**Ю.В. Баланюк, В.В. Козловський, Ю.М. Лисецький, Б.В. Моркляник,
В.О. Хорошко, Ю.Є. Хохлачова, М.Є. Шелест**

КІБЕРБЕЗПЕКА

Міністерство освіти і науки України
Національний авіаційний університет

Ю.В. Баланюк, В.В. Козловський, Ю.М. Лисецький, Б.В. Моркляник,
В.О. Хорошко, Ю.Є. Хохлачова, М.Є. Шелест

КІБЕРБЕЗПЕКА

підручник

За редакцією професорів В.В. Козловського та В.О. Хорошка

Київ – 2024

УДК 004.056.53 (075.8)

Рекомендовано Вченою радою Національного авіаційного університету (протокол №2/22 від 06.05.2024р.)

Рецензенти:
доктор технічних наук, професор Дудикевич В.Б.
доктор технічних наук, професор Євсеєв С.П.
доктор технічних наук, професор Лаптєв О.А.

Хорошко В.О.
Кібербезпека: підручник / Ю.В. Баланюк, В.В. Козловський, Ю.М. Лисецький, Б.В. Моркляник, В.О. Хорошко, Ю.Є. Хохлачова, М.Є. Шелест / За ред. проф. В.В. Козловського та В.О. Хорошка – Київ : ЛАТ&К, 2024. 609 с

ISBN

В підручнику розглядається комплекс проблем, які виникають під час застосування систем кібернетичного захисту інформації в інформаційних системах. У видання здійснено огляд загальних підходів до застосування систем кіберзахисту інформації, розглянуті структури інформаційниого процесу, канали несанкціонованного отримання інформації та загрози їй, основи моделювання процесу кіберзахисту та моделювання інформаційних процесів в системі кіберзахисту. Запропоновані методи керування доступом до інформації та керування кібербезппекою інформаційних технологій.

Видання призначено для студентів вищих навчальних закладів, а також аспірантів, підготовка яких здійснюється за напрямом кібербезпека. Він також буде корисним фахівцям, які працюють в галузі кібербезпеки.

УДК
ISBN

© Ю.В. Баланюк, В.В. Козловський,
© Ю.М. Лисецький, Б.В. Моркляник,
© В.О. Хорошко, Ю.Є. Хохлачова,
© М.Є. Шелест

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ
ВСТУП
РОЗДІЛ 1. ОСНОВНІ ПОНЯТТЯ КІБЕРЗАХИСТУ
Запитання для самокнтролю
РОЗДІЛ 2. ЗВ'ЯЗОК ІНФОРМАЦІЇ З ДІЯЛЬНІСТЮ СУСПІЛЬСТВА
2.1. Види інформації
2.2. Інформація для ухвалення рішень
2.2.1. Інформація для стратегічних рішень
2.2.2. Інформація для тактичних рішень
2.2.3. Інформація для вирішення оперативних питань
2.3. Збір та обробка інформації
2.3.1. Шлях інформації
2.3.2. Канали інформації
2.3.3. Обробка інформації
2.3.4. Цикл інформації
2.3.5. Помилкова інформація
2.3.6. Витік інформації
Запитання для самоконтролю
РОЗДІЛ 3. СТРУКТУРИ ІНФОРМАЦІЙНИОГО ПРОЦЕСУ
3.1. Параметри інформаційного процесу
3.2. Варіаційна матриця інформаційного процесу
3.3. Граф інформаційного процесу та його особливості
3.4. Паралельні форми інформаційного процесу
3.5. Введення у функціональне дослідження інформаційного процесу
Запитання для самокнтролю
РОЗДІЛ 4. НЕОБХІДНІСТЬ КІБЕРЗАХИСТУ
4.1. Класифікація цілей кіберзахисту
4.2. Основні положення концепції кіберзахисту
4.3. Визначення та аналіз поняття кіберзахист інформації
Запитання для самокнтролю
РОЗДІЛ 5. ЗАГАЛЬНІ ПИТАННЯ КІБЕРЗАХИСТУ
5.1. Задачі кіберзахисту
5.2. Вимоги до системи кіберзахисту інформації
5.3. Підходи до створення систем кіберзахисту інформації

5.4. Оцінка захищеності інформації
Запитання для самоконтролю
РОЗДІЛ 6. НАЙПОШИРЕНІШІ ЗАГРОЗИ ІНФОРМАЦІЇ
6.1. Основні означення та критерії загроз
6.2. Найпоширеніші загрози доступності
6.3. Шкідливе програмне забезпечення
6.4. Основні загрози цілісності
6.5. Основні загрози конфіденційності
Запитання для самоконтролю
РОЗДІЛ 7. КАНАЛИ НЕСАНКЦІОНОВАНОГО ОТРИМАННЯ ІНФОРМАЦІЇ
7.1. Структура і загальний зміст алгоритму формування відносно можливостей експертних методів
7.2. Принципи порушення цілісності інформації
7.3. Канали несанкціонованого доступу до інформації
7.4. Методи визначення значень показників уразливості інформації
Запитання для самоконтролю
РОЗДІЛ 8. КЛЕПТОГРАФІЯ ТА ПРИХОВАНІ КАНАЛИ У КІБЕРБЕЗПЕЦІ
8.1. Клептографія
8.2. Приховані канали
8.2.1. Теорія прихованих каналів
8.2.2. Характеристики прихованих каналів
8.2.3. Сучасний погляд на приховані канали
8.2.4. Потайні та побічні канали
8.2.5. Приховані канали у системі обробки інформації
Запитання для самоконтролю
РОЗДІЛ 9. АТАКИ ЗА ПОБІЧНИМИ КАНАЛАМИ
9.1. Класифікація побічних каналів
9.1.1. Спосіб доступу до системи
9.1.2. Контроль над обчислювальним процесом
9.1.3. Застасовані методи аналізу
9.2. Атаки за часом виконання операцій
9.2.1. Причина вразливості в алгоритмі зведення у ступінь
9.2.2. Алгоритм проведення атаки
9.2.3. Як алгаритм атаки працює
9.2.4. Приклад моделювання атаки за часом на комп’ютері
9.2.5. Передумови реалізації за часом та її складність
9.2.6. «Сліпий» захист від атаки за часом
9.3. Напівагресивні атаки
9.3.1. Приклади атак без посереднього вичитування даних з пам’яті
9.3.2. Технології захисту від напівагресивних атак
9.4. Віддалені атаки

