведення обстеження повинен відповідати **ДСТУ 3396.1-96 «Технічний захист інформації. Порядок проведення робіт»**, а в частині, що стосується захисту інформації від витоку технічними каналами, - **НД ТЗІ 3.1-001-07 «Створення комплексу технічного захисту інформації. Передпроектні роботи»**.



Обстеження середовищ функціонування ІТС₁₄

□ Аналізу підлягають такі характеристики фізичного середовища:

- характеристика об'єктів, де розташовані компоненти ІТС (дані про інженерно-технічну споруду, її частину або декілька споруд, приміщення тощо);
- архітектурно-будівельні особливості приміщень: 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, каналізації, 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 сигналізації, системи зв'язку);



Обстеження середовищ функціонування ІТС₁₅

- схеми розміщення комунікацій, обладнання систем електроживлення, у тому числі трансформаторної підстанції;
- дані про складові об'єктів, які виходять за межу КЗ або її перетинають, застосування яких не обґрунтовано виробничою необхідністю і які підлягають демонтуванню, у подальшому застосуванні яких відсутня необхідність);
- опис систем заземлення (дані про перелік технічних засобів ІТС, що підлягають заземленню);
- результати аналізу фізичного середовища та пропозиції щодо необхідності отримання додаткових даних про можливі місця розміщення засобів технічної розвідки; проведення випробувань (у т.ч. спеціальних досліджень технічних засобів, які оброблятимуть ІЗОД); застосування організаційних, інженерно-технічних заходів захисту (у т.ч. застосування засобів оброблення ІЗОД, інших технічних засобів у захищеному виконанні).



Обстеження середовищ функціонування ІТС₁₆

- За результатами комісія складає «Акт обстеження середовищ функціонування ІТС», який затверджується керівником організації-власника (розпорядника) ІТС і складається з таких розділів:
- клас і склад обчислювальної системи,
 - перелік і характеристики інформаційних ресурсів,
 - перелік і повноваження користувачів,
 - опис фізичного середовища (до акту додаються генеральний і ситуаційний плани, схеми систем життєзабезпечення та заземлення).

Донецький національний технічний університет



Тема 4. Проектування КСЗІ.

Лекція 8. Формування завдання та варіанту побудови архітектури ПСЗІ. Основні вимоги до КЗЗ від несанкціонованого доступу (НСД).

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

383

- ☐ Формування завдання та варіанту побудови архітектури ПСЗІ
- ☐ Основні вимоги до КЗЗ від несанкціонованого доступу (НСД)



Формування завдання та варіанту побудови КСЗІ



Формування вимог до КСЗІ

□ Кроки 1-го етапу «Формування вимог до КСЗІ в ІТС» складаються з таких робіт:

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



Формування завдання на створення КСЗІ₁

□ Завданнями захисту інформації можуть бути:

- забезпечення необхідних властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації ІТС;
- своєчасне виявлення та ліквідація загроз для ресурсів ІТС, 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 ІТС;
- ефективне попередження загроз для ресурсів ІТС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;



Формування завдання на створення КСЗІ₂

387

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



Концепція безпеки₁

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

- правових засад;
- вимог безпеки інформації;
- загроз для інформації.



Концепція безпеки₂

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

- мета і пріоритети, яких необхідно дотримуватись в ІТС 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 ІТС, їхні права і обов'язки щодо реалізації завдань безпеки інформації.



Основні рішення з безпеки

- ❑ Вибір основних рішень з безпеки інформації розглядається на 3-х рівнях:
- правовому;
 - організаційному;
 - технічному.



Правовий рівень₁

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

- підтримка керівництвом організації заходів з безпеки інформації в ІТС, визначення відповідальності посадових осіб, організаційної структури, комплектування і розподіл обов'язків співробітників СЗІ;
- розробка політики безпеки, плану захисту та іншої документації згідно вимог нормативно-правових актів з безпеки інформації;



Правовий рівень₂

- визначення процедури доведення до персоналу і користувачів ІТС основних положень політики безпеки інформації, їхнього навчання та підвищення кваліфікації з питань безпеки інформації;
- система контролю за своєчасністю, ефективністю і повнотою реалізації в ІТС рішень з безпеки інформації, дотриманням персоналом і користувачами положень політики безпеки.



Організаційний рівень₁

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

- застосування режимних заходів на об'єктах ІТС;
- забезпечення фізичного захисту обладнання ІТС, носіїв інформації, інших ресурсів;
- визначення порядку виконання робіт з безпеки інформації, взаємодії з цих питань з іншими суб'єктами системи ТЗІ в Україні;



Організаційний рівень₂

- регламентація доступу користувачів і персоналу до ресурсів ІТС;
- організація навчання та підвищення кваліфікації персоналу і користувачів ІТС з питань безпеки інформації;
- реалізація окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до ІТС, використання мереж передачі даних загального користування, зокрема Інтернет тощо).



Технічний рівень₁

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

- інженерно-технічне обладнання приміщень, в яких розміщуються компоненти ІТС;
- реєстрація санкціонованих користувачів ІТС, 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;



Технічний рівень₂

- перевірка і забезпечення цілісності критичних даних на всіх стадіях їхньої обробки в ІТС;
- забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;
- резервне копіювання критичних даних, супроводження архівів даних і ПЗ;
- відновлення роботи ІТС після збоїв, відмов, особливо для систем із підвищеними вимогами до доступності інформації;
- захист ПЗ, окремих компонентів і ІТС в цілому від внесення несанкціонованих доповнень і змін;
- забезпечення функціонування засобів контролю.



Аналіз ризиків реалізації загроз

- ☐ Аналіз ризиків полягає в моделюванні картини появи несприятливих умов з урахуванням всіх можливих чинників, що визначають ризики, які називаються вхідними параметрами. До них відносяться активи, вразливості, загрози та збитки.
- ☐ **Активи** - ключові компоненти ІТС, що залучені в технологічні процеси та мають певну цінність.
- ☐ **Вразливості** - слабкості в засобах захисту, викликані помилками або недосконалістю процедур, які можуть бути використані для проникнення в ІТС або пошкодження активів.
- ☐ **Загрози** - реалізація яких можлива за допомогою використання вразливостей.
- ☐ **Збитки** - втрати після реалізації загрози з урахуванням витрат на відновлення пошкоджених активів.



Керування ризиками₁

□ **Керування ризиками** – це процес послідовного виконання трьох основних етапів:

- визначення початкових ризиків (в незахищеній ІТС);
- застосування засобів захисту для скорочення ризиків;
- прийняття залишкових ризиків.



Керування ризиками₂

□3 метою підвищення ефективності аналізу ризиків він проводиться по різних напрямках:

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



Керування ризиками₃

□ Процес аналізу ризиків включає оцінку:

- можливих втрат в результаті реалізації загроз;
- вірогідності виявлення вразливостей системи, що впливає на оцінку можливих втрат;
- витрат на впровадження заходів і засобів захисту, які скорочують ризик до прийнятного рівня.



Керування ризиками₄

- ❑ Витрати на КСЗІ необхідно співвіднести з цінністю інформаційних ресурсів, які піддаються ризику, а також зі збитком, який може бути нанесений організації в результаті реалізації загроз. По завершенні аналізу ризиків реалізації загроз уточнюються допустимі залишкові ризики та витрати на заходи захисту інформації.
- ❑ На даний час керування ризиками інформаційної безпеки визначає міжнародний стандарт **ISO/IEC 27005-2011** «Інформаційна технологія. Методи забезпечення безпеки. Керування ризиками інформаційної безпеки».



Керування ризиками₅

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

- 1) визначення критеріїв;
- 2) аналіз ризиків;
- 3) обробка ризиків;
- 4) прийняття ризиків.



Керування ризиками₆

- ❑ Кінцевою метою керування ризиком є **мінімізація ризику**.
Мета мінімізації ризику полягає в тому, що застосування ефективних заходів захисту призводить до прийняття залишкового ризику.
- ❑ Мінімізація ризику складається з трьох частин:
 - визначення областей, де ризик неприйнятний;
 - вибір ефективних заходів захисту;
 - оцінювання заходів захисту та визначення прийнятності залишкового ризику.



Основні вимоги до розробки комплексу засобів захисту



ЗУ «Про захист інформації в ІКС»

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



Сертифікація КЗЗ

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



Вимоги до КЗЗ

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

- безперервний захист;
- «модульність» КЗЗ;
- атрибути доступу;
- керування доступом.

□ Крім того, КЗЗ від НСД повинен реалізувати:

- концепцію диспетчера доступу;
- реєстрацію дій користувачів;
- послуги безпеки (функції захищеності);
- гарантії реалізації послуг безпеки.

Донецький національний технічний університет



Тема 4. Проектування КСЗІ.

Лекція 9. Технічне завдання на створення КСЗІ. Проектування КСЗІ в ІТС.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

409

- ☐ Технічне завдання на створення КСЗІ
- ☐ Проектування КСЗІ в ІТС



Технічне завдання на створення КСЗІ



Погодження Технічного завдання

- ❑ Технічне завдання на створення КСЗІ в ІТС розробляється згідно вимог **НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення КСЗІ в АС»**.
- ❑ Після того, як Технічне завдання на створення КСЗІ в ІТС (далі - ТЗ) розроблене, воно має бути погоджено з органами Держспецзв'язку згідно вимог п.13 статті 16 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»:
 - погодження проектів створення ІТС, в яких оброблятиметься інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, проведення їх експертної оцінки і визначення можливості введення в експлуатацію.



Погодження ТЗ для АС класу 1

- ☐ На даний час є 2 варіанти погодження ТЗ в залежності від класу ІТС (АС).
- ☐ Погодження ТЗ для АС класу 1 (ПЕОМ) здійснює регіональний орган Держспецзв'язку згідно вимог п.2.2.14 «Положення про регіональний орган Держспецзв'язку», затвердженого наказом Адміністрації Держспецзв'язку від 17.08.2012 № 450 і зареєстрованого в Міністерстві юстиції України 10.09.2012 за № 1556/21868:
- ☐ «Розглядає і погоджує (у межах своїх повноважень) технічні завдання на створення КСЗІ в ІТС, які призначені для захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, та контролює виконання вимог із технічного та криптографічного захисту інформації».



Погодження ТЗ для АС класу 2 і 3

- Погодження ТЗ для АС класів 2 і 3 (ЛОМ і РОМ) здійснює Адміністрація Держспецзв'язку згідно вимог пунктів 24 і 31 розділу 4 «Положення про Адміністрацію Держспецзв'язку», затвердженого Указом Президента України від 30.06.2011 № 717:
- 24) погоджує проекти створення та розвитку інформаційно-телекомунікаційних систем, в яких оброблятиметься інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом;
 - 31) здійснює погодження технічних завдань на проектування, будівництво і реконструкцію особливо важливих об'єктів, у процесі експлуатації або застосування яких збирається, обробляється, зберігається, передається чи приймається інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, незалежно від виду та змісту такої інформації.



Процедура погодження ТЗ

- ❑ Для погодження ТЗ друкується у 2-х примірниках, які надсилаються для погодження на адресу регіонального органу або Адміністрації Держспецзв'язку. У разі відповідності ТЗ вимогам НД ТЗІ і погодження 1-й його примірник повертається до власника (розпорядника) ІТС або розробника КСЗІ (за його наявності). У разі невідповідності ТЗ вимогам НД ТЗІ і непогодження обидва його примірники повертаються для доопрацювання.
- ❑ Після того, як ТЗ повернулось погодженим органом Держспецзв'язку, воно затверджується розробником КСЗІ (за його наявності) та керівником установи-власника (розпорядника) ІТС.



Проектування КСЗІ в ІТС



Проект КСЗІ₁

- ❑ Проект КСЗІ розробляється на підставі та у відповідності до погодженого та затвердженого «Технічного завдання на створення КСЗІ в ІТС» (далі - ТЗ) згідно вимог розділу 6.4 «Розробка проекту КСЗІ» **НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС»**.
- ❑ Під час розробки проекту обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації.



Проект КСЗІ₂

- ❑ Проект виконується на таких стадіях створення ІТС: ескізна, технічна та робоча. Для всіх стадій розробки проекту склад документації визначається ТЗ, види та зміст - **ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем»** і НД ТЗІ 2.5-004-99 **«Критерії оцінки захищеності інформації в КС від НСД»**.
- ❑ Документація на програмні засоби складається згідно комплексу стандартів Єдиної системи проектної документації (далі - ЄСПД), а на технічні засоби - згідно з комплексом стандартів Єдиної системи конструкторської документації (далі - ЄСКД).



Ескізний проект КСЗІ₁

- ❑ На цій стадії здійснюється розробка попередніх проектних рішень КСЗІ та, у разі необхідності, її окремих складових частин, а також розроблення, оформлення, узгодження та затвердження документації на КСЗІ. Зміст та стиль документації повинні бути достатніми для повного опису проектних рішень рівня ескізного проекту.
- ❑ На цій стадії визначаються:
 - функції КСЗІ в цілому та функції її окремих складових частин;
 - склад заходів протидії технічним розвідкам, організаційних, правових та інших заходів захисту;
 - склад КЗЗ від НСД;
 - склад комплексів ТЗІ від витoku технічними каналами та спеціальних впливів;
 - узагальнена структура КСЗІ та схема взаємодії складових частин.



Ескізний проект КСЗІ₂

- ☐ Пропонуються попередні технічні рішення, за допомогою яких передбачається реалізація завдань і функцій КСЗІ. У документації ескізного проекту КСЗІ мають бути наведені відомості щодо попередніх проектних рішень, які визначають порядок реалізації вимог ТЗ щодо КСЗІ в цілому та, за необхідності, щодо її окремих складових частин.
- ☐ **Дозволяється вилучати стадію ескізного проекту, у такому випадку документація ескізного проекту не розробляється.**



Технічний проект КСЗІ₁

□ На цій стадії виконується розробка:

- загальних проектних рішень, необхідних для реалізації вимог ТЗ;
- рішень щодо структури КСЗІ (організаційної структури, структури технічних і програмних засобів);
- рішень щодо архітектури КЗЗ від НСД (у тому числі щодо АВПЗ, засобів виявлення та попередження про мережеві вторгнення тощо);
- рішень щодо механізмів реалізації послуг безпеки, визначених ФПЗ;
- рішень щодо алгоритмів, порядку та умов функціонування засобів захисту інформації, які використовуються у складі КЗЗ для реалізації певних функцій захисту.



Технічний проект КСЗІ₂

- ☐ Здійснюються організаційно-технічні заходи щодо забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, випробувань, середовища функціонування та експлуатаційної документації КЗЗ у відповідності до заданих рівнем гарантій реалізації послуг безпеки згідно вимог НД ТЗІ.
- ☐ Виконується розробка, оформлення, узгодження та затвердження документації в обсязі, передбаченому ТЗ. Зміст та стиль проектної документації повинні бути достатніми для забезпечення реалізації вимог ТЗ.
- ☐ Готується та оформляється документація на постачання засобів захисту або продукції, що містить їх у своєму складі, для комплектації КСЗІ. Якщо необхідної продукції немає на ринку засобів захисту, то визначаються технічні вимоги (складаються технічні завдання) на розробку відповідних засобів.
- ☐ Здійснюється розроблення, оформлення і затвердження завдань на проектування з суміжних питань, які пов'язані зі створенням КСЗІ або впливають на умови її функціонування (будівельні, електротехнічні, санітарно-технічні та інші підготовчі роботи).



Робочий проект КСЗІ₁

- ☐ На цій стадії здійснюється розробка, оформлення та затвердження робочої та експлуатаційної документації КСЗІ та, у разі необхідності, її окремих складових частин.
- ☐ У документації робочого проекту КСЗІ мають бути наведені детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ та взаємодії її компонентів, а також відомості, необхідні для проведення пусканалагоджувальних робіт і тестування підсистем та засобів КСЗІ.
- ☐ У разі обробки в ІТС секретної інформації до складу робочої документації на комплекси ТЗІ від витоків технічними каналами повинні входити схеми розміщення засобів ІТС, кабельного обладнання, мереж живлення та систем заземлення, які виконуються у відповідності до вимог НД ТЗІ.
- ☐ При цьому враховуються умови їх розміщення та мінімально допустимі відстані між засобами ІТС та іншими технічними засобами, що знаходяться у приміщеннях, де розташоване обладнання ІТС, та у суміжних приміщеннях (засоби зв'язку, системи та засоби кондиціювання, сигналізації, електроосвітлення тощо). Зазначені умови розміщення та мінімально допустимі відстані беруться з експлуатаційної документації, яка супроводжує сертифіковані засоби ІТС.



Робочий проект КСЗІ₂

- ☐ До складу робочої документації на КЗЗ повинні входити описи таких процедур:
 - інсталяції та ініціалізації комплексу,
 - налагодження всіх механізмів розмежування доступу користувачів до ресурсів ІТС,
 - формування та актуалізації баз даних захисту,
 - контролю за діями користувачів,
 - контролю цілісності ПЗ та баз даних захисту.
- ☐ Експлуатаційна документація включає настанови (інструкції) користувачам та опис порядку функціонування та супроводження КСЗІ впродовж життєвого циклу ІТС.
- ☐ Зміст та склад документації кожної стадії проектування повинні бути достатніми для повного опису проектних рішень рівня відповідного проекту. Конкретний перелік документації визначається на підставі **ГОСТ 34.201-89 і РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»** з урахуванням особливостей КСЗІ.
- ☐ Документація кожної стадії проектування має бути затверджена розробником КСЗІ (за його наявності) та керівником установи-власника (розпорядника) ІТС.
- ☐ **Дозволяється поєднувати технічну та робочу стадії проектування в одну стадію техно-робочого проекту.**



Техно-робочий проект КСЗІ₁

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

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



Техно-робочий проект КСЗІ₂

❑ У разі проектування КСЗІ в АС класу 1 всі документи техно-робочого проекту можна об'єднати в один загальний документ під назвою **«Опис КСЗІ»**, який буде складатися з таких розділів:

- 1) зміст;
- 2) нормативні посилання;
- 3) загальні відомості;
- 4) завдання та функції КСЗІ;
- 5) опис АС та умов її функціонування;
- 6) опис інформаційної діяльності;
- 7) заходи антивірусного захисту;
- 8) заходи захисту інформації від НСД;
- 9) організаційні заходи захисту;
- 10) перелік розробленої документації.

Донецький національний технічний університет



Тема 5. Введення в дію КСЗІ.

Лекція 10. Введення ПСЗІ в дію та оцінка захищеності інформації.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

427

- ☐ Введення КСЗІ в дію
- ☐ Підготовчий період
- ☐ Монтажно-пусковий період
- ☐ Оцінка захищеності інформації



Введення КСЗІ в дію



Введення КСЗІ в дію

- ❑ Введення КСЗІ в дію здійснюється на підставі та у відповідності до затвердженого «Техно-робочого проекту КСЗІ в ІТС» згідно вимог розділу 6.5 «Введення КСЗІ в дію та оцінка захищеності інформації в ІТС» НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС».
- ❑ Цей етап складається з трьох періодів:
 - підготовчий;
 - монтажно-пусковий;
 - випробувальний



Періоди етапу введення КСЗІ в дію

1. Підготовчий період складається з таких заходів:
 - підготовка КСЗІ до введення в дію;
 - навчання користувачів;
 - комплектування КСЗІ.
2. Монтажно-пусковий період складається з таких робіт:
 - будівельно-монтажні;
 - пуско-налагоджувальні.
3. Випробувальний період складається з таких заходів:
 - попередні випробування КСЗІ;
 - дослідна експлуатація КСЗІ;
 - державна експертиза КСЗІ.



Підготовчий період



Підготовчий період

☐ 1. Підготовчий період

☐ 1.1. Підготовка КСЗІ до введення в дію

- Проводяться роботи з підготовки організаційної структури та розробки розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС. Здійснюється створення СЗІ (призначаються відповідальні особи за захист інформації), якщо цього не було зроблено на попередніх етапах.

☐ В основному має бути завершена розробка і затверджені документи з питань захисту ІзОД в ІТС (за виключенням тих, для розробки яких необхідні результати наступних етапів робіт), а саме:

- інструкція щодо забезпечення правил обробки ІзОД в ІТС;
- посадові (функціональні) інструкції користувачів;
- технологічні інструкції щодо виконання завдань з адміністрування та обслуговування КСЗІ;
- інструкції про порядок використання засобів криптографічного захисту інформації.



Інструкція з забезпечення правил обробки ІзОД₁

- Основною є **Інструкція щодо забезпечення правил обробки ІзОД в ІТС**, яка розробляється у випадку, якщо в ІТС передбачається обробка ІзОД. В ній має бути окреслений перелік заходів, спрямованих на дотримання визначеного вимогами чинної нормативно-правової бази режиму доступу до ІзОД, визначено порядок дій персоналу та користувачів ІТС з метою реалізації зазначених заходів, а також встановлено їх відповідальність у випадку порушення зазначених вимог.



Інструкція з забезпечення правил обробки ІзОД₂

□ В інструкції рекомендується у вигляді окремих розділів викласти:

- загальні відомості щодо організації захисту ІзОД в ІТС;
- опис порядку доступу до приміщень, в яких розташовані засоби ІТС;
- опис порядку захисту інформації від витоку технічними каналами;
- опис порядку захисту інформації від НСД;
- опис порядку здійснення антивірусного захисту;
- опис порядку впровадження і використання програмного забезпечення;
- опис порядку створення захищених інформаційних ресурсів, реєстрації користувачів та надання прав доступу до інформації користувачам ІТС;
- опис порядку контролю за дотриманням користувачами правил роботи із засобами ІТС;
- опис порядку обліку, зберігання, обігу, резервування, ротації та знищення матеріальних носіїв, що використовуються для зберігання ІзОД;
- опис порядку проведення ремонтних робіт та відновлення працездатності ІТС;
- опис порядку контролю за забезпеченням захисту ІзОД в ІТС;
- обов'язки користувачів та персоналу ІТС стосовно дотримання встановленого порядку оброблення ІзОД;
- відповідальність користувачів та персоналу ІТС за порушення встановленого порядку оброблення ІзОД.



