МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРБЕЗПЕКИ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри кібербезпеки

_____ Анна ІЛЬЄНКО
«_____»_____ 2024 р.

На правах рукопису
УДК 004.056.5:510.(043.3)

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Методи фізичного захисту інформації в інформаційно-комунікаційних системах

Виконавець: Олексій ЖЕРЕБКО

Керівник: к.т.н., доцент Іван ПАРХОМЕНКО

Нормоконтролер: к.т.н., доцент Андрій ПЕТРЕНКО

Київ 2024

ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Факультет комп'ютерних наук та технологій
Кафедра кібербезпеки
Освітній ступінь магістр
Спеціальність 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки

_____ Анна ІЛЬЄНКО
« 30 » 08 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
Жеребка Олексія Вікторовича

1. Тема роботи: «Методи фізичного захисту інформації в інформаційно-комунікаційних системах» затверджена наказом ректора від «30» серпня 2024 № 1696/ст.
2. Термін виконання роботи з 30.08.2024 р. по 15.12.2024 р.
3. Вихідні дані до роботи: сформулювати основні напрямки та завдання фізичного захисту відповідно до вимог національних та міжнародних нормативно-правових документів; сформулювати показники та критерії щодо вибору методів та засобів фізичного захисту; розробити обґрунтовані рекомендації щодо побудови та оптимізації системи фізичного захисту.
4. Зміст пояснювальної записки: Розділ 1. Аналіз сучасних засобів фізичного захисту інформації в інформаційно-комунікаційних системах. Розділ 2. Життєвий цикл систем фізичного захисту інформації. Їх головні функції та

характеристики. Розділ 3. Моделі та процедури оцінювання ступеня порушення СФЗІ та вибору засобів для комплектування системи.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: презентація в Microsoft PowerPoint.

6. Календарний план-графік:

№ з/п	Завдання	Термін виконання	Підпис керівника
1.	Уточнення постановки завдання	30.08.2024 - 02.09.2024	*Виконано*
2.	Аналіз літератури	03.09.2024 - 12.09.2024	*Виконано*
3.	Обґрунтування вибору рішення	13.09.2024 - 22.09.2024	*Виконано*
4.	Збір даних	23.09.2024 - 02.10.2024	*Виконано*
5.	Аналіз сучасних засобів фізичного захисту інформації в інформаційно-комунікаційних системах	03.10.2024 - 12.10.2024	*Виконано*
6.	Життєвий цикл систем фізичного захисту інформації. Їх головні функції та характеристики	13.10.2024 – 22.10.2024	*Виконано*
7.	Моделі і процедури оцінювання ступеня порушення СФЗІ та вибору засобів для комплектування системи.	23.10.2024 - 01.11.2024	*Виконано*
8.	Перевірка на антиплагіат	21.11.2024 - 25.11.2024	*Виконано*
9.	Оформлення та друк пояснювальної записки	26.11.2024 - 30.11.2024	*Виконано*
10.	Отримання рецензій	01.12.2024 - 05.12.2024	*Виконано*
11.	Оформлення презентацій	18.11.2024 - 21.11.2024	*Виконано*
12.	Захист в ЕК	09.12.2024 - 15.12.2024	

7. Дата видачі завдання: « 30 » 08 2024 р.

Керівник кваліфікаційної роботи: _____ Іван ПАРХОМЕНКО
(підпис керівника)

Завдання прийняв до виконання: _____ Олексій ЖЕРЕБКО
(підпис здобувача вищої освіти)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Методи фізичного захисту інформації в інформаційно-комунікаційних системах»: 113 сторінок основного тексту, 34 рис., 17 табл., 30 літературних джерел.

Об'єктом дослідження в роботі є процес захисту інформації, що зберігається, оброблюється і передається в інформаційно-комунікаційних системах і мережах від впливу внутрішніх і зовнішніх втручань та загроз навмисного, випадкового, природного або штучного характеру.

Предмет дослідження – методи й засоби фізичного захисту інформації в інформаційно-комунікаційних системах.

Мета кваліфікаційної роботи та методи дослідження. Основною метою цієї роботи є підвищення рівня захищеності шляхом оптимального використання ресурсів системи їх фізичного захисту. Для цього у роботі використовуються методи системного аналізу та теорії інформаційної безпеки, теорії графів та інформаційного пошуку, а також теорії управління та теорії експертиз.

Як результат у роботі проведено аналіз вітчизняного ринку засобів захисту інформації в ІКС, досліджено методи та засоби реалізації систем фізичного захисту інформації (СФЗІ) в ІКС, розроблено моделі й процедури вибору засобів СФЗІ та проведено їх апробацію, розроблено процедуру оцінювання ступеня порушення СФЗІ в ІКС за метою реалізації.

Запропоновані підходи можуть бути використані при плануванні та реалізації системи фізичного захисту ІКС будь-якої організації.

Практична цінність отриманих результатів створюють базу для розробки ефективної системи фізичного захисту інформації в ІКС, яка враховує вплив внутрішніх і зовнішніх загроз. Це забезпечує потреби державних, комерційних структур та спеціалізованих підрозділів у захисті інформації.

Наукова новизна отриманих результатів полягає в розробці нових підходів до захисту інформації в інформаційно-комунікаційних системах (ІКС). Зокрема, удосконалено технології фізичного захисту інформації від різних типів

загроз, а також розроблено рішення для раціонального вибору засобів захисту на основі аналізу загроз та оцінки потенційних порушень безпеки. Це дозволило забезпечити ефективне використання ресурсів і підвищити рівень захищеності ІКС.

БЕЗПЕКА, ЗАГРОЗА, ІНФОРМАЦІЯ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, ОБ’ЄКТ ФІЗИЧНОЇ БЕЗПЕКИ, ПОРУШНИК, СИСТЕМА ФІЗИЧНОГО ЗАХИСТУ, СТОРОННІЙ ВПЛИВ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

АРМ	–	автоматизоване робоче місце
АС	–	автоматизована система
БД	–	база даних
ДСК	–	для службового користування
ДССЗЗІ	–	Державна служба спеціального зв’язку та захисту інформації
ЕОМ	–	електронно-обчислювальна машина
ІКС	–	інформаційно-комунікаційна система
ІзОД	–	інформація з обмеженим доступом
КЗЗ	–	комплекс заходів захисту
КСЗІ	–	комплексна система захисту інформації
КТЗІ	–	комплекс технічного захисту інформації
ЛЛМ	–	логіко-лінгвістичні методи
ЛОМ	–	локальні обчислювальні мережі
МЗ	–	модель загроз
ОПР	–	особа, яка приймає рішення
ПЕМВН	–	побічні електромагнітні випромінювання та наводки
ПЗ	–	програмне забезпечення
СУБД	–	система управління базою даних
СФЗІ	–	система фізичного захисту інформації
ТНМ	–	теорія нечітких множин
ЦТ	–	цілком таємно

ВСТУП

Актуальність теми. В умовах цифрової ери інформація стала однією з найцінніших ресурсів, яка має ключове значення для ефективної роботи державних установ, бізнесу, фінансових організацій і приватних користувачів. Інформаційно-комунікаційні системи (ІКС) забезпечують обробку, зберігання та передачу даних, що робить їх надзвичайно вразливими до загрози несанкціонованого доступу, крадіжки або втрати інформації. У зв'язку з цим питанням захисту інформації є пріоритетним завданням для всіх, хто працює з великими обсягами даних.

Одним із критичних аспектів забезпечення безпеки є фізичний захист, який охоплює сукупність заходів, спрямованих на захист інфраструктури ІКС та інформаційних ресурсів від фізичних загроз. До таких загроз належать спроби несанкціонованого проникнення, фізичне пошкодження обладнання, крадіжка чи умисне знищення. Фізичний захист є доповненням до програмних і організаційних методів захисту інформації, забезпечуючи комплексний підхід до безпеки.

Захист інформації, як відомо – це сукупність організаційних, технічних та правових заходів, спрямованих на запобігання нанесенню збитків інтересам її власника. Основними об'єктами захисту при цьому є:по-перше, – інформація з обмеженим доступом (ІзОД), а саме інформаційні ресурси, що містять відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України і доступ до яких правомірно обмежений власником таких відомостей); по-друге, технічні засоби приймання, обробки, зберігання та передавання інформації (ТЗПІ), а саме системи та засоби інформатизації (обчислювальна техніка, інформаційно-комунікаційні системи (ІКС)), програмні засоби (операційні системи, системи управління базами даних та інше загальне і прикладне програмне забезпечення), автоматизовані системи управління; системи зв'язку, технічні засоби отримання, передання та обробки ІзОД

(звукозапис, звукопідсилення, звукове супроводження, переговорні та телевізійні пристрої; засоби тиражування і виготовлення документів та інші технічні засоби обробки графічної, алфавітно-цифрової та текстової інформації, їх інформативні фізичні поля) й, по-третє, допоміжні технічні засоби і системи (ДТЗС), тобто технічні засоби і системи, які не належать до ТЗПІ, але розташовані в приміщеннях, де оброблюється ІзОД (технічні засоби відкритого телефонного або гучномовного зв'язку, системи пожежної та охоронної сигналізації, систему енергопостачання, радіотрансляційні мережі, системи часофікації тощо, а також самі приміщення, де циркулює ІзОД).

Особливістю теперішнього часу є перехід від індустріального суспільства до інформаційного. При цьому інформація стає більш важливим ресурсом, ніж матеріальні або енергетичні ресурси, тому отримання доступу до інформації, особливо до інформації яка є конфіденційною та містить основні конкурентні переваги, є першочерговим завданням конкурентної боротьби. Отримання таких відомостей, як правило, пов'язане з порушенням закону і застосуванням спеціальних технічних засобів негласного отримання інформації.

Швидкий розвиток засобів комунікації та техніки призвів не тільки до позитивних, але і до негативних результатів. Виявлення та розпізнавання засобів негласного отримання інформації стає дедалі складнішою задачею, оскільки ситуація обтяжується тим, що засоби негласного отримання інформації нового покоління працюють у цілком легальному частотному діапазоні, методи та режими їх роботи ускладняються. Розробники засобів негласного отримання інформації застосовують все більш складні методи і алгоритми приховування випромінювання своїх виробів.

Наприклад: радіосигнали, по модульовані по амплітуді або частоті акустичним сигналом, або ряд радіосигналів із закриттям мови (інверсія спектра, окремі цифрові алгоритми передачі звукових даних); радіосигнали зі складними алгоритмами закриття мовлення та інші.

В умовах апріорної невизначеності, коли основні параметри радіосигналів невідомі, синтез потрібного алгоритму виявлення, розпізнавання та локалізація

радіосигналів традиційними методами пов’язаний з великими труднощами. Виходячи з цього, питання виявлення, розпізнання та локалізації засобів негласного отримання інформації представляють великі складнощі та потребують постійного вдосконалення.

Першим кроком у напрямку закриття витоку інформації із застосуванням засобів негласного отримання інформації є процес виявлення таких пристроїв. Другим кроком – є розпізнавання сигналів з метою відділення сигналів засобів негласного отримання інформації від сигналів пристроїв, що легально працюють у визначеному радіодіапазоні. Останнім кроком – є локалізація цих пристроїв та прийняття рішення про подальші дії.

З метою визначення сигналів потрібно виконати перетворення сигналів у вигляд, який можна використовувати для подальшого аналізу програмними засобами автоматизованого комплексу пошуку засобів негласного отримання інформації.

З підвищенням значення та цінності інформації, відповідно, зростає і важливість її захисту. З одного боку, інформація має певну вартість. Тобто витік, втрата, спотворення або модифікація інформації спричинять матеріальний збиток. З іншого боку, інформація – це управління.

Несанкціоноване втручання в управління може привести до катастрофічних наслідків в об’єкті управління – промисловому виробництві, транспортній системі, банківській справі, на військовому або інфраструктурному об’єкті.

Питання інформаційної безпеки сьогодні актуальне як ніколи раніше. Кількість використовуваної техніки продовжує зростати, отже, зростає і значення організаційного та програмно-технічного захисту від витоку інформації.

Найбільший інтерес серед визначених об’єктів в процесі побудови систем захисту інформації (СЗІ) становлять передусім ТЗПІ та ДТЗС. Це пояснюється тим, що застосування відповідних технічних й передусім фізичних та програмно-апаратних методів і засобів захисту означених підсистем покликано поставити

бар’єр на шляху зловмисників й максимально виключити можливість ненавмисних порушень персоналу, викликаних їх помилками або недбалістю користувачів ІКС.

Зважаючи на таке та враховуючи відсутність єдиної системної методики концептуального проєктування СЗІ на даний час актуальним і найбільш пріоритетним завданням є передусім проведення повноцінного ефективного вибору засобів і методів фізичного захисту інформації (ФЗІ) в інформаційно-комунікаційних системах, а також складу засобів системи ФЗІ, що, як результат, дозволить приймати певні стратегічні рішення по варіантах побудови системи.

Мета фізичного захисту – це гарантування безперешкодної роботи підприємств за будь-яких обставин з урахуванням усіх застосовних до них особливих вимог та ризиків. Кожне підприємство, зокрема навчальний заклад, несе відповідальність за його фізичний захист.

Система фізичного захисту інформаційних ресурсів охоплює різні сфери, зокрема: контроль доступу; відеоспостереження та інші засоби технічного нагляду та охорони; а також системи запобігання пожежам та зменшення збитків від псування обладнання систем водовідведення та водопостачання, пошкодження електричних мереж та систем кондиціонування повітря, крадіжок зі зломом тощо.

Мінімальні вимоги до усіх заходів та систем, призначених для підвищення рівня безпеки підприємства визначають з урахуванням різноманітних вимог до безпеки, що стосуються певної території, будівлі, окремого об’єкту чи групи об’єктів.

Заходи щодо охорони території, новозбудованих та реконструйованих будівель мають бути впроваджені та покращені відповідно до категорії захисту, які можна застосувати одночасно з проведенням робіт з будівництва чи реконструкції.

Як правило, за управління та заходи безпеки об’єкта несе відповідальність компанія з управління нерухомістю чи власник будівлі. Однак, керівництво підприємства, що несе відповідальність за усі рішення відносно безпеки має

найкраще розуміння потреб безпеки різноманітного функціоналу та рішень щодо інформаційних технологій, які вони використовують. Потреби розвитку охорони території підприємства враховуються в процесі щорічного планування. Всі особи, які виконують монтажні та ремонтні роботи на території підприємства повинні мати чинну ліцензію співробітника служби безпеки.

Мета і завдання дослідження. Мета роботи полягає у підвищенні рівня захищеності інформаційно-комунікаційних систем за рахунок оптимального використання ресурсів системи їх фізичного захисту. Для досягнення цієї мети в роботі необхідно вирішити такі завдання:

1) проаналізувати стан вітчизняного ринку засобів захисту інформації в інформаційно-комунікаційних системах від несанкціонованого доступу (НСД) та витоку її технічними каналами;

2) дослідити життєвий цикл систем фізичного захисту інформації в ІКС, основні засоби реалізації СФЗІ, а також головні функції та характеристики системи;

3) розробити моделі і процедури вибору засобів систем фізичного захисту інформації в ІКС та провести їх апробацію.

Виходячи з такого, у роботі об’єктом дослідження є процес захисту інформації, що зберігається, оброблюється і передається в інформаційно-комунікаційних системах і мережах від впливу внутрішніх і зовнішніх втручань та загроз навмисного, випадкового, природного або штучного характеру.

Предмет дослідження – методи і засоби фізичного захисту інформації в інформаційно-комунікаційних системах.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та теорії інформаційної безпеки, теорії графів та інформаційного пошуку, а також теорії управління та теорії експертиз.

Наукова новизна отриманих результатів. Новими науково обґрунтованими результатами, які отримані в роботі, є:

1) удосконалена технологія застосування методів та засобів забезпечення фізичного захисту інформації в ІКС від впливу внутрішніх і зовнішніх втручань та загроз навмисного, випадкового, природного або штучного характеру, що дозволило шляхом вивчення вітчизняного ринку засобів захисту інформації в ІКС від НСД та витоку її технічними каналами – дослідити життєвий цикл СФЗІ в ІКС, основні засоби реалізації СФЗІ, їх головні функції та характеристики;

2) удосконалена технологія прийняття рішення щодо раціонального варіанту дій при виборі засобів СФЗІ, що дозволило за рахунок розроблених моделі загроз та моделі порушника інформаційної безпеки ІКС та моделі фізичного захисту інформації в системі з повним перекриттям – здійснити обґрунтований вибір серед множини можливих раціонального варіанта засобу СФЗІ в ІКС з повним перекриттям та оцінити ступінь порушення системи фізичного захисту інформації в ІКС за метою реалізації.

Практичне значення отриманих результатів. Нові наукові результати, отримані в роботі, у сукупності складають підґрунтя для розроблення системи фізичного захисту інформації в ІКС від впливу внутрішніх і зовнішніх втручань та загроз навмисного, випадкового, природного або штучного характеру для забезпечення потреб державних і комерційних структур, а також підрозділів спеціального призначення.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Широке використання у процесі інформатизації суспільства сучасних методів і засобів обробки інформації створило не тільки об'єктивні передумови для підвищення ефективності всіх видів діяльності особистості, суспільства й держави в цілому, але й ряд проблем її технічного й фізичного захисту, що забезпечують необхідну якість відповідного інформаційного ресурсу. Загострення зазначеної проблеми демонструється нині широким поширенням таких явищ, як на рис.1.1:

– розголошення інформації (відомостей);

– несанкціонований доступ (НСД) до інформації та інших цінних ресурсів, що втримуються на різних носіях і циркулюють в рамках певної організації.

– перехоплення інформації (витік інформації технічними каналами);

– викрадення носіїв інформації.

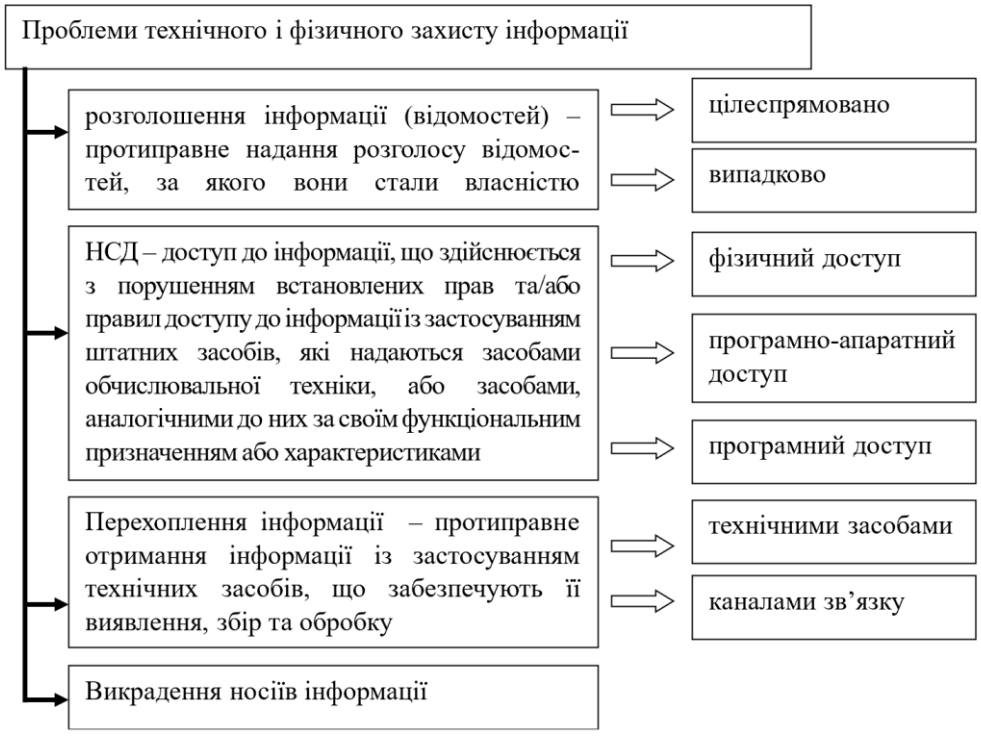

Рис.1.1. Форми витоку інформації

1.1. Методи реалізації НСД та захисту інформації від стороннього деструктивного впливу

1.1.1. Методи реалізації НСД

Під НСД звичайно мається на увазі доступ до інформації, що порушує встановлену в ІКС політику розмежування доступу. НСД може здійснюватися як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу комп'ютерної системи розробником під час розробки або системним адміністратором в процесі експлуатації, що входять у затверджену конфігурацію комп'ютерної системи, так і з використанням програмно-апаратних засобів, включених до складу комп'ютерної системи зловмисника.

Серед методів реалізації НСД до інформації виділяють такі:

Обхідний шлях (люк) – це блок, вбудований у велику програму, який зазвичай керується простими командами електронно-обчислювальної машини (ЕОМ), що дає можливість здійснювати її обробку засобами операційної системи (ОС), що в свою чергу дає змогу обійти систему захисту або реєстрацію в системному журналі. Звичайно ділянки програми, в яких реалізовано обхідний шлях (люк), вбудовуються в процесі розробки великих програмних комплексів, що призначені для виконання трудомістких функцій. Можливе також виявлення обхідних шляхів, вбудованих в ОС, що допомагає зловмиснику здійснювати НСД [1].

Троянський кінь – програма, яка реалізує функції знищення файлів і зміни їх захисту. «Троянський кінь» використовує по суті обман, щоб спонукати користувача запустити програму з прихованою в середині погрозою. Звичайно для цього стверджується, що така програма виконує деякі досить корисні функції. Зокрема, такі програми маскуються під які-небудь корисні утиліти. Небезпека «троянського коня» полягає в додатковому блоці команд, вставленому у вихідну нешкідливу програму, яка надається користувачам інформаційної системи (ІС). Цей блок команд може спрацьовувати при настанні якої-небудь умови (дати, стану системи) або по команді ззовні. Користувач, що запустив таку програму, наражає на небезпеку як свої файли, так й ІС в цілому.

Головними деструктивними функціями, які можуть бути реалізовані «троянськими кіньми» є:

- знищення інформації;
- перехоплення й передача інформації;
- цілеспрямована модифікація тексту програми.

Складний троянський кінь може бути запрограмований таким чином, що при зміні захисту може подавати зловмиснику умовний сигнал про можливість доступу до файлів. Після подачі сигналу троянський кінь деякий час очікує, а потім повертає файл у початковий стан. Отже, такий алгоритм дозволяє програмі зловмисника будь-які несанкціоновані дії з файлами без їх реєстрації. Загалом, «троянські коні» завдають шкоди ІС за допомогою розкрадання інформації і явного руйнування програмного забезпечення системи. «Троянський кінь» є однією з найнебезпечніших загроз безпеки ІС. Радикальний спосіб захисту від цієї загрози полягає в створенні замкнутого середовища виконання програм, які повинні зберігатися й захищатися від несанкціонованого доступу.

Логічна бомба – програма або частина програми, яка реалізує деяку функцію при виконанні певної умови. Логічні бомби використовуються для модифікації або знищення інформації, рідше для крадіжки або шахрайства.

Атака – використання вразливостей програмного забезпечення автоматизованої системи для досягнення цілей, що виходять за межі допуску даного суб'єкта в автоматизовану систему [3]. Наприклад, якщо користувач не має права на читання деяких даних, то він здійснює ряд відомих йому нестандартних маніпуляцій, які або забезпечують йому доступ до них, або завершуються невдачею. Тут мається на увазі також незаконне використання привілеїв. Більшість систем захисту встановлюють певні набори привілеїв для виконання заданих функцій. Кожний користувач одержує свій набір привілеїв: звичайні користувачі-мінімальний, адміністратор-максимальний. Несанкціонований захват привілеїв, приводить до можливості виконання порушником певних дій в обхід системи захисту. Слід зазначити, що незаконний захват привілеїв можливий або

при наявності помилок у системі захисту, або через недбалість адміністратора при керуванні системою й призначенні привілеїв.

Аналіз трафіку – аналіз частоти й методів контактів користувачів в автоматизованій системі. При цьому виявляються правила підключення користувачів до зв'язку, після чого зловмисником здійснюється спроба НСД під виглядом законного користувача.

Розрив лінії – перемикання лінії зв'язку від законного користувача по закінченні його сеансу зв'язку або через розрив лінії; при цьому дана подія не реєструється й автоматизована система працює зі зловмисником, як із законним користувачем.

Маскарад – це виконання яких-небудь дій одним користувачем від імені іншого користувача, що володіє відповідними повноваженнями. Метою «маскараду» є приписування яких-небудь дій іншому користувачеві або присвоєння повноважень і привілеїв іншого користувача. Прикладами реалізації «маскараду» є:

– вхід в систему під іменем і паролем іншого користувача (цьому «маскараду» передує перехоплення пароля);

– передача повідомлень у мережі від імені іншого користувача.

«Маскарад» особливо небезпечний у банківських системах електронних платежів, де неправильна ідентифікація клієнта через «маскарад» зловмисника може привести до більших збитків законного клієнта банку.

Підкладення свині – підключення до лінії зв'язку й імітація роботи системи з метою отримання інформації про ідентифікацію користувача. Наприклад, зловмисник може імітувати підвисання системи і процедуру повторного входу до неї. Користувач, нічого не підозрюючи про це, знову вводить свій ідентифікатор і пароль, після чого зловмисник повертає йому управління з нормально працюючою системою.

Повторне використання ресурсів – зчитування остаточної інформації, що призначена для знищення. Як об'єкти атаки можуть виступати не тільки блоки файлів, а й різного виду буфери, кадри сторінок пам'яті, сектори магнітних дисків, зони магнітних стрічок, реєстри пам'яті і т.д. Для зчитування даних прямо з пам'яті іноді достатньо створити невелику програму, яка робить запит під час виконання динамічного виділення пам'яті великого об'єму. Потім у

результаті навмисної помилки ця програма може аварійно завершитися з видачею «посмертного» дампа, який якраз і містить інформацію всіх ділянок пам'яті, яка використовувалася перед цим.

Використання комп'ютерного вірусу – використання набору команд ЕОМ, який виробляє і розповсюджує свої копії в мережах і навмисно виконує дії, що небажані для законних користувачів. Програми-віруси володіють рядом властивостей: вони народжуються, розмножуються та умирають. Ключовими поняттями у визначенні комп'ютерного вірусу є здатність вірусу до саморозмноження і здатність до модифікації обчислювального процесу. Вірус зазвичай розробляється зловмисниками таким чином, щоб як можна довше залишатися невиявленим у комп'ютерній системі. Вірус проявляється повною мірою в конкретний момент часу, коли відбувається деяка подія виклику, наприклад п'ятниця 13-го, відома дата й т.п [2].

Комп'ютерний вірус намагається таємно записати себе на комп'ютерні диски. Спосіб функціонування більшості вірусів полягає в такій зміні системних файлів комп'ютера, щоб вірус починав свою діяльність при кожному завантаженні. Наприклад, віруси, що вражають завантажувальний сектор, намагаються інфікувати частину дискети або жорсткого диска, зарезервовану, тільки для операційної системи та зберігання файлів запуску. Ці віруси особливо підступні, тому що вони завантажуються в пам'ять при кожному включенні комп'ютера. Такі віруси мають найбільшу здатність до розмноження й можуть постійно поширюватися на нові диски. Інша група вірусів намагається інфікувати виконувані файли, щоб залишитися невиявленими. Звичайно віруси віддають перевагу EXE- або Ком-файлам. Деякі віруси використовують для інфікування комп'ютерної системи як завантажувальний сектор, так і метод зараження файлів. Це ускладнює виявлення та ідентифікацію таких вірусів спеціальними програмами і веде до їхнього швидкого поширення. Існують і інші різновиди вірусів. Комп'ютерні віруси завдають шкоди системі за рахунок розмноження і руйнування середовища перебування.

Використання програми-імітатора – імітація роботи того чи іншого елемента мережі і створення у користувача автоматизованої системи ілюзії

взаємодії з системою з метою, наприклад, перехоплення інформації користувачів [3]. Зокрема, екранний імітатор дозволяє заволодіти паролями або кодами користувачів. При цьому, наприклад, операція перехоплення паролів здійснюється наступним чином. При спробі законного користувача ввійти в систему програма-перехоплювач імітує на екрані дисплея введення імені та пароля користувача, які відразу пересилаються власникові програми-перехоплювача, після чого на екран виводиться повідомлення про помилку та управління повертається операційній системі. Користувач припускає, що припустився помилки при введенні пароля. Він повторює введення і одержує доступ до системи. Власник програми-перехоплювача, що одержав ім'я й пароль законного користувача, може тепер використовувати їх у своїх цілях.

Наведені методи можуть застосовуватися для реалізації таких найбільш поширених сценаріїв НСД: перегляд інформації; копіювання програм та даних; читання даних з лінії зв'язку; зміна потоку повідомлень; закладки; зміна алгоритмів програм; зміна апаратної частини автоматизованої системи; зміна режиму обслуговування або умов експлуатації; перерва функціонування автоматизованої системи або її компонентів; перерва потоку повідомлень; перерва компонент програмного забезпечення; перерва процесу функціонування або його складових; фізичне руйнування апаратних засобів мережі; підробка; додавання фальшивих процесів і підміна справжніх процесів фальшивими; додавання фальшивих апаратних засобів; імітація роботи апаратно-програмних компонент мережі з боку суб'єктів загрози. Звичайно, можуть використовуватися різні комбінації наведених сценаріїв, що дуже ускладнює організацію захисту від НСД.

1.1.2. Методи захисту інформації від НСД

Під захистом від НСД слід розуміти діяльність, спрямовану на забезпечення додержання правил розмежування доступу шляхом створення і підтримки в дієздатному стані системи заходів із захисту інформації. Основні способи захисту інформації від НСД наведено в табл.1.1., до них належать:

– безпосереднє звернення до об’єктів з метою одержання певного виду доступу;

– створення програмно-апаратних засобів, що виконують звертання до об’єктів в обхід засобів захисту;

– модифікація засобів захисту, що дозволяє здійснити НСД;

– впровадження в комп’ютерну систему програмних або апаратних механізмів, що порушують структуру і функції комп’ютерної системи і дають можливість здійснити НСД.

Таблиця 1.1

Основні методи і засоби отримання інформації та її захисту від несанкціонованого доступу

Типова ситуація	Канали витоку інформації	Методи і засоби	
		отримання інформації	захист інформації
Розмова в приміщенні та на вулиці	Акустичний	Диктофон, мікрофон тощо	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
	Віброакустичний	Стетоскоп, вібродатчик	
	Електроакустич-ний	Спеціальний радіоприймач	
	Гідроакустичний	Гідроакустичний датчик	
Розмова через провідний телефон	Акустичний	Диктофон, мікрофон тощо	
	Електросигнал в лінії	Паралельний телефон, пряме підключення, електромагнітний датчик, диктофон, телефонна закладка	Маскування, скремблювання, шифрування, спецтехніка
	Наведення	Спеціальні радіотехнічні пристрої	Спецтехніка
Розмова по радіотелефону	Акустичний	Диктофон, мікрофон тощо	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу, маскування, скремблювання, шифрування, спецтехніка
	ВЧ-сигнал	Радіоприймачі	
Документ на паперовому носії	Безпосередньо документ	Крадіжка, прочитування, копіювання, фотографування	Обмеження доступу, спецтехніка
Виготовлення документа на паперовому носії	Продавлення стрічки або паперу	Крадіжка, причитування	Оргтехзаходи
	Паразитні сигнали (акустичний шум принтера)	Апаратура акустичного контролю	Пристрої шумозаглушування

Закінчення таблиці 1.1

Типова ситуація	Канали витоку інформації	Методи і засоби	
		отримання інформації	захист інформації
	Паразитні сигнали (наведення)	Спеціальні радіотехнічні засоби	Екранування
Поштові відправлення	Безпосередньо документ	Крадіжка, прочитування	Спеціальні методи
Документ на машинному носії	Носій інформації	Крадіжка, копіювання, прочитування	Контроль доступу, фізичний захист, криптозахист
Виготовлення документа на не паперовому носії	Відображення на дисплеї	Візуальний, копіювання, фотографування	Контроль доступу, фізичний захист, криптозахист
	Паразитні сигнали (наведення)	Спеціальні радіотехнічні пристрої	Контроль доступу, криптозахист, пошук закладок, екранування
	Електричні сигнали	Апаратні закладки	
	Програмний продукт	Програмні закладки	
Передача документа по каналах зв’язку	Електричні та оптичні сигнали	Несанкціоноване підключення, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, випромінювання тощо	Спецапаратура різного призначення	Оргтехзаходи, фізичний захист

Можна виділити такі узагальнені категорії методів захисту від НСД: організаційні; технологічні; правові. До першої категорії слід віднести заходи та засоби, що регламентуються внутрішніми інструкціями організації. Приклад такого захисту – присвоєння грифів секретності документам і матеріалам, що зберігаються у виділеному приміщенні, і контроль доступу до них персоналу. Другу категорію становлять механізми захисту, що реалізуються на базі програмно-апаратних засобів, наприклад систем ідентифікації і автентифікації або охоронної сигналізації. Третя категорія включає заходи контролю за виконанням нормативних актів загальнодержавного значення, механізми розробки і удосконалення нормативної бази, яка регулює питання захисту інформації. Методи, що реалізуються на практиці, як правило, об’єднують у собі елементи всіх категорій. Так, управління доступом до приміщень може являти собою комбінацію організаційних (видача допусків і ключів) і технологічних (установка замків і систем сигналізації) способів захисту.