9.4.1. Приклади атак на криптографічні API
9.4.2. Приклади атак на захищені API
Запитання для самоконтролю
РОЗДІЛ 10. КОНЦЕПЦІЯ ТА МОДЕЛІ КІБЕРБЕЗПЕКИ
10.1. Концепція керування кібербезпекою інформаційних технологій
10.2. Елементи кібербезпеки
10.3. Процес керування кібербезпекою інформаційних технологій
10.4. Моделі керування кібернетичною безпекою інформації
10.5. Архітектура систем кібернетичної безпеки інформації
Запитання для самоконтролю
РОЗДІЛ 11. АНАЛІЗ РИЗИКІВ У КІБЕРБЕЗПЕЦІ
11.1. Аналіз аспектів організації
11.2. Оцінювання активів організації
11.3. Побудова моделей загроз
11.4. Побудова моделей порушників
11.5. Аналіз функціонування інформаціної системи
11.6. Підходи до аналізу ризиків
11.7. Методи оцінки ризиків
Запитання для самоконтролю
РОЗДІЛ 12. ОСНОВИ МОДЕЛЮВАННЯ ПРОЦЕСУ КІБЕРЗАХИСТУ
12.1. Методи моделювання систем кіберзахисту
12.2. Аналіз моделей кіберзахисту
12.2.1. Класифікація моделей кіберзахисту
12.2.2. Побудова моделей кіберзахисту інформації
12.3. Аналіз захищеності систем кіберзахистуінформації з повним перекриттям загроз
12.3.1. Визначення математичної моделі конфлікту загроз з комплексною системою кіберзахисту інформації
12.3.2. Проектне моделювання конфлікту загроз з комплексною системою кіберзахисту інформації
12.4. Визначення показників якості захищеності моделі кіберзахисту інформації
Запитання для самоконтролю
РОЗДІЛ 13. МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ В СИСТЕМІ КІБЕРЗАХИСТУ
13.1. Розробка формальних моделей інформаційних відносин в системах кіберзахисту
13.1.1. Модель процесів в системі кіберзахисту інформації, яка заснована на знаковій чутливості
13.1.2. Модель захищеної інформаційно-технологічної системи, яка заснована на принципах функціонування нервової системи людини

13.2. Формалізація взаємовідносин порушника і системи кіберзахисту інформації
13.2.1. Формалізація дій порушника під час впливу на системи кіберзахисту
13.2.2. Метод оцінки стійкості системи кіберзахисту іфнормації при спливі порушника
Запитання для самоконтролю
РОЗДІЛ 14. КЕРУВАННЯ ДОСТУПОМ ДО ІНФОРМАЦІЇ
14.1. Ідентифікація та аутентифікація
14.2. Протокольна аутентифікація
14.3. Одноразові паролі
14.4. Ідентифікація/аутентифікація за допомогою біометричних даних
14.5. Логічне керування доступом
14.6. Рольове керування доступом
14.7. Керування доступом в Java-середовищі
14.8. Можливий підхід до керування доступом у розподіленому об’єктному середовищі
Запитання для самоконтролю
РОЗДІЛ 15. КЕРУВАННЯ РИЗИКАМИ
15.1. Реалізація підходів до аналізування ризиків
15.2. Ідентифікація та оцінювання активів
15.3. Оцінювання загроз
15.4. Оцінювання вразливостей
15.5. Оцінювання ризиків
Запитання для самоконтролю
РОЗДІЛ 16. КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ. ЗАГАЛЬНІ ПОЛОЖЕННЯ
16.1. Політика інформаційної безпеки
16.2. Програма управління кібербезпекою
16.3. Основні заходи процедурного рівня
16.4. Керування інцидентами кібербезпеки
16.5. Керування кіберзахистом автоматизованих робочих місц
Запитання для самоконтролю
РОЗДІЛ 17. КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
17.1. Керування кібернетичною безпекою інформації
17.2. Методика кібербезпеки іфнормаційних технологій
17.3. Організаційні системи кібербезпеки іфнормаційних технологій
17.4. Рекомендації щодо кіберзахисту іфнормаційних технологій
17.5. Методика кіберзахисту системи іфнормаційних технологій
17.6. Впровадження засобів кіберзахисту інформаційних технологій
Запитання для самокнтролю