Інструкція з забезпечення правил обробки ІзОД_з

- ☐ В інструкції повинні бути враховані вимоги «Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» щодо організації та порядку оброблення відповідної інформації в ІТС. Зокрема, мають бути враховані вимоги щодо використання журналів обліку та реєстрації сховищ та матеріальних носіїв ІзОД, а також визначено порядок та особливості використання відповідних журналів.
- ☐ В інструкції мають бути враховані положення посадових (функціональних) інструкцій співробітників СЗІ, персоналу та користувачів ІТС, а також технологічних (операційних) інструкцій (настанов) щодо виконання завдань з адміністрування та обслуговування КСЗІ.
- ☐ Інструкція має бути погоджена з режимно-секретним органом установи, яка є власником (розпорядником) ІТС, погоджені з виконавцем робіт зі створення КСЗІ та затверджені керівником установи.



Посадові інструкції₁

- ❑ Посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС мають визначати їх обов'язки, відповідальність та порядок дій у процесі виконання ними завдань щодо керування засобами КСЗІ і ІТС, а також обробки в ІТС інформаційних ресурсів, що потребують захисту.
- ❑ Перелік та зміст цих інструкцій повинні визначатися з урахуванням:
 - структури та штатного розкладу СЗІ, визначених у Положенні про СЗІ;
 - завдань, функцій та повноважень співробітників СЗІ, наведених у Положенні про СЗІ;
 - категорій персоналу та користувачів ІТС, визначених політикою безпеки інформації щодо розподілу обов'язків користувачів та їх функціональних завдань;
 - порядку дій співробітників СЗІ, персоналу та користувачів ІТС, який впливає з положень політики безпеки інформації, документації техноробочого проекту КСЗІ та експлуатаційної документації компонентів (складових частин) КЗЗ щодо забезпечення визначеного порядку функціонування ІТС та КСЗІ.



Посадові інструкції₂

- ☐ У склад СЗІ входять всі визначені політикою безпеки адміністратори ІТС, тому для кожного з них складається своя настанова або інструкція, а саме:
 - інструкція адміністратора безпеки;
 - інструкція адміністратора системи;
 - інструкція адміністратора мережі.
- ☐ В посадових інструкціях необхідно у вигляді окремих розділів викласти:
 - загальні положення, в яких визначено категорії персоналу, на яких поширюються їх вимоги;
 - завдання та функції персоналу;
 - обов'язки персоналу та порядок їх виконання;
 - повноваження та відповідальність персоналу.
- ☐ У посадових (функціональних) інструкціях персоналу ІТС повинні бути враховані положення технологічних інструкцій (настанов) з адміністрування та обслуговування КСЗІ.
- ☐ Посадові (функціональні) інструкції співробітників СЗІ, персоналу та користувачів ІТС мають бути погоджені з виконавцем робіт зі створення КСЗІ та затверджені керівником установи-власника (розпорядника) ІТС.



Технологічні інструкції

- ☐ Технологічні інструкції щодо виконання завдань з адміністрування та обслуговування КСЗІ повинні детально визначати послідовність дій співробітників СЗІ та персоналу ІТС у процесі виконання відповідних завдань.
- ☐ У технологічних інструкціях необхідно у вигляді окремих розділів викласти:
 - загальні положення, в яких визначено завдання з адміністрування та обслуговування КСЗІ, порядок виконання яких встановлюється інструкцією, категорії співробітників СЗІ або персоналу ІТС, на яких поширюються вимоги відповідних інструкцій (настанов) та які є відповідальними за виконання відповідних завдань;
 - послідовність і порядок здійснення технологічних операцій в ході виконання відповідальними особами певних завдань з адміністрування та обслуговування КСЗІ;
 - порядок реєстрації фактів та результатів виконання певних завдань у відповідних реєстраційних журналах.
- ☐ У технологічних інструкціях повинні бути враховані положення посадових (функціональних) інструкцій персоналу ІТС, а також визначені форми реєстраційних журналів, які планується використовувати (у додатках до інструкцій).
- ☐ Інструкції мають бути погоджені виконавцем робіт зі створення КСЗІ та затверджені керівником установи-власника (розпорядника) ІТС.



Інструкції про порядок використання засобів криптографічного захисту інформації

- ☐ Інструкції про порядок використання засобів криптографічного захисту інформації (далі - КЗІ) (за їх наявності у складі КСЗІ) повинні визначати порядок забезпечення безпеки, порядок керування ключовими даними використовуваних засобів КЗІ і порядок їх користування.
- ☐ Перелік та зміст відповідних інструкцій визначаються вимогами чинної нормативно-правової бази у сфері КЗІ, зокрема «Положенням про порядок розроблення, виробництва та експлуатації засобів КЗІ», затвердженим наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141 і зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129.
- ☐ Згідно вимог Положення розробник засобу КЗІ складає та погоджує з Держспецзв'язку такі інструкції:
 - Інструкція із забезпечення безпеки експлуатації засобів КЗІ;
 - Інструкція щодо порядку генерації ключових даних та поводження з ключовими документами.



Навчання користувачів

1.2. Навчання користувачів

- Проводиться навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та користувачів, які мають повноваження щодо управління засобами КСЗІ тощо) в частині, що їх стосується, основним положенням документів Плану захисту, які необхідні їм для дотримання вимог політики безпеки інформації, правил експлуатації засобів захисту інформації тощо.
- Після завершення навчання здійснюється перевірка знань користувачів ІТС всіх категорій та їх умінь користуватись впровадженими технологіями захисту інформації. За результатами цієї перевірки складається акт довільної форми.



Комплектування КСЗІ

1.3. Комплектування КСЗІ

- Забезпечується придбання та отримання продукції (засобів захисту інформації, матеріалів, обладнання тощо) від постачальників та співвиконавців робіт згідно відомостей техно-робочого проекту створення КСЗІ.
- Приймається рішення щодо підготовки до проведення оцінки на відповідність вимогам НД ТЗІ засобів захисту, які на момент проектування КСЗІ не мали відповідного сертифікату або експертного висновку, а також порядку проведення такої оцінки під час державної експертизи КСЗІ.



Монтажно-пусковий період



Будівельно-монтажні роботи

□ 2. Монтажно-пусковий період

□ 2.1. Будівельно-монтажні роботи

- Будівельно-монтажні роботи виконуються для забезпечення інженерно-технічного захисту інформації, що становить державну таємницю та обробляється технічними засобами ІТС, від витоків технічними каналами за рахунок побічних електромагнітних випромінювань і наведень (далі - ПЕМВН).
- ПЕМВН - це електромагнітні випромінювання, що утворюються під час роботи засобів забезпечення інформаційної діяльності під впливом електричних і магнітних полів на випадкові антени у процесі акусто-електричних перетворень, під час виникнення паразитної високочастотної генерації та паразитної модуляції, шляхом взаємного впливу кіл технічних засобів ІТС і кіл електроживлення, електроосвітлення, заземлення, сигналізації тощо.
- Роботи цього етапу виконуються під час переобладнання існуючих або при будівництві нових спеціалізованих споруд (приміщень), призначених для розміщення технічних засобів ІТС та персоналу, сховищ машинних носіїв інформації.



Заходи захисту від ПЕМВН

- ❑ Виконання заходів захисту від ПЕМВН здійснюється згідно вимог таких НД ТЗІ:
 - ТР ЕОТ - 95 Тимчасові рекомендації з ТЗІ у засобах обчислювальної техніки, АС і мережах від витоку каналами ПЕМВН;
 - НД ТЗІ 2.4-007-08 Захист інформації на об'єктах інформаційної діяльності. Технічний захист інформації, яка обробляється засобами обчислювальної техніки, від витоку за рахунок ПЕМВН. Рекомендації з використання мережевих фільтрів;
 - НД ТЗІ 2.7-007-08 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки щодо зашумлення ліній електроживлення технічних засобів.
- ❑ Передбачається виконання таких заходів в приміщеннях, де встановлені технічні засоби ІТС:
 - незадіяні кабелі демонтуються;
 - незадіяні проводи в кабелях закорочуються та заземлюються;
 - необхідні кабелі прокладаються в екранованих конструкціях;
 - монтується система заземлення, технічні засоби ІТС заземлюються;
 - встановлюються заводозаглушувальні фільтри на лініях електроживлення технічних засобів ІТС;
 - монтується комплекс ТЗІ, до складу якого входять системи просторового та лінійного зашумлення;
 - здійснюється часткове або повне екранування серверного приміщення або технічних засобів ІТС.



Прийняття робіт

- ☐ Монтаж засобів ІТС, кабельного обладнання, мереж живлення та заземлення здійснюється згідно з конструкторською документацією робочого проекту.
- ☐ Будівельно-монтажні роботи здійснюються силами установи-власника ІТС або будівельно-монтажними організаціями згідно з проектною документацією на будівництво, яка розробляється проектною організацією у відповідності до вимог Державних будівельних норм України **ДБН А.2.2-2-96 «Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва»**.
- ☐ Після завершення будівельно-монтажних робіт створюється комісія з прийняття робіт, до складу якої входять представники організації-замовника робіт та організацій-виконавців. За результатами роботи комісії складається за довільною формою акт приймання робіт з ТЗІ з оцінкою їх відповідності вимогам НД ТЗІ, який затверджується керівником організації-замовника робіт.



Пуско-налагоджувальні роботи

2.2.Пуско-налагоджувальні роботи

- ❑ Метою пуско-налагоджувальних робіт є встановлення та налагодження всіх засобів захисту, перевірка їх працездатності та атестація комплексу ТЗІ.
- ❑ Ці роботи виконуються у такій послідовності:
 - інсталяція, ініціація та налагодження АВПЗ;
 - інсталяція, ініціація та налагодження КЗЗ від НСД;
 - інсталяція, ініціація та налагодження засобів КЗІ;
 - перевірка працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії;
 - атестація комплексу ТЗІ від витоків технічними каналами (у разі наявності).



Засоби захисту інформації

- ❑ Для захисту інформації використовуються засоби ТЗІ, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ, а засоби КЗІ - у сфері КЗІ.
- ❑ Згідно з документацією техно-робочого проекту на створення КСЗІ в ІТС здійснюється інсталяція, ініціалізація та перевірка працездатності АВПЗ і КЗЗ від НСД, а у разі необхідності – засобів КЗІ. Інсталяція та ініціалізація засобів захисту, які мають експертний висновок щодо його відповідності вимогам НД ТЗІ, здійснюється у порядку, визначеному в експлуатаційній документації на ці засоби.
- ❑ Під час інсталяції АВПЗ мають бути задіяні всі механізми моніторингу та контролю системи, мережі та встановленого ПЗ, а також цілісності АВПЗ, його антивірусних баз та встановлений режим їх поновлення.
- ❑ Під час інсталяції КЗЗ мають бути задіяні всі механізми розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, а також контролю цілісності ПЗ та бази даних захисту КЗЗ.



Засоби КЗІ

- ☐ До бази даних захисту вносяться відомості про користувачів ІТС, встановлюються їх повноваження щодо доступу до захищених об'єктів ІТС, їх створення, модифікації, архівування, знищення, експорту/імпорту тощо.
- ☐ Під час інсталяції засобів КЗІ мають бути задіяні всі криптоалгоритми автентифікації, авторизації та обліку доступу користувачів до ресурсів ІТС, а також генерації та зберігання ключової інформації, алгоритмів шифрування/розшифрування даних, формування та перевірку ЕЦП.
- ☐ Засобами КЗІ можуть бути електронні ключі автентифікації - носії ключової інформації, призначені для використання в системах інформаційного доступу, електронного документообігу, авторизації користувачів і захищеного зберігання ключової інформації.
- ☐ Після отримання засобів КЗІ організація, яка їх експлуатує, кожний екземпляр засобу КЗІ бере на облік у відповідному журналі.



Передача та експлуатація КЗІ

- ☐ Одиницею обліку кожного екземпляра засобу КЗІ є:
 - для апаратних засобів - конструктивно закінчений технічний засіб;
 - для програмних засобів - інсталяційний компакт-диск тощо.
- ☐ Підставою для початку експлуатації засобів КЗІ в організації (у тому числі її філіях або регіональних представництвах), яка здійснює експлуатацію засобів КЗІ, є відповідний наказ керівника цієї організації.
- ☐ Передача засобів КЗІ здійснюється на підставі відповідних договорів, у яких указуються порядок установаження засобів КЗІ у користувачів та обслуговування цих засобів, забезпечення ключовими документами (ключовими даними), а також ужиття заходів щодо забезпечення режиму безпеки тощо.
- ☐ Ефективність вжитих заходів із захисту інформації у разі створення комплексу ТЗІ повинна бути підтверджена результатами його інструментальної перевірки під час випробувань.
- ☐ Спеціальні дослідження та інструментальні вимірювання рівня ПЕМВН виконуються підрозділом ТЗІ організації-власника ІТС або іншими суб'єктами господарювання за умови наявності ліцензії чи дозволу на здійснення відповідного виду робіт.



Оцінка захищеності інформації



Інструментальна перевірка

□ Інструментальна перевірка здійснюється згідно вимог таких НД ТЗІ:

- НД ТЗІ 2.2-005-08 Технічний захист інформації. Захист інформації, яку обробляють засобами електронної обчислювальної техніки на об'єктах інформаційної діяльності, від витоку інформації за рахунок ПЕМВН. Норми ефективності захисту;
- НД ТЗІ 2.3-014-08 Захист інформації на об'єктах інформаційної діяльності. Методика оцінки ефективності зашумлення ліній електроживлення технічних засобів;
- НД ТЗІ 2.3-015-08 Захист інформації на об'єктах інформаційної діяльності. Технічний захист інформації, яка обробляється засобами обчислювальної техніки, від витоку за рахунок ПЕМВН. Методика оцінки захищеності об'єкта ЕОТ від витоку секретної інформації лініями електроживлення без використання на них засобів захисту;
- НД ТЗІ 2.3-016-08 Захист інформації на об'єктах інформаційної діяльності. Технічний захист інформації, яка обробляється засобами обчислювальної техніки, від витоку інформації за рахунок наведень побічних електромагнітних випромінювань на лінії та комунікації. Методика інструментального контролю ефективності захисту технічних засобів ЕОТ від витоку секретної інформації за рахунок ПЕМВН на лінії сигналізації та зв'язку, які виходять за межі контрольованої зони.



Оцінка повноти та якості виконання робіт з ТЗІ

- ❑ Оцінка повноти та якості виконання робіт з ТЗІ в приміщеннях проводиться шляхом атестації впровадженого комплексу ТЗІ від витоку технічними каналами, за результатами якої **складається «Акт атестації комплексу ТЗІ»**.
- ❑ **Порядок здійснення атестації, зміст та форма Акту визначається НД ТЗІ 2.1-002-2007 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.**



Підсумковий акт

- ☐ Після завершення пуско-налагоджувальних робіт складається підсумковий акт, де зазначаються:
 - обсяг виконаних робіт;
 - оцінка відповідності проведення робіт вимогам експлуатаційних документів на засоби та нормативних документів;
 - пропозиції щодо застосування додаткових заходів захисту (у разі необхідності).
- ☐ До акту додаються:
 - акт атестації комплексу ТЗІ (у разі наявності);
 - акти інсталяції та налагодження всіх засобів захисту;
 - схеми приміщень, де розташовані засоби ІТС, з указанням систем комунікацій та меж контрольованих зон;
 - перелік технічних засобів і комунікацій, що знаходяться у цих приміщеннях.
- ☐ Акт затверджується керівником організації - власника ІТС.
- ☐ Після затвердження акту здійснюється впровадження додаткових заходів захисту, необхідність впровадження яких зафіксована в акті, та відповідне коригування проектної, робочої та експлуатаційної документації.

Донецький національний технічний університет



Тема 5. Введення в дію КСЗІ.

Лекція 11. Попередні випробування та дослідна експлуатація КСЗІ.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

455

- ☐ Попередні випробування КСЗІ
- ☐ Дослідна експлуатація КСЗІ



Попередні випробування КСЗІ



Попередні випробування КСЗІ в ІТС

- Попередні випробування КСЗІ в ІТС здійснюються згідно вимог розділу 6.5 «Введення КСЗІ в дію та оцінка захищеності інформації в ІТС» **НД ТЗІ 3.7-003-2005** «Порядок проведення робіт із створення КСЗІ в ІТС».

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказ Департаменту спеціальних
телекомунікаційних систем та
захисту інформації Служби
безпеки України
від 8 листопада 2005 р. № 125
із змінами згідно наказу
Адміністрації Держспецзв'язку від
28.12.2012 № 806

Порядок проведення робіт із створення комплексної системи захисту
інформації в інформаційно-телекомунікаційній системі

НД ТЗІ 3.7-003 -2005

ДСТСЗІ СБ України
Київ



Мета попередніх випробувань КСЗІ

- ❑ Метою попередніх випробувань КСЗІ є **перевірка її працездатності та визначення можливості прийняття у дослідну експлуатацію**. Під час випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ і НД ТЗІ. Порядок проведення попередніх випробувань може бути визначений наказом керівника установи-власника (розпорядника) ІТС.



Порядок проведення, розробка та узгодження

- ☐ Попередні випробування проводяться згідно програми та методики випробувань (далі - Програма).
- ☐ Програму готує розробник КСЗІ, а узгоджує власник ІТС.
- ☐ Вона має бути погоджена керівником установи-власника (розпорядника) ІТС, та затверджена виконавцем робіт зі створення КСЗІ в ІТС.
- ☐ Попередні випробування організовує власник ІТС, а проводить розробник КСЗІ.
- ☐ Для проведення попередніх випробувань КСЗІ керівником установи-власника (розпорядника) ІТС створюється комісія.
- ☐ Головою комісії попередніх випробувань КСЗІ призначається заступник керівника установи-власника (розпорядника) ІТС.



Програма випробувань КСЗІ

- ☐ Програма призначена для встановлення даних, що забезпечують отримання та перевірку проектних рішень, визначення якості робіт, показників якості функціонування КСЗІ, перевірку відповідності системи вимогам політики безпеки, тривалість і режим випробувань.
- ☐ Вона розробляється та оформлюється згідно вимог РД 50-34.698-90 «Автоматизовані системи. Вимоги до змісту документів» (Мова документа: Російська).



Програма випробувань КСЗІ

- ❑ Програма повинна містити перелік перевірок та опис методик виконання окремих перевірок КСЗІ. Успішне проведення цих перевірок повинно дозволити зробити однозначний висновок щодо відповідності створеної КСЗІ вимогам ТЗ.
- ❑ Якщо в ході створення КСЗІ здійснюються роботи зі створення певних компонентів КЗЗ, до складу Програми може бути введено Програму та методику випробувань ФПБ.



Методики випробувань КСЗІ

- ☐ Методики випробувань КСЗІ розробляються на **основі ТЗ** і затверджених програм випробувань з використанням типових методик (за наявності).
- ☐ При цьому окремі положення типових методик випробувань можуть уточнюватися та конкретизуватися залежно від особливості системи і умов проведення випробувань.
- ☐ При проведенні випробувань у декілька етапів програми випробувань повинні бути оформлені у **вигляді єдиного документа**.
- ☐ Зміст розділів методик встановлює розробник КСЗІ.



Перелік перевірок у програмі випробувань

- ☐ Перелік перевірок, які повинні увійти до програми, включає:
 - відповідність КСЗІ технічному завданню;
 - комплектність КСЗІ та її документації;
 - кількість і кваліфікація персоналу;
 - ступінь виконання КСЗІ своїх функцій;
 - контролездатність КСЗІ тощо.
- ☐ Опис методів випробувань КСЗІ за окремими показниками рекомендується розташовувати в тій же послідовності, в якій ці показники розташовані в технічних вимогах.



Основні розділи програми випробувань КСЗІ

□ Програма випробувань КСЗІ повинна містити такі основні розділи:

- об'єкт випробувань;
- мета випробувань;
- обсяг випробувань;
- умови та порядок випробувань;
- методи випробувань.

□ Залежно від особливостей КСЗІ допускається об'єднувати або виключати окремі розділи за умови викладу їх вмісту в інших розділах програми випробувань, а також включати в неї додаткові розділи (за необхідністю).



Основні розділи програми випробувань КСЗІ₁

- ☐ **У розділі «Об'єкт випробувань»** Програми вказується клас ІТС згідно класифікації НД ТЗІ 2.5-005-99, повне найменування та умовне позначення ІТС, в якій створена КСЗІ.
- ☐ **У розділі «Мета випробувань»** Програми вказуються конкретні цілі та завдання, які повинні бути досягнуті та вирішені в процесі випробувань.



Основні розділи програми випробувань КСЗІ₂

□ У розділі «Загальні положення» Програми вказуються:

- перелік керівних документів, на підставі яких проводять випробування;
- місце і тривалість випробувань;
- організації, що беруть участь у випробуваннях.
- Якщо раніше вже проводились випробування, то також вказуються:
 - перелік проведених випробувань;
 - перелік документів, що пред'являються на випробування, відкоригованих за результатами проведених випробувань.



Основні розділи програми випробувань КСЗІ₃

□ У розділі «Обсяг випробувань» Програми вказуються:

- перелік етапів випробувань і перевірок;
- послідовність проведення та режим випробувань;
- випробування ПЗ;
- перелік робіт, що проводяться після завершення випробувань.