Засоби захисту ІзОД від НСД можуть бути поділені також на:

1) пасивні – програмні, технічні (апаратні та фізичні) й соціально-правові;
2) активні – джерела безперебійного живлення, шумогенератори, скремблери.

Для захисту ІзОД на рівні прикладного й системного програмного забезпечення (ПЗ) можуть використовуватися системи розмежування доступу до інформації, системи ідентифікації й аутентифікації, системи аудита й моніторингу, а також системи антивірусного захисту. Найбільш цікавими пропозиціями на цьому ринку є комплекси засобів захисту інформації (далі – КЗЗ) типу: «ГРИФ-ХР», «ЛОЗА-1», «Бастіон-ХР», «РУБІЖ-РСО», «КРУД-Д», «ГРИФ-МЕРЕЖА», «ЛОЗА-2», «VTI-РУБІЖ», «АЙС», а також система захисту електронної пошти «Бриз». Характеристики та особливості реалізації цих КЗЗ наведені в табл. 1.2.

Таблиця 1.2

Основні характеристики та особливості реалізації комплексів засобів захисту інформації від НСД

№ з/п	Назва КЗЗ	Клас АС	ФПЗ, рівень гарній	Реалізація технології обробки інформації в ІКС	Особливості реалізації КЗЗ та ІКС в цілому
1	«Гриф-ХР»	«1»	КА-2, ДО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НІ-3, НК-1, НЦ-2, НТ-2 на рівні гарантій Г-4	Обробка інформації, що зберігається у вигляді файлів та каталогів на НЖМД з використанням типового прикладного програмного забезпечення (офісні пакети, програмне забезпечення обробки графіки та звуку, локальні бази даних з розмежуванням доступу користувачів на рівні файлів та каталогів)	Блокування завантаження ОС зі знімних носіїв інформації з використанням апаратного компонент
2	«ЛОЗА-1»	«1»	КД-2, КА-2, КО-0, ЦД-1, ЦВ-1, ДЗ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2 на рівні гарантій Г-3		Використання системи «ЛОЗА-1» потребує встановлення програмного продукту Microsoft Word 97/2000/XP/2003
3	«Бастіон-ХР»	«1»	КД-2, КО-0, ЦД-1, ДВ-1, НР-2, НИ-3, НК-1, НО-1, НЦ-1, НТ-2 на рівні гарантій Г-2		Може використовуватись обмежено для створення КСЗІ типових АС з чітко визначеними умовами функціонування.
4	«РУБІЖ-РСО»	«1»	КА-2, КО-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-1, НЦ-1, НТ-2 на рівні гарантій Г-3		–
5	«КРУД-К»	«1»	КА-2, КО-1, КК-3, ЦА-2, ЦО-1, ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2 на рівні гарантій Г-3		Функціонує під керуванням ОС Red Hat Enterprise Linux (версія 5.1)
6	«ГРИФ-МЕРЕЖА»	«2»	КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-5, НИ-3, НК-1, НО-2, НЦ-2, НТ-2 на рівні гарантій Г-4	Обробка інформації засобами локальної обчислювальної мережі, що зберігається у вигляді файлів та каталогів на НЖМД робочих станцій та виділеного файлового сервера (серверів) з використанням типового прикладного програмного забезпечення (офісні пакети, програмне забезпечення обробки графіки та звуку, локальні бази даних з розмежуванням доступу користувачів на рівні файлів та каталогів)	Функціонування локальної мережі організовується на базі домену Microsoft Windows 2000/2003, що складається з одного файлового сервера-контролера домену Microsoft Active Directory і включених у цей домен необхідної кількості файлових серверів та робочих станцій, що функціонують під керуванням ОС Microsoft Windows 2000/XP. Реалізована можливість ведення контролю за всіма подіями, що мають відношення до безпеки інформації з обмеженим доступом, з боку уповноважених осіб в режимі «реального часу».

Продовження таблиці 1.2

№ з/п	Назва КЗЗ	Клас АС	ФПЗ, рівень гарній	Реалізація технології обробки інформації в ІКС	Особливості реалізації КЗЗ та ІКС в цілому
7	«ЛОЗА-2»	«2»	КД-2, КА-2, КО-1, ЦД-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2 на рівні гарантій Г-3		КЗЗ може працювати як в одноранговій локальній мережі, так і в мережі, яка побудована на основі домену.
8	«АЙС»	«2»	ДР-2, НР-5, Г-4, КА-4, ЦА-4, ДС-3, НК-2, НИ-3, ДО-1, ЦО-2, ДЗ-3, НЦ-3, НО-3, КК-2, ДВ-3, НТ-3, НВ-3, КВ-4, ЦВ-3, НА-2, НП-2		–
9	«VTI-Рубіж»	«2», «3»	КД-2, КА-2, ДО-1, ЦД-2, ЦА-2, ЦВ-1, ЦО-2, ДВ-1; ДР-1, ДС-1, ДЗ-2, НР-5, НІ-3, НК-1, НО-3, НЦ-2, НТ-3 Роботи щодо отримання експертного висновку встановленого зразка, на відповідність вимогам нормативних документів в галузі ТЗІ, не завершені	На даний час розробник заявляє про готовність інтеграції в КЗЗ «VTI-Рубіж» власних (вбудованих) механізмів захисту СКБД Oracle, DB2 і операційних систем OS/390, AIX, Microsoft Windows NT/2000. У стадії розробки знаходяться драйвери для інтеграції операційної системи Linux	Багаторівнева ієрархічна система захисту інформації від НСД, яка складається з КЗЗ різних рівнів ієрархії та засобів забезпечення їх взаємодії. КЗЗ кожного з рівнів АС інтегрують у своєму складі визначені платформою та умовами функціонування АС механізми захисту інформації.
10	Захищена електронна пошта «Бриз»	«2», «3»	КВ-2, ЦВ-2, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-1, НО-2, НЦ-1, НТ-2, НА-2, НП-2 на рівні гарантій Г-4	Обмін електронними повідомленнями у форматі SMF-70, захищеними з використанням механізмів криптографічного захисту (електронний цифровий підпис, шифрування/розшифрування, створення імітовставок), між клієнтами електронної пошти, зареєстрованими на вузлах ЕП, через мережу передачі даних довільного типу.	Обмін даними між всіма вузлами АС (клієнтами, поштовими серверами) ведеться по протоколу FTP. Для генерування особистих ключів користувачів, а також для керування сертифікатами відкритих ключів використовує компоненти комплексу реалізації інфраструктури відкритих ключів «Тайфун-PKI».

Зазначені КЗЗ застосовують з метою забезпечення:

– ідентифікації й автентифікації користувачів на підставі імені, пароля й носія даних автентифікації (дискети, USB-Flash, Touch Memory тощо), що дає змогу розпізнавати конкретного легального користувача та надалі реагувати на запити цього користувача відповідно до його повноважень;

– розмежування обов'язків користувачів і визначення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрацію ресурсів, що захищають, реєстрацію користувачів, призначення прав доступу, обробку протоколів аудиту);

– підтримки різних рівнів повноважень користувачів та різних рівнів конфіденційності інформації («цілком таємно», «таємно», «для службового користування», «конфіденційна», «відкрита»);

– керування потоками інформації та блокування потоків інформації, що може привести до зниження її конфіденційності (наприклад, при копіюванні файлів або під час перенесення інформації через системний буфер обміну);

– контролю за виводом інформації на друк;

– контролю за експортом інформації на змінні носії та її імпорт;

– гарантованого знищення інформації шляхом затирання вмісту файлів, які містять інформацію з обмеженим доступом, при їх знищенні, що запобігає атакам типу «збір сміття»;

– контролю цілісності прикладного ПЗ та програмного забезпечення КЗЗ, а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів і дотриматись технології обробки інформації;

– розмежування доступу прикладних програм до захищених каталогів, що дозволяє забезпечити захист інформації з обмеженим доступом від несанкціонованого (випадкового) знищення або модифікації та дотриматися технології її обробки;

– контролю за використанням дискового простору користувачами (квоти), що виключає можливість блокування одним із користувачів можливості роботи інших;

– блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;

– контролю цілісності та самотестування КЗЗ при старті;

– відновлення функціонування КЗЗ після збоїв в роботі, що гарантує доступність інформації при дотриманні правил доступу до неї;

– реєстрації подій (входу користувача в ОС, спроб несанкціонованого доступу, фактів запуску програм, роботи з інформацією з обмеженим доступом, виводу на друк й т.п.) у спеціальних протоколах аудиту, що дозволяє адміністраторам контролювати доступ до інформації, стежити за тим, як використається КЗЗ, а також правильно його конфігурувати.

Система «Бриз», через специфічності покладених на неї функцій, має ряд відмінностей від інших КЗЗ. Вона призначена для забезпечення обміну електронними повідомленнями у форматі SMF-70 між клієнтами електронної пошти, зареєстрованими на вузлах електронної пошти, захищеними з використанням механізмів криптографічного захисту:

– створення/перевірка імітовставки за алгоритмом, встановленим ГОСТом 28147-89;

– шифрування/дешифрування переданих повідомлень за алгоритмом, встановленим ГОСТом 28147-89;

– створення/перевірка повідомлень електронного цифрового підпису (далі – ЕЦП) за алгоритмом, встановленим ГОСТом 34.310-95, ГОСТ 34.311-95;

– створення/перевірку квитанцій ЕЦП за алгоритмом, встановленим ГОСТом 34.310-95, ГОСТ 34.311-95.

Таким чином, порівняно з іншими системами електронної пошти (наприклад Microsoft Exchange) система «Бриз» додатково реалізує:

1) гарантовану доставку повідомлень одержувачеві (або гарантоване сповіщення відправника про неможливість доставки);

2) гарантоване сповіщення відправника про факт одержання повідомлення одержувачем з неможливістю останнього відмовитися від факту одержання;

3) безперервний захист повідомлень на всьому шляху від відправника до одержувача.

Для *захисту ІзОД на апаратному рівні* використовуються апаратні ключі, системи сигналізації, засоби блокування пристроїв і інтерфейсів вводу-виводу інформації. У комунікаційних системах можуть бути використані наступні засоби мереженого захисту інформації [5]:

міжмережні екрани (*Firewall*) – для блокування атак із зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall від компанії Nortel Networks). Вони управляють проходженням мереженого трафіка відповідно до правил (policies) безпеки. Як правило, міжмережні екрани встановлюються на вході мережі й розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;

системи виявлення вторгнень (IDS - Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу «відмова в обслуговуванні» (Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі;

засоби створення віртуальних приватних мереж (VPN - Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;

засоби аналізу захищеності – для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації загроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

1.1.3. Вимоги щодо захисту інформації від НСД

Для забезпечення захисту інформації в ІКС відповідно до вимог НД ТЗІ та НД КЗІ створюється комплексна система захисту інформації (КСЗІ). Її метою є реалізація єдиної політики інформаційної безпеки, що дозволить здійснювати автоматизовану обробку інформації з обмеженим доступом відповідно до нормативних та законодавчих актів України в галузі захисту інформації. В ході створення КСЗІ має бути розроблена політика безпеки АС-Р, мета якої та основні положення визначаються відповідно до НД ТЗІ 1.1-002-99 та НД ТЗІ 1.4-001-2000. Вимоги щодо КСЗІ в ІКС визначаються Законом України «Про захист інформації в автоматизованих системах», «Про державну таємницю» нормативно-правовими актами та нормативними документами систем технічного та криптографічного захисту інформації.

Архітектура КСЗІ щодо напрямків розвитку повинна узгоджуватися і відповідати принципам побудови ІКС та базуватися на ідеології побудови розподілених систем, а саме:

– будуватись на основі сертифікованих спеціалізованих засобів захисту та штатних вбудованих механізмів захисту інформації системного програмного забезпечення – мережних операційних систем, СУБД, комунікаційних пакетів, операційних систем мережних робочих станцій;

– досягатись модульною побудовою, що дозволить включати до її складу додаткових програмно-апаратних засобів захисту;

– забезпечуватись централізованим адмініструванням в неоднорідному середовищі робочих станцій та серверів, яке гарантуватиме реалізацію управління віддаленими локальними мережами та робочими станціями з єдиного центру управління.

При цьому створена КСЗІ повинна відповідати наступним вимогам:

– оперативно реагувати на зміну факторів, які визначають методи і засоби захисту інформації;

– базуватися на кращих алгоритмах закриття інформації, дозволених для використання в Україні для захисту інформації з різним ступенем секретності, що гарантує надійний криптографічний захист;

– мати механізми ідентифікації, аутентифікації користувачів та контролю дійсності переданої і збереженої інформації;

– здійснювати захист від несанкціонованого доступу до інформації у базах даних, файлах, на носіях інформації, а також при передачі її по лініях зв'язку в локальних і глобальних мережах;

– забезпечувати режим обміну інформацією з різним ступенем секретності;

– забезпечувати різні рівні доступу користувачів до інформації;

– мати зручну й надійну ключову систему, тобто гарантію безпеки при розподілі ключів між користувачами;

– забезпечувати використання ЕЦП в підсистемі електронного документообігу.

До складу КЗЗ повинні входити підсистеми, які забезпечують цілісність та доступність інформації, міжмережне екранування, антивірусний захист, виявлення та блокування вразливостей, розмежування доступу, виявлення міжмережних та внутрішньомережних втручань, аутентифікацію та ідентифікацію користувачів системи, у тому числі з використання електронного цифрового підпису, контроль цілісності та доступності мережної архітектури [9]. З метою забезпечення застосування ЕЦП в системі електронного документообігу має бути створений на базі Замовника акредитований центр сертифікації ключів ЕЦП. Вимоги до нього мають визначатись в технічному завданні на КСЗІ або окремому технічному завданні.

Мають бути розроблені організаційні заходи щодо забезпечення захисту інформації, які будуть регламентувати діяльність користувачів ІКС на нормативно-правовій основі чинного законодавства України у галузі захисту інформації.

Відповідність КСЗІ та її елементів вимогам технічного захисту інформації повинні підтверджуватись такими документами: КСЗІ – атестатом відповідності, виданим ДССЗЗІ України за результатами державної експертизи у сфері ТЗІ;

комплекс ТЗІ – актом атестації відповідно до вимог, затверджених наказом ДССЗЗІ України від 12.12.2007 №232; засоби захисту – сертифікатами відповідності або позитивними експертними висновками, отриманими відповідно до «Порядку проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення», затвердженого спільним наказом ДСТСЗІ СБ України від 09.07.2001 №329/32 та «Положення про державну експертизу у сфері технічного захисту інформації», затвердженого ДССЗЗІ України від 16.05.2007 №93; центр сертифікації ключів (за необхідністю) – свідоцтвом про акредитацію відповідно до вимог постанови Кабінету Міністрів України від 13.07.2004 №903.

1.2. Засоби захисту інформації в ІКС від витоку її технічними каналами

Під витоком інформації технічними каналами розуміється неконтрольоване поширення інформації, що може привести до її несанкціонованого одержання, тобто до порушення її конфіденційності. При цьому до загроз порушення конфіденційності інформації відносять спроби її витоку технічними каналами (див. рис.1.2) шляхом [8]:

- несанкціонованого перехоплення електронних і акустичних випромінювань;
- примусового електромагнітного опромінення (підсвічування) ліній зв’язку;
- несанкціонованого застосування закладених пристроїв і програмних закладок;
- відновлення тексту принтера та дистанційного фотографування;
- розкрадання носіїв інформації й документальних відходів;
- читання або копіювання як відкритої, так і конфіденційної інформації, імпорту або експорту такої інформації, а також обміну нею між елементами обчислювальної мережі, що належать до різних класів захищеності;
- копіювання носіїв інформації з подоланням засобів захисту;
- маскування під зареєстрованого користувача або під запити системи;
- використання недоліків мов програмування й операційних систем;
- незаконне підключення до апаратури і ліній зв’язку;

– виведення з ладу механізмів захисту;

– впровадження і використання комп’ютерних вірусів тощо.

Під технічними каналами розуміють при цьому канали побічних електромагнітних випромінювань і наведень (ПЕМВН), акустичні (віброакустичні) та оптичні канали. Їх продуктивній роботі сприяє:

1) протікання електричного струму в технічних засобах ІКС, що за рахунок високочастотного випромінювання (радіоканал), а також створення наводок на мережу електроживлення (мережевий канал), проводи заземлення (канал заземлення) та на лінії зв’язку між ПЕОМ (лінійний канал) може індукувати струми в близько розміщених провідних лініях – канал ПЕМВН;

2) випромінювання засобів відображення інформації ІКС, що за рахунок розповсюдження звукових хвиль в повітрі або пружних коливань в інших середовищах може індукувати акустичні (віброакустичні) наведення;

3) випромінювання оптичних засобів.

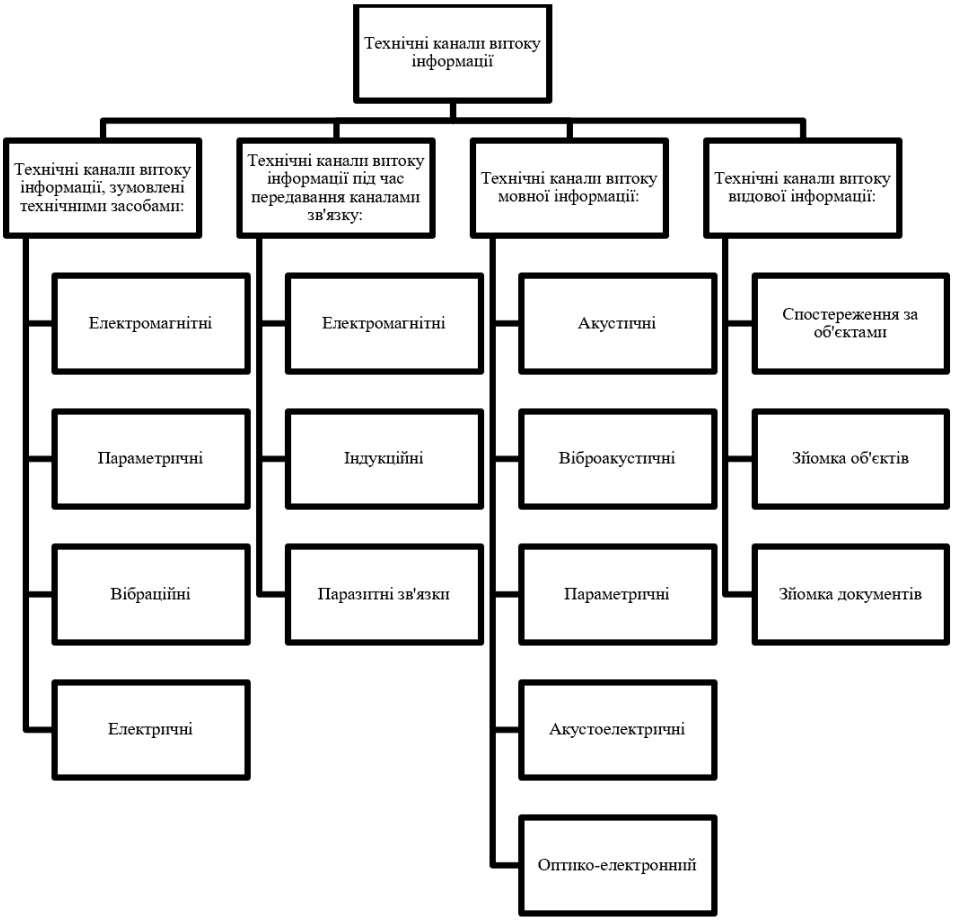

Рис. 1.2. Технічні канали витоку інформації

Захист ІзОД від її витоку технічними каналами зв’язку забезпечується за рахунок використання екранованого кабелю й прокладення проводів і кабелів в екранованих конструкціях, встановлення на лініях зв’язку високочастотних фільтрів та активних систем зашумлення, створення екранованих приміщень («капсул») та використання екранованого устаткування тощо. Серед них найбільшого поширення нині отримали стаціонарні прилади «РІАС-1С», «РІАС-1С/1» та «РІАС-1С/2», мобільний прилад «РІАС-1М», комп’ютерний прилад «РІАС-1К» та високочастотний – «РІАС-1У». Всі вони мають вбудовані системи автоматичного контролю функціонування та звукову індикацію цілісності випромінюючих антен. Їх призначення, склад та технічні характеристики подані у табл. 1.3.

Таблиця 1.3

Призначення, склад та технічні характеристики засобів ТЗІ, носіями якої є електромагніті поля та електричні сигнали

Найменування приладу	Призначення	Склад	Технічні характеристики									
			Смуга використовуваних частот	Коефіцієнт якості шумового сигналу	Спектральна щільність напруженості електричного і магнітного компонентів електромагнітного поля на відстані 1 м від антени	Коефіцієнт міжспектральних кореляційних зв'язків	Регулювання рівня шумового сигналу	Максимальне інтегральне значення вихідної потужності	Електроживлення	Час технічної готовності	Габарити	Маса
Прилад радіочастотного шуму стаціонарний «РІАС-1С»	Захист об'єктів від витоку конфіденційної інформації каналами побічних електромагнітних випромінювань і наведень (далі – ПЕМВН) шляхом генерації шумового сигналу	генератор шуму «РІАС-1ГС» і антени рамкові м'які «РІАС-1АМ»	від 180 Гц до 2 ГГц і вище	не < 0,8	у діапазоні від 0,00018 до 100 МГц – не менш 65 дБ; у діапазоні від 100 до 100 МГц – не менш 70 дБ; у діапазоні від 500 до 1200 МГц – не менш 70 дБ; у діапазоні від 1200 до 2000 МГц – не менш 70 дБ.	не > 6 дБ	не < 20 дБ	не < 10 Вт	мережі змінного струму напругою 220 В плюс 22 В мінус 33 В, частотою (50 ±1) Гц.	не > 1 с	не > 190x187x63 мм	не > 2 кг
Прилад радіочастотного шуму стаціонарний «РІАС-1С/1»		генератор шуму «РІАС-1ГС/1» і антени дипольні телескопічні «РІАС-1АД»	від 180 Гц до 1 ГГц і вище					не < 8 Вт				
Прилад радіочастотного шуму стаціонарний «РІАС-1С/2»		генератор шуму «РІАС-1ГС/2» і антени дипольні, телескопічні «РІАС-1АД»	від 180 Гц до 2,5 ГГц і вище					не < 15 Вт				
Прилад радіочастотного шуму мобільний «РІАС-1М»		генератор шуму «РІАС-1ГМ», антени дипольні телескопічні «РІАС-1АД» і антена рамкова жорстка «РІАС-1АЖ»	від 180 Гц до 2 ГГц і вище					не < 15 Вт			не > 460x380x130 мм	
Прилад радіочастотного шуму комп'ютерний «РІАС-1К»		генератор шуму «РІАС-1ГМ», антени дипольні телескопічні «РІАС-1АД» і антена рамкова жорстка «РІАС-1АЖ»						не < 10 Вт			не > 195x145x43 мм.	
Прилад радіочастотного шуму високочастотний «РІАС-1У»		генератор шуму «РІАС-1ГВ» і антени дипольні телескопічні «РІАС-1АД»	від 0,5 ГГц до 2 ГГц.		у діапазоні від 500 до 1000 МГц – не менш 70 дБ; у діапазоні від 1000 до 2000 МГц – не менш 70 дБ.						не > 153x135x50 мм	

Окрім цього до засобів технічного захисту інформації належать:

- трансформатор поділяючий «PIAC-4T»;
- система заземлення технології «Galma»;
- комплекс засобів обчислювальної техніки у захищеному виконанні на базі ЕОМ «ПЛАЗМА-ЗВ»;
- автоматизоване робоче місце «МЕЖА»;
- персональні комп'ютери із захистом інформації «EXPERT».

Прилад «PIAC-4T» (поділяючий трансформатор) призначений для гальванічної розв'язки ліній електроживлення і являє собою поділяючий трансформатор з обмоткою, що виконує функцію електромагнітного екрана. Прилад обладнаний системою захисту від перевантаження та термозахистом. Системи заземлення є складовою частиною будь-якого об'єкта на якому для роботи з інформацією з обмеженим доступом застосовуються засоби ЕОТ. Визнаним лідером щодо впровадження подібних систем на теренах України є компанія «Watson Telecom» (м. Київ). Вона пропагує системи, що будуються за технологією «Galmar» і являють собою довговічні та надійні пристрої заземлення зі стабільними електричними параметрами, які гарантують як захист обслуговуючого персоналу, так і захист та безперебійну роботу електричного і електронного устаткування.

Системи заземлення за технологією «Galmar» можуть широко застосовуватись для організації та ремонту всіх видів пристроїв заземлення при будівництві та реконструкції різних об'єктів: телекомунікації; енергетики; мобільного зв'язку; відомчих і корпоративних мереж зв'язку та передачі даних; промислових підприємств та установ; нафтогазової галузі, а також на об'єктах, на яких встановлені сучасні системи безпеки, та пожежно-охоронної сигналізації. На цей час пристрої заземлення за технологією «Galmar» сертифіковані в Україні. Їх основні переваги полягають у:

1) модульному принципі побудови (установка вібромолотом шляхом поступового нарощування довжини);
2) можливості встановлення глибинних заземлювачів (до 40 метрів);

3) мінімальній площі пристрою заземлення;

4) значному зменшенню обсягів підготовчих робіт;

5) зручності та технологічності монтажу;

6) високій стійкості до ґрунтової та електролітичної корозії;

7) гарантованій товщині мідного покриття (не менш за 250 мкм), високій стійкості мідного покриття до вигину та відшарування;

8) мінімальних експлуатаційних витратах тощо.

Опір таких пристроїв не залежить від погодних умов і становить 2 Ом.

Комплекс засобів обчислювальної техніки (далі – КЗОТ), що виконаний у захищеному варіанті на базі електронно-обчислювальної машини «ПЛАЗМА-ЗВ» – призначений для захисту інформації, яка обробляється, з будь-яким рівнем обмеження доступу (конфіденційності), включаючи інформацію особливої важливості. Він серійно виготовляється на підприємствах України й забезпечує захист інформації від перехоплення по: каналах ПЕМВ та наведень сигналів від ЗОТ; лініям електроживлення (за рахунок вбудованої в системний блок системи фільтрації, з рівнем загасання наведень на електромережу не менше 80 дБ); випромінюванням вбудованих радіозакладних пристроїв і при високочастотному нав’язуванні або опроміненні [5]. В ньому також передбачений захист від електромагнітного силового впливу з ефіру (від електромагнітного тероризму й зброї). Інформативні сигнали на відстані 1 м від КЗОТ не виявляються. Використання КЗОТ «ПЛАЗМА-ЗВ» не вимагає застосування спеціальних екранованих приміщень та активних технічних засобів захисту інформації. Його системний блок, виконаний у металевому радіоекранованому корпусі із проточною вентиляцією, системою фільтрації по сигнальних ланцюгах і ланцюгу електроживлення, забезпечує практично будь-яку необхідну кількість захищених посадкових місць для знімних накопичувачів (вінчестерів, DVD±RW, Flash-карт) і інших пристроїв. Можливість зберігання конфіденційної інформації поза ЗОТ забезпечує додатковий рівень її захисту в неробочий час і при профілактичному обслуговуванні ЗОТ. Для захисту

інформації від НСД в ЗОТ «ПЛАЗМА-ЗВ» можуть встановлюватись сертифіковані засоби розмежування доступу.

Автоматизоване робоче місце (далі – АРМ) «Межа» призначене для застосування в комплексних системах захисту інформації (КСЗІ) ІКС в якості шлюзів доступу при взаємодії фізично розділених інформаційних систем, що обробляють інформацію різних рівнів конфіденційності (наприклад, мережа – Інтернет та корпоративна мережа – Інтранет), а також для створення спеціалізованих багатофункціональних АРМ з розділеною обробкою інформації.

Рішення, які застосовуються в АРМ «Межа», роблять неможливим несанкціонований доступ до конфіденційної інформації для користувачів відкритої мережі, а також запобігають проникненню вірусів з Інтернету в корпоративну мережу. При цьому об'єктами розмежування доступу в АРМ «Межа» є: жорсткі диски; інші пристрої зберігання інформації (накопичувачі на гнучких магнітних дисках, CD-ROM, CD-RW, магнітооптика і т.п.); мережеві карти; інші (спеціальні) пристрої, які встановлюються на шину PCI.

Персональні комп'ютери із захистом інформації «EXPERT» – призначені для обробки інформації з обмеженим доступом. В комп'ютерах «Expert» забезпечується захист інформації від її несанкціонованого знімання по ПЕМВН, лініям електроживлення та заземлення (у тому числі й по каналу високочастотного нав'язування). Випромінювання знижуються до рівня, який задовольняє найбільш жорстким вимогам до ПЕМВН. Комп'ютер забезпечує надійний захист та водночас зручність звичайного ПК, при цьому зовнішній вигляд ПК з захистом інформації не відрізняється від типових зразків ПК [9]. Використання сучасних пасивних методів захисту в сполученні з оригінальними схемотехнічними рішеннями робить ПК максимально безпечним для здоров'я оператора, а також забезпечує захист ПК від зовнішніх електромагнітних випромінювань та від навмисного зовнішнього електромагнітного впливу, спрямованого на знищення інформації чи порушення працездатності ПК. Склад типового АРМ з захистом інформації включає екранований системний блок з покращеною системою теплообміну та фільтрацією повітря, 15" або 17" TFT

монітор, лазерний принтер, акустична система (за необхідністю), мережевий фільтр УСС-4. Додатково в складі ПК можуть застосовуватись засоби несанкціонованого доступу для створення КСЗІ автоматизованих систем (далі – АС) різних класів.

Завдання щодо захисту ІзОД від витоку технічними каналами вирішуються в межах технічного захисту інформації (ТЗІ). Згідно нормативних документів ТЗІ – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка [14]:

- є важливою для особи, суспільства і держави;
- обробляється, циркулює і відображається в ІКС та засобах ЕОТ;
- становить державну та іншу передбачену законом таємницю;
- є власністю держави або передана їй у власність, користування і розпорядження.