РОЗДІЛ 18. КЕРУВАННЯ КІБЕРЗАХИСТОМ ІНФРМАЦІЙНИХ ТЕХНОЛОГІЙ
18.1. Підходи та рекомендації щодо кіберзахисту інформаційних технологій
18.2. Методика кіберзахисту системи інформаційних технологій
18.3. План кіберзахисту інформаційних технологій
18.4. Провадження засобів кіберзахисту
18.5. Компетентність у кіберзахисті
Запитання для самоконтролю
РОЗДІЛ 19. МЕТОДИ КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ
19.1. Методика керування кібербезпекою інформаційних технологій
19.2. Цілі та стратегії методики кібербезпеки інформаційних технологій
19.3. Варіанти стратегії та аналізу ризику
19.4. Реалізація змішаного підходу до аналізу ризиків
19.5. Застосування плану кібербезпеки інформаційних технологій
Запитання для самоконтролю
РОЗДІЛ 20. МЕТОДИ ТА ПІДХОДИ У КЕРУВАННІ КІБЕРБЕЗПЕКОЮ
20.1. Метод наукового управління кібербезпекою
20.2. Метод адміністративного управління кібербезпекою
20.3. Метод людських відносин
20.4. Метод кількісного підходу в управлінні кібербезпекою
20.5. Процесний підхід в управлінні кібербезпекою
20.6. Системний підхід в управлінні кібербезпекою
20.7. Ситуаційний підхід в управлінні кібербезпекою
20.8. Використання методів та підходів в управлінні кібербезпекою
Запитання для самоконтролю
РОЗДІЛ 21. ШТУЧНИЙ ІНТЕЛЕКТ ТА КІБЕРБЕЗПЕКА
21.1. Штучний інтелект та кіберзахист у кібербезпеці
21.2. Штучний інтелект екскурс в історію
21.3. Можливості посилення кібербезпеки штучним інтелектом
21.4. Машинне навчання в задачах кібербезпеки
21.5. Зростаюча загроза кібербезпеці на основі штучного інтелекту
Запитання для самоконтролю
ЛІТЕРАТУРА

ПЕРЕЛІК СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце
АСОД – автоматизована система обробки даних
АСУ – автоматизована система управління
ВВ – власний вектор
ВЗ – власне значення
ВМІП – варіаційна матриця інформаційного процесу
ДЕ – дескриптор
ЕОМ – електронно-обчислювальна машина
ЗОТ – засоби обчислювальної техніки
ІзОД – інформація з обмеженим доступом
ІКТ – інформаційно-телекомунікаційні технології
ІС – інформаційна система
ІТК – інформаційно-технологічний комплекс
КБ – кібернетична безпека
КЗ – кіберзахист
КНОІ – канал несанкціонованного отримання інформації
КС – комп’ютерна система
КСР – корнева структура
МАІ – метод аналізу ієрархії
МЧМ – матеріальні і часові можливості
НД – нормативний документ
НСЛ – нервова система людина
НСД – несанкціонований доступ
ОЦКК – обчислювальний центр колективного користування
ОС – операційна система
ПЗ – програмне забезпечення
ППЦІ – причини порушення цілісності інформації
ПРД – правила розмежування доступу
РЗН – рівень знань і навичок
РКД – рольове керування доступом
СКЗ – система кіберзахисту
СОД – система обробки даних
СУКБД – система управління кібербезпекою даних
ТЗІ – технічний захист інформації

ВСТУП

Масове створення, впровадження та експлуатація інформаційних систем привели до виникнення нових проблем в сфері безпеки інформації. І це закономірно.

В сучасних умовах все більше розповсюджується аксіома, кібернетичний захист інформаційних технологій повинен за своїми характеристиками бути відповідним масштабам загроз і ризиків. Відхилення від цього правила приведе до додаткових збитків. Для кожної інформаційної системи мається оптимальний рівень кіберзахищеності, який необхідно постійно підтримувати.

Немає сумнівів, що кіберзахист критично важливий для інформаційних систем і масивів. Він повинен відповідати міжнародним, корпоративним, нормативним і методичним документам. Однак,ю немає відповіді на саме важливе питання – наскільки рішення, яке пропонується або реалізується, дійсно гарне, як його плануєма та реальна ефективність. Такому положенню, яке мається в інформаційній системі, по неможливому в області забезпечення кібернетичної безпеки інфнормаційї, є ряд причин [1,2]:

- ігнорування системного підходу до методології, аналізу та синтезу систем кіберзахисту інформації;
- відсутність механізмів повного і достовірногго підтвердження якості систем кіберзахисту іфнормаційї;
- недоліки нормативно-методичного забезпечення кібернетичної безпеки іфнормації, перш за все в області показників і критеріїв.

Усім фахівцям в області захисту іфнормації та кіберзахисту відомі основні постулати, які не втратили актуальності на сьогодні:

- абсолютний захист створити не можливо;
- система захисту іфнормації повинна бути комплексною;
- система захисту іфнормації повинна бути адаптивною до змін обстановки;
- система захисту іфнормації повинна бути системою, а не простим набіром деяких хаотичних засобів і організаційних заходів;
- системний підхід до захисту іфнормації повинен застосовуватися, починаючи з підготовки технічного завдання та закінчуватися оцінкою ефективності та якості системи захисту в процесі її експлуатації.

Слід враховувати, що система кіберзахисту (захисту) іфнормації, повинна мати цільове призначення. Причому, чим більш конкретно сформульована мета кіберзахисту інформації, детально уяснені ресурси, які маються та визначений комплекс обмежень, тим в більшому ступені можливо отримати позитивний результат. Коли мета забезпечення кібернетичної безпеки проста і принципово досягається, то достатньо застосування нескладних елементів по структуризації

системи кіберзахисту іфнормації. Однак, при розширенні кола проблем, які треба вирішувати для забезпечення вимагаємого рівня кібербезпеки, зміст цільового призначення системи на формалізованому рівні визначає багатомірний та багатовекторний характер. При цбому важливість властивостей окремих елементів системи кіберзахисту знижується і на перший план виходять загальносистемні задачі – визначення оптимальної структури та режимів функціонування системи, облік впливів зовнішнього середовища тощо. При целеспрямованому об'єднанні елементів в систему остання потребує специфічних властивостей, яких не має жоден з її елементів. При системному підходжі мають першочергове значення тільки ти властивості елементів, які визначають взаємодію один з одним і не впливають на систему в цілому, а також на досягнення поставленої мети.

Тому, основою цього є ефективність, під якою розуміється ступінь відповідності результатів кіберзахисту інформації до поставленої мети. Остання, в залежності від ресурсів, які маються, знань розробників та інших факторів, може бути досягнута в тій чи іншій мірі, при цьому можливі альтернативні шляхи її реалізації. Ефективний безпосередній зв'язок з інфшими системними властивостями, в тому числі надійністю, живучістю, завадозахищеністю – а, в цілому, стійкістю системи. Тому, кількісна оцінка ефективності дозволяє вимірювати та об'єктивно аналізувати оснвоні властивості системи кіберзахисту іфнормації на всіх стадіях її життєвого циклу.