Основні розділи програми випробувань КСЗІ₄

□ У розділі «Умови та порядок проведення випробувань»

Програми вказуються:

- умови проведення випробувань (умови початку та завершення окремих етапів, наявні обмеження тощо);
- вимоги до технічного обслуговування КСЗІ;
- вимоги до персоналу, що проводить випробування (порядок його допуску до випробувань);
- заходи забезпечення безпеки проведення випробувань.
- Якщо до проведення випробувань залучаються сторонні організації та експерти, то також вказується:
 - порядок взаємодії організацій, що беруть участь у випробуваннях;
 - порядок залучення експертів для дослідження можливих пошкоджень під час випробувань.



Основні розділи програми випробувань КСЗІ₅

- ❑ **У розділі «Методи випробувань»** Програми вказуються описи використовуваних методів випробувань із зазначенням результатів проведення випробувань (переліків тестових прикладів, контрольних роздруківок тестових прикладів тощо).
- ❑ **У розділі «Матеріально-технічне забезпечення випробувань»** Програми вказуються конкретні види матеріально-технічного забезпечення проведення випробувань з розподілом завдань і обов'язків організацій, які беруть участь у випробуваннях.



Основні розділи програми випробувань КСЗІ₆

□ **У розділі «Звітність»** Програми вказується перелік звітних документів, які повинні оформлятися в процесі випробувань та після їх завершення, з визначенням порядку їх погодження і затвердження та термінів оформлення цих документів. До звітних документів відносяться акт, протокол або звіт про результати випробувань, акт технічного стану системи після випробувань тощо.



Протокол попередніх випробувань КСЗІ в ІТС

- ☐ Після завершення попередніх випробувань складається **«Протокол попередніх випробувань КСЗІ в ІТС»**, який повинен містити такі розділи:
 - об'єкт випробувань;
 - мета випробувань;
 - обсяг випробувань;
 - результати випробувань;
 - оцінка повноти та завершення випробувань;
 - висновок.
- ☐ Обсяг викладання розділів Протоколу повинен відповідати обсягу розділів Програми.



Виявлені недоліки

□ Якщо під час випробувань були виявлені недоліки, вони та їхні причини обов'язково фіксуються у відповідних розділах Протоколу. У такому разі висновок Протоколу повинен містити рекомендації та термін усунення всіх виявлених недоліків. Після усунення недоліків проводяться чергові випробування, за результатами яких знову складається Протокол.



Позитивний висновок

- ☐ Після складання Протоколу з позитивним висновком оформлюється «Акт завершення попередніх випробувань КСЗІ в ІТС». Акт має бути підписаний членами комісії установи-власника (розпорядника) ІТС, представником виконавця робіт зі створення КСЗІ (за наявності) та затверджений керівником установи-власника (розпорядника) ІТС.
- ☐ Про завершення проведення попередніх випробувань КСЗІ в ІТС необхідно зробити відповідний запис у формулярі ІТС.



Дослідна експлуатація КСЗІ



Дослідна експлуатація КСЗІ

- Дослідна експлуатація КСЗІ в ІТС здійснюється згідно вимог розділу 6.5 «Введення КСЗІ в дію та оцінка захищеності інформації в ІТС» **НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС».**

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказ Департаменту спеціальних
телекомунікаційних систем та
захисту інформації Служби
безпеки України
від 8 листопада 2005 р. № 125
із змінами згідно наказу
Адміністрації Держспецзв'язку від
28.12.2012 № 806

Порядок проведення робіт із створення комплексної системи захисту
інформації в інформаційно-телекомунікаційній системі

НД ТЗІ 3.7-003 -2005

ДСТСЗІ СБ України
Київ



Дослідна експлуатація КСЗІ в ІТС

- ☐ КСЗІ в ІТС приймається у дослідну експлуатацію після затвердження **«Акту завершення попередніх випробувань»** на підставі його позитивного висновку.
- ☐ Порядок проведення дослідної експлуатації визначається наказом керівника установи-власника (розпорядника) ІТС, де вказується термін її проведення.
- ☐ Для проведення дослідної експлуатації КСЗІ керівником установи-власника (розпорядника) ІТС створюється комісія. Головою комісії з дослідної експлуатації КСЗІ призначається заступник керівника установи-власника (розпорядника) ІТС.



Під час дослідної експлуатації КСЗІ₁

- ☐ Відпрацьовуються технології обробки інформації та обігу її носіїв, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та контролю за їх діями;
- ☐ Співробітники СЗІ та користувачі ІТС засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів, набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації;



Під час дослідної експлуатації КСІ₂

- ☐ У разі необхідності здійснюється доопрацювання ПЗ, додаткове налагоджування КЗЗ та коригування документації.
- ☐ До складу експлуатаційної документації повинні входити документи, що визначають порядок інсталяції, ініціалізації, налаштування та експлуатації всіх компонентів КЗЗ, визначених у документації техно-робочого проекту КСІ.



Етап дослідної експлуатації та документації

- ❑ Згідно вимог **НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД» для КЗЗ** (окремих компонентів) у вигляді окремих документів або розділів інших документів повинні бути розроблені:
 - опис процедур інсталяції та ініціації КЗЗ;
 - опис послуг безпеки, що реалізуються КЗЗ;
 - настанови адміністратору з послуг безпеки;
 - настанови користувачу з послуг безпеки.
- ❑ Етап дослідної експлуатації завершується складанням **«Акту завершення дослідної експлуатації КСЗІ в ІТС»**.



Акт завершення дослідної експлуатації КСЗІ в ІТС

- ❑ **«Акт завершення дослідної експлуатації КСЗІ в ІТС»** повинен містити перелік відпрацьованих заходів дослідної експлуатації та їх результати, а також висновки щодо можливості (або неможливості) представлення КСЗІ на державну експертизу.
- ❑ **Акт має бути підписаний членами комісії** установи-власника (розпорядника) ІТС, представником виконавця робіт зі створення КСЗІ (за наявності) та затверджений керівником установи-власника (розпорядника) ІТС. Про завершення дослідної експлуатації КСЗІ необхідно зробити відповідний запис у формулярі ІТС.



Акт завершення дослідної експлуатації КСЗІ в ІТС

481

□ Акт складається з таких розділів:

- заходи, відпрацьовані адміністраторами;
- заходи, відпрацьовані користувачами;
- заходи з ведення документації;
- заходи з налагоджування ПЗ (за необхідності);
- результати дослідної експлуатації;
- висновок.



Акт завершення робіт зі створення КСЗІ в ІТС

- ❑ Після затвердження «Акту завершення дослідної експлуатації» складається **«Акт завершення робіт зі створення КСЗІ в ІТС»**, який повинен містити:
- загальні відомості;
 - перелік розроблених документів (вказуються реєстраційні номери, інші атрибути документів);
 - перелік проведених робіт;
 - висновок.



Підписання та Затвердження Акту

- ❑ Акт має бути підписаний членами комісії установи-власника (розпорядника) ІТС, представником виконавця робіт зі створення КСЗІ (за наявності) та затверджений керівником установи-власника (розпорядника) ІТС. Про завершення робіт зі створення КСЗІ необхідно зробити відповідний запис у формулярі ІТС.

Донецький національний технічний університет



Тема 6. Державна експертиза КСЗІ.

Лекція 12. Державна експертиза КСЗІ в ІТС.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

485

- ☐ Загальні положення
- ☐ Проведення експертизи
- ☐ Експертний висновок та Атестат відповідності
- ☐ Новий порядок експертизи
- ☐ Проведення експертизи шляхом декларації



Загальні положення



Розвиток Державної експертизи в сфері ТЗІ в Україні

- ❑ 16 травня 2007 року наказом Адміністрації Держспецзв'язку № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087, було затверджене **«Положення про державну експертизу в сфері ТЗІ»** (із змінами згідно наказу від 10.10.2012 № 567), яке визначає такі вимоги:
- ❑ Державна експертиза в сфері ТЗІ (далі - експертиза) проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам НД ТЗІ та можливості їх використання для забезпечення ТЗІ.



Суб'єкти Державної експертизи в сфері ТЗІ в Україні

□ Дія Положення поширюється на всіх юридичних та фізичних осіб, які є суб'єктами експертизи.

□ Суб'єктами експертизи є:

- юридичні та фізичні особи - власники (розпорядники) ІТС, технічних і програмних засобів, які реалізують функції ТЗІ, - замовники експертизи (далі - Замовники);
- Адміністрація Держспецзв'язку (далі - Адміністрація);
- підрозділи Держспецзв'язку, підприємства, установи та організації, які проводять експертизу (далі - Організатори);
- державні органи, які проводять експертизу в сфері свого управління;
- фізичні особи - виконавці експертних робіт з ТЗІ (далі - Експерти).



Об'єкти та процедури експертизи в сфері ТЗІ

□ Об'єктами експертизи є:

- КСЗІ, які є невід'ємною складовою частиною ІТС;
- технічні та програмні засоби, які реалізують функції ТЗІ (далі - засоби ТЗІ).

□ Експертиза КСЗІ є процедурою підтвердження відповідності КСЗІ вимогам НД ТЗІ і проводиться шляхом експертних випробувань або шляхом аналізу декларації про відповідність КСЗІ вимогам НД ТЗІ (далі - декларація).



Процедури експертизи засобів ТЗІ та КСЗІ в Україні

- ☐ Експертиза засобів ТЗІ проводиться шляхом експертних випробувань.
- ☐ Експертиза КСЗІ шляхом аналізу декларації проводиться у випадках, якщо:
 - КСЗІ створено в ІТС, яка згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу» класифікована як АС класу 1 і в якій передбачається обробка інформації, що не становить державної та іншої передбаченої законом таємниці, і де використовуються засоби захисту інформації, які мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ;
 - закінчився строк дії атестата відповідності КСЗІ в ІТС вимогам НД ТЗІ (далі - Атестат), яка згідно з нормативними документами із ТЗІ класифікується як АС класу 1 і в якій передбачається обробка інформації, що не становить державної та іншої передбаченої законом таємниці.
- ☐ У всіх інших випадках експертиза КСЗІ в ІТС проводиться шляхом експертних випробувань.



Типи експертизи в сфері ТЗІ та їх призначення

- ☐ Експертиза може бути первинною, додатковою та контрольною.
- ☐ **Первинна експертиза** є основним видом експертизи і передбачає виконання Організатором усіх потрібних заходів, визначених у розділі 3 цього Положення, для підготовки та прийняття рішення щодо об'єкта експертизи.
- ☐ **Додаткова експертиза** проводиться стосовно об'єктів експертизи, щодо яких відкрилися нові наукові та науково-технічні обставини або в зв'язку з закінченням терміну дії документів, що засвідчують результати експертизи.
- ☐ **Контрольна експертиза** проводиться іншим Організатором з ініціативи Замовника за наявності у нього обґрунтованих претензій до висновку первинної чи додаткової експертизи або з ініціативи Адміністрації для перевірки висновку первинної чи додаткової експертизи.



Проведення експертизи



Порядок організації та проведення експертизи

- ☐ Для проведення експертизи шляхом експертних випробувань Замовник надсилає заяву на ім'я Голови Держспецзв'язку (крім випадків, передбачених у розділі 5 цього Положення) про проведення експертизи КСЗІ в ІТС або засобу ТЗІ, а шляхом аналізу декларації - декларацію про відповідність КСЗІ вимогам нормативних документів із ТЗІ (додаток 3), формуляр ІТС і акт про завершення робіт зі створення КСЗІ.
- ☐ З метою розгляду декларацій і заяв, координації заходів і прийняття рішень щодо проведення експертиз в Адміністрації створюється експертна рада з питань державної експертизи у сфері технічного захисту інформації (далі - Експертна рада).



Процедури реєстрації та управління деклараціями в сфері ТЗІ

- ☐ За результатами аналізу декларації і поданих разом із нею документів Експертна рада в місячний строк приймає рішення про реєстрацію декларації. Зареєстровану декларацію та інші подані документи Адміністрація повертає Замовнику.
- ☐ У разі ненадання документів, зазначених у пункті 3.1 цього розділу, неповноти наданих у них відомостей або невідповідності порядку створення КСЗІ вимогам НД ТЗІ Адміністрація в місячний строк повертає Замовнику декларацію для доопрацювання.
- ☐ Адміністрація має право в установленому порядку зупинити дію декларації або скасувати її реєстрацію



Управління деклараціями та процедури контролю в сфері ТЗІ

- ☐ Строк дії зареєстрованої декларації є необмеженим. У разі внесення змін, не передбачених у технічному завданні на створення КСЗІ, Замовник зобов'язаний надіслати на ім'я Голови Держспецзв'язку декларацію в порядку, передбаченому в пункті 3.1 цього розділу.
- ☐ За результатами розгляду заяви Експертна рада у місячний термін приймає рішення про доцільність проведення експертизи та визначає її Організатора.
- ☐ У разі наявності у Замовника обґрунтованих претензій щодо порядку проведення або результатів експертизи він може звернутися до Адміністрації з пропозицією щодо здійснення контролю за проведенням Організатором експертних випробувань або із заявою на ім'я Голови Держспецзв'язку про проведення контрольної експертизи.



Умови та власність результатів експертизи в сфері ТЗІ

- ☐ Основним документом, що регламентує відносини між Замовником і Організатором, є укладений між ними договір на проведення експертизи.
- ☐ Результати, матеріали, висновки експертизи та створене або придбане за кошти Замовника матеріально-технічне забезпечення є його власністю, якщо інше не передбачено договором між Замовником і Організатором.
- ☐ Термін проведення експертизи визначається договором і не повинен перевищувати, як правило, 6 місяців. У випадку значного обсягу експертних робіт термін проведення експертизи може бути продовжений за згодою Адміністрації та Замовника.



Організація та узгодження методів та програм експертизи в сфері ТЗІ

- ☐ Список Експертів, які залучаються до виконання експертних робіт, визначається Організатором.
- ☐ Організатор, за результатами аналізу наданих документів і з урахуванням загальних методик оцінювання задекларованих характеристик засобів ТЗІ і КСЗІ, формує програму і окремі методики проведення експертизи об'єкта та розробляє, у разі необхідності, порядок відбору зразків засобів ТЗІ для проведення випробувань і відповідне програмно-технічне забезпечення.
- ☐ Програма проведення експертизи узгоджується із Замовником та Департаментом з питань захисту інформації в ІТС (далі – ДЗІ ІТС) Адміністрації, а окремі методики - з зазначеним департаментом.



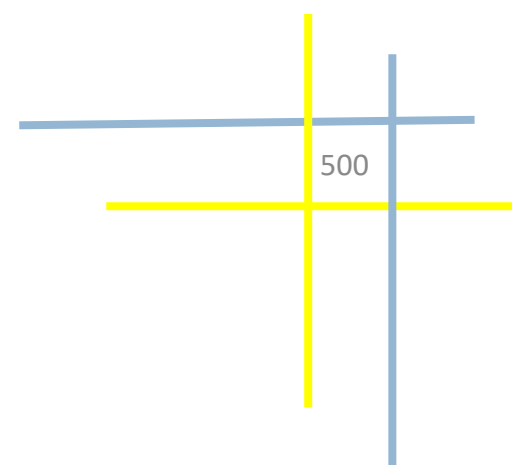
Виконання та оформлення результатів експертизи в сфері ТЗІ

- ☐ Терміни розробки окремої методики та необхідних програмно-апаратних засобів залежать від характеру та складності об'єкта експертизи і визначаються у договорі на проведення експертизи.
- ☐ Під час проведення експертизи кожний Експерт виконує експертні роботи тільки за дорученням Організатора та у відповідності з визначеною окремою методикою.
- ☐ Результати роботи оформлюються у вигляді протоколу виконання робіт (додаток 6) за підписом Експертів, які її виконували. Протокол затверджується Організатором.
- ☐ У протоколі можуть бути зафіксовані особливі думки Експертів відносно результатів виконаних робіт.



Оформлення та представлення результатів експертизи в сфері ТЗІ

- ☐ У разі виявлення невідповідності об'єкта експертизи вимогам НД ТЗІ Організатор може запропонувати Замовнику виконати доробку об'єкта.
- ☐ Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами.
- ☐ Результати робіт, визначених окремою методикою, узагальнюються Організатором в Експертному висновку.
- ☐ Висновки щодо кожного пункту окремої методики, а також особливі думки Експертів, зафіксовані в протоколах, включаються до Експертного висновку як складові частини без унесення до них будь-яких змін.
- ☐ За результатами проведених робіт Організатор складає Експертний висновок відповідного змісту щодо відповідності об'єкта експертизи вимогам НД ТЗІ, підписує його і разом із протоколами виконання робіт подає до Адміністрації.



Експертний висновок та Атестат відповідності



Експертний висновок та Атестат

- ☐ Експертний висновок на засіб ТЗІ розглядається Експертною радою і, у разі затвердження результатів експертизи, реєструється та видається Замовнику.
- ☐ На підставі позитивного рішення щодо експертизи КСЗІ Замовнику видається зареєстрований Атестат відповідності за підписом Голови Держспецзв'язку.
- ☐ Адміністрація має право в установленому порядку зупинити дію або скасувати Експертний висновок або Атестат.



Особливості проведення експертиз КСЗІ державними органами

- ❑ Адміністрація надає державному органу повноваження з організації та проведення первинних або додаткових експертиз КСЗІ в ІТС шляхом експертних випробувань за умови погодження з Адміністрацією порядку їх здійснення.
- ❑ Державні органи, які мають дозвіл Адміністрації на проведення робіт з ТЗІ для власних потреб та отримали від Адміністрації зазначені повноваження:
 - здійснюють організацію та проведення експертиз КСЗІ в ІТС у сфері свого управління шляхом експертних випробувань;
 - видають Атестат відповідності, який реєструється Адміністрацією.



Стандарт надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС

- 19 березня 2009 року наказом Адміністрації Держспецзв'язку № 64 був затверджений «Стандарт надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ», метою якого є підвищення якості надання адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ.
- До заяви про проведення первинної або додаткової експертизи додаються:
 - технічне завдання на створення КСЗІ в ІТС;
 - формуляр ІТС.



Процес проведення та видачі атестатів відповідності КСЗІ в ІТС

- ❑ Прийняте Адміністрацією Держспецзв'язку рішення про можливість проведення експертизи КСЗІ в ІТС за заявою, поданою одержувачем, та про визначення організатора експертизи повідомляється одержувачу у термін, що не повинен перевищувати 15 робочих днів.
- ❑ Атестат відповідності КСЗІ в ІТС вимогам нормативних документів з ТЗІ оформляється протягом 5 робочих днів на підставі позитивного рішення Адміністрації Держспецзв'язку щодо результатів експертизи. Зареєстрований атестат надсилається організатору експертизи для видачі одержувачу разом з експертним висновком.



Інформація та доступність адміністративної послуги з видачі атестатів відповідності КСЗІ в ІТС

- ❑ Адміністративна послуга з видачі атестатів відповідності КСЗІ в ІТС вимогам НД ТЗІ надається безоплатно.
- ❑ Інформація щодо порядку проведення експертизи КСЗІ в ІТС та форми заяв про проведення експертизи КСЗІ в ІТС розміщені на офіційному сайті Держспецзв'язку в мережі Інтернет (електронна адреса: www.dsszzi.gov.ua, розділ «Діяльність» - «Експертиза» - «Технічний захист інформації»).



Організація та роль Експертної ради з питань державної експертизи в сфері ТЗІ

- ☐ 1 жовтня 2010 року наказом Адміністрації Держспецзв'язку № 291 було затверджене «Положення про Експертну раду з питань державної експертизи в сфері ТЗІ», яка є постійно діючим колегіальним органом Адміністрації Держспецзв'язку з питань організації та проведення державної експертизи у сфері ТЗІ.
- ☐ Метою діяльності Експертної ради є координація заходів з дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам нормативно-правових актів і НД ТЗІ та оцінювання результатів експертизи.
- ☐ Формою роботи Експертної ради є засідання, які проводяться за потреби, але не рідше одного разу на місяць.
- ☐ На підставі рішень Експертної ради про затвердження результатів державних експертиз оформляються, реєструються та надаються замовникам Експертні висновки на засоби ТЗІ, оформляються та видаються Атестати відповідності КСЗІ.



Порядок формування Реєстру організаторів державної експертизи та Реєстру експертів у сфері ТЗІ

- ☐ 16 квітня 2008 року наказом Адміністрації Держспецзв'язку № 64 був затверджений «Порядок формування Реєстру організаторів державної експертизи у сфері ТЗІ та Реєстру експертів з питань ТЗІ»
- ☐ До реєстру Організаторів вносяться всі підрозділи Держспецзв'язку, підприємства, установи та організації, визначені Експертною радою як Організатори, за результатами розгляду заяв замовників про проведення державної експертизи у сфері ТЗІ.
- ☐ До реєстру Експертів вносяться всі фахівці з питань ТЗІ, які залучаються Організаторами до виконання експертних робіт під час проведення державних експертиз у сфері ТЗІ.
- ☐ Картки реєстрації Організатора та Експертів зберігаються в окремій справі ДЗІ ІТС відповідно до встановлених у Держспецзв'язку вимог щодо ведення діловодства.



Новий порядок експертизи



Новий порядок державної експертизи засобів ТЗІ та КСЗІ в ІТС₁

□ 25 березня 2011 року наказом Адміністрації Держспецзв'язку № 65 був затверджений НД ТЗІ 2.6-001-11 «Порядок проведення робіт з державної експертизи засобів ТЗІ від НСД та КСЗІ в ІТС», який складається з таких основних розділів:

- вступні положення щодо порядку проведення експертизи засобів ТЗІ від несанкціонованого доступу та КСЗІ;
- опис порядку проведення робіт з експертизи засобів ТЗІ від несанкціонованого доступу;
- опис порядку проведення робіт з експертизи КСЗІ.