Створення комплексу ТЗІ передбачає виконання передпроєктних робіт (1 етап), розроблення та впровадження заходів із захисту інформації (2 етап), а також випробування та атестація комплексу ТЗІ (3 етап) й містить у собі проведення організаційних, інженерних і технічних заходів на об’єктах інформаційної діяльності (ОІД), де передбачається [11]:

– озвучення ІзОД (при проведенні нарад, показів зі звуковим супроводженням кіно- і відеофільмів тощо);

– здійснення обробки ІзОД технічними засобами (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання ІзОД тощо);

– обіг іншої ІзОД при проєктуванні, будівництві, експлуатації об’єктів, виробництві технічних засобів тощо.

У створенні комплексу ТЗІ беруть участь: установа, яка є замовником створення комплексу ТЗІ; виконавець робіт зі створення комплексу ТЗІ; виконавець проведення випробувань щодо створення комплексу ТЗІ, а також виконавець проведення атестації комплексу ТЗІ. Склад засобів забезпечення ТЗІ (див. рис.1.3),

перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, які володіють, користуються і розпоряджається ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами технічного захисту інформації. Їх вибір зумовлюється фрагментарним або комплексним способом захисту інформації. При цьому фрагментарний захист забезпечує протидію певній загрозі, а комплексний – одночасну протидію множині загроз.

Рис.1.3. Заходи та засоби ТЗІ

Засоби ТЗІ можуть функціонувати при цьому або автономно, або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих в них складових елементів. З метою оцінювання стану ТЗІ, що обробляється або циркулює в ІС, комп'ютерних мережах та системах зв'язку, а також підготовки обґрунтованих виводів для прийняття відповідних рішень проводиться експертиза в сфері технічного захисту інформації.

Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізація заходів технічного захисту інформації, розрахунку ефективності захисту та порядку атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами з ТЗІ: НД ТЗІ 3.1-001-07, НД ТЗІ 3.3-001-07, НД ТЗІ 2.1-002-07 [9-10]. Державні стандарти України ДСТУ 3396.0-96, ДСТУ 3396.1-96 при виконанні робіт з ТЗІ використовуються в

частині, що не суперечать вимогам зазначених НД ТЗІ. Однак процедури оцінки сумарних витрат на придбання засобів ТЗІ та/або КЗІ, а також на розробку та впровадження всіх необхідних заходів захисту ІзОД в інформаційній, телекомунікаційній чи автоматизованій системі є доволі складними та суперечливими. Наприклад, при створені об'єктів інформаційної діяльності на яких розміщені АС класу «1» з типовим переліком функціональних сервісів, досить нескладно визначити сумарні витрати на закупівлю засобів захисту інформації від несанкціонованого доступу. Вартість однієї ліцензії на використання комплексів засобів захисту інформації типу «Гриф-ХР», «Лоза-1» або «Рубіж-РСО» складає близько 2000 грн. Вартість послуг, щодо створення КСЗІ типової АС класу «1», складає від 10 до 15 тис. грн Однак, вартість витратних матеріалів, комплектуючих та послуг при створенні комплексу технічних засобів захисту інформації (КТЗІ) можна визначити лише для конкретних умов експлуатації АС на конкретному об'єкті інформаційної діяльності і, в певних умовах, вартість системи захисту в цілому може підвищитись на порядок. При розрахунку сумарних витрат на засоби захисту інформації в АС класу «2» теж можна відштовхуватись від типового варіанту їх реалізації – локальна мережа робочої групи з виділеним файловим сервісом. Вартість комплексів засобів захисту інформації типу «Гриф-Мережа» або «Лоза-2» складає від 800 до 4000 грн (залежно від ліцензії на кількість робочих місць в АС). Вартість послуг, щодо створення КСЗІ типової АС класу «2», складає близько 11 тис. грн на одне робоче місце.

Однак, за необхідності реалізації в АС класу «2» додаткових сервісів (баз даних, електронного документообігу, веб-сервісів тощо) вартість засобів захисту та послуг щодо створення КСЗІ визначити досить складно, оскільки на вітчизняному ринку не існує типових рішень для таких систем.

Відносно захисту ІзОД в АС класу «3» взагалі не існує типових рішень – кожна така система по своєму унікальна.

Досить показовим прикладом є досвід створення системи Електронного реєстру виборців України. Це автоматизована система класу «3», що має близько

800 територіально розподілених вузлів. Сумарні витрати на систему захисту інформації склали близько 40 млн грн, що складає половину загальних витрат на створення системи в цілому.

Висновки до першого розділу

1. Інформація як об’єкт безпеки індиферентна до загроз, небезпек і ризиків. Захищати необхідно не інформацію, а суб’єктів інформаційних відносин від заподіяння їм шкоди за допомогою певних дій з інформацією.

2. Одні й ті самі дії з інформацією (збір, модифікація, знищення, витік, НСД тощо) в одних випадках можуть містити загрозу й у випадку її реалізації приносити шкоду, в інші – не є загрозою й здатні приносити користь.

3. Загрози суб’єктам інформаційних відносин – виробникові, власникові, споживачеві інформації, третім особам, – відрізняються одна від одної так само як і методи й засоби протидії їм.

4. Сама небезпечна загроза інформації – перекручування, а самі небезпечні джерела загроз – ті, що створюють (виробляють) і розпоряджаються інформацією. Саме вони мають максимальні можливості (вільно або мимоволі) спотворити інформацію.

5. На сьогодні, вітчизняний ринок засобів (комплексів) технічного (ТЗІ) та криптографічного захисту інформації (КЗІ) наповнений досить широким спектром продукції, що дає можливість створювати СФЗІ інформаційних та телекомунікаційних систем різного призначення.

6. Рішення щодо доцільності використання конкретних засобів ТЗІ чи КЗІ необхідно приймати за наявності змістовної характеристики інформаційної, телекомунікаційної чи автоматизованої системи в якій необхідно забезпечити захист ІзОД або інформації, яка є власністю держави. Це, як правило, визначається:

- вищим грифом секретності інформації, що обробляється в системі;
- класом автоматизованої системи;

– переліком функціональних послуг (сервісів) які надаються користувачам інформаційної, телекомунікаційної чи автоматизованої системи;

– вимогами, щодо рівня захисту інформації, що обробляється (наприклад, перелік та рівень функціональних послуг захисту інформації);

– прийнятою політикою безпеки інформації;

– характеристикою користувачів та обслуговуючого персоналу системи;

– конкретними умовами експлуатації інформаційної, телекомунікаційної чи автоматизованої системи тощо.

7. Порядок створення та введення в експлуатацію СФЗІ інформаційних та телекомунікаційних систем визначений вітчизняною системою нормативних документів в галузі ТЗІ і є обов’язковим до виконання всіма суб’єктами господарювання.

РОЗДІЛ 2
ЖИТТЄВИЙ ЦИКЛ СИСТЕМ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. ЇХ ГОЛОВНІ ФУНКЦІЇ ТА ХАРАКТЕРИСТИКИ

На рис. 2.1 зображено ефективну систему безпеки ІКС, вона повинна забезпечувати такі базові властивості інформації, як:

доступність – можливість за прийнятний час отримати певну інформаційну послугу або гарантування безперешкодного доступу законних користувачів до захищеної інформації;

цілісність – актуальність та непротиречивість інформації, її захищеності від руйнування і несанкціонованого змінювання;

конфіденційність – захист від несанкціонованого ознайомлення тощо.

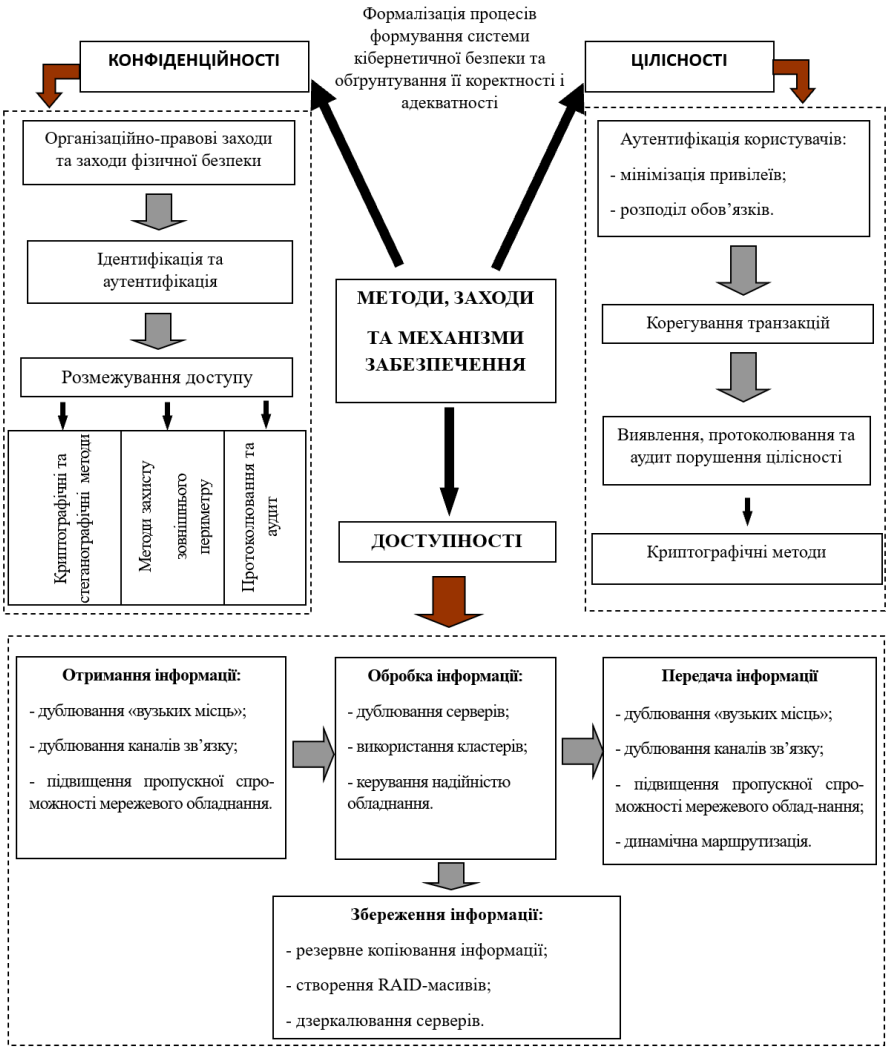

Рис. 2.1. Основні методи і заходи забезпечення безпеки інформації

Структура системи захисту від загроз порушення доступності подана на рис.2.2, а відповідні показники – на рис.2.3.

Рис. 2.2. Структура системи захисту від загроз порушення доступності

Рис. 2.3. Показники критеріїв доступності

Цілісність можна розглядати з двох сторін: як статичну (розуміється як незмінність інформаційних об'єктів) та як динамічну (стосовну до коректного виконання складних дій). Засоби контролю динамічної цілісності застосовуються зокрема при аналізі потоку фінансових повідомлень із метою виявлення крадіжки, перевпорядкування або

дублювання окремих повідомлень. Структура системи захисту від загроз порушення цілісності подана на рис.2.4, а відповідні показники – на рис.2.5.

Рис. 2.4. Структура системи захисту від загроз порушення цілісності

Рис. 2.5. Показники критеріїв цілісності

Забезпечення конфіденційності – нормативно найбільш пророблений аспект інформаційної безпеки. Але у практичній реалізації заходів із забезпечення конфіденційності сучасних інформаційних систем є серйозні труднощі. По-перше, встановлена законом вимога захисту персональних даних нормативно-правовими актами нижчого рівня й технологічно поки ще не забезпечена. По-друге, відсутні відкриті критерії щодо захисту від витоку конфіденційної інформації по технічних каналах, що

ускладнює задачу значної частини власників інформаційно-телекомунікаційних систем по оцінці можливих ризиків від реалізації відповідних загроз. По-третє, слабке пророблення поняття «конфіденційна інформація, що належить державі» не дозволяє диференційовано підходити до її різновидів, При цьому очевидно, що службова (конфіденційна) інформація Міноборони та Міносвіти мають різну цінову вагу. Це досить часто створює передумови для надмірних фінансових витрат на придбання апаратних засобів криптографічного захисту інформації, на шкоду більш дешевим (хоча й менш безпечним) програмним засобам [15]. Схема традиційного ешелонованого захисту від загроз порушення конфіденційності інформації в АС наведена на рис.2.6, а відповідні показники – на рис.2.7.

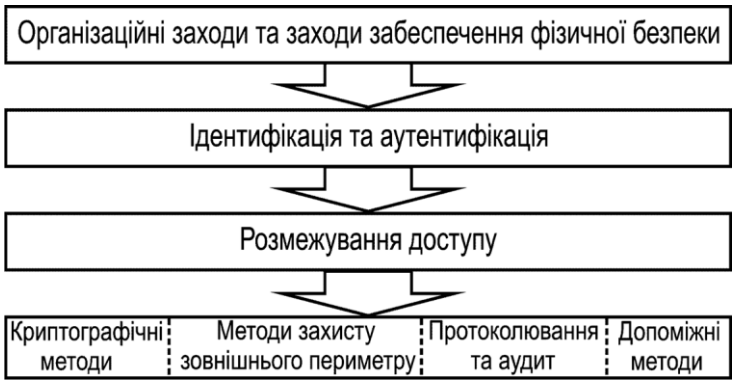

Рис. 2.6. Структура системи захисту від загроз порушення конфіденційності інформації

Рис. 2.7. Показники критеріїв конфіденційності

До загроз порушення конфіденційності, цілісності та доступності інформації в ІКС нині, як правило, відносять спроби щодо [13]:

1) несанкціонованого перехоплення електронних і акустичних випромінювань та застосування закладених пристроїв і програмних закладок, примусового електромагнітного опромінення ліній зв'язку, відновлення тексту принтера та дистанційного фотографування, розкрадання носіїв інформації й документальних відходів, читання або копіювання як відкритої, так і конфіденційної інформації, імпорту або експорту такої інформації, а також обміну нею між елементами обчислювальної мережі, що належить до різних класів захищеності, копіювання носіїв інформації з подоланням засобів захисту, маскування під зареєстрованого користувача або під запити системи, використання недоліків мов програмування й ОС, незаконного підключення до апаратури і ліній зв'язку, виведення з ладу механізмів захисту, впровадження і використання комп'ютерних вірусів тощо;

2) несанкціонованої модифікації та/або видалення програм і даних, вставки, зміни або видалення даних в елементах протоколу в процесі обміну між абонентами обчислювальної мережі, втрати даних у результаті збоїв, порушення працездатності елементів обчислювальної мережі або некомпетентних дій суб'єктів доступу тощо;

3) повторення або вповільнення елементів протоколу, придушення обміну в телекомунікаційних (ТК) мережах, використання помилок або недокументованих можливостей служб і протоколів передачі даних для ініціювання відмови в обслуговуванні, перевитрати обчислювальних або ТК ресурсів тощо.

Вони класифікуються за багатьма ознакам, а саме на рис.2.8:

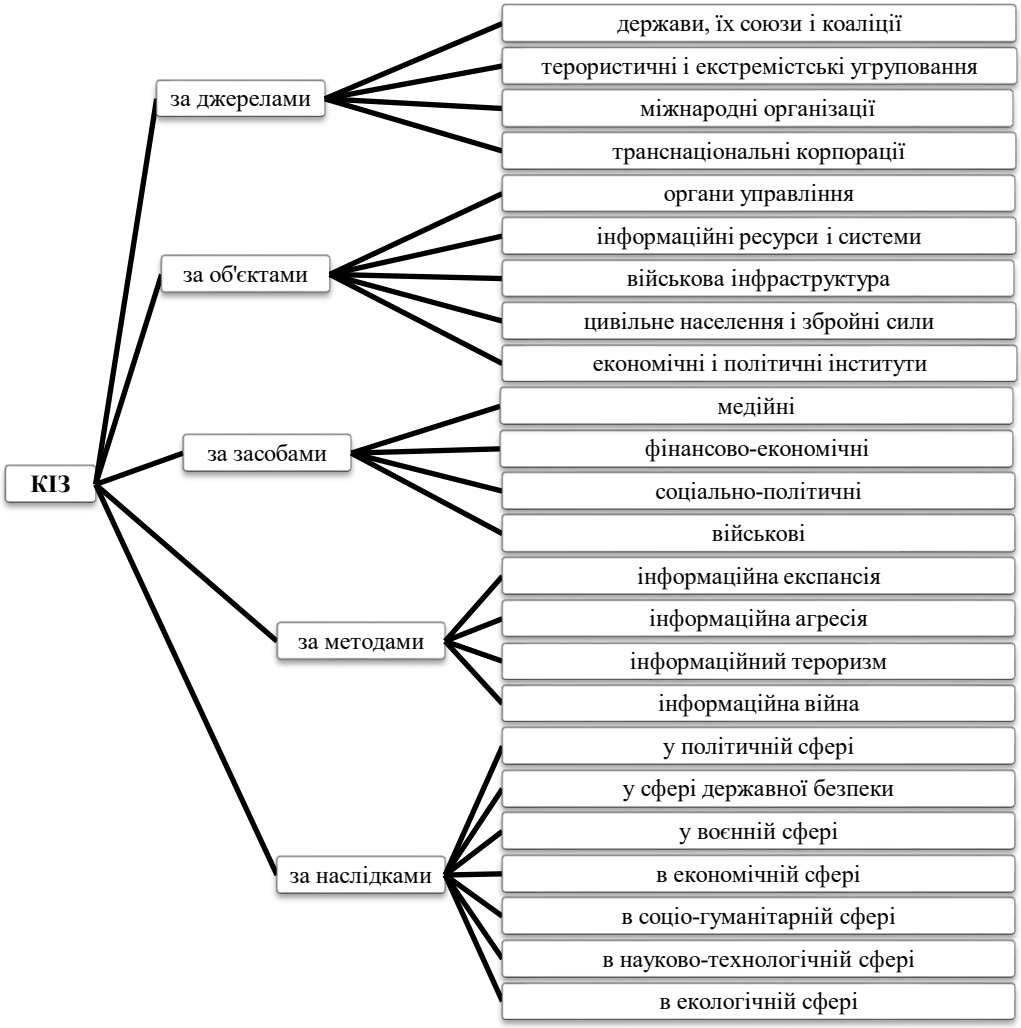

Рис.2.8. Класифікація інформаційних загроз

1) *за природою виникнення* на штучні (такі, що викликані дією людського фактора) та природні (такі, що виникли в результаті дії на АС об'єктивних фізичних процесів або стихійних природних явищ, не залежних від людини);

2) *за ступенем навмисності* на випадкові (обумовлені недбалістю або ненавмисними помилками персоналу) та навмисні (виникають в результаті цілеспрямованої діяльності зловмисника, наприклад, проникнення його на територію, що охороняється, з порушенням встановлених правил фізичного доступу);

3) *залежно від джерела* на загрози, джерелом яких є природне середовище (пожежі, повені і інші стихійні лиха), загрози, джерелом яких є людина (влаштування агентів в ряди персоналу АС з боку конкуруючої організації), загрози, джерелом яких є санкціоновані програмно-апаратні засоби (некомпетентне використання системних

утиліт) та загрози, джерелом яких є несанкціоновані програмно-апаратні засоби (наприклад, інсталяція в систему кейлогерів);

4) *за положенням джерела* на загрози, джерело яких розташовано зовні контрольованої зони (перехоплення побічних електромагнітних випромінювань або перехоплення даних, що передаються каналами зв'язку; дистанційна фото- і відеозйомка; перехоплення акустичної інформації з використанням направлених мікрофонів) та загрози, джерело яких розташовано в межах контрольованої зони (застосування підслуховуючих пристроїв або розкрадання носіїв, що містять конфіденційну інформацію);

5) *за ступенем впливу на ІКС* на пасивні (несанкціоноване копіювання файлів з даними) та активні загрози (порушують структуру ІКС);

6) *за способом доступу до ресурсів ІКС* на загрози, що використовують стандартний доступ (несанкціоноване отримання пароля шляхом підкупу, шантажу, необережного зберігання, або фізичного насильства по відношенню до законного власника) та загрози, що використовують нестандартний шлях доступу (використання незадекларованих можливостей засобів захисту).

Забезпечити захист від цих, а також низки інших подібних загроз здатні системи фізичного захисту інформації (СФЗІ), що спроєктовані на принципах системної єдності, сумісності, розвитку, превентивності та модульності (див. рис. 2.9).

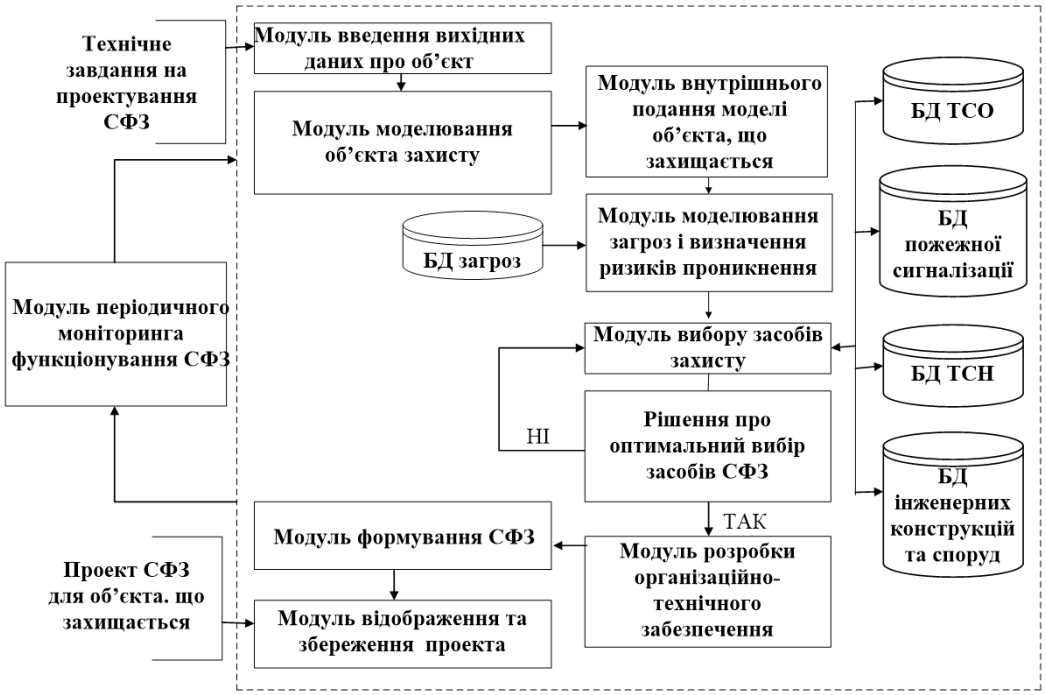

Рис. 2.9. Структурна схема типової систем фізичного захисту

СФЗІ являють собою сукупність правових норм, організаційних заходів та інженерно-технічних рішень, спрямованих на захист життєво важливих інтересів та ресурсів (в тому числі й інформаційних) певного об'єкта, його споруд та приміщень де розташований ІКС, самої ІКС та допоміжного обладнання (принтери, сканери тощо), носіїв інформації (роздруківок, дисків тощо) і каналів передачі/отримання інформації від загроз, джерелами яких є несанкціоновані впливи фізичних осіб (терористів, злочинців, екстремістів тощо). Вони ґрунтуються на застосуванні як фізичних перешкод для зловмисників – механічних, електро- або електронно-механічних пристроїв, що закривають шляхи доступу до ІзОД, так й технічних засобів візуального нагляду, зв'язку та охоронної сигналізації на визначених периметрах безпеки, що закривають шляхи проникнення у контрольовану зону (КЗ) де розмішена апаратура або носії інформації й забезпечується шляхом установки ряду бар'єрів, розташованих у стратегічних місцях (див. рис.2.10). Вимоги до кожного захисного бар'єра СФЗ та його місця розташування повинні визначатися при цьому цінністю інформації, ризиком порушення безпеки, а також необхідністю дотримання наявних захисних мір.

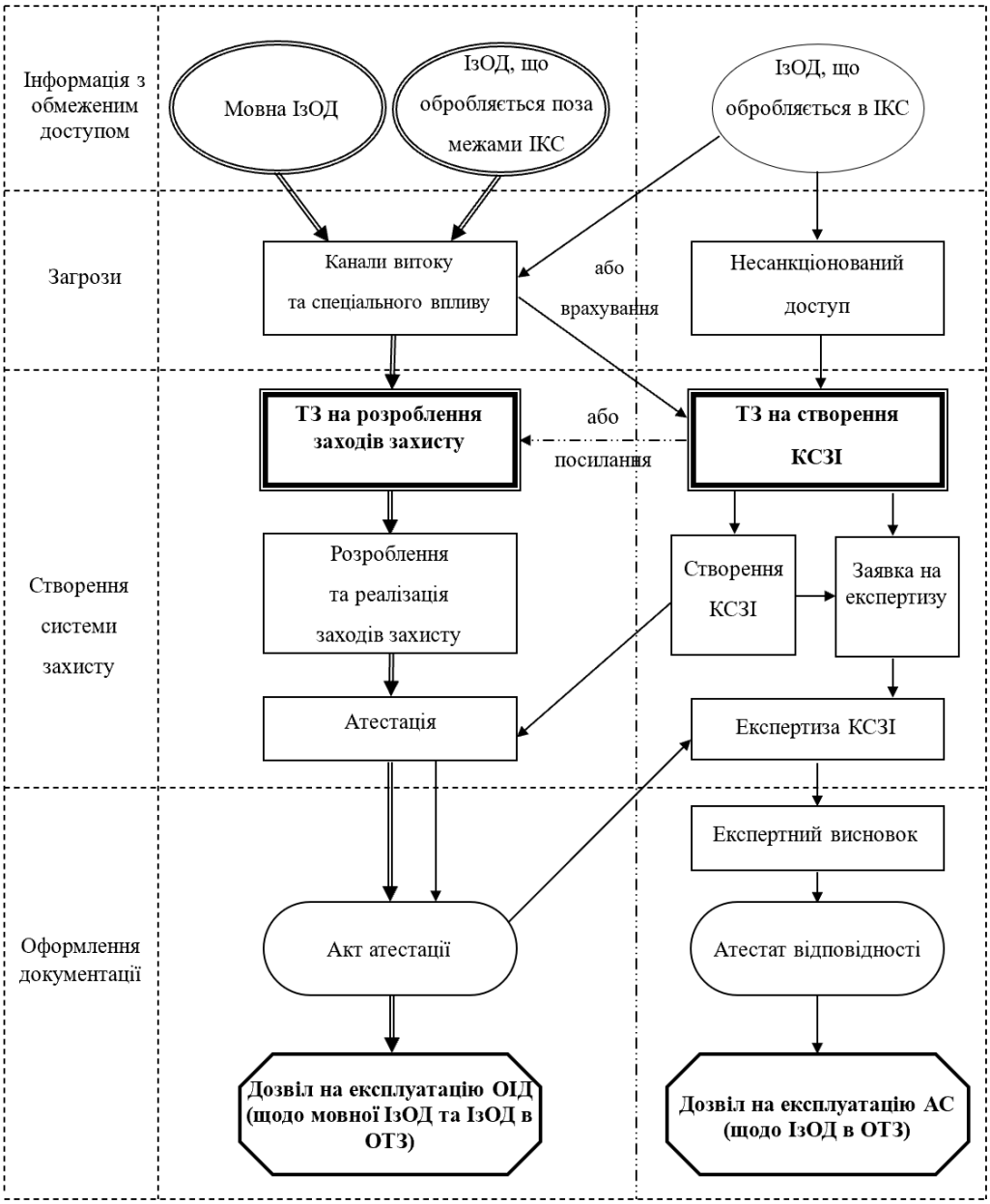

Рис.2.10. Загальний порядок дій при створенні СФЗІ

Головною метою СФЗ є рішення завдання нейтралізації людини (порушника), що ініціює фізичні загрози. Незалежно від ступеня структурної складності й технічної оснащеності вона може бути поділена на такі підцілі (наведені в хронологічному порядку їхнього досягнення):

– своєчасне виявлення джерела загроз, тобто запобігання НСД на життєво важливі зони об’єкта захисту;

– затримка джерела загроз (в ідеальному випадку на час, що перевищує час, необхідний для нейтралізації загрози);

– своєчасне надання протидії виявленому джерелу загроз (припинення загрози);

– нейтралізація наслідків загрози, тобто мінімізація збитку від реалізації або спроби реалізації загрози.

Обов'язковим критерієм доцільності впровадження СФЗ в систему охорони об'єкта є виконання умови:

$$С_{пз} > С_{сфз}$$

де $С_{пз}$ вартість попередженого збитку;

$С_{сфз}$ – витрати на створення передбачуваної СФЗ.

Враховуючи таке можна стверджувати, що вимога щодо забезпечення необхідного рівня захищеності ІР повинна закладатися розроблювачами ще на етапі концептуального проєктування системи й коректуватися на інших етапах її життєвого циклу (експлуатації, модернізації тощо) [18]. При цьому розробником СФЗІ перш за все має бути забезпечене виконання принципу превентивності – чим раніше й вірогідніше буде виявлене джерело загроз (зловмисник, порушник) або спроба її реалізації й оцінений її масштаб, тим успішніше виявиться відбиття або локалізація цієї загрози, тобто тим ефективніше буде СФЗІ.

2.1. Життєвий цикл СФЗІ та основні засоби, що використовуються при створенні системи

Аналізуючи визначення поняття «автоматизована система» (АС), наведене в Держстандарт 34.003-90, і зіставляючи його з визначенням терміну «система фізичного захисту інформації» можна зробити висновок, що СФЗІ володіє сукупністю практично однакових з АС ознак й може розглядатися як автоматизована інформаційно-керуюча система, здатна вирішувати певний клас завдань. Зважаючи на таке у процесі створення СФЗІ можна виділити три основні стадії: передпроєктну стадію; стадію проєктування та стадію впровадження у дію (див. рис. 2.11).

Рис. 2.11. Життєвий цикл системи фізичного захисту інформації

Самою непомітною, але водночас надзвичайно важливою (з погляду визначення оптимальних вимог до СФЗІ) є передпроєктна стадія. Її головними кроками є:

1) проведення обстеження на діючому ОІД;

2) розроблення моделі загроз для ІзОД або доповнення до діючої моделі загроз відповідно до нормативних документів системи ТЗІ;

3) розроблення технічних завдань (ТЗ) на створення комплексу ТЗІ (технічних вимог з питань ТЗІ).

Метою обстеження є підготовка вихідних даних для формування вимог щодо створення комплексу ТЗІ. В його ході проводять аналіз [14]:

– умов функціонування ОІД, особливостей розташування його на місцевості, відносно меж контрольованої зони (КЗ), архітектурно-будівельних особливостей тощо;

– технічних засобів, що оброблятимуть ІзОД, та технічних засобів, які не використовують безпосередньо для її оброблення, визначають місця їх розташування на ОІД;

– розташування інженерних комунікацій та металоконструкцій, виявляють транзитні,

– незадіяні (повітряні, зовнішні, підземні) комунікації (для опрацювання пропозицій щодо їх вилучення чи доопрацювання), а також такі, що виходять за межі КЗ;

– необхідності впровадження інженерних і технічних заходів захисту від витоку ІзОД технічними каналами.

На підставі матеріалів обстеження розробляється окрема модель загроз. Вона повинна включати: генеральний та ситуаційний плани ОІД, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території; схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до ІзОД; оцінку шкоди, яка передбачається від реалізації загроз.

Одним з найважливіших етапів на передпроєктній стадії є здійснення за певних експлуатаційних, технічних та інших обмежень оптимального вибору засобів захисту для її побудови (див. рис. 2.12).