Тому, на перший план стає проблема – як створити таку систему кібернетичного захисту іфнормації, яка б спроможна була б при мінімальних витратах виконувати максимальні задачі захисту.

Все це зумовило оснсвну спрямованість та зміст підручника.

Автори висловлюють гибоку та щиру подяку доктору технічних наук, професору Дудикевичу Валерію Богдановичу (Національний університет «Львівська політехніка»), доктору технічних наук, професору Євсеєву Сергію Петровичу (Національний технічний університету «Харківській політехнічний інститут») та доктору технічних наук, професору Лаптеву Олександру Анатолійовичу (Київський національний університет імені Тараса Шевченка), за висловлені зауваження і поради, які сприяли значному покращенню та поглибленню підручника.

Крім того, автори висловлюють подяку кандидату технічних наук Анатолію Володимировичу Бороді за надані матеріали та допомогу у написані розділу 9 «Атаки за побічними каналами», а також за співробітництво та поради спеціалістам Служби безпеки України та Державної служби спеціального зв'язку та захисту інформації.

На поглад авторів видання стане в нагоді науково-педагогічним працівникам, аспірантам та студентам, а також усім зацікавленим щодо кібернетичного захисту інформації.

РОЗДІЛ 1. ОСНОВНІ ПОНЯТТЯ КІБЕРЗАХИСТУ

Завжди інформація була ключовим фактором продуктивного існування та розвитку людства. Зараз для обробки інформації в усіх сферах людської діяльності використовуються потужні обчислювальні машини. Від результатів їхньої роботи прямо залежить якість нашого життя. ЕОМ аналізують умови ринку й формують бузнес-проекти, розраховують трєкторії руху супутників, управляють складними високотехнологічними процесами, системами життєзабезпечення й безпеки.

Зростання ролі й відповідальності інформаційних технологійу життєдіяльності людини неминуче спричиняє відповідальне відношення до забезпечення надійної та безпечної роботи автоматизованих комп'ютерних систем. Помилки у функціонуванні автоматизованиз комп'ютерних систем (випадкових або навмисних, викликані злочинними діями зловмисників, комп'ютерних хуліганів або конкурентів) можуть призвести до досить серйозних наслідків. Захищена від зовнішніх та внітрішніх загроз комп'ютерна система – це те, до чого прагнуть керівники великих підприємств і власники персональних ЕОМ. Захист інформації (та її складової – кіберзахист) – справа, необхідність і значення якої продиктовано практично. Але створення захищеної комп'ютерної системи не проста справа.

Під інформацією, стосовно до задачі її захисту, розуміють відомості про осіб, предемти, факти, події, явища і процеси незалежно від форми їх подання.

Під інформаційною системою розуміють сукупність інформацйних ресурсів і взаємозалежних засобів, які здійснюють зберігання, обробку й передачу інформації; інформаційна система забезпечує протікання інформаційних процесів, тобто процесів, пов'язаних зі збором, обробкою, накопиченням, збереженням, пошуком й передачею інформації [1,2].

Залежно від форми подання інформація може бути розподілена на мовну, телекомунікаційну та документовану.

Мовна інформація виникає в ході ведення в приміщеннях розмов, роботи систем зв'язку, звукопідсилення та звуковідтворення. Телекомунікаційна інформація циркулює в технічних засобах обробки та зберігання інформації, а також в каналах зв'язку при її передачі. До документованої інформації або документів відносять інформацію, представлену на матеріальних носіях разом з ідентифікуючими її реквізитами.

Інформаційними ресурсами називають документи та масиви документів, що існують окремо або в складі інформаційних систем.

Процес створення оптимальних умов для задоволення інформаційних потреб громадян, організацій, суспільства та держави в цілому називають інформатизацією.

Інформацію поділяють на відкриту та обмеженого доступу. До інформації обмеженого доступу належать: державна таємниця і конфіденційна інформація. До конфіденційної інформації відноситься наступна інформація [1,2]:

- службова таємниця (адвокатська, лікарська тощо);
- комерційна таємниця у тому числі і банківська);
- персональні дані (відомості про факти, події та обставини життя громадянина, що дозволяють ідентифікувати його особу).

Інформація є одним з об'єктів цивільних прав, у тому числі і прав власності, володіння та користування. Власник – розпорядник інформаційних ресурсів, систем і технологій – це суб'єкт з повноваженнями володіння та користування зазначеними об'єктами. Під користувачем інформації розуміється суб'єкт, який звертається до інформаційної системи за отриманням необхідної йому інформації та користується нею [3].

До інформації, яка захищається, відноситься така, якає предметом власності та підлягає захисту відповідно до вимог правових документів або вимог встановлених власником – розпорядником інформації.

Кібернитичним захистом інформації називають діяльність щодо запобігання витоку інформації, що захищається від несанкціонованих і ненавмисних дій на цю інформацію.

Під витоком інформації розуміють неконтрольоване поширення інформації, що захищається, шляхом її розголошення, несанкціонованого доступу до неї та отримання її зловмисником. Розголошення – це доведення інформації, що захищається, до неконтрольованої кількості одержувачів інформації (наприклад, публікація інформації на відкритому сайті в мережі Internet або у відкритій пресі). Несанкіонований доступ – отримання інформації, що захищається, зацікавленим суб'єком з порушенням правил доступу до неї.

Несанкціонований вплив на інформацію, що захищається – вплив з порушенням правил її зміни (наприклад, навмисне впровадження в інформаційні ресурси, що захищаються, шкідливого програмного коду чиумисна відміна електронного документу) [3,4].