□ Він має такі додатки:



Новий порядок державної експертизи засобів ТЗІ та КСЗІ в ІТС₂

- рекомендації щодо складу та змісту проектної, експлуатаційної та нормативно-розпорядчої документації, яка надається Замовником при проведенні експертизи КСЗІ;
- вимоги щодо змісту програми проведення експертизи КСЗІ в ІТС;
- вимоги щодо змісту методики проведення експертизи КСЗІ в ІТС;
- рекомендації щодо викладення змістовної частини протоколу експертизи засобу ТЗІ від несанкціонованого доступу;
- рекомендації щодо викладення змістовної частини протоколу експертизи КСЗІ;
- рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи засобу ТЗІ від несанкціонованого доступу
- рекомендації щодо викладення змістовної частини Експертного висновку за результатами експертизи КСЗІ.



Процес усунення недоліків та доробки об'єкта під час державної експертизи

- ❑ Виявлені під час державної експертизи недоліки усуваються до її завершення, порядок усунення такий самий, як і для попередніх випробувань. Якщо в силу якихось причин усунути недоліки в ході експертизи неможливо, Організатор може запропонувати Замовнику виконати доробку об'єкта. Термін доробки об'єкта експертизи визначається спільним протоколом або додатковою угодою до договору між Замовником та Організатором. Відомості щодо всіх доробок, а також результати додаткових експертних робіт оформлюються окремими протоколами. Після завершення передбачених актом робіт проводиться повторна експертиза.
- ❑ Для інтегрованих ІТС може проводитись державна експертиза кожної складової частини (модуля) КСЗІ окремо. Державна експертиза КСЗІ інтегрованої ІТС полягає у перевірці взаємодії (адміністрування, обміну даними бази даних захисту тощо) вже оцінених модулів. Документи, що містять результати робіт кожного з етапів (протоколи, акти, атестати відповідності) для КСЗІ ІТС в цілому, оформлюються з урахуванням відповідних документів на складові частини КСЗІ.



Процес складання та подання Експертного висновку

- ❑ Результати робіт, визначених методикою, узагальнюються Організатором в Експертному висновку. Висновки щодо кожного пункту методики, а також особлива думка Експерта, зафіксовані в протоколах, включаються до Експертного висновку як складові частини без унесення до них будь-яких змін.
- ❑ За результатами проведених робіт Організатор складає Експертний висновок щодо відповідності об'єкта експертизи вимогам нормативних документів з ТЗІ, підписує його і разом із протоколами виконання робіт подає до Адміністрації.



Видача та дія Атестата відповідності за результатами експертизи КСЗІ

- ❑ На підставі позитивного рішення щодо експертизи КСЗІ Замовнику безоплатно видається зареєстрований Атестат відповідності за підписом Голови Держспецзв'язку згідно вимог «Переліку адміністративних послуг, які безоплатно надаються Адміністрацією Держспецзв'язку», затвердженого наказом Адміністрації Держспецзв'язку від 29.11.2011 № 350, зареєстрованого в Міністерстві юстиції України 15.12.2011 за № 1455/20193.
- ❑ Згідно вимог п.1.6 Стандарту термін дії Атестату відповідності становить 5 років. Отримання Атестату фіксується відповідним записом у формулярі ІТС. Атестат відповідності є підставою для Замовника видати наказ про введення КСЗІ в ІТС в постійну експлуатацію, після чого в ІТС можна обробляти ІзОД.



Проведення експертизи шляхом декларації



Особливості проведення експертизи шляхом декларації

- ❑ Шляхом аналізу декларації може проводитися державна експертиза КСЗІ в ІТС, яка складається з декількох компонентів, які організаційно поєднані в одну систему (окремих АРМ, які призначені для вирішення одного й того самого завдання, але функціонують автономно) і вимоги до захисту інформації від НСД кожної компоненти висуваються як для АС.
- ❑ Процедурою державної експертизи шляхом аналізу декларації можуть скористатися будь-які суб'єкти: органи державної влади, місцевого самоврядування, установи, підприємства та організації незалежно від форми власності та підпорядкування, фізичні та юридичні особи (далі – установа).
- ❑ Запровадження декларативного механізму проведення державної експертизи КСЗІ не зачіпає правових норм, що стосуються визначення вимог, організації робіт та порядку створення КСЗІ, не вносить жодних змін до порядку виконання робіт зі створення КСЗІ.



Подання декларації після завершення робіт зі створення КСЗІ

- ☐ Декларація подається після завершення всіх робіт зі створення КСЗІ у повному обсязі і відображення їх результатів у Формулярі АС і Акті про завершення робіт зі створення КСЗІ, які повинні підтверджувати факт виконання всіх основних етапів та дотримання встановленого порядку виконання робіт.
- ☐ Під словами «всіх основних етапів робіт» згідно вимог НД ТЗІ 3.7-003-05 розуміється, що мають бути виконані роботи з визначення й оцінки загроз для інформації, формування вимог, розроблення й реалізації проекту КСЗІ, проведення випробувань КСЗІ та введення КСЗІ в експлуатацію у складі АС.
- ☐ Типові форми «Формуляру АС» і «Акту про завершення робіт зі створення КСЗІ в АС класу 1» можна знайти на сайті Держспецзв'язку.



Заповнення розділів формуляра з посиланнями на технічні та розпорядчі документи

- ☐ Розділи формуляра мають бути заповнені відповідними відомостями з посиланням на технічні або розпорядчі документи (протоколи, акти тощо) установи з їх реєстраційними номерами, згідно з якими виконувалися або в яких зафіксовано результати виконання тих чи інших робіт.
- ☐ Наприклад, це може бути наказ установи про створення служби захисту інформації чи призначення відповідальних осіб за забезпечення захисту інформації в АС, акт (протокол, звіт тощо) про проведення власником АС випробувань КСЗІ, ТЗ на створення КСЗІ, техноробочий проект КСЗІ, опис КСЗІ, модель загроз для інформації тощо. Зазначаються випадки інтегрування декількох документів, що мають самостійне значення, в один документ.



Заповнення інформації у формулярі та декларації

- ☐ До формуляра вносяться також відомості про проведення робіт із технічного обслуговування, модернізації КСЗІ, внесення інших змін до АС-1, які не впливають на технічні характеристики функціонування КСЗІ (наприклад, заміна окремих технічних засобів чи засобів обробки інформації іншими, нові призначення відповідальних осіб, зміна назви АС, місця розташування, адреси тощо).
- ☐ Усі графи декларації мають бути заповнені.
- ☐ До декларації вносяться відомості про повну назву установи-власника (розпорядника) ІТС, посаду, прізвище, ім'я та по батькові особи, що підписує декларацію (керівника установи), повну назву ІТС, в якій декларується створення і впровадження КСЗІ.



Заповнення переліку документів у декларації

- ☐ До декларації вноситься перелік назв з реєстраційними атрибутами розпорядчих, проектних і експлуатаційних документів (накази про призначення і виконання певних робіт, технічне завдання на створення КСЗІ, техно-робочий проект КСЗІ, опис КСЗІ, модель загроз для інформації, інструкції з експлуатації для адміністратора та користувача ІТС, інструкції з налаштування засобів захисту інформації тощо).
- ☐ У графі «вид інформації за порядком доступу» вказується один або декілька видів інформації, які обробляються в ІТС (відкрита, конфіденційна, службова, персональні дані, інший вид інформації, вимога щодо захисту якої встановлена законом).
- ☐ У графах з даними технічного завдання, проектних та експлуатаційних документів вказуються їх повні назви, реєстраційні атрибути, а також умовні позначення згідно з державним стандартом **ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем»** (у разі наявності).



Документальне підтвердження виконання вимог інформаційно-технічних стандартів

- ☐ Якщо документ потребує погодження з уповноваженим органом, зазначається назва органу, дата погодження, прізвище посадової особи, що його погодила.
- ☐ Має бути документально підтверджено виконання обов'язкових вимог, установлених «Правилами забезпечення захисту інформації в ІТС», а також дотримання критерію щодо використання засобів захисту інформації, які мають чинний сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ.
- ☐ Використання КЗЗ з функціями розмежування доступу, який має чинний на момент подання декларації позитивний експертний висновок за результатами державної експертизи у сфері ТЗІ, документально підтверджується відповідним записом у формулярі АС (вказати номер і дату експертного висновку, заводський номер і дату виготовлення впровадженого зразка засобу). Якщо у складі КСЗІ використовується засіб, термін дії експертного висновку якого закінчився, то необхідно додатково до запису у формулярі надати документ, який підтверджує легітимність засобу на момент його купівлі.



Вимоги щодо антивірусних програм та документації

- ☐ Формуляр повинен містити запис про впровадження антивірусних програм, які мають підтвердження відповідності. Застосування антивірусних засобів аналогічне тому, що і для засобів розмежування доступу.
- ☐ Необхідно вказати реквізити розпорядчого документа установи, згідно з яким утворено службу захисту інформації або призначено відповідальних осіб.
- ☐ Незаповнені графи у декларації та формулярі АС, відсутність висновків про позитивні результати впровадження заходів в акті завершення робіт зі створення КСЗІ, невідповідність наданих відомостей у різних документах, недостовірність відомостей є підставою для відмови у реєстрації декларації.



Роль Адміністрації у підготовці декларації

❑ Адміністрація Держспецзв'язку не втручається у процес підготовки декларації, тому процес підготовки контролюється виключно власником (розпорядником) АС і тільки він є відповідальним за правильність оформлення та комплексність документів, достовірність поданих у декларації відомостей. Адміністрація Держспецзв'язку на прохання суб'єкта може тільки (і повинна) надавати необхідну консультативну та методичну допомогу з питань створення КСЗІ, оформлення результатів виконаних робіт, заповнення тексту декларації тощо.



Процес реєстрації декларації у Держспецзв'язку

- ❑ Декларація складається власником (розпорядником) АС у 2-х примірниках і надсилається разом із «Формуляром АС» та «Актом про завершення робіт зі створення КСЗІ в АС» до Адміністрації Держспецзв'язку. Розгляд декларацій здійснюється Департаментом ТЗІ Адміністрації, яким перевіряється правильність заповнення декларації та дотримання відповідності порядку створення КСЗІ нормативним документам.
- ❑ Якщо декларація відповідає встановленим вимогам оригінал декларації реєструється Адміністрацією, кожен аркуш на звороті візується відповідальним співробітником зазначеного департаменту. Оригінал декларації, формуляр АС та акт завершення робіт зі створення КСЗІ повертається замовнику. Копія декларації залишається в Адміністрації Держспецзв'язку.



Процедура реєстрації декларації в Держспецзв'язку

- ☐ Процедура аналізу декларації Адміністрацією Держспецзв'язку є прозорою, ґрунтується на аналізі документів, визначених у Положенні, і не потребує додаткових перевірок упроваджених на об'єкті експертизи заходів і засобів захисту.
- ☐ Зареєстрована декларація має таку ж саму правову силу, що і атестат відповідності, є законним документом, що підтверджує відповідність створеної КСЗІ в АС.
- ☐ Відповідальність за достовірність внесених до декларації відомостей відповідно до статті 16 Закону України «Про підтвердження відповідності» несе подавець декларації.



Довічна дія декларації: важливість достовірності відомостей

- ☐ Строк дії декларації не обмежений. Декларація зберігає свою чинність до того часу, доки внесені до неї відомості є достовірними. Зокрема, до втрати достовірності відомостей декларації може призводити модернізація КСЗІ, якщо вносяться зміни, які впливають на політику безпеку інформації.
- ☐ Наприклад, це може бути зміна видів об'єктів захисту, моделі загроз, ролей користувачів, правил розмежування доступу чи обраного для їх реалізації комплексу засобів захисту тощо.



Оновлення декларації: процес та вимоги

- ☐ У цьому разі власник (розпорядник) АС повинен задокументувати виконані роботи, внести відповідні відомості до декларації. Складена декларація надсилається до Адміністрації Держспецзв'язку для реєстрації.
- ☐ Розгляд та реєстрація складеної нової декларації здійснюється у тому ж порядку, що і під час первинної реєстрації. Власник (розпорядник) АС надсилає до Адміністрації Держспецзв'язку разом із складеною новою декларацією акт про завершення робіт зі створення КСЗІ, формуляр АС, оригінал чинної декларації. У супровідному листі вказуються причини подання нової декларації та заявляється необхідність скасування реєстрації чинної декларації.



Контроль та Скасування Декларацій: Правила та Послідовність

- ☐ Оригінал скасованої декларації повертається подавцю з відміткою «Скасовано», номером та датою рішення про скасування.
- ☐ Адміністрація Держспецзв'язку має право перевіряти дотримання вимог НД ТЗІ під час експлуатації АС, КСЗІ яких мають зареєстровані декларації, та у разі виявлення порушень скасовувати їх реєстрацію або зупиняти дію до усунення цих порушень.

Донецький національний технічний університет



Тема 7. Супровід КСЗІ. Лекція 13. Супровід КСЗІ в ІТС.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

529

- ☐ Календарний план робіт із захисту інформації в ІТС
- ☐ Обов'язки персоналу та користувачів під час супроводу КСЗІ
- ☐ Особливості супроводу КСЗІ в ІТС в державних установах



Роботи ІТС під час супроводу КСЗІ₁

- Весь період функціонування КСЗІ забезпечується її супроводом, під час якого персоналом ІТС виконуються такі роботи щодо КСЗІ:
- керування КЗСІ згідно плану захисту та експлуатації документації
 - вдосконалення та модернізації КСЗІ.



Роботи ІТС під час супроводу КСЗІ₂

□ Під час супроводу КСЗІ здійснюються такі заходи:

- організаційне забезпечення працездатності ІТС;
- гарантійне та післягарантійне технічне обслуговування засобів КСЗІ;
- періодичне поновлення документів КСЗІ.



Календарний план робіт із захисту інформації в ІТС



Календарний план робіт із захисту інформації в ІТС

- ☐ Всі заходи супроводу та модернізації КСЗІ вносяться до Календарного плану робіт із захисту інформації в ІТС, який щорічно поновлюється.
- ☐ Він складається з 4-х розділів:
 - організаційні заходи;
 - контрольно-профілактичні заходи;
 - інженерно-технічні заходи;
 - кадрові заходи.



Організаційні заходи₁

□ **Організаційні заходи** - це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування КСЗІ.



Організаційні заходи₂

Заходи	Виконавець	Регламент робіт	Терміни/період
Коригування політики безпеки	СЗІ Адміністратори	Коригування політики Розробка додаткових інструкцій	у разі змін умов функціонування ІТС
Коригування Плану захисту	СЗІ Адміністратори	Розробка нових підходів до планування заходів захисту	щорічно
Планування модернізації КСЗІ	СЗІ Адміністратори	Розробка ТЗ на модернізацію КСЗІ згідно НД ТЗІ 3.7-001-99	згідно плану розвитку КСЗІ
Чергове категорію-вання	Комісія установи	Згідно НД ТЗІ 1.6-005-2013	через 5 років після первинного
Чергова державна експертиза	Адміністра-ція ДССЗІУ	Згідно вимог «Положення про державну експертизу»	через 5 років після первинної



Контрольно-профілактичні заходи₁

□ **Контрольні заходи** - це комплекс заходів контролю за виконанням персоналом ІТС вимог нормативно-правових актів України у сфері захисту інформації, розроблених в установі інструкцій і положень, а також заходів, розроблених за результатами попередніх перевірок.



Контрольно-профілактичні заходи₂

□ **Профілактичні заходи** - це комплекс заходів, спрямованих на формування у користувачів мотивів поведінки, які спонукають їх на безумовне виконання у повному обсязі вимог правил проведення робіт із захисту інформації тощо, а також формування відповідного морально-етичного стану в колективі.



Контрольно-профілактичні заходи₃

Заходи	Виконавець	Регламент робіт	Терміни/період
Проведення занять з персоналом ІТС щодо виконання вимог політики безпеки в установі	Служба захисту	Згідно «Плану навчання в установі»	щоквартально
Формування в трудовій угоді розділу відповідальності за виконання вимог політики безпеки	Служба захисту	Згідно вимог трудового законодавства	за рішенням керівника установи
Перевірка стану захисту інформації	Перевірка стану захисту інформації	Згідно «Положення про захист інформації»	щорічно



Контрольно-профілактичні заходи₄

Заходи	Виконавець	Регламент робіт	Терміни/період
Контроль працездатності та виконання вимог політики безпеки	Системний адміністратор	Перевірка справності ОС і ПЗ ІТС	щодня
	Адміністра-тор безпеки	Перевірка виконання вимог політики безпеки користувачами	щомісячно
	Служба захисту	Перевірка виконання політики безпеки адміністраторами	щоквартально
Перевірка наявності МНІ	Комісія установи	Згідно «Інструкції про організацію діловодства»	щорічно



Інженерно-технічні заходи₁

□ **Інженерно-технічні заходи** - це комплекс заходів, спрямованих на налагодження, випробування і введення в експлуатацію, супроводження і технічне обслуговування апаратних і програмних засобів захисту інформації в ІТС, інженерне обладнання споруд і приміщень, в яких розміщуються засоби ІТС.



Інженерно-технічні заходи₂

Заходи	Виконавець	Регламент робіт	Терміни/період
Супровід КСЗІ	Розробник КСЗІ	Гарантійне обслуговування	Гарантійний термін
Технічне обслуговування ІТС	Адміністратори	Згідно «Регламенту техобслуговування»	згідно термінів регламенту
Резервування баз даних і фондів	Адміністратор безпеки	Згідно «Інструкції з резервування баз даних»	щомісячно



Інженерно-технічні заходи₃

Заходи	Виконавець	Регламент робіт	Терміни/період
Поновлення антивірусних баз	Адміністратор безпеки	Згідно «Інструкції з антивірусного захисту»	щодня
Перевірка МНІ і ІТС на наявність вірусів	Користувач (МНІ)	Згідно «Інструкції з антивірусного захисту»	щодня
	Адміністратори (ІТС)		щотижня
Модернізація КСЗІ	Модернізація КСЗІ	Заміна (додавання) окремих компонентів КСЗІ	згідно плану розвитку КСЗІ



Кадрові заходи₁

□ **Кадрові заходи** - це комплекс навчально-педагогічних заходів, спрямованих на розширення світогляду та підвищення професійної майстерності персоналу ІТС, що визначається її особливостями та технологіями захисту інформації, які використовуються в ній.



Кадрові заходи₂

Заходи	Виконавець	Регламент робіт	Термін/період
Вступне ознайомлення з положеннями політики безпеки інформації (під розпис)	Служба захисту	Оформлення допуску до роботи	після прийому на роботу
	Адміністратор безпеки	Згідно «Інструкції користувачу»	під час їхньої реєстрації в ІТС
Інструктаж користувачів щодо дій у випадку позаштатної ситуації	Адміністратор безпеки	Згідно «Плану робіт у випадку позаштатної ситуації»	щорічно



Кадрові заходи₃

Заходи	Виконавець	Регламент робіт	Термін/період
Проведення занять з професійної підготовки персоналу ІТС	Служба захисту Адміністратори	Згідно «Плану професійної підготовки в установі»	щотижня
Направлення на курси підвищення кваліфікації	Служба захисту	Згідно «Плану підвищення кваліфікації в установі»	згідно термінів плану



Кадрові заходи₄

- Виконання Календарного плану забезпечується Службою захисту інформації в ІТС, 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;



Кадрові заходи₅

- вжиття заходів у разі виявлення спроб НСД до ресурсів ІТС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;
- забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;
- організація керування доступом до ресурсів ІТС ;
- супроводження та актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об'єктів, ідентифікатори користувачів тощо);



Кадрові заходи₆

- спостереження за функціонуванням КСЗІ та її компонентів;
- підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в ІТС, впровадження нових технологій захисту і модернізації КСЗІ;
- організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІТС або КСЗІ;
- участь в роботах з модернізації ІТС - узгодженні пропозицій з введення до складу ІТС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;



Кадрові заходи₇

- забезпечення супроводження і актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;
- проведення аналітичної оцінки поточного стану безпеки інформації в ІТС;
- інформування власників інформації про технічні можливості захисту інформації в ІТС і типові правила, встановлені для персоналу і користувачів ІТС;
- негайне втручання в процес роботи ІТС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;



Кадрові заходи₈

- регулярне подання звітів керівництву організації про виконання користувачами ІТС 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 ІТС;



Кадрові заходи₉

- участь в організації і проведенні навчання користувачів і персоналу ІТС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;
- участь в організації забезпечення навчального процесу необхідною матеріальною базою, нормативно-правовими актами, нормативними документами, тощо;
- контроль за виконанням персоналом і користувачами ІТС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації;



Кадрові заходи₁₀

- контроль за забезпеченням охорони і порядку зберігання документів , 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



Супровід КСЗІ₁

- ❑ Супровід КСЗІ забезпечується виконанням вимог інструкцій та веденням журналів, які були розроблені при введенні КСЗІ в експлуатацію.
- ❑ До складу супровідної документації КСЗІ входять:
 - інструкції щодо забезпечення правил оброблення ІзОД в ІТС;
 - інструкції співробітників СЗІ, персоналу та користувачів ІТС;
 - технологічні інструкції щодо адміністрування та обслуговування КСЗІ;
 - інструкція про порядок використання криптографічних засобів;
 - інструкція про порядок супроводження та модернізації КСЗІ;
 - інструкція про порядок резервування інформаційних ресурсів ІТС;



Супровід КСЗІ₂

- порядок обліку і супроводження архівів та ротації носіїв інформації;
- інструкція про порядок оперативного відновлення функціонування ІТС;
- інструкція про організацію контролю за функціонуванням КСЗІ;
- інструкція про порядок проведення ремонтних робіт.
- порядок розробки, впровадження та модернізації ПЗ ІТС;
- правила видачі, вилучення та обліку персональних ідентифікаторів;
- правила управління паролями в ІТС;
- правила класифікації та класифікатор інформації і користувачів ІТС;



Супровід КСЗІ₃

- формуляр (паспорт) ІТС;
- журнали, які використовуються для реєстрації фактів та результатів виконання певних завдань з адміністрування та обслуговування КСЗІ.