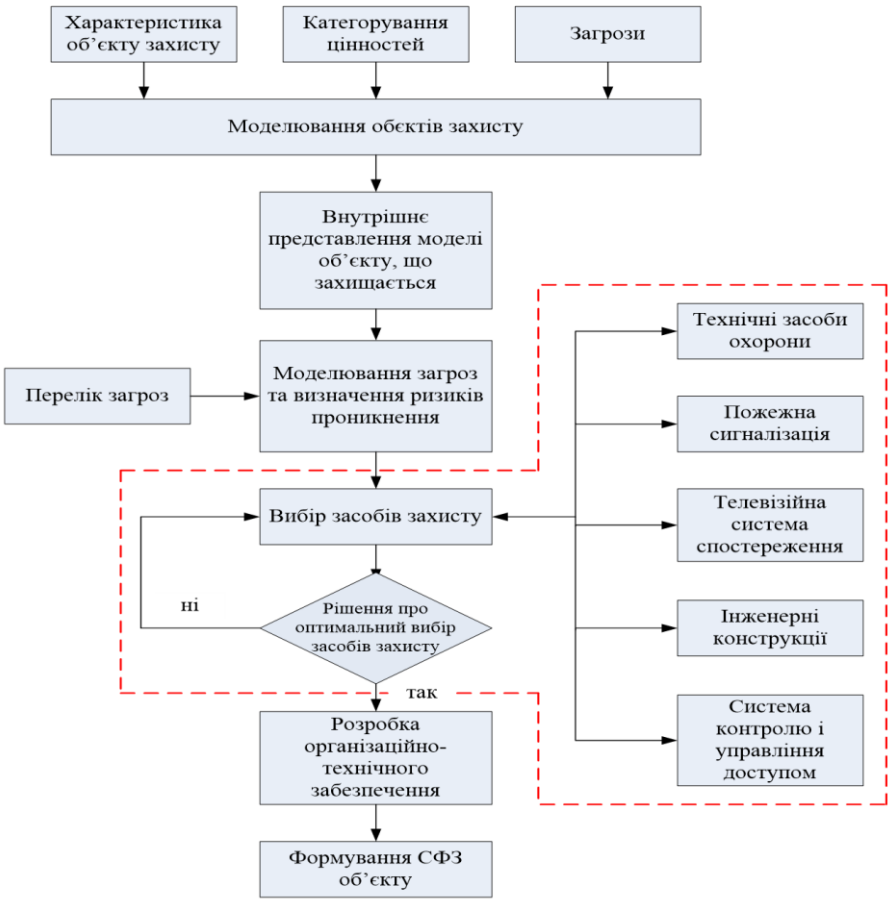

Рис. 2.12. Структурно-функціональна схема вибору засобів СФЗІ

Діапазон таких засобів на сьогодні дуже великий (див. рис. 2.13). Так, наприклад, при організації внутрішньо об’єктового режиму захисту він може бути обмежений низкою організаційних та технічних заходів і правил щодо забезпечення режиму, встановленого в організації. Це дозволить:

– скоротити кількість осіб, допущених до ІзОД;

– забезпечити ступінь відповідальності виконавців за збереження ІзОД;

– забезпечити встановлений порядок користування ІзОД;

– здійснювати контроль за виконавцями при їх роботі з документами, які мають гриф обмеження доступу тощо.

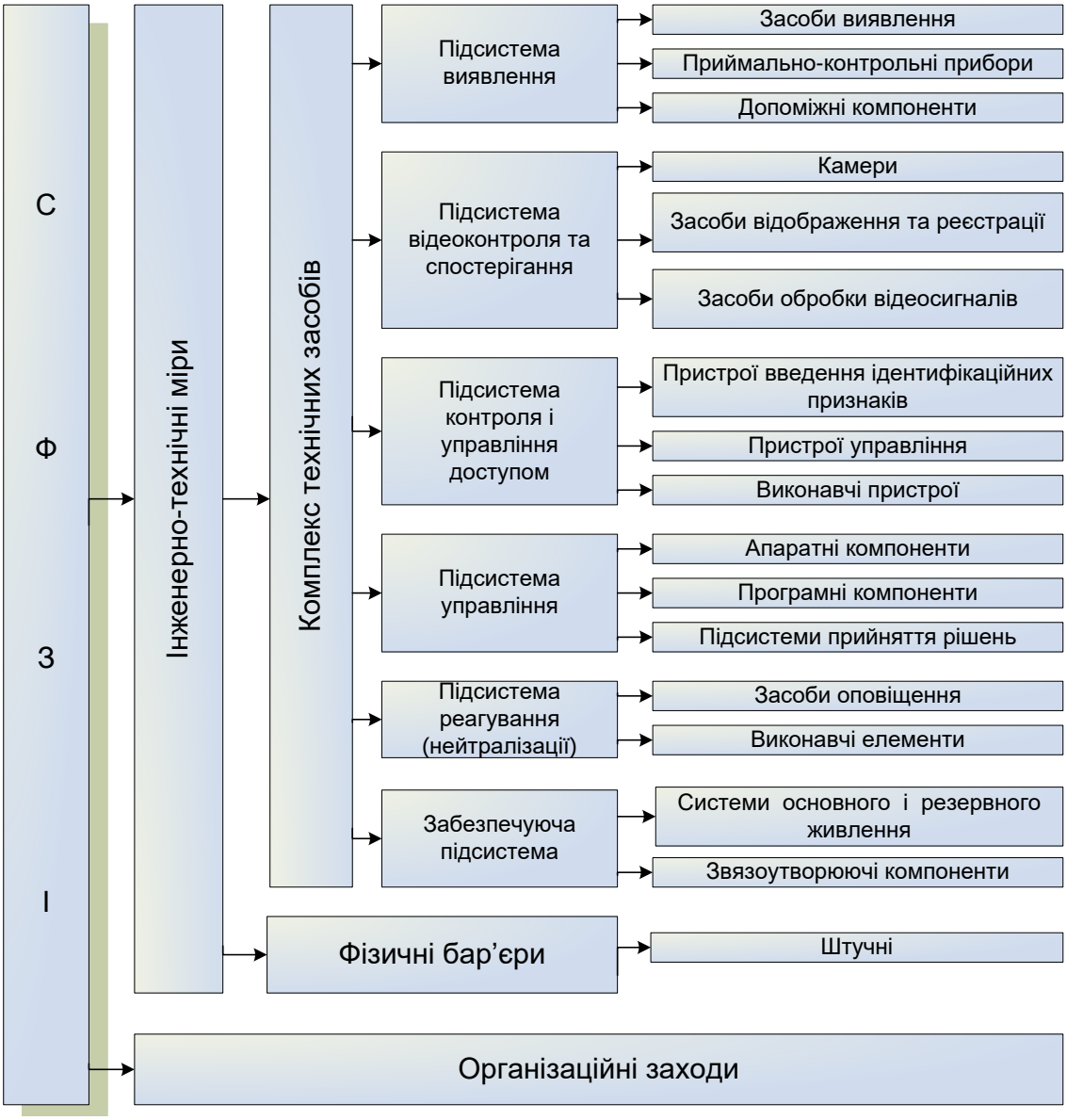

Рис. 2.13. Склад системи фізичного захисту інформації

За для забезпечення зовнішньо об’єктового режиму захисту діапазон використовуваних засобів може бути представлений:

– засобами управління доступом (кодоблокувальними пристроями, домофонами, магнітними картками, механічними пристроями – «вертушками» на КПП, воротами, шлагбаумами тощо);

– засобами збору і відображення інформації (засобами виявлення факту проникнення, контролю за системою охорони та реєстрації фактів спрацювання пристроїв виявлення);

– стаціонарними і мобільними периметричними та об’єктними засобами виявлення;

– технічними засобами спостереження (телесистемами спостереження, перископами, приладами нічного бачення тощо);

– технічними засобами попередження (на паперовому носії та мультимедійними);

– технічними засобами дії (електроогорожами, сигнальними й індикаторними системами) тощо.

Кожен із цих засобів може використовуватися як індивідуально, так й спільно з іншими засобами захисту у визначених зонах (режимних територіях, приміщеннях) в межах яких необхідно забезпечити належний рівень фізичного захисту. Такі зони нині поділяють на ретельно контрольовані зони (КЗ) із захистом високого рівня, захищені зони та слабко захищені зони. До першої групи належать, як правило, серверні кімнати, приміщення з мережевим і зв’язковим обладнанням, архів програм і даних. До другої групи – приміщення, де розташовані робочі місця адміністраторів, які контролюють роботу мережі, а також периферійне устаткування обмеженого користування. У третю групу входять приміщення, в яких обладнані робочі місця користувачів і встановлено периферійне устаткування загального користування. Для захисту периметра таких зон можуть створюватись, наприклад, системи охоронної й пожежної сигналізації, системи цифрового відео спостереження, системи контролю й управління доступом (СКУД) тощо. Для забезпечення ефективного захисту цих

зон необхідно знайти відповідь передусім на такі запитання: що потрібно захищати технічними засобами в конкретній організації (будинку, приміщенні); яким загрозам піддається об'єкт захисту зі сторони зловмисників та їхніх технічних засобів; які способи й засоби доцільно застосовувати для забезпечення безпеки з урахуванням як величини загрози, так і витрат на її попередження й, взагалі, як організувати і реалізувати фізичний захист в організації. Надалі доцільно дотримуватись наступних рекомендацій:

– КЗ (режимні території, приміщення) повинні відповідати цінності інформації, що захищається;

– периметр безпеки КЗ повинний бути чітко визначений;

– допоміжне устаткування (ксерокс, факс тощо) у КЗ повинно бути розміщено так, щоб зменшити ризик несанкціонованого доступу (НСД) до ІзОД;

– фізичні бар'єри, щоб запобігти НСД до КЗ (режимних територій, приміщень) повинні простиратися від підлоги до стелі;

– інформація про те, що робиться в КЗ (режимних територіях, приміщеннях) за жодних умов не повинна потрапити до сторонніх осіб;

– КЗ (режимні території, приміщення) у неробочий час повинні бути фізично недоступні і періодично перевірятися охороною;

– у КЗ (режимних територіях, приміщеннях) варто встановити належний контроль доступу, робота поодинці без належного контролю має бути заборонена;

– у межах КЗ (режимних територій, приміщень) використання фотографічної, звукозаписної й відео апаратури повинно бути заборонено (за винятком санкціонованих випадків) тощо.

Передпроєктна стадія закінчується розробкою технічного завдання (ТЗ) на СФЗІ у цілому й, при необхідності, часткових ТЗ (ЧТЗ) на її складові частини. Головними підрозділами цих документів є: 1) загальні відомості; 2) вихідні дані для виконання робіт; 3) технічні вимоги до комплексу ТЗІ: загальні вимоги; вимоги щодо стійкості до зовнішніх впливів; вимоги з безпеки експлуатації; вимоги до метрологічного забезпечення; вимоги щодо забезпечення охорони державної

таємниці; вимоги щодо технічного забезпечення виконання робіт; вимоги щодо забезпечення безпеки при виконанні робіт; 4) вимоги до документації; 5) етапи виконання робіт та порядок їх приймання [16].

На стадії проєктування в проєктних рішеннях знаходять своє втілення ті вимоги, які викладені в ТЗ. Необхідно відзначити, що проектування СФЗІ має певні особливості. Деякою мірою це пов’язане з дуалізмом СФЗІ. З одного боку, вона є автоматизованою системою, і її проєктування здійснюється відповідно до вимог ДЕРЖСТАНДАРТ 34.601-90. З іншого боку, при створенні (удосконалюванні) СФЗІ неможливо обійтися без проведення значного обсягу будівельно-монтажних і пусконалагоджувальних робіт, і в цьому зв’язку СФЗІ являє собою об’єкт капітального будівництва. Тому розробка проєктної документації повинна здійснюватися відповідно до СНиП 11-01-95. Процес проеєктування (див. рис. 2.14) починається з визначення задач, потім проєктується система, що розв’язує ці задачі, і нарешті шляхом моделювання оцінюється, наскільки добре система їх виконує.

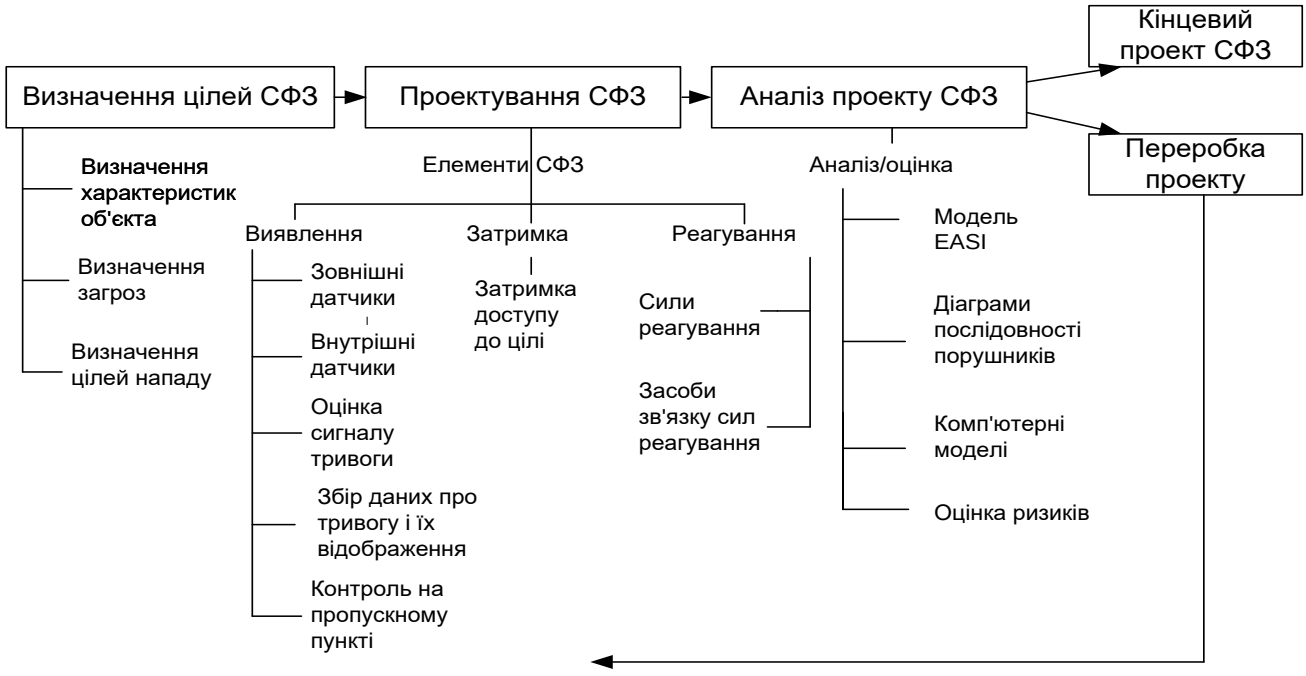

Рис. 2.14. Процес проєктування й оцінки ефективності систем фізичного захисту

Для визначення характеру й умов функціонування об’єкта потрібний ретельний опис самого об’єкта (знаходження границь об’єкта й будинків, планів поверхів будинків з вказівкою входів). Необхідні також характеристики робочих процесів на об’єкті й

виявлення наявних мір захисту. Ця інформація може бути отримана з декількох джерел, включаючи проєктну документацію об'єкта, опис технологічних процесів, звіти по охороні праці й оцінки по впливі об'єкта на навколишнє середовище. Крім збору й вивчення подібної документації необхідне також відвідування досліджуваного об'єкта й опитування працюючого на ньому персоналу, тобто обстеження об'єкта. Це допоможе краще зрозуміти вимоги по фізичному захисту об'єкта, а також обмеження, пов'язані з його функціонуванням і аварійною безпекою, які повинні бути взяті до уваги.

Надзвичайно важливим є визначення загроз для об'єкта захисту. Інформація за цим напрямом може бути отримана при відповідях на три питання про порушника: «який тип порушника варто розглядати?»; «який діапазон його тактичних прийомів?» та «які можливості порушника?». Порушники при цьому можуть бути віднесені до одного із трьох типів – сторонні особи, співробітники об'єкта й сторонні особи, що діють у змові зі співробітниками. Для кожного типу порушників повинен бути розглянутий весь спектр прийомів – обман, насильство, крадіжка і їхні комбінації. Нарешті, на об'єкті треба виявити цілі нападу. Вони можуть включати майно або інформацію, людей, а також критичні області й процеси. Повинна бути виконана ретельна ревізія об'єкта й наявного на ньому майна. Найбільш уразливі від нападів майно і устаткування можуть бути виявлені, якщо відповістити на запитання: які втрати виникнуть у випадку диверсії, спрямованої на виведення з ладу цього встаткування?

Взявши до уваги інформацію, отриману при визначенні характеристик об'єкта й загроз, а також при виявленні цілей нападу, розроблювач може сформулювати задачі СФЗІ. Вони можуть полягати, наприклад, у перериванні дій злочинця, що розташовує тільки підручними засобами й автомобілем, перш ніж готові мікропроцесори вивезуть через службовий вхід. Процес формулювання задач може бути до деякої міри рекурсивним. Це означає, що визначення загроз буде залежати від виявлення цілей нападу й навпаки.

Процес уведення системи в дію є самою помітною стадією, оскільки саме в цей час ведеться весь необхідний комплекс робіт і в підсумку споживач одержує кінцевий

результат – діючу СФЗІ. Його можна розбити на кілька етапів: підготовку об'єкта до уведення СФЗІ у дію; підготовку й навчання персоналу СФЗІ; проведення комплектації СФЗІ; проведення будівельно-монтажних робіт СФЗІ; проведення пусконалагоджувальних робіт СФЗІ; проведення попередніх випробувань СФЗІ і/або його складових частин; проведення експериментальної експлуатації СФЗІ; проведення приймальних випробувань СФЗІ; проведення остаточного приймання СФЗІ. Основним експлуатаційним документом на СФЗІ є паспорт і його складові – паспорти на приміщення, де ІзОД озвучується та/або обробляється технічними засобами (далі – паспорти). Паспорти призначено для [18]:

– ознайомлення з відомостями про інформацію, що підлягає захисту від витоку технічними каналами;

– ознайомлення з проєктними і технічними рішеннями, що реалізовані у комплексі СФЗІ;

– встановлення правил експлуатації (використання за призначенням, технічне

– обслуговування, перевірки основних характеристик, ремонт, перевірки за умови виявлення порушень правил експлуатації приміщення та технічних засобів, а також у разі порушення пломб на технічних засобах та засобах захисту тощо);

– відображення відомостей про технічне обслуговування комплексу, його основні характеристики (визначені під час приймання комплексу), планові перевірки, атестації, а також про ремонт та утилізацію.

Атестація СФЗІ проводиться установою, яка має відповідну ліцензію або дозвіл на провадження діяльності в галузі ТЗІ, одержані у встановленому законодавством порядку з метою визначення відповідності вимогам нормативних документів з питань ТЗІ виконаних робіт зі створення комплексу ТЗІ на ОІД та повноти проведених випробувань. Атестація може проводитися окремо щодо кожного виду ІзОД, що підлягає технічному захисту. Вона може бути первинною, черговою та позачерговою. Термін проведення чергової атестації вказується в акті атестації та паспорті на СФЗІ (строк дії акта атестації не повинен перевищувати два роки). Позачергову атестацію, а також необхідні випробування проводять у разі змін умов функціонування ОІД, що приводять до

змін загроз для ІзОД, яка озвучуватиметься та/або оброблятиметься технічними засобами тощо, та за висновками органів, які контролюють стан ТЗІ.

Стадія функціонування є самою тривалою стадією життєвого циклу СФЗІ, заради якої саме й здійснюються всі попередні роботи. Однак зрозуміло, що для стійкого функціонування системи, ефективного використання вкладених у неї засобів і успішного рішення покладених на неї завдань необхідно забезпечити виконання заходів з планування функціонування СФЗІ, експлуатації системи, підтримки необхідного рівня взаємодії всіх її компонентів, відпрацьовування дій у штатних і надзвичайних ситуаціях, перепідготовку й підвищення кваліфікації персоналу, проведення контролю за станом СФЗІ та проведення аналітичної роботи.

По закінченні встановлених строків експлуатації, як правило, відбувається фізичне й моральне старіння встаткування СФЗІ. Однак практика застосування такого виду апаратури показує, що не завжди по закінченні призначеного терміну служби встаткування необхідно виводити з експлуатації [21]. Добре організована система експлуатації апаратури СФЗІ, як правило, дозволяє використовувати її набагато довше встановленого терміну. Для оцінки стану встаткування СФЗІ по завершенні виробітку ресурсу на об’єктах створюються комісії, у які звичайно включаються як представники об’єкта, так і, у ряді випадків, виробників. За результатами оцінки технічного стану складається відповідний акт і строки експлуатації можуть бути продовжені. Як правило, більш ніж дворазове продовження терміну служби здійснюється вкрай рідко.

2.2. Головні функції та характеристики ефективної СФЗІ

Свої завдання СФЗІ вирішує шляхом комбінації функцій, які зображено на рис. 2.15.

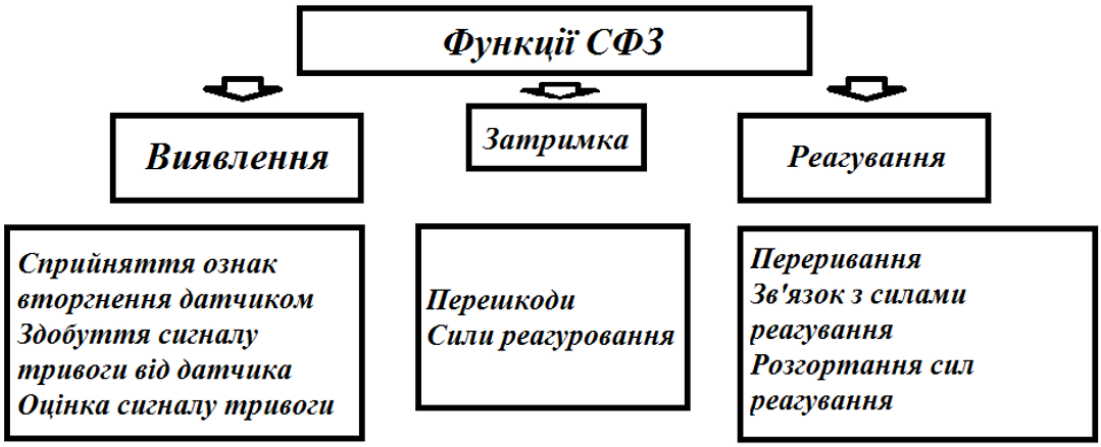

Рис. 2.15. Функції СФЗ

У загальному випадку їх можна розділити на дві групи: пасивну – визначає здатність системи виявляти спробу реалізації загрози, або її джерело (наприклад, несанкціоноване вторгнення) і оцінювати його масштаб у будь-яких умовах обстановки; активну – визначає здатність системи по реагуванню на виявлену загрозу і її нейтралізації, тобто здатність припиняти злочинні дії по завданню збитків об’єкту або предметам захисту [23]. Найбільш застосовними серед них є функції виявлення, затримки, реагування та профілактики, які можуть і повинні виконуватися з використанням як технічних засобів, так і людського резерву й застосовуватися для обґрунтувань і розрахунків рівнів фізичного захисту. Основні категорії функцій СФЗІ та їхніх рішень подано в табл. 2.1.

Таблиця 2.1

Основні категорії функцій СФЗІ та їхніх рішень

Функції КТСФЗ	Технічні засоби, що забезпечують реалізацію функцій	Загальні характеристики вимог
Виявлення	Зовнішня система виявлення (периметрова) Внутрішня система виявлення Відеоспостереження, відеоконтроль, відеопідтвердження Система збору і опрацювання інформації Система контролю і управління доступом Тривожно-виклична сигналізація	Ймовірність виявлення Час передачі повідомлення Час підтвердження повідомлення Ймовірність хибного спрацювання Можливість локалізації (визначення місцезнаходження порушника)

Продовження таблиці 2.1

Функції КТСФЗ	Технічні засоби, що забезпечують реалізацію функцій	Загальні характеристики вимог
Затримка	Фізичні бар'єри Система управління доступом Засоби впливу на порушника	Час затримки Ступінь захисту від подолання
Реагування	Системи оперативного зв'язку Активні фізичні бар'єри Засоби впливу на порушника Технічні оснащення персоналу охорони Система контролю управління доступом	Час на блокування порушника Час на нейтралізацію порушника Ефективність сил реагування Якість та надійність зв'язку із силами реагування
Профілактика	Периметрова система виявлення і фізичні бар'єри Системи контролю та управління доступом Технічні оснащення персоналу охорони	Видимі елементи КТСФЗ Режим підприємстві Навчання та тренування персоналу охорони

Розглянемо їх більш докладно.

Функція виявлення СФЗ, що зображена на рис.2.16, включає спостереження потайливих або відкритих дій.

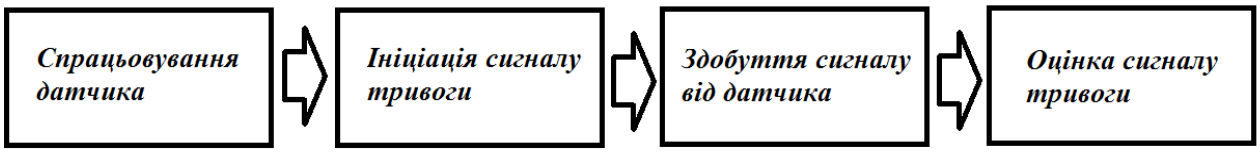

Рис.2.16. Функція виявлення в СФЗ

Показники ефективності для функції виявлення наступні: імовірність виявлення дій порушника; час, необхідне для одержання й оцінки сигналу тривоги; частота фіктивних тривог. Найбільш показовою з них є сумарна ймовірність виявлення порушника $P_{\min}$ у момент, коли в сил реагування ще досить часу для його перехоплення (тобто до досягнення поставленої ним мети). Вона залежить від дій із спостереження потайних або відкритих заходів порушників, проведення контролю на пропускному пункті тощо (див. рис. 2.17).

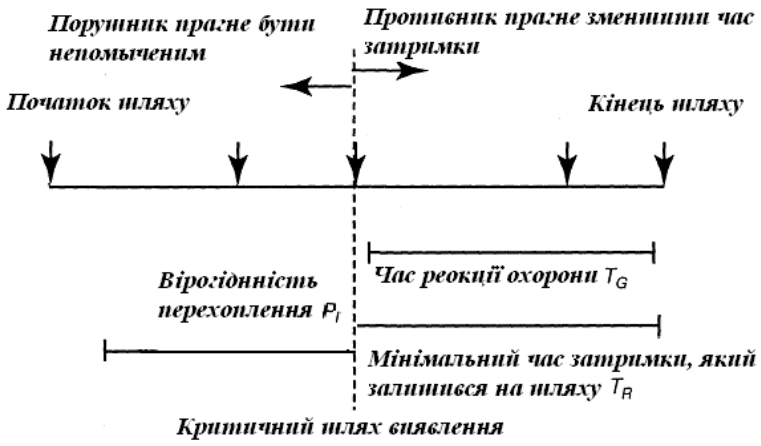

Рис. 2.17. Своєчасне виявлення як міра ефективності

Імовірність виявлення знижується в міру збільшення часу оцінки.

На рис.2.18 зображено другу функцію СФЗ – затримку. Вона сповільнює просування порушника. Ця функція може бути реалізована за допомогою людей, бар'єрів, замків і засобів активованої затримки. Сили реагування можуть розглядатися як елемент затримки, якщо вони перебувають на фіксованих, добре захищених позиціях.

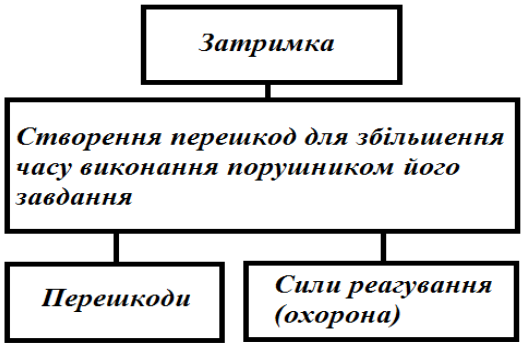

Рис. 2.18. Функція затримки в СФЗ

Показником ефективності затримки служить час затримки T_R тобто час, необхідний виявленому порушникові для того, щоб обійти кожен елемент затримки. Ця функція СФЗІ уповільнює просування порушника. Вона може бути реалізована за допомогою особового складу, бар'єрів, замків і засобів активованої затримки. Третьою мірою ефективності є час реагування T_G, тобто час між отриманням повідомлення про

дії порушника і перериванням цих дій (час дії сил реагування), а також вірогідність доведення до сил реагування точного повідомлення і необхідний для цього час. Точка, у якій час затримки T_R усе ще перевищує час реакції T_G сил реагування, називається критичною точкою виявлення (КТВ). Імовірність переривання P_I є сумарною імовірністю виявлення від початку шляху до КТВ, обумовленою по T_R. Вона фактично служить загальною мірою ефективності системи.

Функція реагування включає дії, що вживають силами реагування для того, щоб перешкодити успіху дій порушника. Фактично реагування – це переривання. Переривання визначається як прибуття достатнього числа персоналу у відповідне місце для зупинки послідовності дій порушника. Воно включає повідомлення силам реагування точної інформації про дії порушника й розгортання сил реагування. Показник ефективності дій сил розгортання – час між одержанням повідомлення про дії порушника й перериванням цих дій (час дії сил реагування). На рис. 2.19 показана виконувана СФЗ функція реагування. При захисті особливо важливих об'єктів застосовується додатковий захід ефективності дій сил реагування – нейтралізація. Нейтралізація – це міра, що визначає результат протиборства сил реагування й порушників. Такий тип реагування рідко використається при захисті промислових об'єктів.

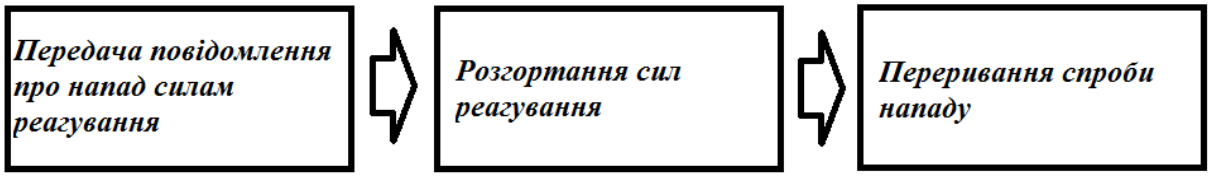

Рис.2.19. Функція реагування СФЗ

Показниками ефективності зв'язку з силами реагування є ймовірність доведення до них точного повідомлення і необхідний для цього час. Час, що пройшов після первинного передавання повідомлення, суттєво залежить від прийнятого методу зв'язку. Після первинного передавання ймовірність доведення правильного повідомлення швидко починає зростати. Як показано на рис. 2.17, з кожною наступною передачею

ймовірність доведення правильної поточної інформації зростає. Через особливості людської поведінки може відбуватися деяка затримка при установленні зв'язку. З першої спроби передати повідомлення оператор приходить до стану готовності його прийняття. Але може не почути всю інформацію, що належить до цієї справи. У зв'язку з цим робиться запит на повторне передавання відомостей. Нарешті, коли оператор зрозуміє повідомлення, він починає його уточнювати.

Рис. 2.20 дозволяє встановити зв'язок між часом, необхідним порушникові для виконання задачі, і часом, необхідним СФЗІ для виконання покладених на неї функцій.