Під навмисним впливом на інформацію, що захищається, розуміють вплив на неї через помилки користувача, збій технічних чи програмних засобів, природних явищ, інших нецілenапраленних впливів (наприклад, знищення документів у результаті відмови накопичуцвача на жорсткому магнітному диску комп'ютера).

Метою кібернетичного захисту інформації (її бажаним результатом) є запобігання шкоди власнику-розпоряднику, власнику та користувачуінформації. Під ефективністю захисту інформації розуміється ступінь відповідності результатів захисту інформації поставленої мети. Об'єктом кіберзахисту виступає інформація, її носії або інформаційний процес, у відношенні яких необхідно забезпечувати кіберзахист у відповідності з поставленою метою [4,5].

Під якістю інформації розуміють сукупність властивостей, що обумовлюють придатність інформації задовільняти певні потреби її користувачів відповідно до призначення інформаціїї. Одним з показників якості інформації є її захищеність – підтримання на заданому рівня тих параметрів інформації, які характеризують встановлений статус її зберігання, обробки та використання.

Основними характеристиками інформації, що захищається, є конфіденційність, цілісніть та доступність.

Конфіденційність інформації – це відомість її змісту тільки тим суб'єктам, які мають відповідні повноваження. Конфіденційність є суб'єктивною характеристикою інформації, пов'язаної зоб'єктивною необхідністю захисту законних інтересів одних суб'єктів від інших.

Цілісністю інформації називають незмінність інформації в умовах її випадкового і/або навмисного викривлення або руйнування. Цілісність є частиною більш широкої характеристики інформації – її достовірності, що включає крім цілісності ще повноту та точність відображення предметної області. Для перевірки цілісності інформації часто використовується її хешування.

Хешуванням інформації називають процес її перетворення в хеш – значення фіксованої довжини.

Під доступністю інформації розуміють здатність забезпечення безперешкодного доступу суб'єктів до інформації, що їх цікавить. Відповідно, в обслуговування називають стан інформаційної систем, при якому блокується доступ до деякого її ресурсу.

Сукупність інформаційних ресурсів та системи формування, розповсюдження та використання інформації називають інформаційним середовищем суспільства.

Під інформаційною безпекою розуміють стан захищеності інформаційного середовища, що забезпечує її формування та розвиток. Вона досягається шляхом реалізації політики безпеки.

Політика безпеки – це набір документованих норм, правил та практичних прийомів, що регулюють управління, захист і розподіл інформації обмеженого доступу.

Комп'ютерною системою обробки інформації називають організаційно-технічну систему, що включає в себе [4,5,6,7]:

- технічні засоби обчислювальної техніки та зв'язку;
- методи та алгорити обробки інформації, реалізовані у вигляді програмних засобів;
- іфнормацію (файли, бази даних) на різних носіях;
- обслуговуючий персонал та користувачі, об'єднані за організаційно-структурними, тематичними, технологічними чи іншими ознаками.

Під програмним засобами захисту інформації розуміють спеціальні програми, що включається до складу програмного забезпечення КС виключно для виконаня захисних функцій [1,2,6].

Під ідентифікацією, стосовно забезпечення інформаційної безпеки КС, розуміють однозначне розпізнавання унікально імені суб'єкта КС. Аутентифікація означає підтвердження того, що пред'явлене ім'я відповідає даному суб'єкту (підтвердження автентичності суб'єкта). Авторизація – надання суб'єкту прав на доступ до об'єкта.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

- Яка інформація відноситься до інформації, що захищається?
- Що таке захист інформації?
- Що таке несанкціонований доступ?
- Що є несанкціонованим впливом на інформацію, яка захищається?
- Що таке ненавмисний вплив на інформацію, яка захищається?
- В чому полягає мета кіберзахисту інформації?
- Які основні характеристики інформації, що захищається?
- Що розуміють під інформаційною безпекою?
- Що таке ідентифікація, авторизація та аутентифікація?

РОЗДІЛ 2. ЗВ'ЯЗОК ІНФОРМАЦІЇ З ДІЯЛЬНОСТЮ СУСПІЛЬСТВА

2.1. Види інформації

Розрізняють два основних види інформації [1,2,7]:

- Біологічна інформація.
- Соціальна інформація.

Соціальна інформація викликає найбільший інтерес при дослідженні в галузі життєдіяльності суспільства.

Соціальна інформація тісно пов'язана з практичною діяльністю людини, тому тут можна виділити стільки типів і різновидів, скільки є видів діяльності людини.

Прикладами можуть слугувати політична, військова, естетична, етична, економічна, технологічна (ноу-хау), вимірювальна, науково-технічна інформації. При цьому можливі різноманітні класифікації за різноманітними ознаками. Зокрема соціальна інформація ділиться на два класи:

- масова інформація;
- спеціальна інформація.

Масова інформація адресована всім членам суспільства незалежно від їхнього становища і роду діяльності. Спеціальна інформація адресована не всім членам суспільства, а певним соціальним групам (вченим даної спеціальності, економістам, військовим і т.д.). Для сприйняття цілей інформації необхідний початковий запис спеціальних знань і володінно професійною мовою. Ось найбільш важливі різновиди спеціальної соціальної інформації.

НАУКОВА ІНФОРМАЦІЯ утворюється в результаті науково-технічної діяльності. Наукову інформацію можна визначити як передане в інформаційному процесі наукове знання. Наукова інформація, як і наукове знання, є результатом абстрактно-логічного мислення й адекватно уособлює об'єктивні закономірності, явища і процеси реального світу, суспільства і духовної діяльності людини, вона повинна бути природно отримана науковими методами, що забезпечують істинність знання.