Супровід КСЗІ₄

- ❑ Перелік та форми реєстраційних журналів повинні відповідати визначеним у технологічних інструкціях щодо виконання завдань з адміністрування та обслуговування КСЗІ.
- ❑ Як приклади реєстраційних журналів можна розглядати такі:
 - обліку користувачів ІТС;
 - обліку роботи користувачів ІТС;
 - обліку захищених інформаційних ресурсів ІТС;
 - реєстрації проведених робіт з технічного обслуговування, ремонту, модернізації;
 - реєстрації перевірок складу програмних засобів ІТС;
 - реєстрації позаштатних ситуацій у роботі ІТС.



Супровід КСЗІ₅

- ❑ Якщо в ІТС передбачається оброблення службової інформації, під час функціонування ІТС використовуються журнали, форми та правила ведення яких встановлені «Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію», затвердженою постановою Кабінету Міністрів України від 27.11.98 № 1893.
- ❑ Зокрема, необхідно вести такі журнали обліку службової інформації:
 - обліку документів та видань з грифом «ДСК»;
 - обліку машинних носіїв інформації з грифом «ДСК».



Супровід КСЗІ₆

- ❑ Якщо в ІТС передбачається оброблення секретної інформації, під час функціонування ІТС використовуються такі журнали, форми та правила ведення яких встановлені «Порядком організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях», затвердженим постановою Кабінету Міністрів України від 02.10.2003 № 1561-12.
- ❑ Зокрема, необхідно вести такі журнали обліку секретної інформації:
 - обліку сховищ матеріальних носіїв секретної інформації та ключів від них;
 - здавання (приймання) з-під охорони режимних приміщень, сховищ матеріальних носіїв секретної інформації та ключів від них;
 - обліку вхідних і підготовлених секретних документів;
 - обліку робочих зошитів, спецблокнотів, окремих аркушів і бланків.



Обов'язки адміністратора КСЗІ₁

□ Адміністратор безпеки під час супроводу КСЗІ зобов'язаний:

- контролювати встановлення ПЗ, його працездатність та оновлення, конфігурування політики безпеки ІТС;
- забезпечувати конфігурування КЗЗ, ПЗ для захисту інформації, налагодження антивірусного ПЗ та елементів ІТС, які мають вбудовані функції захисту;
- забезпечувати надійне функціонування КЗЗ і ПЗ для захисту інформації, антивірусного ПЗ та контролювати його працездатність;
- встановлювати в ІТС обмежені права доступу до операційної системи та «BIOS»,
- визначати користувачів, їх ідентифікатори та паролі, встановлювати користувачам захищені каталоги;



Обов'язки адміністратора КСЗІ₂

- керувати обліковими записами та атрибутами користувачів,
- керувати правами доступу к захищеним каталогам з боку користувачів і програмних засобів;
- керувати рівнями конфіденційності та квотами на використання дискового простору ІТС;
- відновлювати роботу засобів захисту у разі їх збоїв або виходу з ладу;
- брати участь у впровадженні заходів захисту інформації в ІТС та здійснювати контроль умов використання ІТС відповідно до експлуатаційної документації та вимог приписів на експлуатацію об'єктів ІТС;
- здійснювати адміністрування в частині захисту інформації та оновлення баз даних захисту ІТС;



Обов'язки адміністратора КСЗІ₃

- забезпечувати проведення технічного обслуговування та контролю за функціонуванням засобів захисту інформації;
- здійснювати опечатування вузлів, блоків, усіх портів ІТС та щоденний контроль за його станом;
- проводити поточний контроль за забезпеченням режиму обробки та захисту інформації в ІТС згідно затвердженої інструкції;
- проводити інструктаж та навчання персоналу з питань дотримання вимог забезпечення режиму обробки та захисту інформації в ІТС;
- здійснювати контроль за роботою користувачів та виконанням ними вимог щодо захисту інформації шляхом періодичних спостережень за діями користувачів під час роботи в ІТС (вибірково);
- здійснювати контроль за проведенням робіт з ремонту та заміни технічних засобів ІТС або комплексу ТЗІ;
- вносити пропозиції та брати участь у проектуванні, створенні та дослідній експлуатації КСЗІ в ІТС;
- доповідати керівнику СЗІ про всі виявлені порушення режиму обробки та захисту інформації в ІТС.



Обов'язки системного адміністратора

КСЗІ₁

□ Системний адміністратор під час супроводу КСЗІ зобов'язаний:

- встановлювати та налаштовувати ОС та необхідне для роботи апаратне й програмне забезпечення (далі - АПЗ);
- встановлювати на ІТС сертифіковане антивірусне програмне забезпечення (далі - ПЗ) та оновлювати його бази даних, після чого перевіряти ІТС на наявність комп'ютерних вірусів;
- підтримувати робочий стан ОС і АПЗ ІТС та контролювати їх працездатність;
- навчати користувачів роботі на ІТС і формуванню її інформаційного фонду;
- зберігати еталони ПЗ та резервні копії інформаційних фондів ІТС для відновлення її роботи після аварійних ушкоджень або ураження комп'ютерними вірусами;
- вести та оновлювати фонд дозволеного до використання ПЗ ІТС, щорічно проводити його інвентаризацію;
- щомісячно контролювати копіювання інформаційних фондів ІТС на зареєстровані зовнішні носії інформації згідно затвердженої інструкції;



Обов'язки системного адміністратора КСЗІ₂

- оперативно відновлювати працездатність ІТС при збоях і виході з ладу ОС і АПЗ ІТС згідно затвердженої інструкції;
- брати участь у проведенні інвентаризації ІТС;
- здійснювати контроль за проведенням ремонту та монтажу устаткування ІТС фахівцями сторонніх організацій;
- виявляти помилки користувачів та проводити їх інструктаж;
- готувати пропозиції з модернізації та придбання ІТС, АПЗ, розвитку автоматизації обробки даних;
- готувати пропозиції до планів роботи підрозділів стосовно заходів із забезпечення надійного та безперебійного функціонування ІТС;
- інформувати керівника СЗІ про випадки порушень правил експлуатації ІТС та обробки інформації.



Обов'язки користувача КСЗІ₁

□ Користувач під час супроводу КСЗІ зобов'язаний:

- використовувати надані інформацію ідентифікації та автентифікації (пароль) виключно для роботи з ІТС;
- зберігати особистий пароль (інформацію автентифікації) в таємниці, негайно інформувати адміністратора безпеки та безпосереднього начальника про факти компрометації (втрати, розголошення) паролю, при введенні пароля забезпечувати захист паролю від несанкціонованого спостереження іншими посадовими особами;
- виконувати вимоги нормативно-правових актів у сфері захисту інформації та НД ТЗІ щодо порядку поводження з МНІ та документами в електронному вигляді;
- при залишенні робочого місця на тривалий час здійснювати заходи щодо переведення системи в режим блокування;



Обов'язки користувача КСЗІ₁

- формувати перелік та періодично (щомісячно) здійснювати з залученням адміністратора ІТС резервне копіювання на з'ємні носії інформації, яка важлива для забезпечення службової діяльності установи;
- спільно з адміністратором ІТС визначати «папки» (файли) зі службовою інформацією, розпорядником якої є користувач, для встановлення аудиту прав доступу;
- негайно інформувати адміністратора про відхилення в нормальній роботі ІТС, системного та прикладного ПЗ, виходу із ладу або нестійкого функціонування технічних засобів ІТС, а також порушення цілісності або невідповідності печаток (пломб) вузлів та блоків, портів введення-виведення інформації технічних засобів ІТС.



Контроль обробки ІзОД в ІТС

- ❑ Складовою супроводу КСЗІ є контроль за забезпеченням режиму під час обробки ІзОД в ІТС, який полягає у перевірці виконання персоналом ІТС вимог нормативно-правових актів з питань збереження ІзОД і нормативних документів з технічного та криптографічного захисту інформації.
- ❑ Контроль обробки ІзОД в ІТС здійснюється шляхом:
 - планових перевірок;
 - позапланових перевірок;
 - повсякденного контролю.



Планові та позапланові перевірки₁

- ❑ Планові перевірки здійснюються комісіями, до складу яких входять начальники РСО і підрозділу ТЗІ, співробітники СЗІ та представники інших підрозділів установи. Головою комісії призначається керівник СЗІ. Підстави проведення перевірки, строки роботи і склад комісії, а також перелік об'єктів ІТС, які підлягають перевірці, зазначаються в наказі керівника установи.
- ❑ Позапланові перевірки здійснюються у разі наявності відомостей щодо порушень виконання вимог «Інструкції щодо забезпечення правил оброблення ІзОД в ІТС», НД ТЗІ та інших нормативно-правових актів у сфері захисту інформації. Вони організовуються СЗІ та здійснюються комісіями, до складу яких входять начальники РСО і підрозділу ТЗІ, співробітники СЗІ та представники інших підрозділів установи.



Планові та позапланові перевірки₂

- ❑ Планова або позапланова перевірка проводиться у присутності начальника підрозділу установи, в якому проводиться перевірка, або особи, яка його заміщає, представника СЗІ та співробітника, відповідального за користування об'єкта ІТС.
- ❑ Під час планових та позапланових перевірок перевіряється:
 - дотримання користувачами ІТС встановлених вимог щодо забезпечення режиму обробки та захисту ІзОД;
 - комплектація ІТС згідно з Формуляром;
 - наявність та дотримання вимог приписів на експлуатацію об'єктів ІТС;
 - виконання заходів щодо забезпечення захисту ІзОД від НСД на відповідність вимогам технічної та експлуатаційної документації, згідно з якими здійснюється експлуатація ІТС;



Планові та позапланові перевірки₃

- відповідність ступеня обмеження доступу інформації, яка обробляється з використанням ІТС, наданій категорії об'єкта ІТС;
- відповідність ступеня обмеження доступу інформації, яка зберігається на машинних носіях даних, грифу обмеження доступу машинних носіїв даних;
- наявність атестата відповідності КСЗІ вимогам НД ТЗІ, організаційно-технічних документів та експлуатаційної документації.



Планові та позапланові перевірки₄

- ❑ За результатами перевірки складається акт, в якому зазначаються результати оцінки відповідності забезпечення режиму обробки та захисту ІзОД в ІТС вимогам НД ТЗІ та інших нормативно-правових актів у сфері захисту інформації, виявлені недоліки та рекомендації щодо їх усунення. Акт затверджується керівником установи, після чого з ним ознайомлюється начальник підрозділу, в якому проводилася перевірка.
- ❑ Акт направляється в установленому порядку вищестоящому органу згідно з підпорядкованістю установи та регіональному органу Держспецзв'язку на його вимогу.



Повсякденний контроль забезпечення режиму роботи

- ❑ Повсякденний контроль за забезпеченням режиму під час обробки інформації в ІТС здійснюється СЗІ. Порядок його проведення та усунення виявлених недоліків або порушень вимог НД ТЗІ та інших нормативно-правових актів у сфері захисту 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 ІТС державних установ



Особливості супроводу КСЗІ в ІТС державних установ₁

- ❑ 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.



Особливості супроводу КСЗІ в ІТС державних установ₂

- Згідно з цим Порядком органи державної влади, органи місцевого самоврядування, утворені відповідно до законів України військові формування, підприємства, установи і організації державної форми власності зобов'язані:
- не менше ніж раз на день отримувати антивірусні оновлення АВПЗ за допомогою веб-серверу ЦАЗІ;
 - інсталювати отримані за допомогою веб-серверу ЦАЗІ антивірусні оновлення АВПЗ відповідно до технічної документації АВПЗ;
 - для забезпечення авторизованого доступу до ресурсів веб-серверу ЦАЗІ щороку до 1 березня та, у разі внесення змін, протягом 3 днів надавати до Адміністрації Держспецзв'язку відомості щодо кожного користувача у паперовому вигляді за визначеною формою.



Особливості супроводу КСЗІ в ІТС державних установ_з

❑ Крім того, всі міністерства, інші центральні органи виконавчої влади, обласні державні адміністрації, а також підприємства, установи та організації, що належать до сфери їх управління, (далі – державні органи) подають відомості про створені ІТС, у тому числі, і АС класу «1», до Адміністрації Держспецзв'язку згідно вимог «Положення про Реєстр ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління», затвердженого постановою КМ України від 03.08.2005 № 688 із останніми змінами згідно постанови КМ України від 07.09.2011 № 938.



Особливості супроводу КСЗІ в ІТС державних установ₄

□ Це Положення визначає порядок утворення та функціонування Реєстру ІТС державних органів (далі - Реєстр), ведення якого забезпечує Адміністрація Держспецзв'язку як Адміністратор Реєстру згідно вимог **«Порядку формування й користування інформаційним фондом Реєстру ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління»**, затверджений наказом Адміністрації Держспецзв'язку від 24.04.2007 № 72, зареєстрований в Міністерстві юстиції України 14.05.2007 за № 500/13767, із змінами згідно наказу Адміністрації Держспецзв'язку від 06.08.2012 № 425, зареєстрованого в Міністерстві юстиції України 22.08.2012 за № 1412/21724.



Особливості супроводу КСЗІ в ІТС державних установ₅

□ Цей Порядок визначає види та форми надання відомостей до інформаційного фонду Реєстру ІТС державних органів (далі - Інформаційний фонд) та правила користування ним. Відомості про ІТС подаються ще на стадії технічного проектування систем, а у разі модернізації функціонуючих ІТС - на стадії створення КСЗІ в цих системах. У разі введення в експлуатацію або припинення функціонування ІТС відповідний державний орган у 10-денний строк повідомляє про це адміністратора Реєстру.



Особливості супроводу КСЗІ в ІТС державних установ₆

- ❑ Відомості до Інформаційного фонду подаються на оптичних носіях типу CD-R із супровідним листом за підписом керівника державного органу. Після впровадження в державному органі електронно-цифрового підпису зазначені відомості надаються з додержанням вимог чинного законодавства в електронному вигляді мережами передачі даних або надсилаються поштою на електронних носіях інформації. Носії інформації адресату не повертаються.
- ❑ Державні органи двічі на рік (станом на 1 січня - до 1 лютого та станом на 1 липня - до 1 серпня) надають Адміністратору Реєстру узагальнені відомості про власні ІТС. Надалі в ті ж самі терміни державними органами надсилаються Адміністратору Реєстру відомості лише про ІТС, у яких відбулися зміни з моменту останнього надання інформації про них.

Донецький національний технічний університет



Тема 8. Системи захисту інформації для різних автоматизованих систем.

Лекція 14. Побудова і структура гарантій реалізації послуг безпеки та вимоги щодо захисту інформації від НСД в автоматизованих системах (АС) класу 1.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

581

- ☐ Побудова і структура гарантій реалізації послуг безпеки
- ☐ Вимоги щодо захисту інформації від НСД в автоматизованих системах (АС) класу 1
- ☐ Приклад політики послуг безпеки ФПЗ



Побудова і структура гарантій реалізації послуг безпеки



Рівні гарантій

- ❑ Рівні гарантій функціональних послуг безпеки, їх структура і семантичне позначення наведені в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».
- ❑ В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації.
- ❑ З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю та доступністю. Виходячи з цього, кожний клас АС ($X=1,2,3$) поділяється на підкласи, які визначають підвищені вимоги до забезпечення однієї чи декілька цих властивостей.



Класи, підкласи

□ Кількість сполучень з трьох властивостей зумовлює наявність семи груп підкласів АС:

- 1) підклас Х.К - конфіденційності інформації;
- 2) підклас Х.Ц - цілісності інформації;
- 3) підклас Х.Д - доступності інформації;
- 4) підклас Х.КЦ - конфіденційності та цілісності інформації;
- 5) підклас Х.КД - конфіденційності та доступності інформації;
- 6) підклас Х.ЦД - цілісності та доступності інформації.
- 7) підклас Х.КЦД - конфіденційності, цілісності та доступності інформації.

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



Стандартний функціональний профіль захищеності (СФПЗ)₁

- НД ТЗІ 2.5-005-99 «Класифікація АС і стандартні функціональні профілі захищеності оброблюваної інформації від НСД» вводить таке поняття як **«стандартний функціональний профіль захищеності»** (далі - СФПЗ). Він являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.
- Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних СФПЗ, яка може бути різною для кожного класу і підкласу АС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (К, Ц і Д). Зростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.



Стандартний функціональний профіль захищеності (СФПЗ)₂

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



Визначення ФПЗ

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

- усі АС можна віднести до одного з трьох класів за наступними ознаками: конфігурація апаратних засобів, їх фізичне розміщення, кількість категорій оброблюваної інформації, кількість користувачів і категорій користувачів;
- у межах класу АС можна віднести до одного з підкласів, що визначені за критерієм необхідності забезпечення К, Ц і Д;
- вимоги до безпеки АС різних класів суттєво відрізняються, що дозволяє сформулювати для їх підкласів множини СФПЗ, що знаходяться у ієрархічній залежності;
- для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної ІТС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.



Кількість СФПЗ для підкласів АС

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



Етапи визначення ФПЗ

□ Стандартний підхід визначення ФПЗ вимагає таких етапів:

1. Визначення підкласу АС.
2. Визначення призначення АС та вибір підказки, яку треба використовувати у цьому випадку для вибору одного із СФПЗ, використовуючи довідковий додаток «А» з НД ТЗІ 2.5-005-99. Якщо призначення АС відрізняється від наведених у НД ТЗІ 2.5-005-99 необхідно власноруч обрати підмножину СФПЗ відповідно до підкласу АС.
3. Аналіз сутності вимог, відібраних СФПЗ.
4. Вибір одного із СФПЗ, який найбільш відповідає політиці безпеки.
5. У випадку, коли жоден із СФПЗ не підходить повною мірою, необхідно змінити рівень послуги, що міститься у СФПЗ, або додати нову послугу.



Ідентифікатор профіля

- ❑ Згідно НД ТЗІ 2.5-005-99 кожний профіль має свій буквено-числовий ідентифікатор, який включає:
 - номер класу АС (1 - ПЕОМ, 2 - ЛОМ, 3 - РОМ),
 - букви, що характеризує види загроз, від яких забезпечується захист (К, Ц, Д),
 - номер профілю.
- ❑ Всі частини ідентифікатора відділяються один від одного крапкою.
- ❑ Наприклад, СФПЗ АС класу «2» номер 1 з підвищеними вимогами до забезпечення конфіденційності інформації виглядає таким чином:
 - $2.K.1 = \{ KD-2, NP-2, NI-2, NK-1, NO-1, NC-1 \}$
- ❑ А СФПЗ АС класу «1» номер 2 з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності інформації виглядає таким чином:
 - $1.KCD.2 = \{ KA-1, KO-1, CA-1, CO-1, DP-1, DV-1, NP-2, NI-2, NK-1, NO-1, NC-1, NT-1 \}$



Найскладніший профіль

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



Сутність ФПЗ

- ❑ ФПЗ по суті є варіантом технічної реалізації системи захисту інформації. За рахунок реалізації певного ФПЗ забезпечується виконання політики безпеки ІТС й зменшення збитку, що завдається АС впливом загроз. Вирішення завдання вибору оптимального ФПЗ включає формування множини припустимих варіантів ФПЗ, визначення сукупності показників якості та критерію оптимальності, а також вибір варіантів ФПЗ, оптимальних за цим критерієм.
- ❑ Завданням розробника КСЗІ є обстеження властивостей конкретної АС, як об'єкта захисту та вибір необхідного СФПЗ із списку, наведеного у НД ТЗІ 2.5-005-99. У випадку, коли жоден з наявних СФПЗ не підходить до конкретної АС, розробник має створити свій, найбільш придатний для нього ФПЗ, обґрунтувати й затвердити його.



Вимоги щодо захисту інформації від НСД в автоматизованих системах (АС) класу 1



АС клас 1

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



Типові умови функціонування АС

□ Умови функціонування будь-якої АС визначаються такими її складовими:

- обчислювальна система,
- фізичне середовище,
- середовище користувачів,
- інформація, що обробляється,
- технології обробки інформації.



Характеристика обчислювальної системи

❑ Обчислювальна система А складається з:

- стандартної ПЕОМ з периферійними пристроями введення, виведення, накопичення та відображення інформації (системний блок, клавіатура, монітор, миша, принтер тощо);
- ПЗ (системного та спеціалізованого для обробки інформації);
- КЗЗ від НСД (у тому числі антивірус).

❑ Склад апаратного та програмного забезпечення АС вказується у формулярі АС.

❑ Типові умови функціонування обчислювальної системи вимагають таке:

- ПЗ має відповідним чином оформлену ліцензію на право його легального використання;
- КЗЗ від НСД (у тому числі антивірус) має відповідним чином оформлений експертний висновок або сертифікат, який свідчить про відповідність КЗЗ вимогам НД ТЗІ;
- у разі обробки інформації, що становить державну таємницю, комплекс ТЗІ, який забезпечує захист інформації від витоку технічними каналами, має акт атестації, оформлений згідно вимог НД ТЗІ.



Характеристика фізичного середовища

❑ До фізичного середовища відноситься:

- приміщення, де розташована АС з усіма її компонентами (обчислювальна система, сховище носіїв інформації та ПЗ, робочі місця користувача та обслуговуючого персоналу);
- всі технічні засоби, встановлені в цьому приміщенні (засоби комунікації, сигналізації, електроживлення, заземлення, кондиціонування та побутові прилади).

❑ Типові умови функціонування АС стосовно фізичного середовища вимагають таке:

- у приміщенні, де розташована АС з усіма її компонентами, запроваджений режим обмеження та контролю доступу згідно вимог діючого законодавства;
- у разі обробки інформації, що становить державну таємницю, всі технічні канали витоку інформації з АС блоковані засобами ТЗІ.