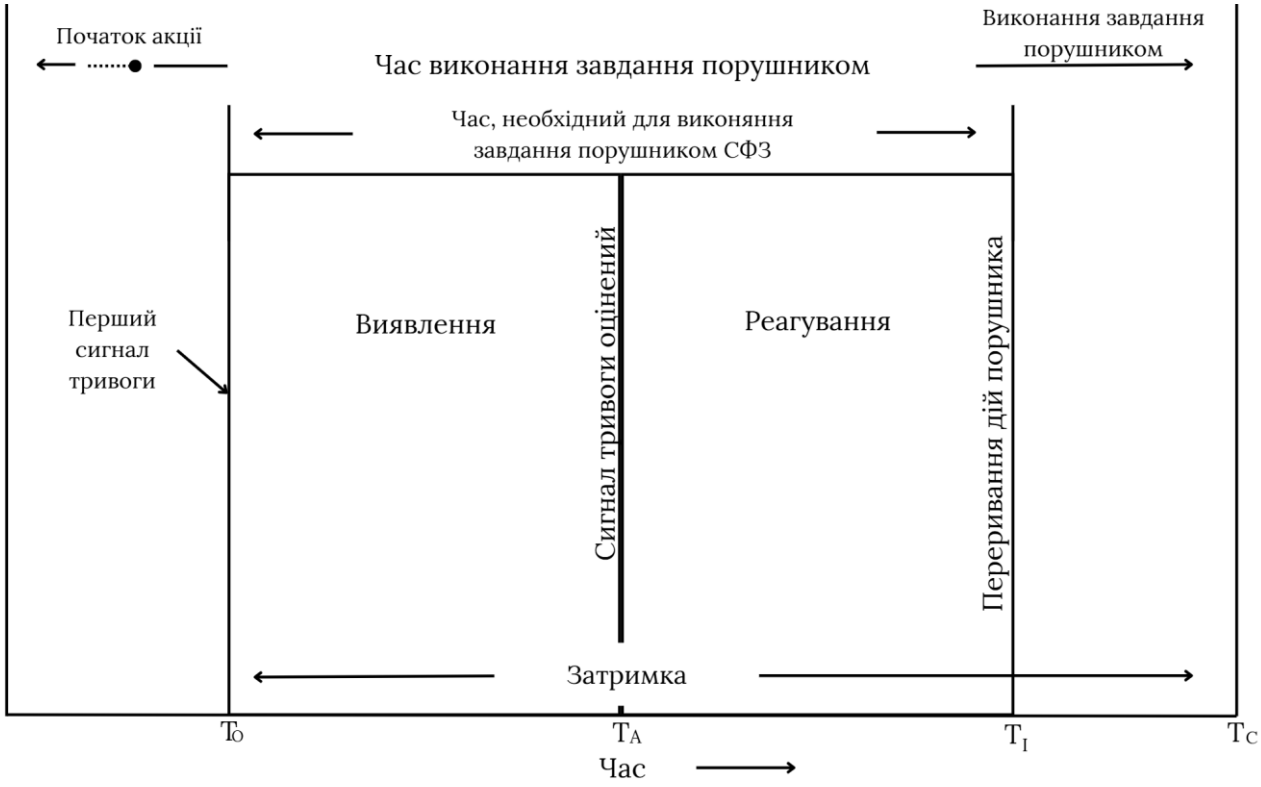

Рис. 2.20. Зв'язок між функціями СФЗІ

Сумарний час, необхідний порушникові для досягнення його цілей, позначений як час розв'язування задачі порушником. Він залежить від затримки, створюваної СФЗІ. Порушник може почати розв'язування своєї задачі в деякий момент часу до виникнення першого сигналу тривоги в момент часу T_0. Час, протягом якого порушник уже виконував свою задачу, показано штриховою лінією (тому що до виявлення затримка неефективна). Після виникнення сигналу тривоги він повинен бути отриманий і оцінений для визначення істинності. У момент часу T_A, коли сигнал тривоги оцінений як щирий,

повідомлення про місцезнаходження джерела тривоги повинне передаватися силам реагування. Для того, щоб сили реагування в достатній кількості й з необхідним оснащенням були готові перервати дії порушника, потрібне додатковий час. Момент часу, у який сили реагування переривають дії порушника, позначається T_I, а момент завершення виконання задачі порушником – T_C. Очевидно, що для успішного відбиття нападу момент T_I повинен перебувати на часовій осі лівіше T_C, а виявлення (перший сигнал тривоги) відбуватися якомога раніше, тобто моменти часу T_0, T_A й T_I повинні лежати як можна лівіше на осі часу. Функція затримки сповільнює дії порушника для того, щоб дати силам реагування час для розгортання. СФЗ повинна забезпечити досить часу для того, щоб сили реагування зупинили напад порушника.

Таким чином, ефективна СФЗІ повинна виконувати всі три функції – виявлення, затримки й реагування. Вони повинні реалізовуватися в зазначеному порядку протягом меншого інтервалу часу, чим час, необхідний порушникові для виконання своєї задачі. Цього можна досягти якщо СФЗІ буде надійною (ешелонованою, багаторівневою) та збалансованою за захистом й до того ж матиме мінімальні наслідки у випадку відмов її компонентів. Наявність ешелонованого захисту означатиме при цьому, що для досягнення мети нападу порушникові буде потрібно послідовно обійти або перебороти кілька захисних технічних засобів. Наприклад, йому необхідно перебороти один датчик і проникнути через два бар'єри, перш ніж потрапити в пункт управління або в архів бухгалтерії. Час і дії, необхідні для того, щоб перебороти кожен із цих рівнів захисту, не обов'язково однакові, ефективність кожного з них може бути зовсім різною, однак у кожному разі буде потрібна окрема дія в міру просування порушника до мети. СФЗІ, що забезпечує ешелонований захист, дозволить: підвищити невизначеність очікувань щодо властивостей системи; забезпечити більш ретельну підготовку до нападу порушників; створити додаткові перешкоди для порушників. Збалансованість захисту означає, що незалежно від того, яким чином порушник намагатиметься досягти своєї мети, він зіштовхнеться з активними елементами СФЗІ. У повністю збалансованій системі мінімальний час, необхідний для проникнення через кожну з таких перешкод, повинен бути однаковим, так само як і мінімальна ймовірність виявлення проникнення.

При цьому, наприклад, роль персоналу сил реагування в реалізації функцій виявлення порушника і його затримок при використанні відповідних технічних засобів може бути практично повністю виключена. Це дозволить зменшити роль людського фактору, тобто знизити ймовірність його помилкових дій і можливість змови порушників з персоналом охорони, а також забезпечити необхідну гнучкість СФЗІ і необхідний рівень внутрішньої, режимної, екологічної, пожежної та технологічної безпеки системи, а також її технічної і функціональної надійності.

Висновки до другого розділу

Бурхливий розвиток сучасних технологій і технічних засобів сприяє постійному розширенню спектра можливих каналів витоку інформації, тому їх дослідження стає все більше актуальним, і складним завданням.

На ефективність систем безпеки істотно впливають характеристики реальних каналів витоку, тому створення ефективних систем захисту інформації має відбуватися з урахуванням їх особливостей. Цей висновок не є тривіальним, як може здатися, на перший погляд. Наприклад, сам факт наявності випромінювання дисплея ще не говорить про витік інформації. Усе визначається конкретним рівнем напруженості поля за межами зони безпеки й технічних можливостей противника, тому остаточний висновок про витік інформації може зробити тільки кваліфікований фахівець, що використовує спеціальні технічні засоби. З іншого боку, особливості реальних каналів витоку інформації можуть бути успішно використані й противником для забезпечення НСД до інформації, про що необхідно постійно пам’ятати. Так, знімання інформації з акустичних каналів може бути здійснено через скло вікон, будівельні, сантехнічні, вентиляційні, теплотехнічні й газорозподільні конструкції, з використанням для передачі сигналів радіо, радіотрансляційних, телефонних і комп’ютерних комунікацій, антенних, і телевізійних розподільних мереж, охоронно-пожежної й тривожної сигналізації, мереж електроживлення й часофікації, гучномовного й диспетчерського зв’язку, ланцюгів заземлення й т.п. Випадковий

пропуск хоча б одного можливого каналу витоку може практично нанівець звести всі витрати й зробити систему захисту неефективною.

Таким чином основна мета СФЗІ, незалежно від ступеня структурної складності й технічної оснащеності ІКС, може бути поділена на такі підцілі:

– своєчасне виявлення джерел загроз, тобто запобігання НСД на територію об’єкта й у його життєво важливі зони;

– затримка джерел загроз на час, що в ідеальному випадку перевищує час нейтралізації загрози;

– своєчасне надання протидії виявленому джерелу загроз (припинення загрози);

– нейтралізація наслідків загрози, тобто мінімізація збитку від реалізації або спроби реалізації загрози.

За повної невизначеності щодо вхідних даних вона може бути досягнута за рахунок застосування вивіреного підходу до проєктування системи фізичного захисту та обґрунтованого вибору засобів, раціональних з точки зору комплектування спроєктованої системи, а також за умови дотримання двох суперечливих вимог – мінімізації сумарних витрат на створення СФЗІ $(\varphi \to \min)$ та максимізації захищеності організації або її ресурсів від впливу внутрішніх і зовнішніх загроз $(S \to \max)$.

РОЗДІЛ 3
МОДЕЛІ І ПРОЦЕДУРИ ОЦІНЮВАННЯ СТУПЕНЯ ПОРУШЕННЯ СФЗІ ТА ВИБОРУ ЗАСОБІВ ДЛЯ КОМПЛЕКТУВАННЯ СИСТЕМИ

З погляду системного аналізу, СФЗІ являє собою модель (див. рис. 3.1), що поєднує сили й засоби певного об’єкта, спрямовані на забезпечення захисту його інформаційних або будь-яких інших цінних ресурсів.

Рис. 3.1. Модель системи фізичного захисту інформації

Модель повинна задовольняти наступним вимогам, які зображено на рис. 3.2:

1) використовуватися в якості: керівництва по створенню СФЗІ, методики щодо формування показників і вимог до неї, інструменту (методики) оцінки СФЗІ та моделі для проведення досліджень (матриця стану) СФЗІ;

2) володіти властивостями: універсальності, комплексності, простоти використання, наочності, практичної спрямованості та можливості нарощування знань, функціонування в умовах високої невизначеності початкової інформації;

3) дозволяти встановити взаємозв’язок між показниками (вимогами), задавати різні рівні захисту, отримувати кількісні оцінки, контролювати стан СФЗІ,

застосовувати різні методики оцінок, оперативно реагувати на зміни умов функціонування; об’єднати зусилля різних фахівців єдиним задумом.

Її складовими при цьому як правило є: модель загроз, модель порушника та модель оцінки ефективності виконання СФЗІ функцій виявлення, затримки і реагування. Метою першої моделі є обґрунтування достатності якісних і кількісних вимог до рівня захищеності об’єкта захисту. Метою другої – оцінювання уразливості об’єкта захисту та завдання рівня його захищеності. Метою третьої моделі – забезпечення захисту інформації або інших цінних ресурсів певного об’єкта шляхом поєднання усіх його можливих сил і засобів. Входами для цих моделей є загрози, які можуть бути внутрішніми й зовнішніми, у тому числі й такими, які важко локалізувати [24]. До них відносять: слабку правову дисципліну співробітників, неякісну експлуатацію засобів обробки інформації, наявність у приміщенні допоміжних технічних засобів побічні фізичні процеси в яких сприяють несанкціонованому поширенню інформації, яка підлягає захисту. Джерелами загроз можуть бути зловмисники, технічні засоби усередині організації, співробітники організації, внутрішні й зовнішні поля, стихійні сили й т.д. При цьому особливу увагу доцільно приділяти загрозам безпосередньо самій СФЗІ та її елементам, оскільки від їхнього функціонування залежить безпека об’єкта захисту з усією його інформаційною інфраструктурою. Цілі задають необхідний результат функціонування системи та алгоритм дій для досягнення поставленої мети.

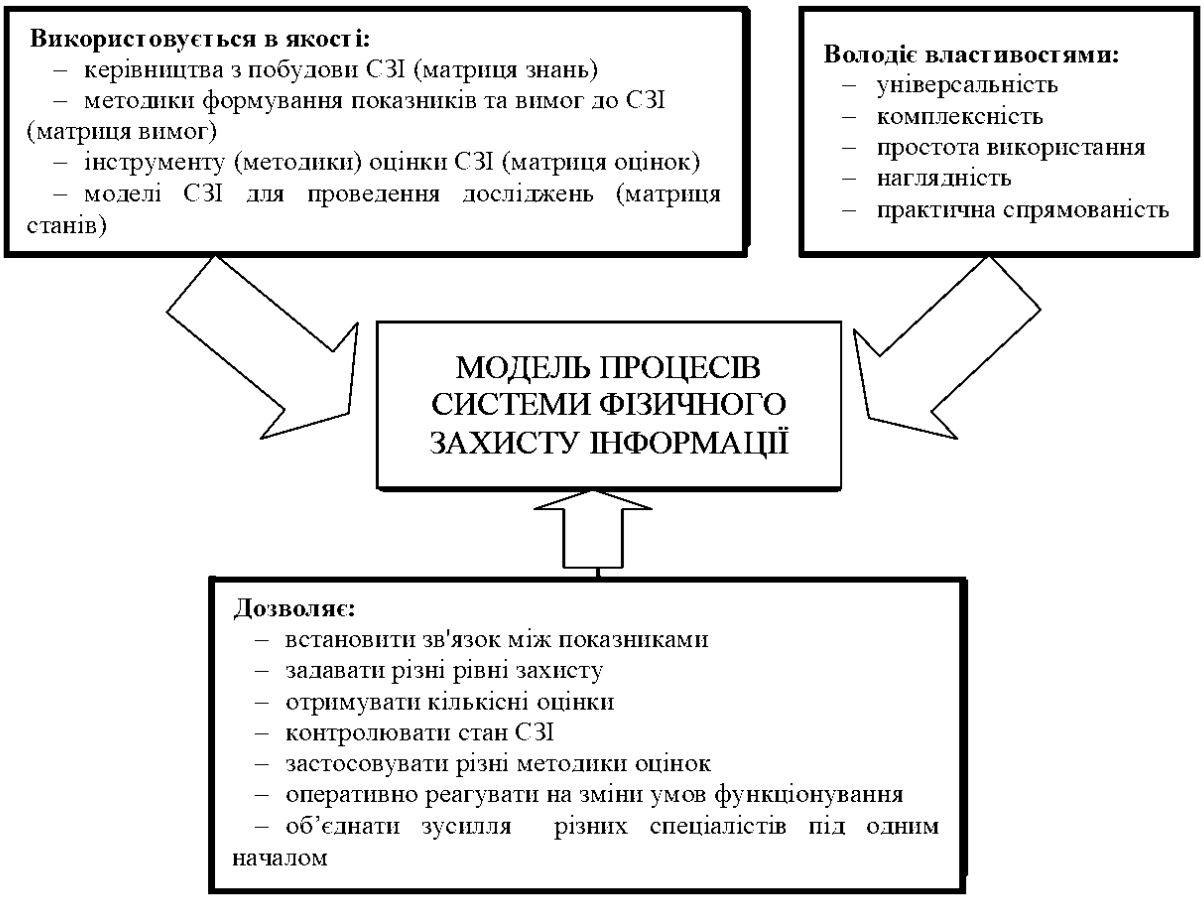

Рис. 3.2. Вимоги до моделі СФЗІ

Можливість реалізації цих вимог залежить від ресурсів, що виділяються для захисту інформації: фінансових і технічних, співробітників, які вирішують завдання безпеки тощо. На ресурси, як правило, накладаються певні обмеження, які необхідно враховувати при проєктуванні СФЗІ на етапі її створення, при її модернізації або оптимізації на етапах впровадження та експлуатації. Виходи системи являють собою реакцію на вхідні впливи, тобто сукупність мір по забезпеченню безпеки цінних ресурсів. Однак локалізувати в просторі виходи системи так само складно, як і входи. Кожен співробітник, наприклад, у міру своєї відповідальності зобов'язаний займатися завданнями захисту інформації й вживати заходів по забезпеченню її безпеки. Заходи щодо захисту інформації також включають різноманітні способи й засоби, у тому числі інструкції, що визначають доступ співробітників у конкретному структурному підрозділі організації до інформації, яка захищається.

3.1. Побудова моделі загроз інформаційній безпеці ІКС

Для аналізу загроз ресурсам ІКС необхідним є, перш за все визначення можливих каналів та видів загроз ресурсам системи, а також виявлення основних джерел їх походження. Як відомо, основними видами джерел загроз є [26]:

1) зміна умов фізичного середовища (стихійні лиха й аварії, як землетрус, пожежа чи інші випадкові події);

2) наслідки помилок під час проєктування і розробки компонентів ЛОМ (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних і т.п.);

3) збої і відмовлення в роботі устаткування і технічних засобів ЛОМ;

4) помилки користувачів комп'ютерних систем під час експлуатації;

5) навмисні дії (спроби) потенційних порушників – спроби несанкціонованого доступу до інформаційних ресурсів ІКС.

Аналіз загроз, які створюються навмисними діями потенційних порушників, доцільно розглядати з використанням моделі захищеного об'єкта, приклад якої наведено на рис. 3.3.

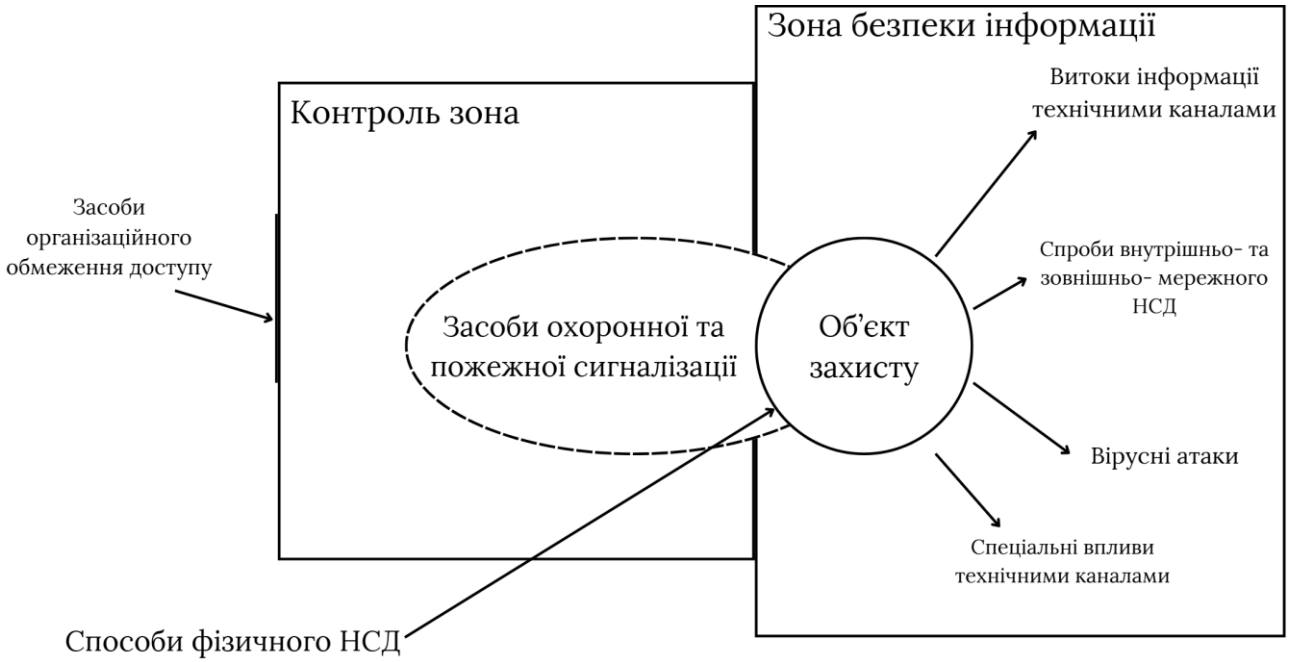

Рис. 3.3. Приклад моделі захищеного об'єкта

Модель об’єкта являє собою граф, представлений у вигляді матриці суміжності M [a, b]. Вершинами даного графа є області однорідності (ОО) – області на об’єкті, де збігаються три основні характеристики СФЗ (див. рис. 3.4): час реакції охорони, час подолання даної області порушником і ймовірність виявлення порушника пристроями виявлення, що діють у даній області.

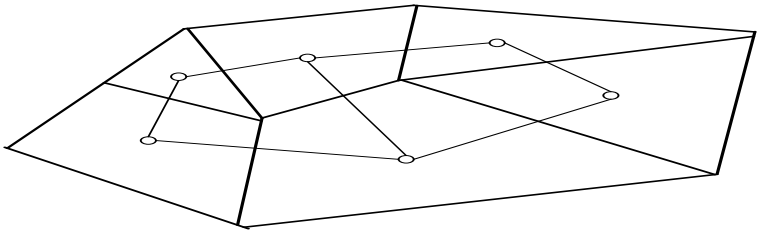

Рис. 3.4. Області однорідності із графом (просторовою моделлю) об’єкта

Характеристиками власне ОО служать:

– набір пристроїв і інженерних засобів охорони, установлених або діючих у даній зоні;

– час реакції сил охорони.

Завдання аналізу СФЗІ полягають у тому, щоб визначити наявність критичних шляхів (таких, де ймовірність своєчасного виявлення $P_{об}$ буде більше мінімально заданої ймовірності виявлення P_{min}). Пошук критичних шляхів здійснюється за таким алгоритмом.

Етап 1. За модифікованим алгоритмом Дейкстри знаходимо всі шляхи з множини точок початку руху $N = (n_1, n_2, ..., n_i, ..., n_k)$ (областей однорідності, розташованих на периметрі об’єкта) до множини цільових точок $C = (c_1, c_2, ..., c_j, ..., c_m)$ (областей однорідності, у яких перебувають критичні елементи об’єкта). Одержуємо набір векторів виду:

$$v = (n_i ... m_a .. c_j). \tag{3.1}$$

Етап 2. Розрахунок робимо відповідно до оптимальної стратегії дій порушника. На кожному векторі v, знаходимо КТВ – точку, у якій $\sum_{i=k}^{u} T_j < T_{охр.КТО}$, де $T_{охр.КТВ}$ – час реакції охорони в критичній точці виявлення; T_j – час подолання j-ї

зони однорідності СФЗ, розташованої між КТВ й цільовою зоною. Час подолання береться з матриці навичок порушника *T* (3.2). Він повинен бути мінімальним при подоланні елементів СФЗ в *j*-й зоні однорідності. Підсумкова оцінка знайденого шляху *v* (3.3) (імовірність своєчасного виявлення) $P_{ОБ}$ буде ймовірністю виявлення порушника до КТВ й знаходиться за формулою (3.2):

$$P_{об} = 1 - \prod_{j=1}^{к} (1 - P_j) \cdot \tag{3.2}$$

Імовірність виявлення P_j береться з матриці ймовірностей навичок порушника *P*. Обрана ймовірність повинна бути мінімальною із усього набору ймовірностей виявлення НСД при подоланні елементів СФЗ в *j-й* зоні однорідності. При $P_{об} \le P_{\min}$ знайдений шлях *v* буде критичним. По наявності або відсутності критичних шляхів робиться висновок про достатність або недостатність заходів щодо фізичного захисту.

Можливими способами впливу загроз на об’єкт захисту при цьому є [20]:

1) безпосередній вплив (з безпосереднім доступом до об’єкту захисту). Є можливим при умові подолання порушником:

– засобів організаційного обмеження доступу;

– засобів охоронної сигналізації;

– засобів адміністрування доступу (проблемно-орієнтованих засобів захисту базового програмного забезпечення – операційних систем та систем управління базами даних (при їх наявності), включаючи маскування під зареєстрованого користувача з метою використання інформації чи нав’язування помилкової інформації, застосування заставних пристроїв чи програм і впровадженням комп’ютерних вірусів);

2) дистанційний вплив. Можливий за рахунок:

– технічних каналів побічних електромагнітних випромінювань і наведень, акустичних каналів;

– каналів спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту чи порушення цілісності інформації.

Модель загроз визначає перелік можливих загроз і класифікацію їх за результатами впливу на інформацію, тобто на порушення конфіденційності (к), цілісності (ц) і доступності інформації (д), а також порушення спостережності і керованості комп'ютерних систем (с). Вона будується за допомогою спеціального запитальника, який містить назви передбачуваних загроз, згруповані по категоріях, і деякі кількісні параметри для оцінки їхньої сили (небезпеки) і ймовірності прояву. Для об'єктів, по яких не потрібно проводити атестацію на відповідність вимогам якого-небудь нормативно-технічного документа, модель загроз може бути складена у формі текстового опису.

У загальному випадку актуальні загрози пов'язані із несанкціонованим доступом до інформації, що здійснюється при безпосередньому фізичному доступі до засобів ІКС. Вони можуть мати суб'єктивну або об'єктивну природу [29]. Загрози, що мають суб'єктивну природу, включають випадкові (ненавмисні) та навмисні (див. рис. 2.1). Варіант моделі загроз інформації, яка циркулює в довільній ІКС подано у табл. 3.1.

Таблиця 3.1

Варіант моделі загроз інформації, яка циркулює у довільній ІКС

№ з/п	Тип та визначення загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз або причини	Наслідки (порушення властивостей)			
				К	Ц	Д	С
1	Загрози об'єктивної природи						
1.1	Зміна умов фізичного середовища: аварії, стихійні лиха (землетрус, повінь, пожежа) або інші випадкові події (зміна температури, вологості тощо)	Середовище	Стихійні лиха, кліматичні зміни		+	+	+
1.2	Відмови та збої у роботі основних технічних засобів:	Апаратура					
	системи електроживлення				+	+	+
	систем забезпечення				+	+	+
	носіїв інформації				+	+	+

Продовдження таблиці 3.1

№ з/п	Тип та визначення загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз або причини	Наслідки (порушення властивостей)			
				К	Ц	Д	С
2	Загрози суб'єктивної природи						
2.1	Випадкові (ненавмисні)						
2.1.1	Тимчасова відсутність персоналу (хвороба, відрядження, відпустка)	Персонал, користувачі	Сімейні обставини, епідемії, службова необхідність, непередбачені заздалегідь		+	+	+
2.1.2	Дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.)	Персонал, користувачі	Неуважність, недбалість, некомпетентність		+	+	
2.1.3	Ненавмисне пошкодження носіїв інформації	Персонал, користувачі	Неуважність, недбалість, некомпетентність		+	+	
2.1.4	Неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо)	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+			
2.1.5	Ініціювання тестуючих або технологічних процесів, які здатні викликати втрату працездатності системи (зависання або зациклення) або здійснити необоротні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних і т.п.)	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+	
2.1.6	Ненавмисне зараження ПЗ комп'ютерними вірусами	Персонал, користувачі	Неуважність, недбалість, некомпетентність		+	+	
2.1.7	Невиконання організаційних заходів захисту	Персонал, користувачі	Неуважність, недбалість, некомпетентність			+	+
2.1.8	Неправомірне впровадження і використання програм, що не є необхідними для виконання користувачем своїх службових обов'язків та непередбачені відповідними розпорядчими документами (навчальні, ігрові програми, системне і прикладне забезпечення та ін.) з наступною необґрунтованою витратою ресурсів	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+	
2.1.9	Помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+	
2.1.10	Неправильне використання, настроювання або неправомірне відключення засобів захисту	Персонал	Неуважність, недбалість, некомпетентність	+	+	+	+

Продовження таблиці 3.1

№ з/п	Тип та визначення загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз або причини	Наслідки (порушення властивостей)			
				К	Ц	Д	С
2.1.11	Порушення порядку зберігання та обліку: документів, носіїв інформації, даних, технічних засобів	Персонал, користувачі	Неуважність, недбалість, некомпетентність	+	+	+	+
2.1.12	Виведення з ладу технічних засобів	Персонал, користувачі	Неуважність, недбалість, некомпетентність		+	+	
2.1.13	Порушення технології введення та виведення інформації	Персонал, користувачі			+	+	
2.2	Навмисні загрози						
2.2.1	Збір за допомогою спеціальних технічних засобів електромагнітних випромінювань ОТЗ (пристроїв наочного відображення; процесора; ліній зв'язку тощо)	Апаратура	Каналами ПЕМВІН	+			
2.2.2	Збір за допомогою спеціальних технічних засобів паразитних наведень на допоміжні засоби та системи (у мережах теплопостачання; системах вентиляції; шинах заземлення; мережах живлення)	Апаратура	Каналами ПЕМВІН	+			
2.2.3	Прослуховування телефонних розмов.	Апаратура Люди	Каналами ПЕМВІН Несанкціоноване підключення	+			
2.2.4	Використання оптичних засобів, дистанційне фотографування	Апаратура	Недотримання організаційних заходів	+			
2.2.5	Незаконне підключення: до апаратури, до системи електроживлення, заземлення	Персонал, користувачі, апаратура	Каналами ПЕМВІН	+	+	+	+
2.2.6	Читання «сміття» (залишкової інформації з запам'ятовувальних пристроїв)	Апаратура, програми, персонал, користувачі	Отримання доступу до МНІ або оперативної пам'яті сторонніх осіб	+			
2.2.7	Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду віддрукованих на принтері документів	Персонал, користувачі	Знаходження в службових приміщеннях сторонніх осіб	+			
2.2.8	Несанкціоноване використання технічних пристроїв	Персонал, користувачі	Недостатній контроль	+	+	+	+
2.2.9	Використання заборонених технічних пристроїв	Персонал, користувачі, апаратура	Недостатній контроль	+	+	+	+

Завершення таблиці 3.1

№ з/п	Тип та визначення загроз	Джерела виникнення загроз	Можливі методи, способи здійснення загроз або причини	Наслідки (порушення властивостей)			
				К	Ц	Д	С
2.2.10	Використання закладних та дистанційних підслуховуючих пристроїв	Персонал, користувачі, апаратура	Каналами ПЕМВІН	+			
2.2.11	Несанкціоноване внесення змін (підміни) в КТЗ, в програмне забезпечення, в компоненти інформаційного забезпечення	Персонал, користувачі, апаратура	Недостатній контроль	+			+
2.2.12	Копіювання вихідних документів, магнітних та інших носіїв інформації (у тому числі при проведенні ремонтних та регламентних робіт)	Апаратура, програми, персонал, користувачі	Отримання доступу до МНІ сторонніх осіб	+			
2.2.13	Розкрадання магнітних носіїв та документів (оригінали і копії інформаційних матеріалів, ГМД), отримання не облікованих копій	Персонал, користувачі	Недостатній контроль	+			
2.2.14	Включення в програми програмних закладок типу «троянський кінь», «бомба» тощо	Персонал, користувачі, програми	Використання неперевіреного ПЗ	+	+	+	+
2.2.15	Використання вад мов програмування, операційних систем	Персонал, користувачі, програми	Використання неперевіреного ПЗ	+	+	+	+

- *К* - порушення конфіденційності інформації.
- *Д* - порушення достовірності інформації.
- *Ц* - порушення цілісності інформації.
- *С* - порушення спостережності та керованості ІКСС.

Серед найбільш розповсюджених загроз шляхом несанкціонованого доступу (НСД) до інформаційних ресурсів ІКСС – методів подолання («зламу») засобів управління доступом – слід відзначити [27]:

1) комплексний пошук можливих методів НСД: зловмисники винятково ретельно вивчають системи безпеки перед проникненням у неї; дуже часто вони знаходять очевидні й дуже прості методи подолання системи, які розробники просто «прогледіли», створюючи можливо дуже гарну систему ідентифікації або шифрування;

2) НСД через термінали захищеної інформаційної системи – точки входу користувача в інформаційну мережу: у тому випадку, коли до них мають доступ кілька людей або взагалі будь-який охочий, при їхньому проєктуванні й експлуатації необхідно ретельно дотримуватися комплексу заходів безпеки, в тому числі, а можливо і насамперед організаційних;

3) НСД шляхом спроб входу в систему зовсім без знання пароля, ґрунтуючись на викривленнях у реалізації програмного або апаратурного забезпечення, тобто шляхом підбору пароля;

4) НСД шляхом маскування під авторизованого користувача передбачає попереднє отримання паролю тим чи іншим чином, наприклад, на основі помилок адміністратора та користувачів.