ТЕХНІЧНА ІНФОРМАЦІЯ створюється в сфері техніки і призначена для вирішення технічних задач (розробка нових технічних виробів, матеріалів, технологій). Структура та властивості наукової і технічної інформації досить близькі, тому ці два види часто об'єднують терміном «науково-технічна інформація». Проте, розрізняючи науку і техніку як сфери суспільного виробництва, розрізняють й інформаційні процеси, характерні для цих сфер, зокрема документи, призначені для техніки (патенти,

стандарти, комп'ютерні програми, конструкторська документація), або переважно для науки (звіти про науково-дослідні роботи, монографії, теоретичні журнали, збірники наукових праць).

ТЕХНОЛОГІЧНА ІНФОРМАЦІЯ безпосередньо використовується для створення матеріальних благ. Нові високоефективні технології створюють певний імідж суспільства, держави.

ПЛАНОВО-ЕКОНОМІЧНА ІНФОРМАЦІЯ про стан і перспективи розвитку народного господарства використовується для організації планування і впливу на управління суспільним виробництвом, у тому числі й в умовах ринкових відносин.

Інформація має деякі загальні для всіх її видів властивості. Основною властивістю інформації варто вважати її нерозривний зв'язок з певною самостійно організовувальною системою. Іншими важливими властивостями інформації є структурованість, значення і цінність.

Структурування інформації відбувається паралельно з формуванням моделі зовнішнього світу, а найчастіше є першим етапом у наукових дослідженнях.

Для системи, що самостійно організовується, характерно прямування-прагнення до мети, до більш сприятливого становища стосовно власних критеріїв або стабілізації та зберігання зайнятого становища. Усе, що забезпечує цей рух, є цінним для системи. Звідси випливає, що цінними є і речовина, і енергія, і інформація. Цінність інформації виражається в таких поняттях, як змістовність, своєчасність, повнота, достовірність, оперативність.

2.2. Інформація для ухвалення рішення

Фундаментом для побудови інформації слугує 3B/buns–besoins–bases/ цілі – потреби – бази[7,8]. Цілі пов'язані одна з одною в ієрархічну структуру. Кожна мета обумовлюється метою вищого порядку, залишаючись при цьому автономною за характером своїх потреб і баз для спостереження. Кожній з цих цілей відповідають різноманітні потреби в інформації й, отже, різні бази для спостереження. Це є справедливим для будь-якої організації і, зокрема, для підприємств, де варто розрізняти стратегічний (будівництво фабрики, впровадження нової технології і т. п.) і тактичний (вибір майданчика для будівництва фабрики, розробка нової технології власними силами і т.п.) рівні. Правильне визначення цілей на кожному рівні дозволяє правильно визначити потреби в інформації і, одночасно, бази для спостереження.

2.2.1. Інформація для стратегічних рішень

Стратегічні рішення прямо впливають на долю підприємства, на його розвиток і життєздатність. Навколишній світ постійно змінюється і швидкість

цих змін постійно збільшується. Тому кількість стратегічних рішень постійно зростає, їхні наслідки усе складніше і складніше прогнозувати, а ціна помилки постійно підвищується. Цим і визначається значення стратегічної інформації, без якої неможливо прийняти правильне рішення. Рішення полягає в поетапному підході відповідно до методу «ЗВ»: робота, а потім і бази для спостереження, повинна починатися з визначення цілей, що обумовлюють потреби в інформації.

Таким чином, перше, що необхідно зробити, це визначити стратегічні цілі, які повинні визначити подальший розвиток підприємства. Наступний етап – це визначення стратегічних потреб, що містять у собі все, що може чинити довгостроковий вплив на діяльність підприємства. На підставі виявлених потреб визначають стратегічні бази. Для цього складають картотеку напрямків для спостереження. Для полегшення цієї роботи розділяють сферу на три галузі [7,8,9]:

безпосередня сфера дій містить у собі все, що знаходиться в прямому зв'язку з діяльністю підприємства;

сфера впливу містить у собі все, що може вплинути на дії, здійснювані в рамках попередньої сфери;

сфера інтересів містить у собі галузі діяльності, якими підприємство поки не займається, але може зайнятися в майбутньому, а також ті галузі діяльності, що можуть вторгнутись в основну сферу діяльності підприємства.

Користь такого розподілу полягає в тому, що він змушує звернути увагу на межі звичайної сфери діяльності, тобто туди, звідки, зазвичай виходять найбільш значні сприятливі можливості і найбільші небезпеки.

Чим більше поставлені цілі віддалені в часі, тим ширшим повинно бути поле зору, тим більшою повинна бути сфера інтересів. Особливе значення це має на стратегічному рівні. На тактичному й оперативному рівнях можна обмежитися двома першими сферами.

2.2.2. Інформація для тактичних рішень

Інформація для тактичних рішень складається з вибору [8,9]:

тактичних цілей;

тактичних потреб першого і другого типів;

тактичних баз першого і другого типів.

Тактична мета полягає у виборі найкращого способу досягнення стратегічної мети й у контролі незмінності умов, що зумовили цей вибір.

Тактичні потреби полягають у необхідності розрізнення постійних і змінних величин, пов'язаних з тимчасовою шкалою дій. Зокрема, це полягає в правильному виборі напрямків. Для правильного вибору необхідно знати загальні характеристики кожного з напрямків, що належить до *потреб*

першого типу. Необхідність постійного спостереження за станом навколишнього середовища для своєчасного виявлення всіх завад, що можуть стати причиною значних відхилень від наміченого шляху, відносять до *потреб другого типу*.

Ці два види потреб настільки різні, що відповідні їм бази практично не мають нічого спільного одна з одною. У першому випадку створюються і знищуються бази для інформації, що збирається «за запитом»: щораз, коли з'являється новий напрямок, починається спроба максимально повного ознайомлення з характеристиками для ухвалення рішення про те, чи варто йти в цьому напрямку. В другому випадку ведеться всеосяжне спостереження навколишнього середовища, тому що невідомо, звідки може прийти небезпека.

До *тактичних баз першого типу* відносять бази інформації, що збираються «за запитом», які потребують ретельного дослідження нових напрямків з урахуванням політичної, соціально-культурної й економічної інформації.