Характеристика середовища користувачів₁

- ❑ За рівнем повноважень доступу до інформації, характером та змістом робіт, які виконуються в процесі функціонування АС, суб'єкти, що мають доступ до АС, поділяються на такі групи:
 - користувач, що має повноваження доступу до КЗЗ від НСД (адміністратор безпеки);
 - користувачі, що мають повноваження доступу до інформації, що обробляється в АС;
 - персонал, що забезпечує працездатність АС;
 - персонал, що обслуговує приміщення, де розташована АС.
- ❑ Повноваження користувачів першої та другої груп повинні бути фізично розділені, тобто виконуватися різними особами. Допускається виконання адміністратором безпеки додаткових функцій системного адміністратора.



Характеристика середовища користувачів₂

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

- усі користувачі допущені до інформації, що обробляється в АС;
- доступ користувачів до службової інформації дозволяється після ознайомлення під розпис з вимогами «Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» (ПКМУ від 27.11.98 № 1893);
- доступ користувачів до інформації, що становить державну таємницю, дозволяється лише у разі наявності відповідного допуску згідно вимог «Порядок організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях» (ПКМУ від 02.10.2003 № 1561-12).



Характеристика інформації, що обробляється в АС

□ Інформація згідно вимог захисту поділяється на такі групи:

- дані у вигляді файлів різних форматів, записів баз даних та інших структур машинного представлення (далі - дані), які містять ІЗОД;
- дані, які не містять ІЗОД;
- бази даних захисту (списки зареєстрованих користувачів, їх ідентифікаторів і повноважень, матриці доступу, журнали обліку тощо);
- дані, захищені ліцензійними умовами використання та розповсюдження, або такі, що належать деяким групам та окремим користувачам.

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

- дані, які входять до бази даних захисту, повинні бути віднесені до ІЗОД із встановленням ступеня обмеження, не нижчим ступеня обмеження інформації, що обробляється в АС;
- реєстрація, обіг, зберігання та знищення ІЗОД здійснюються згідно вимог діючого законодавства та відомчих інструкцій.



Характеристика технологій обробки інформації

- ☐ ІзОД під час обробки в АС повинна мати атрибути з визначенням встановленого ступеня її обмеження відповідно до вимог діючого законодавства. Машинні носії, на які виводиться ІзОД, повинні мати встановлені відповідно до порядку забезпечення режиму обмеження реквізити.
- ☐ Технології обробки ІзОД в АС вимагають реєстрацію її носіїв, видачу їх користувачу під розпис і зберігання в металевому сховищі. Якщо на носії зберігаються дані різних ступенів обмеження, гриф обмеження носія повинен відповідати вищому ступеню обмеження даних, що на ньому зберігаються.
- ☐ Технології обробки інформації залежать від повноважень доступу користувачів до даних, розміщених на носії інформації, до якого вони мають доступ:
 - 1) всі користувачі мають однакові повноваження;
 - 2) користувачі мають різні повноваження, що ускладнює функціональний профіль захищеності (далі - ФПЗ) АС.



Визначення ФПЗ₁

- ☐ Для умов середовищ АС можна визначити ФПЗ - мінімальний перелік послуг безпеки, які, за умови впровадження комплексу необхідних організаційних заходів, є функціонально достатніми для виконання завдань захисту інформації в АС.
- ☐ Сукупність цих послуг забезпечує підтримання програмно-апаратними засобами АС процедур автентифікації користувачів АС, адміністративного розмежування доступу користувачів до даних, що зберігаються на носіях інформації, а також процедур контролю за діями користувачів із цими об'єктами.
- ☐ На даний час у системі НД ТЗІ відсутній документ, що встановлює вимоги до КЗЗ від НСД в АС, де обробляється відкрита або конфіденційна інформація. Разом з тим, загальні вимоги захисту інформації висуваються «Правилами забезпечення захисту в ІТС», затвердженими ПКМУ від 29.03.2006 № 373 (далі - Правила). Тому вихідні дані для визначення ФПЗ отримуємо з цих Правил.



Визначення ФПЗ₂

□ Пункт 5 Правил висуває такі вимоги:

1. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією, що вимагає наявності послуги використання ресурсів (ДР).
2. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. Це вимагає наявності послуг ідентифікації і автентифікації (НИ) і адміністративної цілісності (ЦА).
3. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень або не підтверджені під час автентифікації пред'явленим ідентифікатором повинні блокуватися. Це вимагає наявності послуги «одиначна ідентифікація і автентифікація» (НИ-2), для якої потрібна також послуга «однонаправлений достовірний канал» (НК-1).



Визначення ФПЗ₃

□ Пункт 11 Правил висуває такі вимоги:

1. У системі здійснюється обов'язкова автоматична реєстрація небезпечних для ІТС подій, що вимагає наявності послуги реєстрації (НР).
2. Реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки, що вимагає наявності послуги «захищений журнал» (НР-2).
3. Забезпечується можливість проведення аналізу реєстраційних даних виключно спеціально уповноваженим користувачем, що вимагає наявності послуги виділення адміністратора (НО-1).



Визначення ФПЗ₄

□ Пункт 15 Правил висуває такі вимоги:

1. У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. Це вимагає наявності послуг самотестування (НТ), відкату (ЦО) і відновлення після збоїв (ДВ).
2. Контролюється також цілісність програмних та технічних засобів захисту інформації, а у разі порушення їх цілісності обробка інформації в системі припиняється. Це вимагає наявності послуги цілісності КЗЗ (НЦ).



Визначення ФПЗ₅

- ❑ За умови наявності лише користувачів з однаковими повноваженнями доступу до інформації послуги безпеки базуються на довірчому розмежуванні доступу (КД і ЦД).
- ❑ Виходячи з вище зазначеного, виписуємо всі визначені послуги безпеки в один рядок і обираємо схожий СФПЗ із НД ТЗІ 2.5-005-99 для АС класу 1. В результаті отримуємо необхідний СФПЗ для оброблення в АС відкритої інформації з мінімальними вимогами до забезпечення її цілісності та доступності:
 - 1.ЦД.1 = { ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }
- ❑ А СФПЗ у разі оброблення службової інформації повинен мати мінімальні вимоги до забезпечення не тільки цілісності та доступності інформації, а ще її конфіденційності.



Визначення ФПЗ₆

□ Пункт 6 Правил висуває такі вимоги:

- Під час обробки службової інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення. У системі забезпечується можливість надання користувачу права на обробку службової інформації або позбавлення його такого права. Це вимагає наявності послуг адміністративної конфіденційності (КА) та повторного використання об'єктів (КО-1).
- Виходячи з вище зазначеного, додаємо до СФПЗ 1.ЦД.1 послуг адміністративної конфіденційності (КА) та повторного використання об'єктів (КО-1) і в результаті отримаємо СФПЗ для обробки в АС службової інформації з мінімальними вимогами до забезпечення її конфіденційності, цілісності та доступності:
 - 1.КЦД.1 = { КА-1, КО-1, ЦА-1, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }
- У випадку, коли усі користувачі допущені до обробки службової інформації в АС, реалізація послуги повторного використання об'єктів (КО-1) необов'язкова. А у разі наявності користувачів, що допущені до обробки лише відкритої інформації в АС, її реалізація обов'язкова.



Приклад політики послуг безпеки ФПЗ



Політика послуг безпеки ФПЗ₁

№2	Загальні вимоги щодо захисту інформації	ІТЗ	ОЗ	ФПЗ	Windows 8 Professional	Windows Server 2012 R2
1.	Захист від несанкціонованого					
	ознайомлення	+	=	КА-1 КО-1 ДВ-1	- КО-1 ДВ-2	- КО-1 ДВ-2
	розмноження		+			
	розповсюдження	+	+			
	копіювання	+	+			
	відновлення		+			
	спотворення	+	=	ЦА-1	-	-
2.	Надання доступу до ІзОД за умови достовірного розпізнавання користувачів		=	НК-1 НИ-2	НК-1 НИ-2	НК-1 НИ-2
	з урахуванням наданих згідно з службовою необхідністю повноважень		=	КА-1 НО-1	- НО-3	- НО-3
3.	Надання можливості своєчасного доступу зареєстрованих користувачів АС до ІзОД		=	НЦ-1 НТ-1 ДВ-1	НЦ-2 НТ-2 ДВ-2	НЦ-2 НТ-2 ДВ-2
4.	Контроль цілісності КЗЗ, а у разі її порушення припиняти обробку інформації		=	НЦ-1	НЦ-2	НЦ-1
5.	Забезпечення реєстрації дій всіх користувачів АС щодо обробки ІзОД		=	НР-2	НР-2	НР-2
	Забезпечення захисту реєстраційних даних від модифікації користувачами, які не мають адмін. повноважень		=	НР-2 НО-1	НР-2 НО-3	НР-2 НО-3



Політика послуг безпеки ФПЗ₂

№	Загальні вимоги щодо захисту інформації	ІТЗ	ОЗ	ФПЗ	Windows 8 Pro-fessional	Windows Server 2012 R2
6.	Блокування доступу до ІзОД у разі порушення політики безпеки		=	НК-1 НИ-2	НК-1 НИ-2	НК-1 НИ-2
7.	Встановлення ступеня обмеження ІзОД під час її обробки в АС		+			
8.	Встановлення адміністратором обмежень на використання ресурсів користувачами			ДР-1	ДР-1	ДР-1
9.	Можливість модифікації та знищення ІзОД користувачами, яким надано відповідні повноваження		=	ЦА-1 НИ-2	- НИ-2	- НИ-2
10	Контроль цілісності ПЗ, що забезпечує обробку ІзОД, запобігання його несанкціонованій модифікації та ліквідація наслідків такої модифікації		=	НТ-1 ЦО-1 ДВ-1	НТ-2 ЦО-1 ДВ-2	НТ-2 ЦО-1 ДВ-2
12	Забезпечення рівня гарантій реалізації ПБ			Г2	Г2	Г2

Донецький національний технічний університет



Тема 8. Системи захисту інформації для різних автоматизованих систем.

Лекція 15. Особливості захисту секретної інформації в АС класу 1.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

612

- ☐ Загальна характеристика технічних каналів витоку інформації, що обробляється в АС
- ☐ Захист інформації в АС від витоку каналами ПЕМВН
- ☐ Створення комплексу технічного захисту інформації



Загальна характеристика технічних каналів витоку інформації, що обробляється в АС



Витік інформації

- ❑ Інформація, що становить державну таємницю та обробляється технічними засобами (у тому числі АС), згідно вимог НД ТЗІ підлягає захисту від витоку технічними каналами. Захист іншої ІзОД від витоку технічними каналами здійснюється за рішенням власника або розпорядника цієї інформації.
- ❑ Витік інформації по технічних каналах треба розуміти як неконтрольоване поширення інформативного сигналу від його джерела через фізичне середовище до технічного засобу, який здійснює перехоплення інформації.



Перехоплення інформації₁

- ☐ **Перехоплення інформації** - це неправомірне отримання інформації з використанням технічного засобу, який здійснює її виявлення та обробку. В результаті перехоплення інформації можливе неправомірне ознайомлення з нею або неправомірний запис її на носій.
- ☐ Разом з технічними засобами АС у приміщеннях, де вони встановлені, як правило, знаходяться ще інші технічні засоби і системи, які в обробці інформації безпосередньої участі не беруть.
- ☐ До них відносяться: системи і засоби автоматичного телефонного зв'язку; відеонагляду та сигналізації; сповіщення та кондиціонування; прийому програм радіомовлення і телебачення; засоби електронної оргтехніки тощо.
- ☐ Через приміщення, де встановлені технічні засоби АС, можуть проходити проводи та кабелі, що не відносяться до АС, та інші струмопровідні металоконструкції (металеві труби систем опалювання, водопостачання тощо), які називаються сторонніми провідниками.



Перехоплення інформації₂

- ❑ Електроживлення технічних засобів здійснюється від розподільчих пристроїв і силових щитів, які спеціальними кабелями з'єднуються з трансформаторною підстанцією міської електромережі.
- ❑ Усі технічні засоби, що живляться від електромережі та мають металевий корпус, повинні бути заземлені. Типова система заземлення включає загальний пристрій та кабель заземлення, шини і дроти, що з'єднують пристрій заземлення з технічними засобами.
- ❑ З'єднувальні лінії АС, сторонні провідники, а також лінії електроживлення та заземлення можуть виходити за межі контрольованої зони об'єкту (далі - КЗ), під якою розуміється простір (територія, будівля, частина будівлі), де виключено неконтрольоване перебування сторонніх осіб (відвідувачів, працівників комунальних служб тощо) та транспортних засобів.
- ❑ Межею КЗ може бути периметр території організації, що охороняється, а також огорожувальні конструкції будівлі або частини будівлі, що охороняється, якщо вона розміщена на території, що не охороняється.



Технічний канал витоку інформації

- ❑ При розгляді АС, як об'єкту захисту від витоку інформації по технічних каналах, його необхідно розглядати як об'єкт, що включає :
 - технічні засоби, що безпосередньо обробляють інформацію, разом з їх з'єднувальними лініями (під ними розуміють сукупність дротів і кабелів, що прокладаються між окремими елементами АС);
 - допоміжні технічні засоби і системи разом з їх з'єднувальними лініями;
 - сторонні провідники;
 - систему електроживлення;
 - систему заземлення.
- ❑ Сукупність джерела інформативного сигналу, технічного засобу, що здійснює перехоплення інформації, і фізичного середовища, в якому поширюється інформативний сигнал, називається технічним каналом витоку інформації (далі - ТКВІ).



Класифікація ТКВІ

- ❑ Залежно від природи утворення інформативного сигналу ТКВІ можна розділити на:
 - природні;
 - спеціально створювані.
- ❑ Природні ТКВІ утворюються ненавмисно за рахунок побічних електромагнітних випромінювань і наведень (далі - ПЕМВН) АС. Вони складаються з електромагнітних та електричних ТКВІ.
 - Електромагнітні ТКВІ утворюються за рахунок побічних електромагнітних випромінювань (далі - ПЕМВ), що виникають при обробці інформації в АС.
 - Електричні ТКВІ утворюються внаслідок наведень інформативних сигналів в лініях електроживлення, з'єднувальних лініях АС і сторонніх провідниках.
- ❑ Спеціально створювані ТКВІ утворюються навмисно шляхом впровадження в АС «закладних» електронних пристроїв перехоплення інформації та шляхом високочастотного (далі - ВЧ) опромінення АС.



Електромагнітні ТКВІ

□ Головними причинами виникнення електромагнітних ТКВІ в АС є:

- ПЕМВ, що виникають внаслідок протікання інформативних сигналів по елементах АС;
- модуляція інформативним сигналом ПЕМВ генераторних або підсилювальних блоків АС із-за паразитних зв'язків.

□ ПЕМВ виникають при таких режимах обробки інформації в АС:

- виведення даних на екран монітора;
- введення даних з клавіатури;
- запис даних на накопичувачі;
- зчитування даних з накопичувачів;
- обмін даними по каналах зв'язку;
- виведення даних на принтер;
- запис даних від сканера тощо.



Технічні засоби розвідки ПЕМВН

- ❑ При кожному режимі роботи АС виникають ПЕМВ, що мають свої характерні особливості. Діапазон можливих частот ПЕМВ АС може бути від 10 кГц до 2 ГГц.
- ❑ Для перехоплення ПЕМВ АС використовуються спеціальні стаціонарні, транспортні або ручні прийомні комплекси, які називаються технічними засобами розвідки побічних електромагнітних випромінювань і наведень (далі - ТЗР ПЕМВН).
- ❑ Типовий комплекс ТЗР ПЕМВН включає: спеціальний приймальний пристрій, ноутбук, спеціальне програмне забезпечення і широкодіапазонну спрямовану антену. Він може встановлюватися в будівлях або машинах, розташованих за межами КЗ.
- ❑ Найбільш небезпечним з точки зору витоку інформації режимом роботи АС є виведення інформації на екран монітора. Враховуючи широкий спектр ПЕМВ відеосистеми АС (більше 100 МГц) і їх незначний рівень, перехоплення зображень, виводимих на екран монітора, є досить важким завданням.



Дальність перехоплення ПЕМВ

- ❑ Дальність перехоплення ПЕМВ сучасних АС, як правило, не перевищує 50 метрів. Якість перехопленого зображення значно гірше якості зображення, що виводиться на екран монітора. Особливо важке завдання - перехоплення тексту, що виводиться на екран монітора та написаний дрібним шрифтом.
- ❑ Простір навкруги АС, за межами якого напруженість електромагнітного поля (далі - ЕМП) не перевищує допустимого (нормованого) значення, називається небезпечною зоною R2. Вона визначається інструментально-розрахунковим методом після спеціальних досліджень АС на наявність ПЕМВ і вказується в приписі на її експлуатацію або сертифікаті відповідності.
- ❑ Таким чином, для перехоплення електромагнітного ТКВІ АС необхідно, щоб відстань від АС до межі КЗ була менше зони R2, в межах якої встановлений ТЗР ПЕМВ.



Електричні ТКВІ

- ❑ Причинами виникнення електричних каналів витоку інформації є наведення інформативних сигналів, під якими розуміються струм і напруга в струмопровідних елементах, що викликаються ПЕМВ, ємнісними та індуктивними зв'язками.
- ❑ Наведення інформативних сигналів за рахунок ПЕМВ можуть виникнути у:
 - лініях електроживлення АС і інших технічних засобів;
 - лініях заземлення АС;
 - з'єднувальних лініях АС і інших технічних засобів;
 - сторонніх провідниках (металевих трубах систем опалювання, водопостачання, металоконструкціях будівлі тощо).
- ❑ Залежно від причин можливі наведення інформативних сигналів у:
 - електричних колах АС, викликані ПЕМВ АС;
 - з'єднувальних лініях технічних засобів і сторонніх провідниках, викликані ПЕМВ АС;
 - електричних колах АС, викликані внутрішніми ємнісними та/або індуктивними зв'язками («витік» інформативних сигналів у колі електроживлення через блоки живлення АС);
 - колах заземлення АС, викликані ПЕМВ АС, а також гальванічним зв'язком «схемної землі» та блоків АС.



Випадкові антени

- ❑ Різні допоміжні технічні засоби, їх з'єднувальні лінії, а також лінії електроживлення, сторонні провідники та лінії заземлення виконують роль випадкових антен, при підключенні ТЗР до яких можливе перехоплення наведених інформативних сигналів.
- ❑ Випадкові антени можуть бути **зосередженими та розподіленими**.
 - **Зосереджена випадкова** антена є компактим технічним засобом (телефонний апарат, гучномовець оповіщення, датчик охоронної сигналізації, камера відеонагляду тощо), підключеним до лінії, що виходить за межі КЗ.
 - До **розподілених випадкових** антен відносяться кабелі, дроти, металеві труби та інші струмопровідні комунікації, що виходять за межі КЗ. Рівень сигналів, що наводяться в них, значною мірою залежить не лише від потужності випромінюваних сигналів, але й відстані до них від засобів АС.
- ❑ Простір навкруги АС, за межами якого рівень наведеного від АС інформативного сигналу в зосереджених антенах не перевищує допустимого (нормованого) значення, називається небезпечною зоною r_1 , а в розподілених антенах - небезпечною зоною r_1' .



Виникнення електричного ТКВІ

- ❑ На відміну від зони R2 розмір зони $r1/r1'$ залежить не лише від рівня ПЕМВ АС, але й від довжини випадкової антени (від приміщення, де встановлена АС, до місця можливого підключення ТЗР).
- ❑ Зони $r1$ і $r1'$ для кожної АС визначаються інструментально-розрахунковим методом, і їх значення вказуються в приписі на експлуатацію АС.
- ❑ Для виникнення електричного ТКВІ необхідно, щоб:
 - відстань від АС до випадкової антени була менше зони $r1/r1'$;
 - випадкова антена виходила за межі КЗ і мала гальванічне підключення ТЗР.



Спеціально створювані ТКВІ

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



Закладні пристрої₁

- ❑ Для перехоплення інформації, що обробляється в АС, можливо також використання «закладних» електронних пристроїв перехоплення інформації, потайно впроваджених в технічні засоби АС.
- ❑ Перехоплена за допомогою «закладних» пристроїв інформація або безпосередньо передається по каналу зв'язку на приймальний пристрій ТЗР, або записується в спеціальний запам'ятовуючий пристрій, та передається тільки за сигналом дистанційного керування.
- ❑ Для передачі інформації на приймальний пристрій можуть використовуватися радіоканал, оптичний (інфрачервоний) канал або лінії електроживлення АС.



Закладні пристрої₂

- ❑ «Закладні» пристрої впроваджуються в АС для перехоплення інформації, що:
 - вводиться з клавіатури;
 - виводиться на екран монітора;
 - виводиться на принтер;
 - записується на жорсткий диск.
- ❑ «Закладні» пристрої, як правило, складаються з блоків перехоплення, обробки, передавання, дистанційного керування та живлення (перетворювача АС/DC). Блок дистанційного керування призначений для прийому сигналів дистанційного включення й виключення «закладки» та встановлення параметрів роботи передавального блоку.
- ❑ Приймальний комплекс ТЗР ПЕМВН складається з радіоприймального пристрою, модему, ноутбука і спеціального програмного забезпечення.



Апаратна закладка₁

- ❑ Апаратна «закладка» для перехоплення зображень з екрану монітора потайно встановлюється, як правило, в корпусі монітора (можливе встановлення і в системному блоці) та контактно підключається до кабелю монітора.
- ❑ Перехоплена інформація (відеозображення) в цифровому вигляді передається по радіоканалу, лінії електромережі або виділеній лінії на приймальний комплекс ТЗР, де перехоплене зображення відновлюється та відображається на екрані комп'ютера в реальному масштабі часу, створюючи «копію» екрану, а додаткова інформація може записуватися на жорсткий диск для подальшої обробки.