3.2. Формалізація моделі потенційного порушника інформаційної безпеки ІКС

Модель порушника розробляється, як відомо, у кожному конкретному випадку виходячи з технології обробки інформації інформаційно-комунікаційною системою. Фактично це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дій тощо. Модель порушника має визначити [28]:

- категорії осіб, з-поміж яких може бути порушник та рівень їх можливостей;
- припущення про кваліфікацію та можливий рівень знань порушника;
- методи і способи, що використовуються при здійсненні порушень;
- можливу мету порушника та її градацію за ступенями небезпечності;
- можливі місця та способи здійснення порушень;
- припущення про характер дій порушника.

Як порушника слід розглядати особу, яка прагне чи може одержати НСД до роботи з включеними до складу ІКС засобами. При побудові моделі порушника слід враховувати, що особливістю ресурсів ІКС, в першу чергу інформаційних, є їх принадливість для окремих осіб чи певних груп осіб, які з метою використання цих

ресурсів прагнуть бути чи є користувачами ІКС. Ця принадливість найчастіше є обумовленим характером та об'ємом інформації, яка вводиться, обробляється, зберігається та циркулює в ІКС. Якщо та чи інша особа – користувач ресурсами ІКС здійснює спробу НСД до об'єктів захисту, то такий користувач є порушником.

До категорій осіб, які можуть бути порушниками відносять внутрішніх і зовнішніх порушників. Зовнішніми порушниками можуть бути суб'єкти, що не мають права доступу до контрольованої зони (КЗ) або суб'єкти, що мають право постійного або разового доступу в КЗ ($Н_{внеш}$). Вони, як правило, впливають на всі рівні об'єкта захисту з метою розкрадання інформації, самоствердження, а також з метою виведення ІКС з ладу. Для цього внутрішніми порушниками використовуються методи й засоби активного впливу (модифікація й підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм тощо).

Внутрішні порушники можуть бути поділені на такі категорії:

1) порушники першої категорії ($Н_1$) – суб'єкти, що мають санкціонований доступ у КЗ, але не мають доступу до ІКС. Вони можуть впливати на фізичний рівень стека протоколів TCP/IP, рівень шкідливого впливу з метою розкрадання інформації або самоствердження. При цьому використовують технічні засоби перехоплення без модифікації компонентом системи (пасивні засоби атак);

2) порушники другої категорії ($Н_2$) – зареєстровані користувачі ІКС, які здійснюють обмежений доступ до ресурсів системи з АРМ. Можуть впливати на фізичний, транспортний і прикладний рівні стека протоколів TCP/IP» рівень системного й прикладного програмного забезпечення, рівень шкідливого впливу з метою розкрадання інформації, самоствердження або ненавмисно При цьому використовують технічні засоби перехоплення без модифікації компонентів системи (пасивні засоби атак), а так само штатні засоби й недоліки СЗІ для її подолання;

3) порушники третьої категорії ($Н_3$) – зареєстровані користувачі ІКС, які здійснюють вилучений доступ до ІКС по локальним і (або) розподіленим каналам передачі даних. Можуть впливати на фізичний, мережний, транспортний і

прикладний рівні стека протоколів TCP/IP, рівень системного й прикладного програмного забезпечення» рівень шкідливого впливу з метою розкрадання інформації, самоствердження або ненавмисно. При цьому використовують технічні засоби перехоплення без модифікації компонентів системи (пасивні засоби атак), а так само штатні засоби й недоліки СЗІ для її подолання;

4) порушники четвертої категорії (H_4) – зареєстровані користувачі з повноваженнями системного адміністратора ІКС. Можуть впливати на всі рівні стека протоколів TCP/IP, рівень системного н прикладного програмного забезпечення, рівень шкідливого впливу, рівень технічних каналів з метою розкрадання інформації, або метою виводу з ладу ІКС. При цьому використовують всі можливі засоби атак. Можлива змова з порушниками п’ятої й шостої категорій. Не мають доступу до СрЗІ протоколювання й до частини ключових елементів ІКС;

5) порушники п’ятої категорії (H_5) – зареєстровані користувачі з повноваженнями адміністратора ІБ ІКС. Можуть впливати на всі рівні стека протоколів TCP/IP, рівень системного й прикладного програмного забезпечення, рівень шкідливого впливу, рівень технічних каналів, рівні СЗІ криптографічними й не криптографічними засобами з метою розкрадання інформації, а так само з метою виводу з ладу ІКС. При цьому використовують всі можливі засоби атак. Можлива змова з порушниками четвертої й шостої категорій. Не мають прав доступу до конфігурування технічних засобів мережі, за винятком контрольних (інспекційних);

6) порушники шостої категорії (H_6) – розроблювачі прикладного програмного забезпечення й технічних засобів, а також особи, які забезпечують їхню поставку, супровід і ремонт на об’єкті, що підлягає захисту. Можуть впливати на всі рівні стека протоколів TCP/IP, рівень системного й прикладного програмного забезпечення, рівень шкідливого впливу, рівень технічних каналів, рівень заставних пристроїв з метою розкрадання інформації, а так само з метою виводу з ладу ІКС. При цьому використовують всі можливі засоби атак. Можлива змова з порушниками четвертої й п’ятої категорії. Мають можливості внесення помилок, недекларованих можливостей, програмних закладок, шкідливих програм у програмне забезпечення й технічні засоби ІКС.

За рівнем можливостей, що надаються їм штатними засобами ІКС, порушників доцільно класифікувати за чотирма рівнями. При цьому:

– перший рівень визначає найнижчий рівень можливостей проведення діалогу з ІКС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням ІКС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проєктування, реалізацію і ремонт апаратних компонентів ІКС, аж до включення до складу ІКС власних засобів з новими функціями обробки інформації.

За рівнем знань усіх порушників слід класифікувати як таких, що:

– володіють інформацією про функціональні особливості ІКС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами:

– володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проєктування та експлуатації ІКС;

– володіють інформацією про функції та механізм дії засобів захисту.

Зрозуміло, що найбільш небезпечні порушники можуть знати:

1) склад, розміщення, функціональні особливості, умови та режими функціонування елементів ІКС, включаючи траси прокладених чи можливих ліній зв’язку комунікаційних мереж та трафіки відповідних каналів передачі даних;

2) порядок, засоби та режими здійснення охорони елементів ІКС, місць їх розташування (включаючи пункти підсилення, як такі, що обслуговуються, так і ті, що не обслуговуються) та прилеглої території;

3) порядок, засоби та режими здійснення організаційно-правових та технічних заходів захисту інформаційних та інших цінних ресурсів;

4) основні закономірності формування баз даних та потоків запитів до них.

За застосовуваними методами і способами порушників можна класифікувати як таких, що використовують:

– виключно агентурні методи одержання відомостей:

– пасивні технічні засоби перехоплення інформаційних сигналів;

– виключно штатні засоби ІКС або недоліки проєктування КСЗІ для реалізації спроб НСД;

– способи і засоби активного впливу на ІКС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального програмного забезпечення тощо).

Можливою метою будь-якого порушника при цьому може бути [30]:

1) особиста авторизація, тобто отримати особисті легальні атрибути доступу, бажано з найширшими правами, до ресурсів ІКС з метою їх використання, отримання необхідної інформації у потрібному обсязі та асортименті, ознайомлення з конфіденційною інформацією. її модифікації чи знищення відповідно до своїх намірів (інтересів, планів);

2) авторизація своїх прихильників чи довірених осіб, які б мали змогу отримати легальні атрибути доступу, бажано з найширшими правами, до ресурсів ІКС з метою їх використання, отримання необхідної інформації у потрібному обсязі та асортименті, ознайомлення з конфіденційною інформацією, її модифікації чи знищення згідно з своїми намірами (інтересами, планами);

3) пошук прихильників чи довірених осіб серед персоналу чи користувачів ІКС, які мають змогу отримувати легальні атрибути доступу, бажано з найширшими правами, до ресурсів ІКС і можуть їх використовувати, отримувати бажано конфіденційну інформацію. її модифікувати чи знищувати.

При відсутності змоги чи безуспішності реалізації пунктів 1-3 метою порушника може бути реалізація спроб щодо:

1) здобуття атрибутів доступу авторизованих користувачів шляхом використання технічних засобів, крадіжок, купівлі, чи отримання іншим шляхом;

2) проникнення на місця розміщення тих чи інших компонентів, елементів чи ресурсів АС (обчислювальних ресурсів, інформаційних ресурсів, базового, прикладного програмного забезпечення та програмного забезпечення системи ТЗІ. включаючи носії резервних копії, ресурсів вводу/ виводу, телекомунікаційного обладнання, включаючи мережу передачі даних) шляхом подолання перешкод (огорожі, елементів будівельних конструкцій, охорони чи охоронної сигналізації та ін.) та нанесення збитків шляхом знищення матеріальних та інформаційних цінностей;

3) зміна режимів функціонування чи виводу з ладу фізичних ресурсів ІКС;

4) установка фізичних засобів (апаратурних закладок) чи інших засобів технічної розвідки в місцях розміщення елементів ІКС (в тому числі і віддалених, наприклад в елементах комунікаційної мережі зв'язку) для знімання інформації;

5) установка апаратурних закладок в місцях розміщення елементів ІКС (в тому числі і віддалених, наприклад, в елементах комунікаційної мережі зв'язку) для генерації несправжніх сигналів, інформаційних символів чи повідомлень;

6) установка програмних засобів (програмних закладок) знімання інформації з метою її того чи іншого використання;

7) установка програмних засобів (програмних закладок чи вірусів) для модифікації як програмних засобів, так і інформації ІКС шляхом генерації (впровадження) програмних вірусів, несправжніх сигналів, інформаційних символів чи повідомлень з метою перевантаження систем ІКС і порушення, таким чином, доступності компонентів ІКС чи ІКС в цілому;

8) здійснення спроб НСД до обчислювальних ресурсів, інформаційних ресурсів, базового та прикладного програмного забезпечення та програмного забезпечення системи ТЗІ як власне ІКС, так і її телекомунікаційної підсистеми шляхом подолання системи управління доступом.

За місцем здійснення злочину дії порушника можна класифікувати на:

1) без одержання доступу на контрольовану територію (ІКС центрального рівня, ІКС регіональних рівнів чи робочих місць ІКС місцевих рівнів, пунктів

підсилення з обслуговуванням) з використанням технічних засобів дистанційної розвідки (наприклад, оптичними, акустичними каналами, каналами побічних електромагнітних випромінювань та ін.) або з використанням засобів здобуття інформації з мережі передачі даних (наприклад, шляхом підключення чи «врізання» в лінії зв'язку) – дистанційний вплив;

2) з одержанням доступу на контрольовану територію (ІКС центрального рівня, ІКС регіональних рівнів чи робочих місць кінцевих, в тому числі віддалених користувачів ІКС, пунктів підсилення з обслуговуванням, але без доступу до технічних засобів ІКС) – також з використанням технічних засобів дистанційної розвідки (наприклад, оптичними та акустичними каналами, каналами побічних електромагнітних випромінювань тощо) з подальшим НСД до будівель, споруд чи приміщень, в яких розміщено елементи ІКС (безпосередній вплив);

3) з одержанням доступу до робочих місць кінцевих (в тому числі віддалених кінцевих робочих місць та пунктів підсилення без обслуговування) користувачів ІКС з подальшим несанкціонованим доступом до пристроїв вводу/виводу, копіювання, канального чи каналоутворюючого обладнання та інших елементів ІКС – безпосередній, як і в наступних пунктах 4-5 вплив;

4) з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів) з подальшим несанкціонованим копіюванням власне носіїв даних, їх копій чи інформації з цих накопичувачів та баз даних;

5) з одержанням доступу до засобів адміністрування ІКС і засобів управління комплексною системою ТЗІ з подальшими, практично необмеженими можливостями доступу до ресурсів АС, їх використання, модифікації чи знищення (за виключенням, можливо, того, що його дії будуть зафіксованими компонентом спостережності системи ТЗІ).

За характером дій він може здійснювати активні чи пасивні загрози ресурсам ІКС. Під активною загрозою розуміється спроба навмисної несанкціонованої зміни стану системи, а під пасивною загрозою – спроба несанкціонованого проникнення в систему без зміни її стану. При цьому за характером дій порушників можна класифікувати на:

1) «випадкових порушників» – авторизованих користувачів, які порушили політику безпеки тієї чи іншої послуги не навмисно, а помилково - шляхом випадкового подолання засобів управління (адміністрування) доступом до об’єкту захисту, виконання непередбачених дій відносно цього об’єкту та т.п.:

2) «терплячих зловмисників» – авторизованих користувачів, які порушили політику безпеки тієї чи іншої послуги навмисно, але без рішучих дій. маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою прихованого подолання засобів управління (адміністрування) доступом до нього та т.п.;

3) «рішучих зловмисників», які мають на меті будь-що порушити ту чи іншу властивість захищеної інформації; для цього такі зловмисники прагнуть подолати засоби організаційного обмеження доступу, охоронної сигналізації, управління доступом до фізичних ресурсів, елементи будівельних конструкцій тощо і отримати змогу фізичного доступу до засобів оброблення, зберігання чи передавання інформаційних об’єктів з метою виведення їх з ладу, зміни режимів функціонування, крадіжки чи пошкодження носіїв, наприклад, накопичувачів на жорстких чи гнучких магнітних дисках тощо;

4) зловмисників, які використовують засоби віддаленого доступу до інформаційних об’єктів: витоки інформації технічними канапами, спеціальні впливи на інформацію по технічним каналам, мережне обладнання локальних чи розподілених мереж, в тому числі і засоби телекомунікаційних мереж.

Така класифікація дозволяє більш чітко визначати способи несанкціонованих дій порушників – перелік загроз ресурсам ІКС та засоби, які потрібні для їх унеможливлення.

Формування типової моделі порушника має здійснюватися з урахуванням вимог, які забезпечують її функціональність і практичну ефективність. За критерій ефективності при цьому приймається, як правило, критерій своєчасності виявлення НСД. Під своєчасним виявленням розуміється ухвалення рішення про виявлення НСД у такий момент часу, коли залишається ще досить часу для розгортання сил охорони й перехоплення порушника. Час реагування сил охорони T_p визначає критичну точку виявлення (КТВ). КТВ – це точка на маршруті руху порушника, після якої виявлення НСД не дозволяє силам охорони вчасно прибути до місця перехоплення й зробити

ефективну протидію порушникам. У цій точці час реагування сил охорони ще не перевершує мінімальний час здійснення НСД:

$$T_{нсд} \geq T_p. \tag{3.3}$$

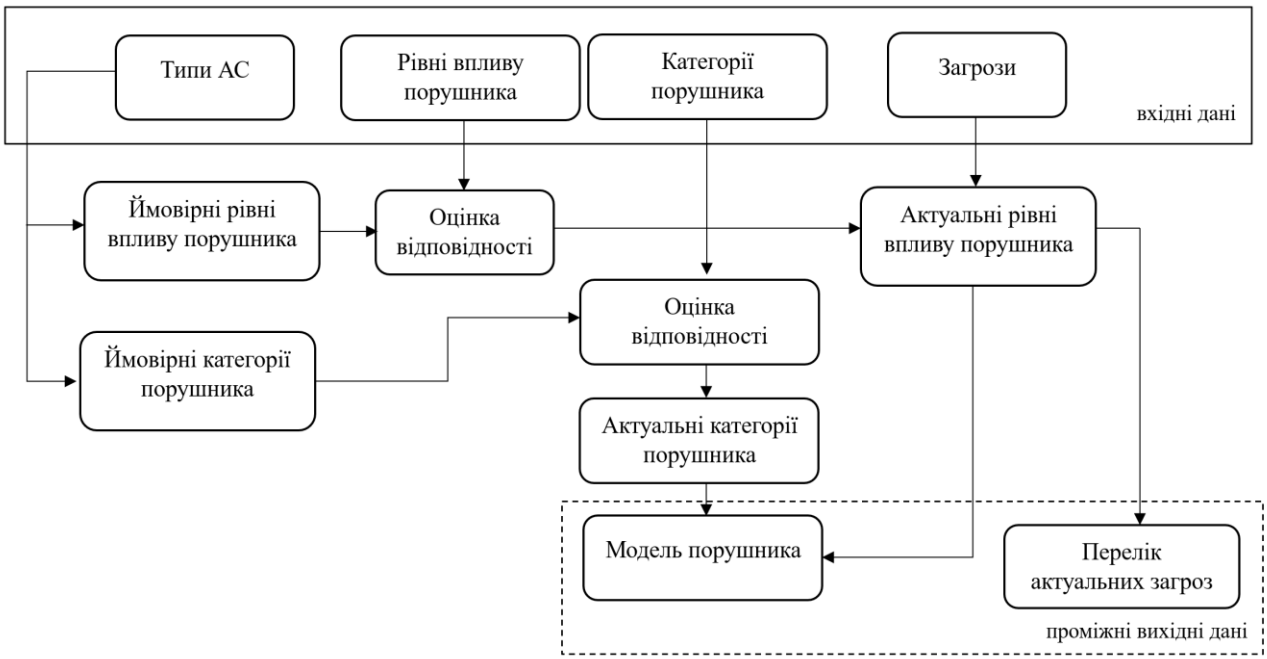

Рис. 3.4. Узагальнена схема побудови моделі порушника

Основними стадіями формування моделі порушника при цьому є (рис. 3.4):

1) визначення типу ІКС по різних класифікаційних ознаках;

2) визначення на підставі отриманого типу ІКС категорії порушників і рівнів впливу порушників, характерні для даного типу системи;

3) оцінка відповідності отриманих категорій порушників і рівнів впливу порушників заявленим у типовій моделі порушника;

4) формування за результатами оцінки актуальних категорій порушників актуальних рівнів їхнього впливу, характерних для конкретної ІКС, тобто формування приватної моделі порушника для конкретної системи;

5) формування на основі актуальних рівнів впливу порушників переліку актуальних загроз ІБ, джерелом яких є порушник. У випадку виключення суб’єктів атак з-поміж потенційних порушників додатково до вищеописаних стадій необхідно виконати наступне:

6) з категорій порушників приватної моделі порушника для конкретної ІКС, виключаються категорії порушників, віднесені до довірених;

7) проводиться оцінка відповідності актуальних категорій порушників з урахуванням виключень категорій порушників, віднесених до довірених, з актуальними рівнями впливу порушників, отриманими із приватної моделі порушника для конкретної ІКС;

8) за результатами оцінки формуються актуальні рівні впливу порушників, характерні для конкретної ІКС із урахуванням виключення категорій порушників, віднесених до довірених, тобто формується приватна модель порушника для конкретної ІКС із урахуванням виключення категорій порушників, віднесених до довіреного;

9) на основі актуальних рівнів впливу порушників, характерних для конкретної ІКС формується перелік актуальних загроз ІБ, джерелом яких є порушник, для конкретної ІКС із урахуванням виключення категорій порушників, віднесених до довіреного.

Як результат модель порушника являтиме собою сукупність стратегічних дій порушника *P* та його навичок *T*:

$$P = \begin{pmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ \dots & \dots & \dots & \dots \\ p_{m1} & p_{m2} & \dots & p_{mn} \end{pmatrix}, \qquad T = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ p_{21} & p_{22} & \dots & t_{2n} \\ \dots & \dots & \dots & \dots \\ t_{m1} & t_{m2} & \dots & t_{mn} \end{pmatrix} \tag{3.4}$$

Елементом матриць p_{ij} та t_{ij} є ймовірність виявлення НСД та час подолання елемента СФЗ *i-го* типу, використовуючи *j*-у навичку з набору навичок порушника. При цьому доцільно розглядати такі основні стратегії порушника щодо подолання бар'єрів СФЗ: мінімізація часу подолання, мінімізація ймовірності виявлення й оптимальна стратегія. При оптимальній стратегії до досягнення критичної точки виявлення дії порушника спрямовані на мінімізацію ймовірності виявлення (приховане проникнення), а після КТВ – відповідно до стратегії мінімізації часу подолання (силовий прорив). Дана комбінована стратегія показана на рис. 3.5. Застосування даної стратегії в моделі порушника

відповідає принципу гарантованого результату й знімає невизначеність у стратегії поводження порушника.

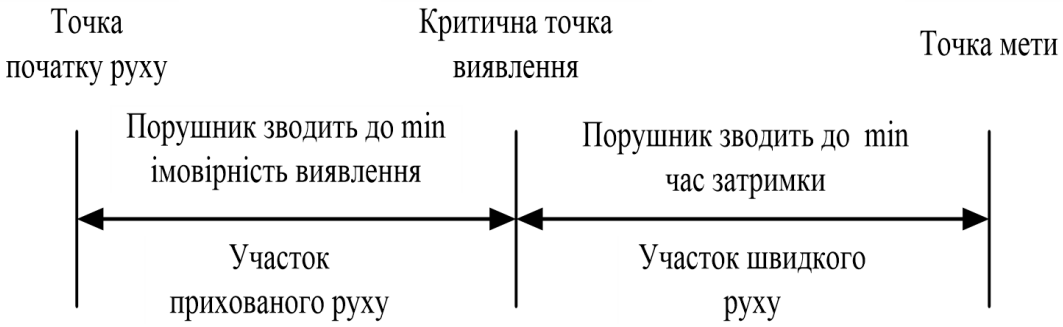

Рис. 3.5. Модель комбінованої стратегії дій порушника

Отримані в результаті приватна модель порушника, представлена актуальними категоріями порушників і актуальних рівнів впливу порушників, і перелік актуальних загроз ІБ, джерелом яких є порушник, дозволяють створити СЗІ для конкретної ІКС без додаткових фінансових витрат, тому що надлишкових вимог до СЗІ не пред’являють. Разом з цим це дозволить:

– сформувати класифікаційні ознаки й категорії порушників;

– розробці правил розмежування доступу відповідно до функціональних обов'язків;

– детально описати категорії порушників з обліком запропонованих класифікаційних ознак;

– деталізувати основні класифікаційні ознаки класифікації порушників.

При цьому як критерій класифікації, що дозволяє однозначно класифікувати порушників, у методиці запропоновано використовувати рівні впливу порушників з урахуванням запропонованої деталізації.

3.3. Розробка моделі фізичного захисту інформації з повним перекриттям

Модель фізичного захисту інформації повинна, як відомо, відображати взаємозалежність всієї сукупності параметрів, що визначають міру загрози безпеці для розглянутого об’єкта від всієї сукупності або від окремо взятих уразливостей

(дестабілізуючих факторів) у співвіднесенні з тими втратами, які можуть спостерігатися при реалізації загрози. Під уразливістю системи захисту в цьому сенсі будемо розуміти можливість здійснення загрози u_i відносно об'єкта o_j (на практиці під уразливістю системи захисту за звичай розуміється не сама можливість здійснення загрози безпеці, а ті властивості системи, які сприяють успішному здійсненню загрози або можуть бути використані зловмисником для здійснення загрози).

Спрощено процес зіставлення загроз U та уразливостей об'єкта захисту O може бути представлений моделлю, поданою на рис. 3.6.

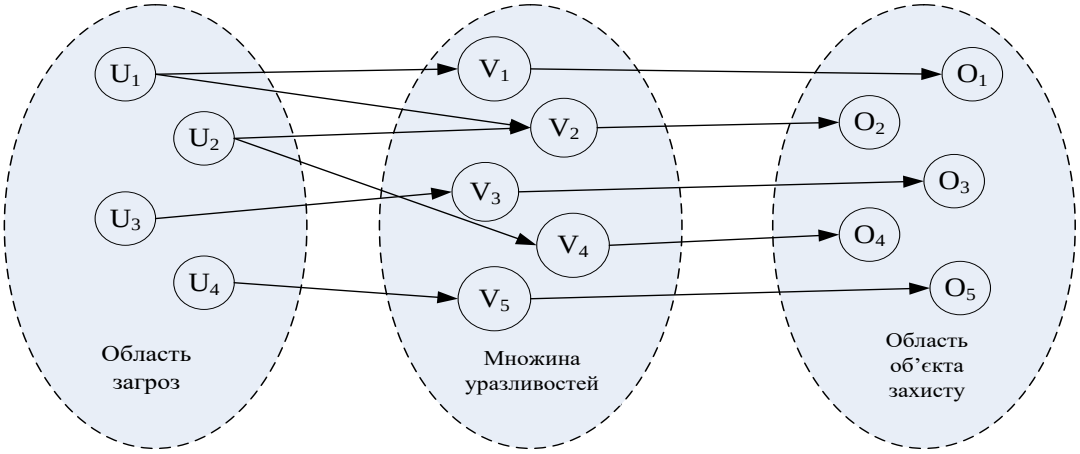

Рис. 3.6. Графова модель зіставлення загроз і уразливостей

Відношення U і O у цій моделі реалізується через множину елементів V – набору уразливих місць (див. табл. 3.2).

Таблиця 3.2

Зіставлення фізичних загроз і уразливостей ІКС підприємства

ЗАГРОЗИ АРМ	**УРАЗЛИВОСТІ АРМ**
1. Фізичний доступ порушника до АРМ	1. Відсутність системи контролю доступу співробітників до чужих АРМ
	2. Відсутність системи відеоспостереження в організації
	3. Непогодженість у системі охорони периметра
2. Розголошення конфіденційної інформації, що зберігається на АРМ співробітника організації	1. Відсутності угоди про нерозголошення між працівником і роботодавцем
	2. Нечітка регламентація відповідальності співробітників організації

Продовження таблиці 3.2

ЗАГРОЗИ СЕРВЕРІВ	УРАЗЛИВОСТІ СЕРВЕРІВ
1. Фізичний неавторизований доступ порушника в серверну кімнату	1. Неорганізований контрольно-пропускний режим в організації
	2. Відсутність відеоспостереження в серверній кімнаті
	3. Відсутність охоронної сигналізації
2. Розголошення конфіденційної інформації	1. Відсутність угоди про нерозповсюдження конфіденційної інформації 2. Нечітка регламентація відповідальності співробітників організації
ЗАГРОЗИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ	**УРАЗЛИВОСТІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ**
1. Фізичний доступ порушника до носіїв конфіденційної інформації	1. Неорганізованість контрольно-пропускного пункту
	2. Відсутність системи відеоспостереження в організації
	3. Відсутність системи охоронної сигналізації
2. Розголошення конфіденційної інформації, у документах, винос носіїв за межі контрольованої зони	1. Відсутність угоди про нерозголошення конфіденційної інформації
	2. Нечіткий розподіл відповідальності за документи (носії конфіденційної інформації) між співробітниками організації
3. Несанкціоноване копіювання, печатка й розмноження носіїв конфіденційної інформації	1.Нечітка організація конфіденційного документообігу в організації
	2. Неконтрольований доступ співробітників до копіювальної й розмножувальної техніки
ЗАГРОЗИ МЕРЕЖНИХ ПРИСТРОЇВ І КОМУТАЦІЙНОГО ВСТАТКУВАННЯ	**УРАЗЛИВОСТІ МЕРЕЖНИХ ПРИСТРОЇВ І КОМУТАЦІЙНОГО ВСТАТКУВАННЯ**
1. Фізичний доступ до мережного пристрою	1. Неорганізований контрольно-пропускний режим в організації
	2. Відсутність системи відеоспостереження в організації
	3. Непогодженість у системі охорони периметра
	4. Нечітка регламентація відповідальності співробітників підприємства
2. Руйнування (ушкодження, втрата) мережних пристроїв і комутаційного встаткування	1. Відсутність обмеження доступу до мережних пристроїв і комутаційного встаткування, внутрішній мережі підприємства
	2. Нечітка регламентація відповідальності співробітників підприємства

Завершення таблиці 3.2

ЗАГРОЗИ ПРИСТРОЇВ КЕРУВАННЯ	УРАЗЛИВОСТІ ПРИСТРОЇВ КЕРУВАННЯ
1. Фізичний доступ порушника до пристроїв керування	1. Неорганізованість контрольно-пропускного режиму в організації
	2. Відсутність відеоспостереження в організації
2. Руйнування, ушкодження пристроїв керування	1. Неорганізованість контрольно-пропускного режиму в організації
	2. Неконтрольований доступ співробітників до техніки

Найбільш застосовною нині моделлю фізичного захисту є модель системи з повним перекриттям (модель Клементса-Хоффмана). У формуванні моделі беруть участь три множини, що представляють області:

«загроз» – $U = \{u_i\},\ i = \overline{1,m}$;

«об'єктів, що захищаються» – $O = \{o_j\},\ j = \overline{1,n}$;

«системи або механізмів захисту» – $M = \{m_k\},\ k = \overline{1,r}$.

Елементи множин U і O перебувають між собою в певних відносинах «загроза-об'єкт», обумовлених дводольним графом $G(X,E)$, де X – множина вершин графа $X = \{x_{i+j}\},\ i = \overline{1,m},\ j = \overline{1,n}$, а E – множина дуг графа. Дуга $< U_i, O_j >$ існує тільки тоді, коли U_i є засобом одержання доступу до об'єкта O_j. Мета захисту полягає в тому, щоб «перекрити» кожну дугу графа й спорудити бар'єр для доступу цим шляхом. Введення множини засобів (механізмів) захисту M забезпечить захист множини об'єктів O від множини загроз U. Їх застосування перетворить 2-дольний граф в 3-дольний (рис. 3.7). В ідеалі кожний засіб (механізм) захисту m_k повинен усувати деяке ребро $< U_i, O_j >$ із зазначеного графа. У такій системі всі ребра представляються у вигляді $< U_i, M_k >$ й $< M_k, O_j >$. При цьому один і той самий засіб (механізм) захисту може перекривати більше однієї загрози й захищати більше одного об'єкта, виконуючи при цьому функцію «брандмауера» й забезпечуючи певний ступінь опору спробам проникнення.

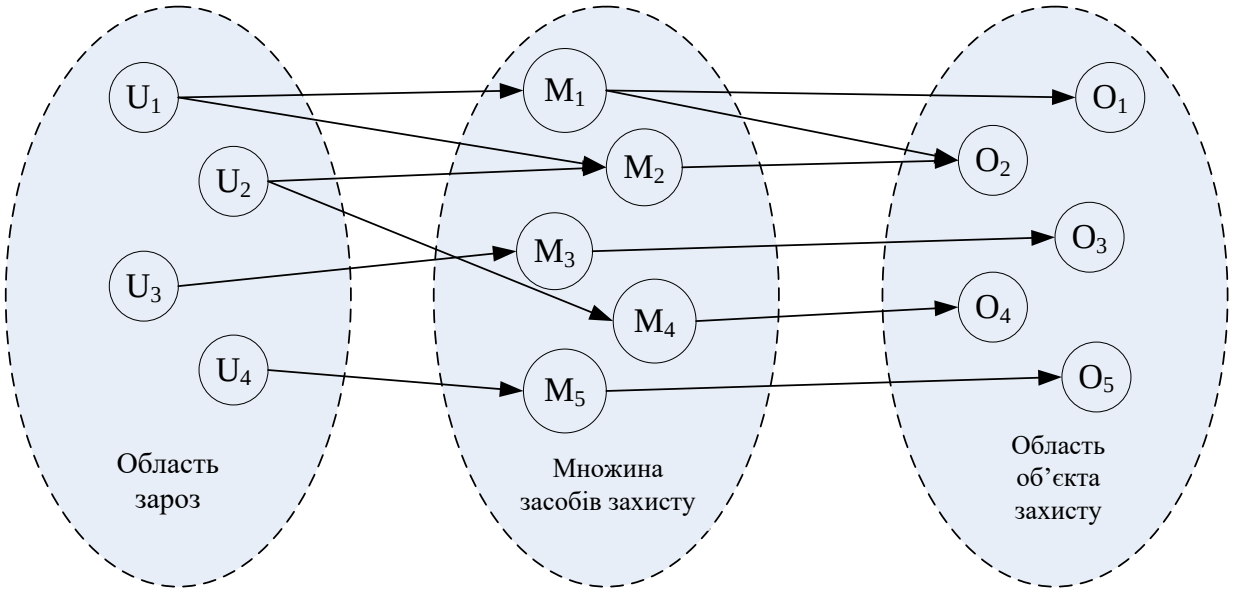

Рис. 3.7. Множина відносин «об'єкт-механізм захисту-загроза»

Додатково увівши ще дві множини, а саме V – набір уразливих місць та B – набір бар'єрів, процес фізичного захисту інформації можна представити за допомогою 5-мірного кортежу (рис. 3.8):

$$S = \{O, U, M, V, B\}, \tag{3.5}$$

де O – множина об'єктів, що захищаються; U – множина можливих загроз; M – множина засобів захисту; V – множина уразливих місць, що являють собою шляхи проникнення до системи, де $v_p =< u_i, o_j >$; B – множина бар'єрів, що представляють собою точки, у яких потрібно здійснити захист, де $b_q =< u_i, o_j, m_k >$.