Тактичні бази другого типу з девізом «всеосяжне спостереження навколишнього середовища» містять у собі всі чинники навколишнього середовища, зміна яких може мати середньостроковий вплив на діяльність підприємства. Перелік критеріїв, що враховуються на стратегічному рівні, продовжується на тактичному і містить у собі [9,10]:

основної галузі діяльності і види продукції (теперішні і майбутні), зони і території діяльності;

виробничі потужності і засіб виробництва;

патентна і ліцензійна активність.

Природно, тактичні бази і параметри, що враховуються, змінюються залежно від політичної лінії, наміченої керівництвом.

2.2.3. Інформація для вирішення оперативних питань

ОПЕРАТИВНІ ЦІЛІ. На цьому рівні стратегічна мета уже визначена, шлях її досягнення обраний, і тепер необхідно забезпечити просування вперед у найкращих умовах, уникаючи дрібних останніх завад і, по можливості, скорочуючи шлях.

ОПЕРАТИВНІ ПОТРЕБИ. Мова йде про сприятливі можливості або про загрози. В усіх випадках потрібна свіжа, точна, надійна і цілеспрямована інформація, тому що мова йде про максимально швидке реагування, тобто про реагування без найменших зволікань і без імпровізації: сприятливі можливості не повторюються двічі, і загрози, якщо їм вчасно не запобігти, можуть виявитися згубними.

ОПЕРАТИВНІ БАЗИ. Мова йде про найближче оточення підприємства, за котрим необхідно стежити з підвищеною увагою. Сюди входять

конкуренти та їхня комерційна політика. Не варто забувати про інші не менш важливі напрямки спостереження: постачальники, система торгівлі і численні інші об'єкти спостереження, вибрані з урахуванням специфічних потреб кожного конкретного випадку.

Для того, щоб інформація, яка збирається, принесла користь, необхідно навчитися правильно збирати її. Цілком природно, що спочатку ви будете робити помилки, приймаючи необґрунтовані чутки за справжню інформацію. Лише в процесі пошуку інформації можна навчитися збирати її. Використання методу «ЗВ» допоможе вам розпізнати корисну інформацію з першого погляду [5,11,12].

КАРТОТЕКА СПОСТЕРЕЖЕНЬ. Вважається раціональним об'єднання всіх баз у рамках однієї картотеки. Основними базами є:

конкуренція (вся інформація про діючих і потенційних конкурентів);

ринок (уся ринкова інформація, смаки і запити споживачів, канали збуту і т.п.);

технологія виробництва і використання продукції;

законодавство (вся інформація з законодавства, що стосується діяльності підприємства, а також інформація з діяльності органів, що розробляють і приймають нові законодавчі положення);

ресурси (вся інформація з матеріально-технічних ресурсів, необхідних для нормальної діяльності підприємства, щодо сировини, постачання, робочої сили і фінансів);

загальні тенденції (політична, економічна, соціальна, демографічна і т.п. інформація);

інші чинники, що впливають на діяльність підприємства (чинники, не враховані в попередніх базах).

Метод «ЗВ» дозволяє вам забезпечити спостереження за потрібними базами. Проте при розвитку підприємства можуть з'явитися нові цілі, ринок і навколишнє середовище постійно змінюватимуться. Тому ви повинні передбачити можливість періодичного перегляду ваших баз на основі повторного аналізу цілей і потреб вашого підприємства.

Інформація є цінною тільки тоді, коли вона може використовуватися. Якщо інформація не слугує для ухвалення рішення, то вона є безпредметною, а, отже, – неіснуючою.

Таким чином, для одержання якісної інформації необхідно сформулювати цілі, визначити потреби і побудувати бази для спостереження. Для діяльності підприємства звичайно достатньо шести баз для спостереження: конкуренція, ринки, технологія, законодавство, ресурси, спільні тенденції.

2.3. Збір та обробка інформації

2.3.1. Шлях інформації

Намітимо загальну методику одержання інформації на прикладі запуску нової продукції [12,13].

При запуску нової продукції більша частина інформації вже пройшла через ті етапи, де виток імовірний, навіть можливий: рішення фінансистів, що повинні встановити ціни, вивчити ринок і дати кредит з бюджету на дослідження; заявлені патенти або такі, що купуються. В усі ці операції залучено багато людей, не рахуючи сторонніх учасників (банки, професійні організації і т. п.), що робить цілком неможливим повне дотримання таємності.

Для збуту продукції створюється команда, про існування якої добре відомо всім співробітникам підприємства. Нові дії команди розширюють коло посвячених (створення нового цеху або заводу і т. п.). Ці посвячені більш-менш відірвані один від одного у своїй професійній діяльності або особистому житті настільки, що інформація випаровується. Нарешті з'являються чутки. Тоді інформація виявляється на межі приватного і громадського життя. Іноді такий етап виявляється досить пікантним, оскільки конкурент насторожується і може почати вживати контрзаходів раніше, ніж становище стабілізується.

Робиться повідомлення. Публікується інформація. Слово «публікується» не означає «широко поширюється». Деякі виробництва користуються потоком статей та інформації. У інших випадках інформація не потрапляє в поле зору спеціалізованих видань і конфіденційних збірників, хоча найчастіше саме вони містять важливі нові технології. На такій стадії реальні характеристики продукції ще невідомі.

Випускається продукція. Усі можуть її купити, споживачі її досліджують і порівнюють з іншою. Конкуренти її розбирають і розгвинчують, а всі характеристики продукції стають надбанням громадськості і тим або іншим чином публікуються.

Продукція фіксується, класифікується і, можливо, стає статистичним об'єктом. При нагоді її характеристики займають своє місце в банку даних, що являє собою електронну бібліотеку, де накопичуються, часто з запізненням, резюме статей журналів і збірників.