Апаратна закладка₂

- ❑ Апаратна «закладка» для перехоплення інформації, що вводиться з клавіатури (далі - кейлогер), потайно встановлюється в корпусі клавіатури або всередині системного блоку та підключається до інтерфейсу клавіатури. Вона є найпоширенішою «закладкою» та призначена в основному для перехоплення паролів користувачів і текстових документів, що набирають на клавіатурі. Перехоплена інформація може передаватися по радіоканалу або записуватися на флеш-пам'ять.
- ❑ Кейлогер з передачею інформації по радіоканалу складається з блоку перехоплення, передавального або запам'ятовуючого блоку та блоку управління. Живлення кейлогера здійснюється від інтерфейсу клавіатури. Він має невеликі розміри і важить декілька грам.



Апаратна закладка₃

- ❑ Блок перехоплення здійснює перехоплення сигналів, що передаються з клавіатури до системного блоку при натисненні клавіші. Перехоплені сигнали в цифровому вигляді передаються по радіоканалу (наприклад, Bluetooth) на приймальний комплекс ТЗР, де в реальному масштабі часу відновлюються та відображаються на екрані комп'ютера у вигляді символів, що набираються на клавіатурі.
- ❑ Апаратні кейлогери, що здійснюють запис перехопленої інформації на флеш-пам'ять, складаються з датчика перехоплення сигналів, що передаються з клавіатури до системного блоку при натисненні клавіші, мікроконтроллера та флеш-пам'яті.
- ❑ Вони працюють під управлінням будь-якої операційної системи та не вимагають додаткового живлення, оскільки живляться від клавіатури АС. При об'ємі пам'яті 1 МГб забезпечується запис до двох мільйонів натиснень клавіш або 500 сторінок тексту. Записана на флеш-пам'ять інформація шифрується з використанням 128-бітового ключа.



Апаратна закладка₄

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



Апаратна закладка₅

- ☐ Апаратна «закладка» для перехоплення інформації, що виводиться на принтер, встановлюється в корпусі принтера та за принципом роботи аналогічна «закладкам», розглянутим вище.
- ☐ Апаратна «закладка» для перехоплення інформації, що записується на жорсткий диск, є найбільш складною з розглянутих вище. Вона потайно встановлюється в системному блоці та контактено підключається через блок перехоплення до інтерфейсу, що з'єднує жорсткий диск з материнською платою.
- ☐ Перехоплені сигнали поступають у блок обробки, що включає спеціалізований процесор, де здійснюється їх обробка за спеціальною програмою. Файли з заданим розширенням (наприклад, *.doc) записуються в оперативну або флеш-пам'ять.
- ☐ За сигналом дистанційного керування записана в пам'яті інформація в цифровому вигляді по радіоканалу або лінії електромережі передається на приймальний комплекс ТЗР, де у вигляді окремих файлів записується на жорсткий диск для подальшої обробки.



Шляхи перехоплення інформації в АС

❑ Перехоплення інформації, що обробляється в АС, може здійснюватися шляхом:

- перехоплення ПЕМВ, що виникають при роботі АС;
- перехоплення наведень інформативних сигналів з ліній електроживлення та заземлення АС;
- перехоплення наведень інформативних сигналів із з'єднувальних ліній технічних засобів і сторонніх провідників у приміщенні, де розташована АС;
- ВЧ опромінення засобів АС;
- встановлення в засобах АС «закладних» пристроїв.



Захист інформації в АС від витоку каналами ПЕМВН



ТР ЕОТ-95

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

- випромінювань технічних засобів АС;
- наведень на системи, що мають вихід за межі КЗ;
- колами заземлення;
- колами електроживлення.

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

- екранувальних конструкцій;
- системи просторового зашумлення.



НД ТЗІ

- ❑ У 2007 році в Україні були розроблені нормативні документи серії «Захист інформації на об'єктах інформаційної діяльності (далі - ОІД)» щодо створення комплексу ТЗІ:
 - НД ТЗІ 1.1-005-07 Створення комплексу ТЗІ. Основні положення;
 - НД ТЗІ 2.1-002-07 Випробування комплексу ТЗІ. Основні положення;
 - НД ТЗІ 3.1-001-07 Створення комплексу ТЗІ. Передпроектні роботи;
 - НД ТЗІ 3.3-001-07 Створення комплексу ТЗІ. Порядок розроблення та впровадження заходів із захисту інформації.
- ❑ Ці НД ТЗІ вимагають застосування у складі комплексу ТЗІ лише тих засобів захисту інформації, які мають сертифікат відповідності Системи УкрСЕПРО вимогам НД ТЗІ або позитивний висновок державної експертизи у сфері ТЗІ.
- ❑ Застосування імпортованих засобів захисту інформації можливе лише за умови відсутності вітчизняних аналогів за умови наявності відповідних техніко-економічних обґрунтувань і проведення їх сертифікації або одержання позитивного експертного висновку.



Створення комплексу технічного захисту інформації



Створення КТЗІ

- ❑ Основні вимоги до порядку створення комплексу ТЗІ вписані у НД ТЗІ 1.1-005-07 «Захист інформації на ОІД. Створення комплексу ТЗІ. Основні положення».
- ❑ Замовник (підрозділ установи) на створення комплексу ТЗІ разом із СЗІ готує та подає на затвердження керівнику установи-замовника:
 - протокол про визначення вищого ступеня обмеження доступу до інформації;
 - проект рішення щодо створення комплексу ТЗІ.
- ❑ Створення комплексу ТЗІ передбачає такі основні етапи:
 - 1) передпроектні роботи;
 - 2) впровадження заходів захисту;
 - 3) випробування комплексу ТЗІ



Етапи створення КТЗІ₁

□ 1-й етап: передпроектні роботи

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

□ 2-й етап: впровадження заходів захисту

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



Етапи створення КТЗІ₂

□ 3-й етап: випробування комплексу ТЗІ

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



Варіанти побудови КТЗІ

Перший варіант обладнання для комплексу ТЗІ в АС класу 1

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

Другий варіант обладнання для комплексу ТЗІ в АС класу 1

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

Донецький національний технічний університет



Тема 8. Системи захисту інформації для різних автоматизованих систем.

Лекція 16. КЗЗ від НСД, що мають експертні висновки.

Предмет: АСЗІ

Розділ: Кібербезпека

Галузь: Інформаційні технології

Укладачі: проф. Дорогий Я.Ю.
доц. Алтухова Т.В.



Лекційні питання

643

- ☐ Системи захисту в АС класу 1
- ☐ Системи захисту в АС класу 2
- ☐ Системи захисту Web-ресурсів від НСД



Системи захисту в АС класу 1



«Рубіж-PCO» (версія 2)₁

645

- ☐ Комплекс призначений для забезпечення захищеної інформаційної технології в частині збирання, оброблення, зберігання і представлення інформації з обмеженим доступом в АС класу 1.
- ☐ ФПЗ комплексу:
 - КА-2, КО-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-1, НТ-2
 - Рівень гарантій – Г-3.
 - Розробник: ПАТ «КП ОІІ», м. Київ
 - Експертний висновок № 422 дійсний до 01.03.2016
- ☐ Комплекс може використовуватися у якості програмно-технічного ядра КСЗІ в АС класу 1 для обробки конфіденційної інформації, а також інформації, що становить державну таємницю, при виконанні відповідних організаційних заходів та забезпеченні захисту від витоку інформації технічними каналами.
- ☐ Використання передбачається: на робочих станціях «Intel» архітектури в середовищі операційної системи (далі - ОС) Windows 2000 / XP.
- ☐ При автентифікації в Windows використовуються логін і пароль та додатково перевіряється PIN-код на оптичному носії CD-R/RW, який повинен бути зареєстрований адміністратором безпеки в базі даних комплексу за правилами обліку носіїв. Тільки при наявності усіх цих чинників може бути здійснена автентифікація користувача АС.



«Рубіж-PCO» (версія 2)₂

646

❑ Технологія обробки конфіденційної інформації передбачає виконання таких вимог:

- ІзОД зберігається тільки на зйомних магнітних (Flash диски) та оптичних носіях (CD-R/RW), які зареєстровані адміністратором в базі даних;
- на одному носії зберігаються дані одного ступеню конфіденційності, який відповідає встановленому для носія грифу конфіденційності.



«Рубіж-PCO» (версія 2)₃

647

□ Комплекс забезпечує вирішення таких функцій захисту:

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



«Рубіж-PCO» (версія 2)₄

648

□ Комплекс складається з:

- комплексу технічних засобів обробки ІзОД;
- засобів захисту інформації від витоку фізичними каналами, які підключаються до певних входів приладу;
- «РІАС-4КА» - пристрою автоматизованого контролю працездатності засобів просторового та лінійного захисту інформації з видаванням сигналів на КЗЗ.



«Рубіж-PCO» (версія 2)₅

649

□ Опис функціонування

- Посилена автентифікація – при спробі користувача авторизуватись в ОС відбувається перевірка КЗЗ від НСД. Якщо виявлені порушення, то користувач, що не є Адміністратором безпеки не зможе здійснити вхід до системи.
- Моніторинг – вмикається тоді, коли адміністратор безпеки переведе КЗЗ в режим роботи Нормальний, і, вимикається, коли КЗЗ переводиться в режим роботи Службовий.
- Інформування – у випадку виявлення порушень функціонування Комплексу буде надано користувачеві інформативне повідомлення з певним часом аварійного завершення сеансу на виявлення та можливого вирішення ситуації зі сторони користувача, якщо це можливо, та здійснений запис в базу даних КЗЗ.
- Якщо час аварійного завершення сеансу вийшов і Комплекс не був відновлений, система примусово завершить сеанс користувача і переведеться в режим Службовий.



«Рубіж-PCO» (версія 2)₆

650

□ Обробка ІзОД передбачає виконання такої послідовності дій:

- отримати носій у відповідального за зберігання носіїв працівника;
- пройти процес автентифікації при вході в ОС;
- створити або скопіювати з носія до власної робочої папки необхідні для роботи документи;
- виконати планові операції з документами (створення, перегляд, редагування, друк та збереження);
- скопіювати необхідні документи на носій;
- всі документи робочих папок та тимчасово створені файли знищити;
- завершити сеанс роботи;
- здати носій на зберігання працівнику PCO.



«Лоза-1» (версія 4)₁

651

- ☐ Система - це програмний засіб захисту інформації від НСД в АС класу 1, який працює під керуванням ОС Windows XP / Vista / 7.
- ☐ Система постачається у двох конфігураціях:
 - «Підвищена безпека» - для захисту інформації, що становить державну таємницю;
 - «Стандартна безпека» - для захисту службової та конфіденційної інформації (в тому числі персональних даних).
- ☐ ФПЗ системи у конфігурації «Підвищена безпека»:
 - КА-3, КО-1, ЦА-1, ДВ-1, ДЗ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2.
- ☐ ФПЗ системи у конфігурації «Стандартна безпека»:
 - КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДВ-1, ДЗ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2.
- ☐ У конфігурації «Стандартна безпека» рівень надання послуги безпеки «Ідентифікація та автентифікація» залежить від значення параметра конфігурації «Перевіряти ключовий диск під час входу до Windows». Якщо для нього встановлене значення «Так», зазначена послуга надається на рівні НИ-3 «Множинна ідентифікація та автентифікація».
- ☐ У протилежному випадку послуга надається на рівні НИ-2 «Одиночна ідентифікація та автентифікація». У конфігурації «Підвищена безпека» послуга безпеки НИ-3 забезпечується автоматично. Як ключові диски можуть використовуватись модулі пам'яті USB Flash та CD/DVD-диски.
- ☐ Рівень гарантій: Г-4.
- ☐ Експертний висновок № 540 дійсний до 08.08.2017.
- ☐ Розробник: ТОВ НДІ «Автопром», м. Київ



«Лоза-1» (версія 4)₂

652

□ Система забезпечує:

1. Захист інформації від НСД:

- дозволяє захистити будь-які дані на знімних та стаціонарних носіях; захист здійснюється на рівні папок Windows та знімних дисків;
- забезпечує надійний захист документів Microsoft Word та Microsoft Excel за рахунок тісної інтеграції з Microsoft Office (відключаються небезпечні команди, макроси, шаблони тощо); підтримуються версії Microsoft Office XP / 2003 / 2007 / 2010;
- дозволяє контролювати роботу із знімними дисками: компакт-дисками та флешками; для флешек дозволи на доступ до диска можуть встановлюватись для окремих носіїв (вони ідентифікуються за «залізним» серійним номером);
- дозволяє встановлювати дозволи або заборони на запуск процесів.

2. Контроль друку та експорту:

- забезпечує можливість встановлення дозволу/заборони друку та експорту на рівні окремих документів;
- для підсилення контролю дозволяє забезпечити присутність адміністратора або іншої уповноваженої особи під час друку та експорту (за рахунок необхідності введення пароля).



«Лоза-1» (версія 4)₃

653

3. Контроль входу користувачів до системи:

- у конфігурації «Підвищена безпека» вхід здійснюється тільки після введення пароля та встановлення ключового диска (може використовуватись флешка або диск); діє жорстка політика паролів та політика блокування користувачів, яка протидіє підбору паролів;
- у конфігурації «Стандартна безпека» для входу достатньо ввести пароль; політика паролів менш жорстка, ніж в конфігурації «Підвищена безпека».

4. Реєстрацію подій:

- веде захищений журнал, в якому реєструються всі події, важливі для захисту інформації;
- аналіз журналу та протоколів роботи не потребує спеціальної кваліфікації;
- журнал подій ніколи не перезаписується: після досягнення граничного розміру журналу всі події зберігаються у файлі на жорсткому диску;
- забезпечує докладну реєстрацію подій друку та експорту; поряд із стандартною інформацією у журналі фіксуються гриф та обліковий номер документа, а також серійний номер носія, на якому зберігається документ, та носія, на який здійснюється експорт; адміністратор має можливість формування протоколу друку документів.



«Гриф» (версія 3)₁

- ☐ Комплекс призначений для забезпечення захисту ІзОД від НСД при її обробці в АС класів 1 і 2 під керуванням ОС Windows XP / Vista / 7 / Server 2008 / Server 2008 R2.
 - Рівень гарантій - Г-4.
 - Розробник: ТОВ «Інститут комп'ютерних технологій», м. Київ
 - Експертний висновок № 450 дійсний до 12.07.2016.
- ☐ Комплекс повністю замінює штатні засоби адміністрування ОС власними засобами, що підтримують реалізацію адміністративного розмежування доступу до захищених ресурсів.
- ☐ Комплекс забезпечує захист інформації, представленої у вигляді файлів даних довільного типу (електронних документів, електронних таблиць, конструкторських креслень, цих геоінформаційних систем тощо).
- ☐ ФПЗ комплексу :
 - КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-3, НО-2



«Гриф» (версія 3)₂

□ Комплекс реалізує такі основні функції захисту :

- ідентифікацію і аутентифікацію користувачів на підставі логіна, пароля і носія даних автентифікації (зйомного файлового носія або облаштування Touch Memory);
- розмежування обов'язків користувачів і виділення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрації ресурсів, реєстрації користувачів, надання прав доступу, обробки протоколів аудиту тощо);
- розмежування доступу користувачів до вибраних папок, розміщених на жорсткому магнітному диску ПЕОМ, і файлів, які містяться в них, що дозволяє організувати спільну роботу декількох користувачів, що мають різні службові обов'язки і права по доступу до ІзОД;
- керування потоками інформації і блокування потоків інформації, що призводять до зниження рівня її конфіденційності;
- контроль за виведенням інформації на друк з можливістю маркування друкарських аркушів документів згідно вимог чинних нормативних документів в області охорони державної таємниці;
- контроль за експортом інформації на зйомні носії з забезпеченням можливості їх реєстрації та обмеження (для певних користувачів) їх переліку тільки зареєстрованими;
- контроль за імпортом інформації зі зйомних носіїв;
- гарантоване видалення ІзОД шляхом затирання вмісту файлів при їх видаленні;



«Гриф» (версія 3)_з

□ Комплекс реалізує такі основні функції захисту :

- розмежування доступу застосовних програм до вибраних папок і файлів, що містяться в них, що дозволяє забезпечити захист ІзОД від випадкового видалення або модифікації і дотриматися технології її обробки;
- контроль цілісності прикладного ПЗ і ПЗ комплексу, а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів і дотримання технології обробки ІзОД;
- контроль за використанням дискового простору користувачами (квоти), що унеможливорює блокування одним з користувачів можливості роботи інших;
- можливість блокування облаштувань інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;
- контроль цілісності і самотестування комплексу при старті;
- відновлення функціонування комплексу після збоїв, що гарантує доступність інформації при дотриманні правил доступу до неї;
- реєстрацію, аналіз і обробку інформації про критичні для безпеки події (входу користувача в ОС, спроб несанкціонованого доступу, фактів запуску програм, роботи з ІзОД, імпорту/експорту інформації, виводу на друк і т.п.), що дозволяє адміністраторам контролювати доступ до ІзОД, стежити за тим, як використовується комплекс, а також правильно його конфігурувати;
- ведення архіву зареєстрованих даних аудиту;
- взаємодія з прикладними програмними системами (ППС) через визначений інтерфейс, що дозволяє забезпечити безперервність захисту ІзОД при її обробці як штатними засобами ОС, так і засобами різних ППС.



Операційні системи, в середовищі яких працюють КЗЗ

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



Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ₁

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



Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ₂

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

- разом з послугами безпеки ОС усі КЗЗ забезпечують визначений ФПЗ АС-1;
- «Гриф» є найсильнішим КЗЗ, оскільки у порівнянні з «Лозою» забезпечує вищий рівень послуги адміністративної цілісності ЦА-2 і додаткові послуги обмеженого відкату ЦО-1 і використання ресурсів ДР-1, а також автентифікацію користувачів з використанням технології «Touch Memory»;
- «Лоза» у порівнянні з «Гриф» забезпечує вищий рівень адміністративної конфіденційності КА-3.



Системи захисту в АС класу 2



«VTI-Рубіж» (версія 2)₁

- ☐ Комплекс призначений для реалізації механізмів захисту інформації від НСД, автоматизації процесів керування ними та створення захищеної технології оброблення, зберігання та представлення ІзОД в АС класів 1 і 2.
- ☐ ФПЗ комплексу:
 - КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-3
 - Рівень гарантій – Г-3.
 - Експертний висновок № 482 дійсний до 13.12.2016.
- ☐ Комплекс може розглядатися як централізована багаторівнева ієрархічна система захисту інформації від НСД, яка складається з КЗЗ рівнів та засобів забезпечення їх взаємодії.
- ☐ До складу КЗЗ кожного рівня входять монітор безпеки (МБ) у складі автоматизованого робочого місця (АРМ) адміністратора безпеки та серверу МБ. Крім МБ в комплекс входять агенти МБ, які інсталюються на кожному з хостів і здійснюють взаємодію з програмно-технічними та проблемно-орієнтованими засобами захисту (ПОЗЗ).



«VTI-Рубіж» (версія 2)₂

- ❑ МБ є програмно-технічним ядром системи захисту, яке забезпечує централізоване управління КЗЗ та взаємодію його елементів.
- ❑ МБ інтегрує в єдину систему керування захистом такі засоби:
 - захисту домену;
 - захисту функціональних робочих місць у складі засобів автентифікації, захисту ОС та управління фізичним доступом до робочих станцій - «Рубіж-РС»;
 - підсистеми управління фізичним доступом до території та приміщень вузла АС - «Рубіж-Ф»;
 - захисту баз даних (БД) рівня АС;
 - захисту комунікаційної мережі зв'язку;
 - криптографічного захисту інформації;
 - антивірусного захисту;
 - резервного копіювання та відновлення інформації КЗЗ, операційного середовища та БД.



«VTI-Рубіж» (версія 2)₃

❑ Сервер МБ забезпечує:

- реалізацію бізнес-логіки функціонування системи захисту інформації АС від НСД,
- зберігання параметрів моделі системи захисту, конфігурації системи, ведення та обробку журналів подій,
- зберігання параметрів аудиту системи та реагування на критичні події, автентифікацію адміністраторів (агентів),
- мережеву взаємодію з АРМ адміністратора безпеки та агентами МБ,
- формування команд для взаємодії з ПОЗЗ,
- відслідковування подій та видачу інформації на АРМ адміністратора безпеки для керування КЗЗ.



«VTI-Рубіж» (версія 2)₄

- ❑ Взаємодія МБ з ПОЗЗ з проблемно-орієнтованими засобами захисту (функціональних АРМ, контролера домену, операційних систем та СКБД) забезпечується його структурним елементом - сервером МБ за схемою: АРМ адміністратора ? сервер МБ ? агент монітора безпеки ? ПОЗЗ.
- ❑ Взаємодія з програмно-технічними та проблемно-орієнтованими засобами захисту інформаційних ресурсів кожного з хостів здійснюється через окремі функціональні компоненти - агенти МБ, які інстальються на окремих серверах та робочих станціях АС. Кожний агент для взаємодії з проблемно-орієнтованими засобами захисту має набір драйверів відповідно до складу ПОЗЗ.
- ❑ Агенти МБ призначені для:
 - керування механізмами захисту ПОЗЗ;
 - видачі інформації на АРМ про параметри системи захисту за запитами адміністратора безпеки;
 - реєстрації подій ПОЗЗ;
 - видачі повідомлень на АРМ адміністратора безпеки про події, що зв'язані з безпекою системи.