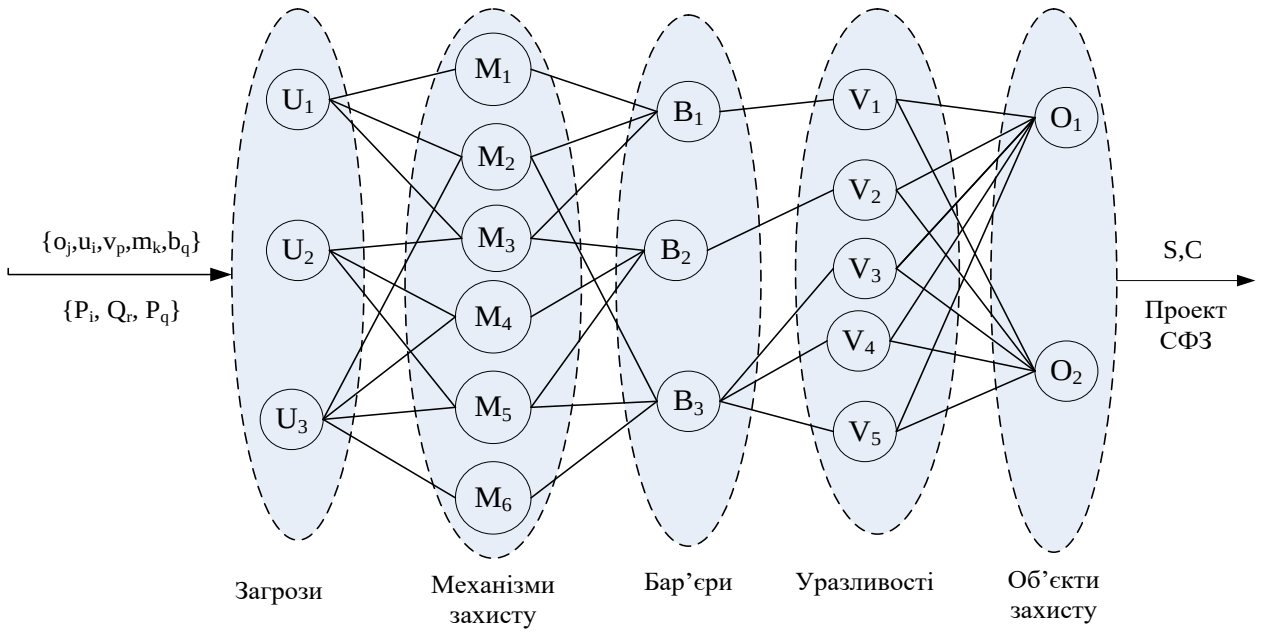

Рис. 3.8. Структурна схема моделі системи фізичного захисту інформації з повним перекриттям

У такій системі кожному уразливому місцю v_p відповідає бар'єр b_q. Головне завдання полягає в знаходженні раціонального вибору технічних засобів у кожному бар'єрі захисту. Їх міцність може бути при цьому охарактеризована величиною залишкового ризику $Risk_i$, пов'язаного з можливістю здійснення загрози u_i відносно об'єкта o_j при використанні бар'єра b_q:

$$Risk_i = P_i \cdot Q_j \cdot (1 - B_q),\ i = \overline{1,m},\ j = \overline{1,n}, q = \overline{1, m \times n}; \quad (3.4)$$

де P_i – імовірність появи загрози y_i, Q_j – величина збитку при вдалому здійсненні загрози y_i відносно об'єкта o_j, який захищається, B_q – ступінь опору бар'єра b_q, що характеризується ймовірністю його подолання.

У загальному випадку стійкість бар'єра визначатиметься за формулою:

$$P = \sum_i P_{mi} - \sum_{ij} (P_{mi} P_{mj}) + \sum (P_{mi} P_{mj} P_{mk}) - \ldots + (-1)^{n-1} P_{m1} P_{m2} \ldots P_{mn}, \quad (3.5)$$

де n – кількість механізмів бар'єра захисту.

У свою чергу, стійкість механізму може визначатися за формулою:

$$P_{i(мех)} = (1 - P_{i(чф)})(1 - P_{i(тех)}), \tag{3.6}$$

де $P_{i(чф)}$ – імовірність відмови механізму через людський фактор (відсутність на робочому місці, порушення правил безпеки й т.д.), $P_{i(тех)}$ – імовірність відмови механізму з технічних причин.

Порівняння варіантів побудови СФЗІ представлено в табл. 3.3.

Таблиця 3.3

Варіанти побудови бар'єрів

№ з/п	Позначення варіанта	Опис бар'єрів
1	a_0	Система захисту відсутній
2	a_1	$B_1\{M_1\}$; $B_2\{M_4, M_5\}$; $B_3\{M_5, M_6\}$
3	a_2	$B_1\{M_1, M_2, M_3\}$; $B_2\{M_3, M_4, M_5\}$; $B_3\{M_2, M_5, M_6\}$

Оцінка стійкості використовуваних у таких системах бар'єрів захисту повинна ґрунтуватися на статистичних даних, що характеризують роботу як персоналу, так і технічних засобів. Найбільш застосовуваним методом збору і обробки таких даних є експертні оцінки.

Величину захищеності всієї системи визначимо за формулою:

$$S = \frac{1}{\Sigma(\forall b_q \in B)(P_i \cdot Q_i \cdot (1 - B_q))}, \quad P_i, Q_j, B_q \in [0,1) \tag{3.7}$$

У формулі (3.7) знаменник визначає сумарну величину залишкових ризиків, пов'язаних з можливістю здійснення загроз безпеки *U* відносно об'єктів захисту *O*, при використанні механізмів захисту *M*. Сумарна величина залишкових ризиків характеризує загальну уразливість системи захисту, а захищеність системи визначається як величина, зворотна її уразливості. При

відсутності в системі бар'єрів b_q, що перекривають певні уразливості, ступінь опору механізму захисту B_q приймається рівним 0.

За умови існування множини альтернатив (можливостей вибору) – A, множини негативних факторів (загроз), що впливають на об'єкти організації – F та множини можливих рішень – Y результат, очікуваний від реалізації будь-якого бар'єра захисту b_q відповідатиме сумарним витратам на проєктування СФЗІ:

$$\varphi_{iq} = Q_i + c_q. \tag{3.8}$$

При цьому під альтернативою $a_i \in A,\ i = \overline{1,m}$ слід розуміти варіанти побудови бар'єрів b_q з наявних механізмів захисту $m_k \in M$, $k = \overline{1,r}$, а під факторами $f_j \in F$, $j = \overline{1,n}$, матимемо на увазі загрози u_i безпеці ІКС.

Для визначення показника сумарних витрат необхідно сформувати оцінну матрицю (табл. 3.4) виду:

$$< A, F, Y >. \tag{3.9}$$

де a_0 – початковий стан системи без засобів захисту; a_i – захищений стан системи без засобів захисту.

Таблиця 3.4

Матриця оцінки сумарних витрат

№	f_1	Y_1	f_j	Y_j
a_0	$\varphi_{01} = Q_1$	S_{01}	$\varphi_{0j} = Q_j$	S_{0j}
a_1	$\varphi_{11} = Q_1 + c_1$	S_{11}	$\varphi_{1j} = Q_j + c_1$	S_{1j}
…	…	…	…	…
a_m	$\varphi_{m1} = Q_1 + c_m$	S_{m1}	$\varphi_{mj} = Q_j + c_m$	S_{mj}

Для ухвалення рішення всі значення матриці необхідно привести до безрозмірного виду. При використанні методу згортки й нормалізації критеріїв це завдання зводиться до знаходження екстремуму функції (у такому випадку – мінімуму, оскільки витрати необхідно мінімізувати):

$$Z = extr\sum_j Y_j = \min\sum_j Y_j . \tag{3.10}$$

Усі φ_{ij} приводяться до безрозмірного виду за формулою:

$$A_{ij} = \frac{\varphi_{ij}}{\max(\varphi_{ij})}, \tag{3.11}$$

де $\max(\varphi_{ij})$ – максимальне значення φ_{ij} в даному стовпці.

Для виключення впливу розмірності шкал, уводяться нормувальні коефіцієнти L_j (один на стовпець). Кожний коефіцієнт L_j розраховується за формулою:

$$L_j = \frac{1}{\sum_i A_{ij}}. \tag{3.12}$$

Потім усе приводиться до нормального виду

$$\varphi_{ij} = A_{ij} L_j . \tag{3.13}$$

Надалі безрозмірні й нормовані значення можна порівнювати між собою. При цьому для одержання результату необхідно построково скласти значення виходів $Y(\varphi_{ij} = A_{ij} L_j)$ й вибрати у векторі, що утворився, оптимум, який і відповідає рішенню завдання, у цьому випадку – максимуму.

$$\begin{cases} \tilde{\varphi} \to \min(\lambda_1) \\ \tilde{C} \to \max(\lambda_2) \end{cases} \quad \lambda_1(1-\tilde{\varphi}) + \lambda_2\tilde{C} \to \max . \tag{3.14}$$

Якщо значення сумарних витрат для альтернативи a_i відповідає заданим вимогам по мінімуму, а показник захищеності S для цієї альтернативи – вимогам по максимуму, то ця альтернатива, тобто варіант побудови бар'єрів захисту b_q, є оптимальним. Дана процедура використовується, якщо точно відомі витрати на створення СФЗІ й можливий збиток у грошовому вираженні.

3.4. Розробка методики вибору засобів фізичного захисту інформації

Методика вибору засобів фізичного захисту інформації може бути представлена схемою, поданою на рис. 3.9. На першому кроці реалізації методики здійснюється збір вихідних даних про об'єкт захисту, необхідних для опису характеристик його окремих елементів (виділення матеріальних та інформаційних цінностей, категорування об'єкта захисту і його елементів тощо). На другому кроці здійснюється ранжирування актуальних загроз фізичної безпеки. При цьому кожному носію інформації ставиться у відповідність численний набір загроз, реалізованих при ненульовому значенні просторового, часового та енергетичного факторів. На третьому кроці проводиться визначення найбільш уразливих місць об'єкта захисту. Враховуючи, що СФЗІ з повним перекриттям передбачає створення для кожного шляху проникнення загрози певного бар'єра захисту (бар'єр – сукупність механізмів фізичного захисту, спрямованих на локалізацію уразливостей системи), головне завдання третього кроку алгоритму полягає у знаходженні раціонального набору засобів ФЗІ в кожному бар'єрі. Вибір засобів здійснюється на користь альтернативи, що має найбільший коефіцієнт відповідності. На четвертому кроці алгоритму будується оцінна матриця та здійснюється розрахунок показника захищеності системи. Якщо бар'єр відповідає заданим вимогам, приймається рішення про його розміщення на об'єкті захисту. Якщо вимоги не дотримуються відбувається повторний вибір. Завданням роботи є вибір засобу ФЗІ в автоматизованій системі підприємства.

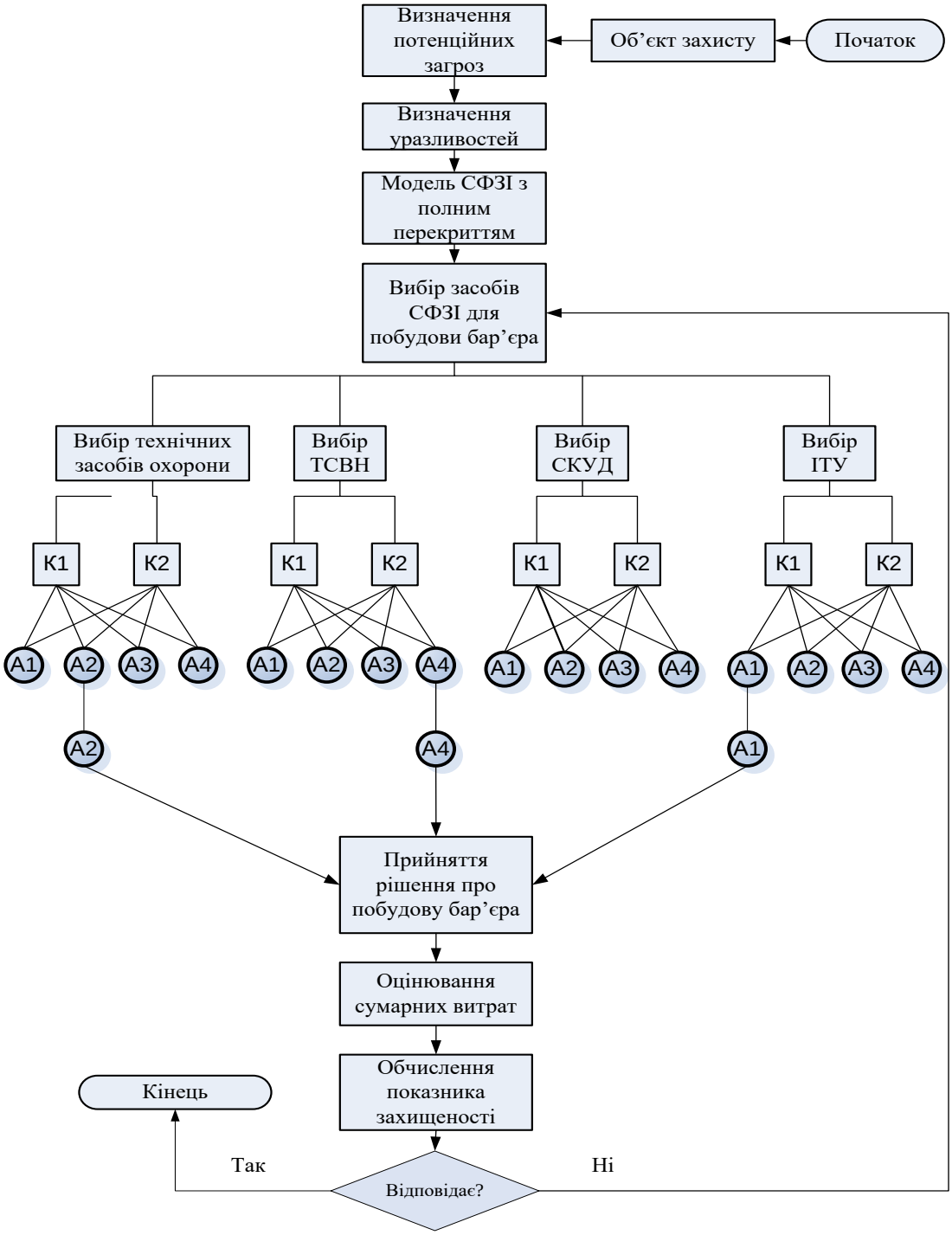

Рис. 3.9. Алгоритм вибору засобів для комплектування СФЗІ

Декомпозиція завдання вибору засобів ФЗІ може бути представлена схемою, поданою на рис. 3.10.

Припустимо, що існує:

1) кілька однотипних альтернатив (засобів захисту);

2) головний критерій порівняння альтернатив;

3) кілька груп однотипних факторів (часткових критеріїв, об’єктів, дій і т.п.), що певним чином впливають на добір альтернатив.

Необхідно: кожній альтернативі поставити у відповідність пріоритет (число) й таким чином сформувати рейтинг альтернатив. Причому чим більш кращою є альтернатива за вибраним критерієм, тим більшим буде її пріоритет.

Рішення. Процедуру вибору засобу ФЗІ в інформаційно-комунікаційній системі розглянемо на прикладі технічних засобів охорони (ТЗО). При побудові бар’єра захисту з використанням ТЗО скористаємося такими критеріями:

- імовірністю виявлення ($к_1$);
- авторитетом фірми виробника ($к_2$);
- гарантією на працездатність ($к_3$);
- оснащеністю технічною документацією ($к_4$).

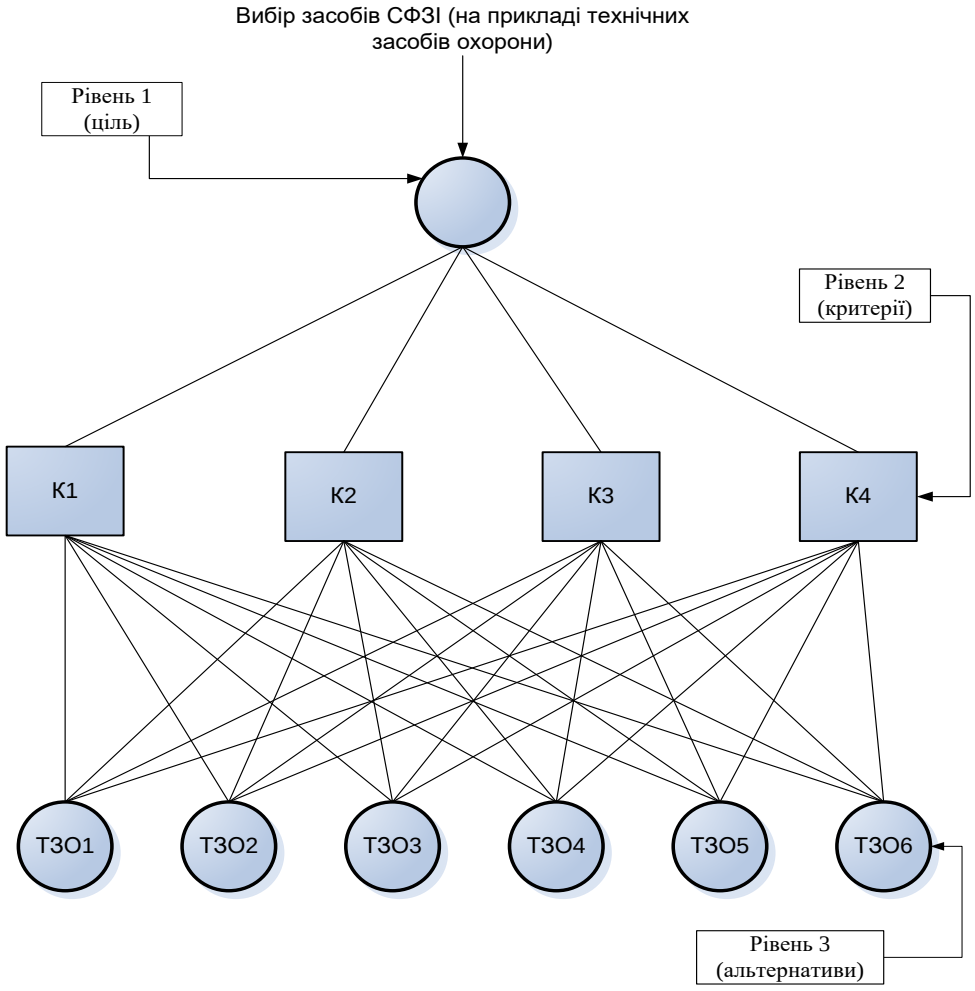

Рис. 3.10. Декомпозиція завдання вибору засобів СФЗІ

Після докладного розгляду кожного із критеріїв побудуємо табл. 3.5.

Таблиця 3.5

Таблиця ієрархій

Мета	Вибір найкращого засобу (ТЗО) при побудові системи фізичного захисту інформації					
Критерії	Імовірність виявлення *(к1)*		Авторитет фірми виробника *(к2)*	Гарантія на працездатність *(к3)*		Оснащеність технічною документацією *(к4)*
Альтернативи	ТЗО1	ТЗО2	ТЗО3	ТЗО4	ТЗО5	ТЗО6

Складемо порівняльну матрицю для всіх альтернатив за обраними критеріями. Для заповнення матриці зрівняємо зазначені критерії між собою (табл. 3.6).

Таблиця 3.6

Матриця порівняння критеріїв

Критерії	(к1)	(к2)	(к3)	(к4)	Корисність	Вага критерію
(к1)	1	2	5	3	1,97	0,43
(к2)	0,5	1	3	4	1,43	0,31
(к3)	0,2	0,33	1	0,5	0,51	0,11
(к4)	0,33	0,25	2	1	0,7	0,15
Сума:	2,03	3,58	11	8,5	4,61	1

Для визначення ваги кожного елемента визначимо середнє геометричне рядків матриці:

$$a^1 = \sqrt[4]{a_{11} \cdot a_{12} \cdot a_{13} \cdot a_{14}} = \sqrt[4]{1 \cdot 2 \cdot 5 \cdot 3} = 1{,}97; \quad (3.15)$$

$$a^2 = \sqrt[4]{a_{21} \cdot a_{22} \cdot a_{23} \cdot a_{24}} = \sqrt[4]{0{,}5 \cdot 1 \cdot 3 \cdot 4} = 1{,}43; \quad (3.16)$$

$$a^3 = \sqrt[4]{a_{31} \cdot a_{32} \cdot a_{33} \cdot a_{34}} = \sqrt[4]{0{,}5 \cdot 0{,}33 \cdot 1 \cdot 0{,}5} = 1{,}51; \quad (3.17)$$

$$a^4 = \sqrt[4]{a_{41} \cdot a_{42} \cdot a_{43} \cdot a_{44}} = \sqrt[4]{0{,}33 \cdot 0{,}25 \cdot 2 \cdot 1} = 0{,}7 \quad (3.18)$$

Проведемо нормування отриманих значень:

$$a^1_н = \frac{a^1}{a_1 + a_2 + a_3 + a_4} = 0{,}43; \quad (3.19)$$

$$a_н^2 = \frac{a^2}{a_1 + a_2 + a_3 + a_4} = 0{,}31; \tag{3.20}$$

$$a_н^3 = \frac{a^3}{a_1 + a_2 + a_3 + a_4} = 0{,}11; \tag{3.21}$$

$$a_н^4 = \frac{a^4}{a_1 + a_2 + a_3 + a_4} = 0{,}15. \tag{3.22}$$

На наступному кроці за формулою (3.23) перевіримо рівень погодженості локальних пріоритетів:

$$K_{злаг}^{відн} = \left(I_{злаг} / I_{злаг}^{випад}\right) \cdot 100\%, \tag{3.23}$$

де $I_{злаг}^{випад}$ – індекс погодженості матриць, що згенеровані випадковим чином (табл. 3.7); $I_{злаг} = \left(\lambda_{\max} - N\right)/\left(N - 1\right)$ – індекс погодженості цих матриць;

$\lambda_{\max}$ – максимальне власне значення кожної з матриць парних порівнянь;

N – кількість порівнюваних елементів (розмірність матриць).

Таблиця 3.7

Середні погодженості для випадкових матриць різного порядку

Розмірність матриці	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$I_{злаг}^{вип}$	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,54	1,56	1.57	1,59

У даному випадку:

$$\lambda_{\max} = 0{,}87 + 1{,}11 + 1{,}21 + 1{,}28 = 4{,}47 \tag{3.24}$$

$$I_{злаг} = (4{,}47 - 4)/(4 - 1) = 0{,}16 \tag{3.25}$$

$$K_{злаг}^{відн} = \frac{0{,}16}{0{,}9} = 0{,}17 \tag{3.26}$$

При цьому слід враховувати, що від міри наближення $\lambda_{\max}$ до N залежить ступінь послідовності суджень експертів. Чим вони ближче один до одного, тим

результат роботи експертів є більш достовірним. Якщо коефіцієнт відносної погодженості локальних пріоритетів виходить за межі 10–20 %, то експертам потрібно переглянути свої судження та провести другий тур експертизи.

Наступним кроком має бути порівняння альтернатив за кожним із чотирьох критеріїв: імовірністю виявлення, авторитетом фірми виробника, гарантією на працездатність, оснащеністю технічною документацією. Результати порівняння альтернатив за цими критеріями подані у табл 3.8, табл. 3.9, табл. 3.10 та табл. 3.11.

Таблиця 3.8

Порівняння ТЗО за критерієм «Імовірність виявлення»

Альтернатива	Числове значення ймовірності виявлення	Нормоване значення
ТЗО1	0,93	0,168
ТЗО2	0,89	0,161
ТЗО3	0,95	0,172
ТЗО4	0,92	0,166
ТЗО5	0,89	0,161
ТЗО6	0,95	0,172
∑:	5,53	1

Таблиця 3.9

Порівняння ТЗО за критерієм «Авторитет фірми виробника»

Альтернативи	ТЗО1	ТЗО2	ТЗО3	ТЗО4	ТЗО5	ТЗО6	Корисність	Нормоване значення
ТЗО1	1	3	8	5	2	6	3,36	0,38
ТЗО2	0,33	1	5	2	0,25	4	1,22	0,14
ТЗО3	0,13	0,2	1	0,33	0,17	0,33	0,28	0,03
ТЗО4	0,25	0,5	3	1	0,2	1	0,63	0,07
ТЗО5	0,5	4	6	5	1	7	2,74	0,31
ТЗО6	0,17	0,25	3	1	0,14	1	0,51	0,06
∑:	2,33	8,95	26	14,33	3,76	19,33	8,74	1

Для визначення корисності кожного ТЗО визначимо середнє геометричне рядків матриць:

$$a^1 = \sqrt[6]{a_{11} \cdot a_{12} \cdot a_{13} \cdot a_{14} \cdot a_{15} \cdot a_{16}} = \sqrt[6]{1 \cdot 3 \cdot 8 \cdot 5 \cdot 2 \cdot 6} = 3{,}36; \quad (3.27)$$

$$a^2 = \sqrt[6]{a_{21} \cdot a_{22} \cdot a_{23} \cdot a_{24} \cdot a_{25} \cdot a_{26}} = \sqrt[6]{0{,}33 \cdot 1 \cdot 5 \cdot 2 \cdot 0{,}25 \cdot 4} = 1{,}22; \quad (3.28)$$

$$a^3 = \sqrt[6]{a_{31} \cdot a_{32} \cdot a_{33} \cdot a_{34} \cdot a_{35} \cdot a_{36}} = \sqrt[6]{0{,}13 \cdot 0{,}2 \cdot 1 \cdot 0{,}33 \cdot 0{,}17 \cdot 0{,}33} = 0{,}28; \quad (3.29)$$

$$a^4 = \sqrt[6]{a_{41} \cdot a_{42} \cdot a_{43} \cdot a_{44} \cdot a_{45} \cdot a_{46}} = \sqrt[6]{0{,}25 \cdot 0{,}5 \cdot 3 \cdot 1 \cdot 0{,}2 \cdot 1} = 0{,}63; \quad (3.30)$$

$$a^5 = \sqrt[6]{a_{51} \cdot a_{52} \cdot a_{53} \cdot a_{54} \cdot a_{55} \cdot a_{56}} = \sqrt[6]{0{,}5 \cdot 4 \cdot 6 \cdot 5 \cdot 1 \cdot 7} = 2{,}74; \quad (3.31)$$

$$a^6 = \sqrt[6]{a_{61} \cdot a_{62} \cdot a_{63} \cdot a_{64} \cdot a_{65} \cdot a_{66}} = \sqrt[6]{0{,}17 \cdot 0{,}25 \cdot 3 \cdot 1 \cdot 0{,}14 \cdot 1} = 0{,}51 \quad (3.32)$$

та проведемо нормування зазначених значень:

$$a^1_н(авт.ф.) = \frac{a^1}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}38; \quad (3.33)$$

$$a^2_н(авт.ф.) = \frac{a^2}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}14; \quad (3.34)$$

$$a^3_н(авт.ф.) = \frac{a^3}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}03; \quad (3.35)$$

$$a^4_н(авт.ф.) = \frac{a^4}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}07; \quad (3.36)$$

$$a^5_н(авт.ф.) = \frac{a^5}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}31; \quad (3.37)$$

$$a^6_н(авт.ф.) = \frac{a^6}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}06. \quad (3.38)$$

Максимальне власне значення матриці суджень при цьому дорівнюватиме:

$$\lambda_{\max} = 0{,}89 + 1{,}25 + 0{,}78 + 1 + 1{,}17 + 1{,}16 = 6{,}25. \quad (3.39)$$

Визначимо індекс погодженості та загальну погодженість матриці:

$$I_{злаг} = (6{,}25 - 6)/(6 - 1) = 0{,}05. \quad (3.40)$$

$$K^{відн}_{злаг} = \frac{0{,}05}{1{,}24} = 0{,}04. \quad (3.41)$$

Таблиця 3.10

Порівняння ТЗО за критерієм «Гарантія на працездатність»

Альтернатива	Строк гарантії (мес.)	Нормоване значення
ТСО1	24	0,17
ТСО2	12	0,09
ТСО3	24	0,17
ТСО4	36	0,26
ТСО5	18	0,14
ТСО6	24	0,17
Сума:	138	1

Таблиця 3.11

Порівняння ТЗО за критерієм «Оснащеність технічною документацією»

Альтернативи	ТЗО1	ТЗО2	ТЗО3	ТЗО4	ТЗО5	ТЗО6	Корисність	Нормоване значення
ТЗО1	1	3	7	5	2	7	3,37	0,39
ТЗО2	0,33	1	6	3	0,33	4	1,41	0,16
ТЗО3	0,14	0,17	1	0,33	0,2	0,5	0,3	0,04
ТЗО4	0,2	0,33	3	1	0,25	1	0,61	0,07
ТЗО5	0,5	3	5	4	1	6	2,38	0,28
ТЗО6	0,14	0,25	2	1	0,17	1	0,46	0,06
∑:	2,31	7,75	24	14,33	3,95	19,5	8,55	1

Для визначення корисності кожного ТЗО визначимо середнє геометричне рядків матриць:

$$a^1 = \sqrt[6]{a_{11} \cdot a_{12} \cdot a_{13} \cdot a_{14} \cdot a_{15} \cdot a_{16}} = \sqrt[6]{1 \cdot 3 \cdot 7 \cdot 5 \cdot 2 \cdot 7} = 3{,}37; \quad (3.42)$$

$$a^2 = \sqrt[6]{a_{21} \cdot a_{22} \cdot a_{23} \cdot a_{24} \cdot a_{25} \cdot a_{26}} = \sqrt[6]{0{,}33 \cdot 1 \cdot 6 \cdot 3 \cdot 0{,}33 \cdot 4} = 1{,}41; \quad (3.43)$$

$$a^3 = \sqrt[6]{a_{31} \cdot a_{32} \cdot a_{33} \cdot a_{34} \cdot a_{35} \cdot a_{36}} = \sqrt[6]{0{,}14 \cdot 0{,}17 \cdot 1 \cdot 0{,}33 \cdot 0{,}2 \cdot 0{,}5} = 0{,}3; \quad (3.44)$$

$$a^4 = \sqrt[6]{a_{41} \cdot a_{42} \cdot a_{43} \cdot a_{44} \cdot a_{45} \cdot a_{46}} = \sqrt[6]{0{,}2 \cdot 0{,}33 \cdot 3 \cdot 1 \cdot 0{,}25 \cdot 1} = 0{,}61; \quad (3.45)$$

$$a^5 = \sqrt[6]{a_{51} \cdot a_{52} \cdot a_{53} \cdot a_{54} \cdot a_{55} \cdot a_{56}} = \sqrt[6]{0{,}5 \cdot 3 \cdot 5 \cdot 4 \cdot 1 \cdot 6} = 2{,}38; \quad (3.46)$$

$$a^6 = \sqrt[6]{a_{61} \cdot a_{62} \cdot a_{63} \cdot a_{64} \cdot a_{65} \cdot a_{66}} = \sqrt[6]{0{,}14 \cdot 0{,}25 \cdot 2 \cdot 1 \cdot 0{,}17 \cdot 1} = 0{,}46 \quad (3.47)$$

та проведемо нормування зазначених значень:

$$a^1_н(тех.док.) = \frac{a^1}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}39; \quad (3.48)$$

$$a_н^2(тех.док.) = \frac{a^2}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}16; \quad (3.49)$$

$$a_н^3(тех.док.) = \frac{a^3}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}04; \quad (3.50)$$

$$a_н^4(тех.док.) = \frac{a^4}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}07; \quad (3.51)$$

$$a_н^5(тех.док.) = \frac{a^5}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}27; \quad (3.52)$$

$$a_н^6(тех.док.) = \frac{a^6}{a_1 + a_2 + a_3 + a_4 + a_5 + a_6} = 0{,}06. \quad (3.53)$$

Максимальне власне значення матриці суджень при цьому дорівнюватиме:

$$\lambda_{\max} = 0{,}9 + 1{,}24 + 0{,}96 + 1 + 1{,}11 + 1{,}17 = 6{,}38. \quad (3.54)$$

Визначимо індекс погодженості та загальну погодженість матриці:

$$I_{злаг} = (6{,}38 - 6)/(6 - 1) = 0{,}076. \qquad K_{злаг}^{відн} = \frac{0{,}076}{1{,}24} = 0{,}06. \quad (3.55)$$

Остаточні результати порівняння альтернатив заносяться в табл. 3.12.