«VTI-Рубіж» (версія 2)₅

- ❑ Агент МБ приймає команди на адміністрування ПОЗЗ від АРМ адміністратора, виконує команди і відправляє монітору безпеки інформацію про результати їх виконання. Крім того, агент МБ відслідковує події на ПОЗЗ, видає інформацію про події монітору безпеки і забезпечує реагування на критичні події.
- ❑ У випадку відсутності зв'язку з МБ (або його непрацездатністю) агент МБ автономно виконує функції захисту інформаційних ресурсів хосту, відслідковує події, забезпечує реагування на критичні події. При відновленні зв'язку з МБ всю необхідну інформацію агент пересилає на МБ для подальшої обробки і прийняття відповідних рішень.
- ❑ Програмні засоби АРМ адміністратора безпеки забезпечують зручний та інтуїтивно зрозумілий інтерфейс для адміністратора безпеки і представляють собою програмні модулі, що функціонують у середовищі Windows NT / 2000.
- ❑ Інтерфейс забезпечує введення та відображення інформації, необхідної для налагодження та керування механізмами захисту АРМ адміністратора безпеки, а також відслідкування подій, що впливають на стан захищеності АС.



«VTI-Рубіж» (версія 2)₆

□ Засоби комплексу забезпечують автоматизовану побудову моделі захищеної системи, яка включає:

- структуру системи, що захищається;
- структуру власне СЗІ;
- структуру суб'єктів інформаційної діяльності;
- структуру об'єктів захисту;
- правила розмежування доступу;
- правила забезпечення спостереженості за станом систем;
- правила реагування на критичні події.



«VTI-Рубіж» (версія 2)₇

□ Об'єктами захисту комплексу є:

- системні ресурси АС – ресурси операційних систем, системних та мережних служб, власне СЗІ;
- інформаційні ресурси АС (об'єкти СКБД, файли);
- інформаційні ресурси власне КЗЗ АС (об'єкти БД КЗЗ: параметри моделі і конфігурація системи захисту, параметри автентифікації користувачів, журнали подій, журнали дії адміністраторів, архіви журналів, звіти про стан захищеності системи, параметри аудиту подій, параметри реагування на події тощо);
- прикладні ресурси (програмне забезпечення АС).

□ Правила розмежування доступу визначаються встановленою власником АС політикою безпеки і полягають у наданні повноважень суб'єктам АС на доступ до ресурсів, які захищаються, а також у встановленні типів доступу суб'єктам до об'єктів захищеної системи. На основі такої інформації за внутрішніми алгоритмами перевірки повноважень диспетчери доступу ПОЗЗ реалізують санкціонування доступу суб'єкта до об'єкта. Таким чином забезпечується довірчий та адміністративний принципи керування доступом.



«Лоза-2» (версія 4)

- ❑ Система - це програмний засіб захисту інформації від несанкціонованого доступу в АС класу 2 (ЛОМ). Система може працювати під керуванням операційних систем Windows XP / Vista / 7 / Server 2003 / Server 2008 / Server 2008 R2.
- ❑ Система може працювати як в одноранговій мережі, так і в мережі, побудованій на основі домену. Один із комп'ютерів мережі повинен виконувати роль сервера системи. В одноранговій мережі серверна частина системи може бути встановлена на будь-якому з комп'ютерів мережі.
- ❑ В мережі, побудованій на основі домену, серверна частина системи встановлюється на первинному контролері домену. На всіх інших комп'ютерах встановлюється клієнтська частина системи.
 - ФПЗ для конфігурації «Стандартна безпека»:
 - КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-2, НК-1, НО-2, НЦ-2, НТ-2
 - ФПЗ для конфігурації «Підвищена безпека»:
 - КА-3, КО-1, ЦА-1, ДС-1, ДЗ-1, ДВ-1, НР-4, НИ-3, НК-1, НО-2, НЦ-2, НТ-2
 - Рівень гарантій: Г-4.
 - Експертний висновок № 383 дійсний до 16.10.2015
- ❑ Система забезпечує ті ж функції, що й «Лоза-1»:
 - захист інформації від НСД;
 - контроль друку та експорту;
 - контроль входу користувачів до системи;
 - реєстрацію подій.



«Гриф-Мережа» (версія 3)₁

- ❑ Комплекс призначений для забезпечення захисту інформації з обмеженим доступом, що обробляється в ЛОМ і РОМ. До складу мережі можуть входити файлові сервери, що функціонують під управлінням ОС Windows Server 2003 / Server 2008 / Server 2008 R2, і робочі станції, що функціонують під управлінням ОС Windows XP / Vista / 7, об'єднані в єдиний домен Active Directory.
 - Рівень гарантій Г-4.
 - Експертний висновок № 402 дійсний до 19.12.2015
- ❑ Комплекс дозволяє створити на базі ЛОМ спеціалізовану АС класу 2 для обробки ІзОД і забезпечити її захист від загроз порушення цілісності, конфіденційності і доступності при реалізації політики адміністративного керування доступом до інформації. Комплекс поставляється у двох конфігураціях: базовій і підвищеної спостереженості. Відмінність між вказаними конфігураціями комплексу полягає в тому, що у конфігурації підвищеної спостереженості реалізована можливість збору і аналізу в реальному часі інформації про критичні з точки зору захищеності інформації події, зареєстровані на серверах, робочих станціях і активних мережевих пристроях, що функціонують у складі захищеної ЛОМ.



«Гриф-Мережа» (версія 3)₂

□ ФПЗ у базовій конфігурації:

- КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-3, НО-2
- У базовій конфігурації в реальному часі виконується тільки збереження інформації про критичні з точки зору захищеності інформації події, зареєстровані на серверах і робочих станціях, що функціонують у складі захищеної ЛОМ, її аналіз виконується у відкладеному режимі.
- Комплекс у базовій конфігурації доцільно застосовувати для захисту інформації в ЛОМ, кількість робочих станцій в яких відносно невелика (до 30) і при цьому усі робочі станції розташовуються в одному або декількох суміжних приміщеннях.

□ ФПЗ у конфігурації підвищеної спостереженості:

- КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-5, НК-1, НЦ-2, НТ-2, НИ-3, НО-2
- Комплекс доцільно застосовувати для захисту інформації в ЛОМ, кількість робочих станцій в яких досить велика (більше 30) або в яких робочі станції розташовуються у великій кількості територіально рознесених приміщень (наприклад, по декілька робочих станцій на різних поверхах багатоповерхової будівлі).



«Гриф-Мережа» (версія 3)₃

□ Комплекс реалізує такі функції:

- ідентифікацію і автентифікацію користувачів на підставі логіна, пароля і персонального носія даних автентифікації (Touch Memory, Flash Drive тощо) при завантаженні ОС робочої станції до завантаження будь-якого ПЗ з дисків, що дозволяє заблокувати використання робочої станції сторонньою особою, а також упізнати авторизованого користувача та надалі реагувати на його запити згідно його повноважень;
- розмежування обов'язків користувачів і виділення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрації ресурсів, реєстрації користувачів, надання прав доступу, обробки протоколів аудиту тощо);
- блокування облаштувань інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;
- контроль цілісності та самотестування КЗЗ при старті і за запитом адміністратора, що дозволяє забезпечити стійке функціонування КЗЗ і не допустити обробку ІзОД у разі порушення його працездатності;
- розмежування доступу користувачів до вибраних папок, розміщених на робочих станціях і файлових серверах ЛОМ, і файлів, які знаходяться в них, що дозволяє організувати одночасну спільну роботу декількох користувачів ЛОМ, що мають різні службові обов'язки і права по доступу до ІзОД;
- керування потоками інформації і блокування потоків інформації, що призводять до зниження її рівня конфіденційності;



«Гриф-Мережа» (версія 3)₄

- контроль за виведенням інформації на друк з можливістю маркування друкарських аркушів документів, що виводяться, згідно вимог чинних нормативних документів в області охорони державної таємниці;
- контроль за експортом інформації на зйомні носії з можливістю обмеження переліку використовуваних змінних носіїв;
- контроль за імпортом інформації зі зйомних носіїв;
- гарантоване видалення інформації шляхом затирання вмісту файлів при їх видаленні;
- розмежування доступу застосовних програм до вибраних папок і файлів, що знаходяться в них, що дозволяє забезпечити захист ІзОД від випадкового видалення, модифікації і дотримання технології її обробки;
- контроль цілісності прикладного і системного ПЗ і ПЗ КЗЗ, а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів і дотримання технології обробки ІзОД;
- контроль за використанням користувачами дискового простору файлових серверів (квоти), що унеможлиблює блокування одним з користувачів можливості роботи інших;
- відновлення функціонування КЗЗ після збоїв, що гарантує доступність інформації із забезпеченням дотримання правил доступу до неї;
- безперервну реєстрацію, аналіз і обробку подій (входу користувачів в ОС, спроб НСД, фактів запуску програм, роботи з ІзОД, виводу на друк і т.п.) в спеціальних протоколах аудиту, що дозволяє адміністраторам контролювати доступ до ІзОД, стежити за тим, як використовується КЗЗ, а також правильно його конфігурувати;
- ведення архіву зареєстрованих даних аудиту;
- негайне сповіщення адміністратора безпеки про всі виявлені порушення ПРД (у конфігурації підвищеної спостереженості).



Операційні системи, в середовищі яких працюють КЗЗ

Windows	NT	2000	XP	Vista	7	Server 2003	Server 2008	Touch Memory	Захист папок
VTI-Рубіж	+	+							
Лоза-2			+	+	+	+	+		
Гриф-Мережа			+	+	+	+	+	+	+



Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ₁

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



Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ₂

- Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту ОС і вище зазначених КЗЗ, можна зробити такі висновки:
- разом з послугами безпеки ОС КЗЗ «Гриф» забезпечують визначений ФПЗ АС-2 у повному обсязі, а «Лоза» не забезпечує рівень послуги ЦА-2;
 - «Гриф-Мережа» у конфігурації підвищеної спостереженості є найсильнішим КЗЗ, оскільки у порівнянні з «Лоза» забезпечує вищий рівень послуги адміністративної цілісності ЦА-2 і реєстрації НР-5 (аналіз у реальному часі), а також додаткові послуги обмеженого відкату ЦО-1 і використання ресурсів ДР-1 та автентифікацію користувачів з використанням технології «Touch Memory»;
 - «Лоза» у порівнянні з «Гриф» і «Гриф-Мережа» у базовій конфігурації забезпечує додаткові послуги довірчої конфіденційності КД-2 і цілісності ЦД-1 та вищий рівень послуги реєстрації НР-4 (захищений журнал).



Системи захисту Web-ресурсів від НСД



«Megapolis. Portal Manager»₁

❑ Система забезпечує керування адміністративною частиною, зовнішнім виглядом та наповненням будь-якого Web-ресурсу. Однією з його головних переваг є простота і гнучкість використання.

❑ ФПЗ системи:

- КА-2, ЦА-1, ЦО-1, ДВ-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НВ-1
- Рівень гарантій: Г-2.
- Розробник: ТОВ «Софтлайн ІТ», м. Київ
- Експертний висновок № 327 дійсний до 02.12.2014.

❑ Система на Web-порталі забезпечує розподіл прав доступу користувачів до визначених ресурсів, надає ці права, в залежності від «ролей» користувачів (відвідувач порталу, адміністратор або контент-менеджер), стежить за дотриманням цих прав доступу згідно встановлених правил.

❑ Система реалізує технологію «MDI Framework», який потрібен для того, щоб у зручному форматі відображати інформацію, яку сервіси отримують із будь-яких джерел за допомогою технологічних інтерфейсів.



«Megapolis. Portal Manager»₂

□ Основні характеристики системи:

- реалізація в архітектурі клієнт-сервер, що забезпечує роботу в «багато-користувацькому» режимі;
- простота та зручність налаштувань за рахунок використання стандартного інтерфейсу користувача файлових менеджерів (папки, дерева тощо);
- можливість роботи з сучасними промисловими СКБД;
- забезпечення роботи віддаленого адміністрування порталів;
- розподіл прав доступу користувачів до елементів порталу;
- модульність побудови системи, що дозволяє більш гнучко налаштувати керування кожним конкретним порталом.



«Megapolis. Portal Manager»₃

□ Система має такі властивості:

- керування сервісами порталу за допомогою модулів, які входять до складу кожного сервісу;
- інформація про складові кожного сервісу (елементи), що зберігається у відповідних записах;
- однотипні записи складають окремий реєстр;
- всі реєстри складають базу даних усіх записів (елементів);
- керування контентом порталу здійснюється за допомогою модулів, в яких створюються записи в реєстрах;
- реєстри можуть бути в довільний спосіб пов'язані між собою;
- над записами будь-якого реєстру можна виконувати наступні операції:
 - створення нових записів;
 - редагування існуючих записів;
 - видалення записів;
 - пошук з можливістю урахування морфології;
 - фільтрація записів реєстрів за різноманітними критеріями;
 - групування записів;
- інтеграція з програмними пакетами Microsoft Office для підготовки матеріалів публікацій;
- автоматична публікація вже готових матеріалів;
- можливість одночасної роботи з декількома реєстрами або модулями кожного сервісу.



«Тайфун-Web»₁

680

❑ Комплекс призначений для криптографічного захисту та розмежування доступу до інформації, оброблюваної в ІТС, побудованих на базі Web-технологій.

❑ ФПЗ комплексу:

- КА-2, KB-2, ЦА-1, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-1, НИ-1, НО-1, НЦ-1, НТ-2, НВ-2
- Рівень гарантій: Г-4.
- Розробник: ТОВ «Інститут комп'ютерних технологій», м. Київ
- Експертний висновок № 336 дійсний до 29.12.2014.

❑ При використанні комплексу забезпечується:

- взаємна автентифікація (підтвердження справжності) клієнта та сервера за протоколом, побудованим з використанням асиметричних криптоалгоритмів;
- захист конфіденційності та цілісності інформації, що передається між клієнтом та сервером, з використанням симетричних криптоалгоритмів і вироблення/перевіряння кодів автентифікації повідомлень;
- розмежування доступу користувачів до інформаційних ресурсів, представлених у вигляді статичних або динамічних Web-сторінок, що зберігаються та оброблюються на захищених Web-серверах.



«Тайфун-Web»₂

681

- ❑ Реалізована технологія інтеграції серверної та клієнтської компонентів комплексу до стеку мережевих протоколів ОС, які реалізують функції «Winsock», забезпечує незалежність від використовуваних Web-браузерів та Web-серверів. Для забезпечення сумісності із засобами «MS Internet Information Server» (IIS), в якому функції «Winsock» не використовуються, реалізована можливість підключення серверної компоненти комплексу безпосередньо до «MS IIS» через інтерфейс «ISAPI».
- ❑ Програмні засоби комплексу функціонують на IBM-сумісних комп'ютерах (робочих станціях користувачів, Web-серверах, Proxy-серверах) в ОС Windows 2000 / XP / 2003 / Vista / 7 / Server 2008. При використанні засобів комплексу на Proxy-серверах, жодних обмежень щодо ОС Web-серверів, на яких зберігаються та оброблюються захищені Web-ресурси, не висувається.
- ❑ Для керування ключовою інформацією (для вироблення відкритого та особистого ключів користувачів) у комплексі «Тайфун-Web» (у модулі адміністрування) використовуються програмні засоби генерації ключів та обслуговування сертифікатів користувачів комплексу «Тайфун-PKI».



«Тайфун-Web»₃

682

□ Комплекс реалізує такі основні функції:

- ідентифікацію та автентифікацію користувачів комплексу на основі атрибутів, отриманих від ОС, що дозволяє однозначно встановити певного користувача та у подальшому коректно оброблювати його запити на доступ до захищеної інформації або до засобів адміністрування;
- виділення, на підставі результатів виконаної автентифікації, користувачів-адміністраторів, яким надані повноваження із керування засобами комплексу;
- сувору взаємну автентифікацію клієнтської та серверної компонентів комплексу та їхніх користувачів з використанням відповідних протоколів, у яких використовується механізм вироблення / перевірки ЕЦП за алгоритмом, установленим ДСТУ 4145, з використанням відповідних атрибутів;
- керування доступом користувачів до захищених Web-ресурсів (окремих Web-сторінок та їх сукупностей), представлених відповідними URL-адресами, на основі атрибутів доступу, призначених спеціально вповноваженими адміністраторами;



«Тайфун-Web»₄

683

- зашифрування/розшифрування інформації, що передається між Web-браузером, який функціонує на робочій станції (PC) користувача, та захищеним Web-сервером (Proху-сервером), що забезпечує захист конфіденційності інформації на всьому шляху її передачі по каналах мережі Internet;
- контроль цілісності інформації, що передається між Web-браузером, яке функціонує на PC користувача, та захищеним Web-сервером (Proху-сервером), що забезпечує захист від її несанкціонованої модифікації на всьому шляху її передачі по мережі Internet;
- контроль цілісності та самотестування програмних засобів комплексу при старті та в процесі функціонування, що дозволяє забезпечити стійке функціонування засобів захисту та не допустити обробки повідомлень у випадку порушення працездатності;
- протоколювання критичних з погляду захищеності оброблюваної інформації подій у захищеному журналі ОС із забезпеченням можливості аналізу зареєстрованих даних аудита вповноваженими адміністраторами;
- можливість використання для збереження особистих (секретних) ключів користувачів, як незахищених (диск, flash-drive тощо), так і захищених носіїв (пристрій eToken Pro; SecureToken тощо).



Операційні системи, в середовищі яких працюють КЗЗ

Windows	2000	XP	2003	Vista	7	Server 2003	Server 2008	Крипто захист
Портал Менеджер								
Тайфун-Web	+	+	+	+	+		+	+



Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ₁

№	Комплекс засобів захисту	ФПЗ WEB	Windows Server 2008 R2	Портал Менед- жер 1.0	Тайфун-Web версія 1
1	рівень гарантій	Г2	Г2	Г2	Г4
2	базова адміністративна конфіденційність	КА-2	-	КА-2	КА-2
3	базова довірча конфіденційність	КД-2	КД-2	-	-
4	мінімальна / базова конфіденційність при обміні	КВ-1	КВ-1	-	КВ-2
5	мінімальна адміністративна цілісність	ЦА-1	-	ЦА-1	ЦА-1
6	обмежений відкат	ЦО-1	ЦО-1	-	ЦО-1
7	мінімальна / базова цілісність при обміні	ЦВ-1	ЦВ-1	-	ЦВ-2
8	використання ресурсів - квота	ДР-1	ДР-1	-	-
9	ручне відновлення	ДВ-1	ДВ-2	ДВ-1	ДВ-1
10	захищений журнал / зовнішній аналіз	НР-2	НР-2	НР-2	НР-1
11	один. / множинна ідентифікація і автентифікація	НИ-2	НИ-2	НИ-2	НИ-1
12	однонаправлений достовірний канал	НК-1	НК-1	НК-1	-
13	розподіл обов'язків адміністраторів / виділення адміністратора	НО-1	НО-3	НО-2	НО-1
14	КЗЗ з контролем цілісності	НЦ-1	НЦ-2	НЦ-1	НЦ-1
15	самотестування при старті	НТ-1	НТ-2	НТ-2	НТ-2
16	автентифікація вузла / джерела даних	НВ-1	НВ-1	НВ-1	НВ-2



Порівняння послуг безпеки ФПЗ механізмів захисту ОС і КЗЗ₂

- ❑ Здійснивши порівняльний аналіз послуг безпеки ФПЗ механізмів захисту вище зазначених КЗЗ, можна зробити такі висновки:
 - з урахуванням послуг безпеки ОС усі КЗЗ забезпечують визначений ФПЗ WEB;
 - «Тайфун-Web» є найсильнішим КЗЗ, оскільки у порівнянні з іншим має найбільшу кількість послуг безпеки, вищий рівень гарантій та забезпечує додатково послуги базової конфіденційності при обміні KB-2, базової цілісності при обміні ЦВ-2, стійкості при обмежених відмовах ДС-1 і модернізації ДЗ-1;
 - «Портал Менеджер» є найслабкішим КЗЗ, оскільки у порівнянні з іншим має найменшу кількість послуг безпеки.
- ❑ Разом з тим, «Портал Менеджер» у порівнянні з іншим забезпечує додатково послуги обмеженого відкату ЦО-1 і однонаправленого достовірного каналу НК-1, а також вищий рівень послуг ідентифікації і автентифікації НІ-2 (одиначна), реєстрації НР-2 (захищений журнал), розподілу обов'язків НО-2 (адміністраторів).
- ❑ Крім того, головна відмінність КЗЗ «Тайфун-Web» від КЗЗ «Портал Менеджер» є застосування симетричних криптоалгоритмів для захисту конфіденційності та цілісності інформації, що передається між клієнтом та сервером.



Список рекомендованих джерел для самопідготовки



Список рекомендованих джерел для самопідготовки₁

1. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця: ВНТУ, 2018. – 118 с.
2. Гребенніков В. В. Комплексні системи захисту інформації: проектування, впровадження, супровід /В. В. Гребенніков/ Litres, 2019. – 613 с.
3. Конспект лекцій з дисципліни «Архітектура та проектування програмного забезпечення» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Інженерія програмного забезпечення» із спеціальності 121 – «Інженерія програмного забезпечення» / Укл. В. В. Завгородній, К. М. Ялова.– Кам'янське: ДДТУ, 2019.– 144с.
4. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.
5. Хорошко В. О. Проектування комплексних систем захисту інформації: підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць/ Львів: Видавництво Львівської політехніки, 2020. - 320 с.
6. Богуш В.М. Основи кіберпростору, кібербезпеки та кіберзахисту: Навч.посіб. /В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін - К.: Ліра-К, 2020. - 554 с.



Список рекомендованих джерел для самопідготовки₂

7. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.
8. Закон України «Про інформацію»: поточна редакція від 27.07.2023 р. №2657-XII / Верховна Рада України. – Офіц. вид. – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
9. Закон України «Про захист інформації в інформаційно-комунікаційних системах»: поточна редакція від 31.12.2023 р. №80/94-ВР / Верховна Рада України. – Офіц. вид. – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
10. НД ТЗІ 3.7-003-05 Порядок проведення робіт зі створення КСЗІ. – Режим доступу до ресурсу: <https://tzi.com.ua/downloads/3.7-003-2005.pdf>