Таблиця 3.12

Результати порівняння альтернатив за ступенем переваги

Вага критер / Альтернат	($к_1$) 0,42	($к_2$) 0,27	($к_3$) 0,11	($к_4$) 0,2	Корисність
ТЗО1	0,168	0,38	0,17	0,39	0,27
ТЗО2	0,161	0,14	0,09	0,16	0,15
ТЗО3	0,172	0,03	0,17	0,04	0,11
ТЗО4	0,166	0,07	0,26	0,07	0,13
ТЗО5	0,161	0,31	0,14	0,28	0,22
ТЗО6	0,172	0,06	0,17	0,06	0,12

$$ТЗО1 = 0{,}42 \cdot 0{,}168 + 0{,}27 \cdot 0{,}38 + 0{,}11 \cdot 0{,}17 + 0{,}2 \cdot 0{,}39 = 0{,}27; \quad (3.56)$$

$$ТЗО2 = 0{,}42 \cdot 0{,}161 + 0{,}27 \cdot 0{,}14 + 0{,}11 \cdot 0{,}09 + 0{,}2 \cdot 0{,}16 = 0{,}15; \quad (3.57)$$

$$ТЗО3 = 0{,}42 \cdot 0{,}172 + 0{,}27 \cdot 0{,}03 + 0{,}11 \cdot 0{,}17 + 0{,}2 \cdot 0{,}04 = 0{,}11; \quad (3.58)$$

$$ТЗО4 = 0,42 \cdot 0,166 + 0,27 \cdot 0,07 + 0,11 \cdot 0,26 + 0,2 \cdot 0,07 = 0,13; \quad (3.59)$$

$$ТЗО5 = 0,42 \cdot 0,161 + 0,27 \cdot 0,31 + 0,11 \cdot 0,14 + 0,2 \cdot 0,28 = 0,22; \quad (3.60)$$

$$ТЗО6 = 0,42 \cdot 0,172 + 0,27 \cdot 0,06 + 0,11 \cdot 0,17 + 0,2 \cdot 0,06 = 0,12. \quad (3.61)$$

У процесі прийняття рішень на вибір найоптимальнішого ТЗО для системи фізичного захисту інформації із шести альтернатив, виявлено, що кращим є ТЗО1, якому притаманний найбільший коефіцієнт корисності. Це означає, що саме воно буде обрано при побудові бар'єра СФЗІ (див. рис. 3.11).

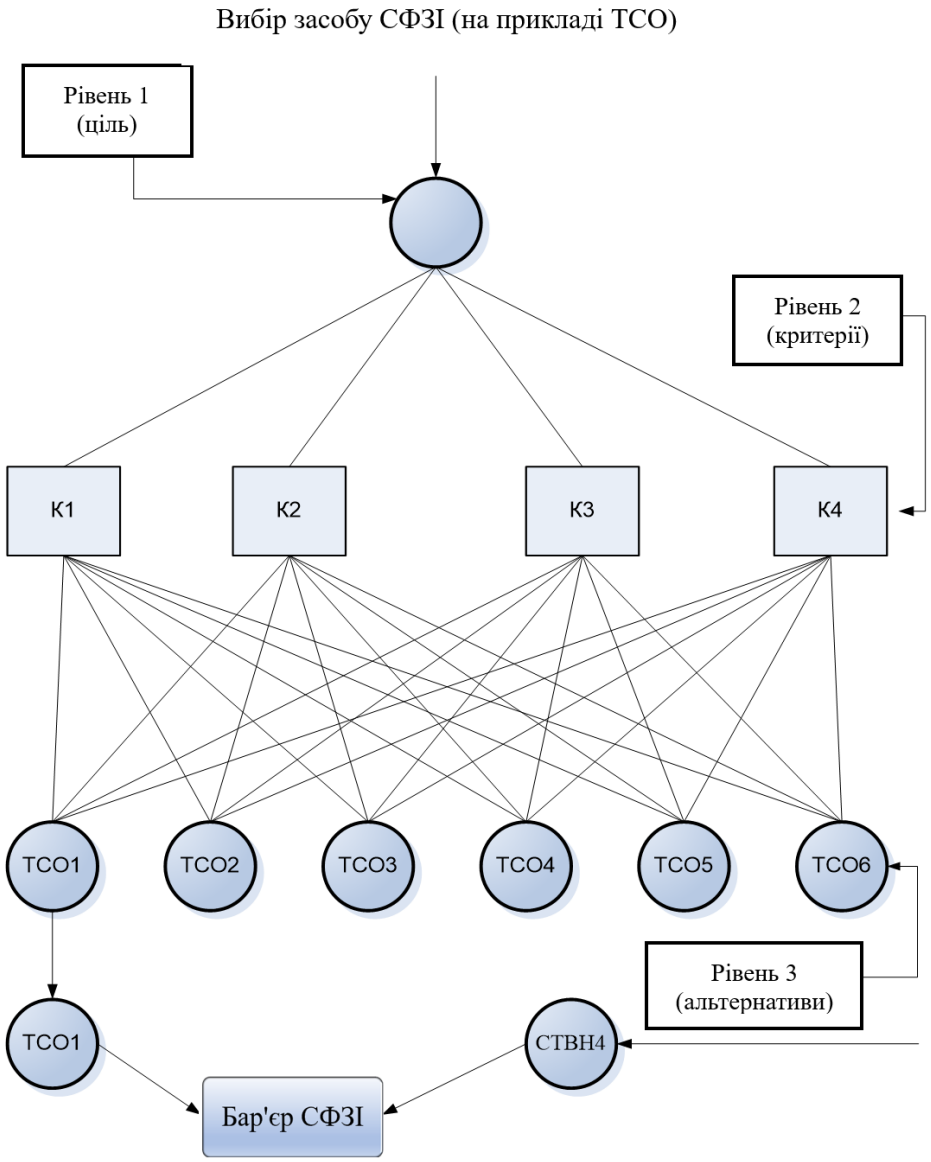

Рис. 3.11. Визначення механізму захисту при побудові СФЗІ

У розглянутому випадку не врахований ціновий критерій, тому доцільно провести аналіз альтернатив за критерієм «ефективність-вартість». Використовуючи відношення отриманої інтегральної оцінки до нормованої вартості засобу, найкращим також є ТЗО1, для якого зазначене відношення максимально (див. табл. 3.13).

Таблиця 3.13

Відношення « ефективність-вартість» для засобів СФЗІ

	Вартість, грн	Вартість нормована	Корисність	Відношення
ТЗО1	3000	0,18	0,27	1,5
ТЗО2	2900	0,17	0,15	0,88
ТЗО3	2600	0,155	0,11	0,7
ТЗО4	2800	0,175	0,13	0,74
ТЗО5	3100	0,18	0,22	1,2
ТЗО6	2400	0,11	0,12	0,86
∑:	16800	1	1	

У такий спосіб, згідно з отриманими результатами, особа яка уповноважена приймати рішення (ОПР) для побудови бар'єра фізичного захисту інформації в ІКС підприємства свою увагу має зосередити на альтернативі ТЗО1, яка за ступенем захищеності задовольняє необхідному для об'єкта показника. Якщо вимоги не відповідають заданим, проводиться повторна процедура вибору засобів для побудови бар'єра захисту.

3.5. Розробка методу оцінювання ступеня порушення СФЗІ в ІКС за метою реалізації

Згідно з нормативними документами ТЗІ України (НД ТЗІ 1.1-002-99 та НД ТЗІ 2.5-004-99) загрози для ІКС полягають у порушенні:

– конфіденційності інформації (властивість інформації бути відомою в плані читання або копіювання тільки допущеним або інакше авторизованим суб'єктам ІКС – користувачам, програмам, процесам);

– цілісності інформації (властивість інформації бути незмінною в семантичному змісті, що досягається сукупністю заходів щодо її захисту від збоїв, видалення і несанкціонованого доступу до неї);

– доступності до інформації (властивість інформації бути захищеною від несанкціонованого блокування, часткової або повної втрати працездатності системи).

При цьому до загроз порушення конфіденційності інформації у ІКС згідно з відносимо спроби:

– несанкціонованого перехоплення електронних і акустичних випромінювань;

– примусового електромагнітного опромінення (підсвічування) ліній зв'язку;

– несанкціонованого застосування закладених пристроїв і програмних закладок;

– відновлення тексту принтера та дистанційного фотографування;

– розкрадання носіїв інформації й документальних відходів;

– читання або копіювання як відкритої, так і конфіденційної інформації, імпорту або експорту такої інформації, а також обміну нею між елементами обчислювальної мережі, що належить до різних класів захищеності;

– копіювання носіїв інформації з подоланням засобів захисту;

– маскування під зареєстрованого користувача або під запити системи;

– використання недоліків мов програмування й операційних систем;

– незаконне підключення до апаратури і ліній зв'язку;

– виведення з ладу механізмів захисту;

– впровадження і використання комп'ютерних вірусів тощо.

З урахуванням положень, вони ймовірно можуть бути реалізовані порушником за умови подолання ним засобів:

1) організаційного обмеження доступу (p_{ood});

2) охоронної сигналізації (p_{oc});

3) захисту від вірусних атак ($p_{атак}$);

4) канального захисту від несанкціонованого доступу із телекомунікаційної мережі до ресурсів ЛОМ ($p_{кзткм}$);

5) управління доступу, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо ($p_{уфд}$);

6) адміністрування доступу до відповідних суб'єктів і об'єктів з використанням механізмів загального і спеціального ПЗ ($p_{ад}$).

Виходячи з такого ймовірність подолання неавторизованим користувачем зазначених засобів захисту може бути визначена з виразу:

$$p_{пзз} = p_{уфд} \cdot p_{ад} \cdot \left[1 - (1 - p_{ооД}) \cdot (1 - p_{ос}) \cdot (1 - p_{атак}) \cdot (1 - p_{кзктм})\right]. \quad (3.62)$$

Подальше розкриття змісту інформації з обмеженим доступом може статися лише за умови, якщо порушник після її отримання:

а) знає мову, якою інформація представляється (ймовірність події – $p_{мова}$);

б) знає і може застосовувати програмні засоби або апаратуру криптографічного перетворення (ймовірність події – $p_{пз/ктп}$);

в) має необхідні ключі або ключові набори для такого перетворення (ймовірність події – $p_{ключі}$).

Виходячи з такого ймовірність подолання неавторизованим користувачем засобів криптографічного захисту може бути визначена з виразу:

$$p_{кзі} = p_{мова} \cdot p_{пз/ктп} \cdot p_{ключі}. \quad (3.63)$$

Тоді ймовірність порушення конфіденційності інформації з подоланням розглянутих вище засобів може бути визначена як:

$$P_{ПКІ} = p_{кзі} \cdot \left[1 - (1 - p_{пзз})\right]. \quad (3.64)$$

До загроз порушення цілісності інформації згідно з відносимо:

– несанкціоновану модифікацію та/або видалення програм і даних;

– вставку, зміну або видалення даних в елементах протоколу в процесі обміну між абонентами обчислювальної мережі;

– втрату даних у результаті збоїв, порушення працездатності елементів обчислювальної мережі або некомпетентних дій суб'єктів доступу тощо.

Вони можуть бути реалізовані порушником за умови подолання засобів:

1) організаційного обмеження доступу, охоронної сигналізації та управління доступом, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо та адміністрування доступу, як й при аналізі

2) загроз конфіденційності інформації (ймовірність такої події – $p_{пзз}$ визначена раніше);

3) захисту цілісності від загроз у телекомунікаційних мережах ($p_{цткм}$);

4) захисту від спеціальних впливів на інформацію по ТКМ ($p_{сп.вп}$);

5) контролю та поновлення цілісності інформації ($p_{конт.ц}$).

З урахуванням можливостей попереднього підходу, ймовірність порушення цілісності $P_{ПЦІ}$ може бути знайдена з виразу:

$$P_{ПЦІ} = p_{конт.ц} \cdot \left[1-(1-p_{пзз})\cdot(1-p_{сп.вп})\cdot(1-p_{цткм})\right]. \quad (3.65)$$

До загроз порушення доступності інформації відносимо:

– повторення або вповільнення елементів протоколу;

– придушення обміну в телекомунікаційних мережах;

– використання помилок або недокументованих можливостей служб і протоколів передачі даних для ініціювання відмови в обслуговуванні;

– перевитрата обчислювальних або телекомунікаційних ресурсів тощо.

Вони, як і в попередніх випадках, можуть бути реалізовані за умови подолання неавторизованим користувачем систем управління доступом до ІР ЛОМ (ідентифікації, аутентифікації, надання певних повноважень чи привілеїв, з наступною їх перевіркою під час кожної із спроб доступу до ресурсів) та фільтрації. Виходячи з такого стійкість системи управління доступом – (в розумінні ймовірності її не подолання) визначається стійкістю процесів ідентифікації та аутентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями:

$$p_{ссуд} = 1 - p_{пзз}. \quad (3.66)$$

Ця задача може вирішуватися застосуванням у ІКС засобів фільтрації типу міжмережевих екранів (firewall, брандмауерів), сервісів-посередників (proxyservices) тощо. При середній тривалості обслуговування в ІКС одного запиту і пуассонівському законі розподілу ймовірностей впливу, ймовірність того, що під час звернення до ресурсу він уже використовується, дорівнює:

$$p_{вик.рес} = 1 - p_0 = 1 - \exp\{- t_{вик.рес} \cdot \lambda_{зап}\}, \quad (3.67)$$

де p_0 – ймовірність відсутності впливів (ймовірність того, що на певному часовому інтервалі виникне рівно нуль впливів); $t_{вик.рес}$ – середнє значення часу використання ресурсу.

Враховуючи таке, ймовірність порушення доступності ресурсу дорівнюватиме:

$$P_{ПДІ} = 1 - (1 - p_{вик.рес}) \cdot (1 - p_{ссуд}). \quad (3.68)$$

Виходячи з наведених вище формульних залежностей комплексна величина ймовірності порушення системи фізичного захисту інформації в ІКС та їх специфічному класі – ЛОМ може бути, як результат, знайдена з виразу:

$$P_{ПСЗІ} = 1 - (1 - P_{ПКІ}) \cdot (1 - P_{ПЦІ}) \cdot (1 - P_{ПДІ}). \quad (3.69)$$

Висновки до третього розділу

З погляду системного аналізу, СФЗІ являє собою модель системи, яка поєднує сили й засоби об’єкта захисту, що забезпечують захист циркулюючої в ньому інформації або інших цінних ресурсів. Метою створення СФЗІ є рішення проблемної ситуації, пов’язаної із захистом ресурсів організації. Проблемна ситуація (завдання ухвалення рішення) може бути розв’язаною лише за наявності альтернатив (різних способів досягнення мети) та існування певних факторів, що обмежують можливості досягнення мети (у першу чергу – фінансові).

Як результат, з урахуванням моделей загроз і моделі порушника, а також моделі фізичного захисту інформації з повним перекриттям у роботі розроблена методика вибору складу засобів системи фізичного захисту інформації та метод оцінювання ступеня порушення СФЗІ в ІКС за метою реалізації. Їх реалізація дозволить підрозділам інформаційної безпеки з огляду на специфіку певних установ (відомств) та підприємств робити порівняльний аналіз технічних засобів і пропозицій по укомплектуванню СФЗІ об’єкта захисту та обирати серед них зразки, раціональні з точки зору забезпечення захисту інформації або інших цінних ресурсів від впливу внутрішніх і зовнішніх загроз.

Інтерпретація отриманих результатів математично підтверджує, що в реальності розроблений науково-методичний апарат працює правильно й може видавати достовірні результати. Використовуючи запропонований підхід можна забезпечити необхідний рівень захисту з урахуванням економічності безпеки.

ВИСНОВКИ

1. В умовах воєнного стану в Україні постає питання щодо забезпечення безпеки держаних і комерційних промислових об’єктів здобувають останнім часом особливу актуальність. Такий стан справ пояснюється передусім діями певних фізичних осіб (порушників) – терористів, злочинців, несумлінних конкурентів тощо, які створюють небезпеку перш за все для інформаційного ресурсу установ (відомств), що циркулює та обробляється у відповідних ІКС.

2. Одним із ефективних заходів щодо забезпечення захисту будь-яких об’єктів від розкрадання майна й фінансової документації, проявів надзвичайних ситуацій (пожежі, руйнування, затоплення, аварій тощо) та втрати інформаційного ресурсу є створення високо ефективної СФЗІ з повною автоматизацією виконуваних неї завдань і функцій, яка може бути спрямованою на:

– суб’єкт загрози з метою його фізичної нейтралізації;

– об’єкт охорони з метою підвищення його резистивних властивостей протистояти загрозливим впливам;

– фізичне середовище, що розділяє суб’єкт загрози й об’єкт охорони, з метою затримки і послаблення загрозливих впливів.

3. Інформація як об’єкт безпеки індиферентна до загроз, небезпек і ризиків. Захищати необхідно не інформацію, а суб’єктів інформаційних відносин від заподіяння їм шкоди за допомогою певних дій з інформацією.

4. Одні й ті самі дії з інформацією (збір, модифікація, знищення, витік, НСД тощо) в одних випадках можуть містити загрозу й у випадку її реалізації приносити шкоду, в інші – не є загрозою й здатні приносити користь.

5. Загрози суб’єктам інформаційних відносин – виробникові, власникові, споживачеві інформації, третім особам, – відрізняються одна від одної так само, як і методи й засоби протидії їм.

6. Сама небезпечна загроза інформації – перекручування, а самі небезпечні джерела загроз – ті, що створюють (виробляють) і розпоряджаються інформацією. Саме вони мають максимальні можливості (вільно або мимоволі) спотворити інформацію.

7. На сьогодні, вітчизняний ринок засобів (комплексів) технічного (ТЗІ) та криптографічного захисту інформації (КЗІ) наповнений досить широким спектром продукції, що дає можливість створювати СФЗІ інформаційних та телекомунікаційних систем різного призначення.

8. Рішення щодо доцільності використання конкретних засобів ТЗІ чи КЗІ необхідно приймати за наявності змістовної характеристики інформаційної, телекомунікаційної чи автоматизованої системи в якій необхідно забезпечити захист ІзОД або інформації, яка є власністю держави. Це, як правило, визначається:

– вищим грифом секретності інформації, що обробляється в системі;

– класом автоматизованої системи;

– переліком функціональних послуг (сервісів) які надаються користувачам інформаційної, телекомунікаційної чи автоматизованої системи;

– вимогами, щодо рівня захисту інформації, що обробляється (наприклад, перелік та рівень функціональних послуг захисту інформації);

– прийнятою політикою безпеки інформації;

– характеристикою користувачів та обслуговуючого персоналу системи;

– конкретними умовами експлуатації інформаційної, телекомунікаційної чи автоматизованої системи тощо.

9. Порядок створення та введення в експлуатацію СФЗІ інформаційних та телекомунікаційних систем визначений вітчизняною системою нормативних документів в галузі ТЗІ і є обов’язковим до виконання всіма суб’єктами господарювання.

В основу створення СФЗІ в ІКС покладено принцип так званої «превентивності» який означає, що чим раніше буде виявлене вторгнення,

оцінені його масштаб і з високим ступенем ймовірності буде відбита загроза, тим ефективнішою буде сама СФЗІ. Це потребує комплексного наукового підходу перш за все до проєктування інтегрованої системи, а також кількісного оцінювання уразливості її складових та ефективності СФЗІ в цілому.

10. Одним з найважливіших етапів при проєктуванні СФЗІ є здійснення оптимального вибору засобів для комплектування перспективної системи, при певних експлуатаційних і технічних обмеженнях. Зважаючи на те, що на цей час єдиної системної методики концептуального проєктування СФЗІ й зокрема методики вибору засобів СФЗІ не існує у роботі були проаналізовані фізичні загрози інформаційної безпеки в ІКС та підтверджено необхідність здійснення їхньої локалізації.

11. На основі цих даних побудована узагальнена модель СФЗІ та модель системи з повним перекриттям, що надає можливість урахувати весь спектр загроз відносно об’єктів захисту й протиставити кожній загрозі відповідний засіб фізичного захисту. Використання запропонованого підходу дозволить порівнювати різні засоби захисту й вибрати серед них більш раціональні з точки зору забезпечення необхідного рівня захисту.

Практична значущість кваліфікаційної роботи полягає в тім, що її матеріали і результати можуть бути використані при проєктуванні СФЗІ та вибору засобів для її комплектування.

Бурхливий розвиток сучасних технологій і технічних засобів сприяє постійному розширенню спектра можливих каналів витоку інформації, тому їх дослідження стає все більше актуальним, і складним завданням.

На ефективність систем безпеки істотно впливають характеристики реальних каналів витоку, тому створення ефективних систем захисту інформації має відбуватися з урахуванням їх особливостей. Цей висновок не є тривіальним, як може здатися, на перший погляд. Наприклад, сам факт наявності випромінювання дисплея ще не говорить про витік інформації. Усе визначається конкретним рівнем напруженості поля за межами зони безпеки й технічних можливостей противника, тому остаточний висновок про витік інформації може

зробити тільки кваліфікований фахівець, що використовує спеціальні технічні засоби. З іншого боку, особливості реальних каналів витоку інформації можуть бути успішно використані й противником для забезпечення НСД до інформації, про що необхідно постійно пам’ятати. Так, знімання інформації з акустичних каналів може бути здійснено через скло вікон, будівельні, сантехнічні, вентиляційні, теплотехнічні й газорозподільні конструкції, з використанням для передачі сигналів радіо, радіотрансляційних, телефонних і комп’ютерних комунікацій, антенних, і телевізійних розподільних мереж, охоронно-пожежної й тривожної сигналізації, мереж електроживлення й часофікації, гучномовного й диспетчерського зв’язку, ланцюгів заземлення й т.п. Випадковий пропуск хоча б одного можливого каналу витоку може практично нанівець звести всі витрати й зробити систему захисту неефективною.

Таким чином основна мета СФЗІ, незалежно від ступеня структурної складності й технічної оснащеності ІКС, може бути поділена на такі підцілі:

– своєчасне виявлення джерел загроз, тобто запобігання НСД на територію об’єкта й у його життєво важливі зони;

– затримка джерел загроз на час, що в ідеальному випадку перевищує час нейтралізації загрози;

– своєчасне надання протидії виявленому джерелу загроз (припинення загрози);

– нейтралізація наслідків загрози, тобто мінімізація збитку від реалізації або спроби реалізації загрози.

За повної невизначеності щодо вхідних даних вона може бути досягнута за рахунок застосування вивіреного підходу до проєктування системи фізичного захисту та обґрунтованого вибору засобів, раціональних з точки зору комплектування спроєктованої системи, а також за умови дотримання двох суперечливих вимог – мінімізації сумарних витрат на створення СФЗІ та максимізації захищеності організації або її ресурсів від впливу внутрішніх і зовнішніх загроз.

З погляду системного аналізу, СФЗІ являє собою модель системи, яка поєднує сили й засоби об’єкта захисту, що забезпечують захист циркулюючої в ньому інформації або інших цінних ресурсів. Метою створення СФЗІ є рішення проблемної ситуації, пов’язаної із захистом ресурсів організації. Проблемна ситуація (завдання ухвалення рішення) може бути розв’язаною лише за наявності альтернатив (різних способів досягнення мети) та існування певних факторів, що обмежують можливості досягнення мети (у першу чергу – фінансові).

Як результат, з урахуванням моделей загроз і моделі порушника, а також моделі фізичного захисту інформації з повним перекриттям у роботі розроблена методика вибору складу засобів системи фізичного захисту інформації та метод оцінювання ступеня порушення СФЗІ в ІКС за метою реалізації. Їх реалізація дозволить підрозділам інформаційної безпеки з огляду на специфіку певних установ (відомств) та підприємств робити порівняльний аналіз технічних засобів і пропозицій по укомплектуванню СФЗІ об’єкта захисту та обирати серед них зразки, раціональні з точки зору забезпечення захисту інформації або інших цінних ресурсів від впливу внутрішніх і зовнішніх загроз.

Інтерпретація отриманих результатів математично підтверджує, що в реальності розроблений науково-методичний апарат працює правильно й може видавати достовірні результати. Використовуючи запропонований підхід можна забезпечити необхідний рівень захисту з урахуванням економічності безпеки.

Для роботи на тему «Методи фізичного захисту інформації в інформаційно-комунікаційних системах» можна зробити наступні висновки:

1. Значущість фізичного захисту. Фізичний захист є першою лінією оборони в інформаційно-комунікаційних системах (ІКС), після чого він захищає обладнання та дані від фізичних загроз, таких як крадіжка, вандалізм чи природні катастрофи. Ефективний фізичний захист дозволяє зменшити ризик несанкціонованого доступу до інформації.

2. Різноманіття методів захисту. До методів фізичного захисту належать механічні засоби (замки, сейфи, захисні двері), електронні системи (відеонагляд,

сигналізація, контроль доступу) та організаційні заходи (охорона периметра, ідентифікація персоналу). Комбінація цих методів має високий рівень безпеки.

3. Роль технологій у підвищенні рівня захисту. Сучасні технології, такі як біометричні системи доступу, інтелектуальні датчики руху, та аналітика відеоспостереження, дозволяють більш ефективно контролювати доступ і виявляти популярні загрози. Ці системи інтегровані з програмним забезпеченням для централізованого моніторингу та управління безпекою.

4. Протидія внутрішнім загрозам. Фізичні методи захисту допомагають боротися не лише із зовнішніми, але й із внутрішніми загрозами, адже персонал також може становити ризик. Контроль доступу, використання ідентифікаційних карток та моніторинг дозволяє відстежувати дії співробітників та обмежувати їх доступ лише до потрібних об’єктів.

5. Важливість постійного вдосконалення системи захисту. Загрози в ІКС постійно еволюціонують, що вимагають регулярного оновлення засобів захисту. Періодичне оцінювання ризиків та модернізація захисних систем дозволить забезпечити високий рівень безпеки.

6. Зниження фінансових втрат. Інвестиції у фізичні методи захисту дозволяють уникнути великих фінансових втрат у випадках витоку або знищення конфіденційної інформації, що може відбутися внаслідок фізичного доступу зловмисників до даних або пошкодження обладнання.

Таким чином, фізичний захист є фундаментальним елементом безпеки інформації в ІКС, забезпечуючи захист не тільки від зовнішніх атак, але й від внутрішніх загроз, що дозволяє зберегти цілеспрямованість і конфіденційність інформації.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.09.2024).

2. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних : Указ Президента України від 24.09.2001 № 891/2001. URL: https://zakon.rada.gov.ua/laws/show/891/2001#Text (дата звернення: 10.09.2024).

3. Про затвердження Концепції технічного захисту інформації в Україні : Постанова Каб. Міністрів України від 08.10.1997 № 1126 : станом на 13 жовт. 2011 р. URL: https://zakon.rada.gov.ua/laws/show/1126-97-п#Text (дата звернення: 16.09.2024).

4. ТР ЕОТ – 95. Тимчасові рекомендації з технічного захисту інформації в засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок.

5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

7. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

8. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення

9. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроєктні роботи.

10. НД ТЗІ 3.3-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації

11. НД ТЗІ 2.1-002-07. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення

12. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Затверджено наказом ДСТСЗІ СБУ від 24 грудня 2001 року, № 76.

13. Алаухов С.Ф, Коцеруба В.Я. Вопросы создания систем физической защиты для крупных промышленных объектов // Системы безопасности, 2001, № 41, С. 93.

14. Богуш В.М., Юдін О.К. Інформаційна безпека держави. – К.: "МК-Прес", 2005. – 432 с.

15. Бурячок В.Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем // Захист інформації. – 2011. – № 3(52). – С. 19–27.

16. Василенко Д.П., Маслак В.І. Законодавство провідних країн світу в сфері захисту інформації. // Вісник КДУ імені Михайла Остроградського. Випуск 2/2010 (61). Частина 1. – С. 128-132

17. Василенко В.С. Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах. / В.С. Василенко, О.С. Бордюк, С.М. Полянський. URL: http://www.rusnauka.com/11_EISN_2010/ Informatica/64068.doc.htm. (дата звернення: 17.10.2024).

18. Василюк Володимир. Об'єкти захисту інформації. Методи та засоби захисту інформації. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (13), 2006 р. – С. 88-102

19. Галатенко В.А. Основы информационной безопасности. – М.: Университет информационных технологий, 2004. – 328 с.

20. Гарсиа М. Проектирование и оценка систем физической защиты. Пер. с англ. – М.: Мир: «ООО Издательство АСТ», 2002, - 386 с.

21. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.:Кн.1.-М.:Энергоатомиздат, 1994.-400 с.

22. Герасимов Б.М., Домарев В.В. Вибір оптимального варіанту системи захисту інформації на основі застосування методів нечіткої багатокритеріальної оптимізації//Захист інформації. №3.2002.-К.С.24-28.

23. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: ДиаСофт, 1999. – 480 с.

24. Дорошенко Д.В. Защита информации от утечки по техническим каналам. // Техника радиосвязи. Випуск 12, 2007 р. – С. 127-132

25. Измайлов А.В. Методы системного проектирования комплексов технических средств физической защиты российских ядерных объектов // Российско-американский семинар по физической защите ядерных материалов и установок, ГП СНПО "Элерон", М., Россия. 1995.

26. Котенко И.В., Степашкин М.В., Богданов В.С. Анализ защищённости компьютерных систем на различных этапах их жизненного цикла. // Изв. вузов. Приборостроение, 2006. – Т. 49, №5 – С. 3–8.

27. Мишин Е.Т., Оленин Ю.А.,Капитонов А.А. Системы безопасности предприятия - новые акценты. // Конверсия в машиностроении, 1998, № 4.

28. Оленин Ю.А., Алаухов С.Ф. К вопросу категорирования объектов с позиции охранной безопасности // Системы безопасности, связи и телекоммуникаций, 1999, № 30. – С. 26.

29. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. “АйТи”; ДМК Пресс, 2004. – 384 с.

30. Торокин А.А. Основы инженерно-технической защиты информации. М.: Ось-89, 1998. – 334 с.