Продукція зникає, її місце займає нова. Стирається інформація про стару, про неї не залишається нічого, крім інформації в архіві.

Досвід показує, що зміни і накопичення інформації відбуваються в невеликому переліку привілейованих місць, що називаються «Сімейство джерел».

Ось перелік основних сімейств джерел для будь-якого підприємства: КЛІЄНТИ – покупці клієнтів; їхні інженери і кадри; ПОСТАЧАЛЬНИКИ – відповідно до їхньої діяльності;

БАНКІРИ – розділені на банківські, фінансові, біржові і кредитні установи;

СУСПІЛЬНІ СЛУЖБИ – рекламні агенції, фірми суспільних зв'язків, мисливці за інтелектами та ін.;

РОЗПОДІЛЬНИКИ і АГЕНТИ – поза залежністю від особливостей, варто брати до уваги як торговців, так і покупців;

КОНСУЛЬТАНТИ і ЕКСПЕРТИ – незалежні фахівці, або такі, що працюють на підприємстві, які продають свої знання у формі порад або спеціальних розробок;

ШИРОКА ПУБЛІКА – місцева, національна або міжнародна преса;

СПЕЦІАЛЬНІ ВИДАННЯ і БАНКИ ДАНИХ – їхня галузь діяльності припускає щомісячне опрацювання матеріалів конфіденційних видань, що потрапляють у наукові, технічні і фахові збірники. Разом з банком даних вони складають ресурси бази даних;

ЯРМАРКИ, САЛОНИ і КОНФЕРЕНЦІЇ – ці демонстрації дозволяють обновити контакти з клієнтами, конкурентами і т.д., а також побачити різноманітну продукцію, презентовану на ринку. Наукові і технічні виставки дозволяють визначити країну, що йде попереду у своїх дослідженнях;

АДМІНІСТРАЦІЯ – усі нормативні зобов'язання і вимоги керівництва для майже всіх видів промисловості, комерційної і фінансової діяльності підприємства. Вони зібрані в архівах і здебільшого є опублікованою інформацією. Виділення необхідної кількості джерел з усього сімейства в більшості випадків дозволяє добратися прямо до інформації без того, щоб проходити всі шляхи її просування.

Назвемо шляхи пошуку інформації – **шляхом інформації**.

2.3.2. Канали інформації

Аналізуючи бази і джерела інформації, можна визначити канали інформації, перегрупувавши сімейство джерел таким чином [3,11,14]:

канал тексту – загальні публікації + спеціальні публікації і банки даних. Цим каналом підприємство одержує 30–40% всієї інформації;

канал фірма – клієнти + постачальники + банкіри + розподільники й агенти. Через цей канал проходить від 30 до 40% інформації. Разом із персоналом, який більш-менш контактує зі сторонніми організаціями, це складає внутрішню мережу підприємств;

канал консультант – суспільні служби + консультанти + адміністрація. Цим каналом проходить 10–15% інформації;

канал розмова – ярмарки + салони і конференції. Через цей канал проходить 5–6% інформації;

канал джокер – додатковий канал.

Методика пошуку інформації, що враховує всі п’ять каналів, називається **4К+1** (1 – частина, що відповідає джокерові).

Розглянемо варіанти пошуку джерел інформації [11,15,16].

Методика 4К+1 у формі «дощ, що мрячить». У цьому випадку бази спостереження підживлюються регулярно чотирма каналами.

Методика 4К+1 за методом «гроза». Цей метод полягає в постійному поповненні інформації й одержанні своєчасної відповіді або виявленні небезпеки шляхом спостереження за каналом джокер.

Перед тим, як займатися пошуком інформації в незручних місцях, варто переконатися, що вона не отримана і тому потрібно починати свої дії, особливо активізуючи основні два канали: текст і фірму.

Методика багатоджерельного пошуку. Якщо попередні пошуки довго не завершуються або ви дійшли висновку, що небагато шансів швидко завершити пошук у силу екстраординарності проблеми, – звертайтеся до кількох джерел. Щоб це зробити, необхідно встановити, які із сімейства джерел вже опрацьовані, проробивши попередню роботу з самим джерелом, і з’ясувати чи містить воно пошукову інформацію. Все це необхідно для того, щоб визначитися у формі подання і доступу до інформації.

Така методика, так само як і наступні, набагато складніша і дорожча, ніж попередня.

Стежина інформації. Якщо проблема за своєю природою не може бути відзначена серед сімейств, тоді необхідно відновити стежину просування інформації.

Методика 3В. Для досягнення певної мети необхідно користуватися всіма базами і джерелами інформації.

Таємність інформації. Більша частина корисної інформації не є таємницею. Таємницею можна назвати те, що тримається осторонь, удалині від сторонніх очей. Мова йде про таку інформацію, що з політичних або комерційних міркувань вважається ключовим моментом певної ситуації. Промислові таємниці стосуються, в основному, виробництва, особливо технології. Вони повинні охоронятися. Звідси і поняття «захист інформації» і «дотримання таємності».

2.3.3. Обробка інформації

Обробка інформації складається з трьох основних операцій – це аналіз, синтез і циркуляція [9,15,16].

Першою і найважливішою операцією є аналіз, що слугує додатковим фільтром, який відкидає непотрібне і є захистом від шуму без підстави. Ця

операція складається, насамперед, у визначенні важливості, точності і значущості інформації.

Важливість інформації. Побудова баз спостереження, згідно з процедурою ЗВ, гарантує зв'язок з інформацією, що спостерігається. Але інформація, пов'язана тематично, може не мати особливого значення. Інформація є важливою, якщо вона пов'язана, тобто має зв'язок з елементами бази і якщо вона спроможна внести вклад в організацію. Коли внесок значний і безпосередній, інформація потребує термінових дій. Інформація, що не має значення, повинна бути вилучена, щоб уникнути втрати часу і енергії.

Точність інформації. Не завжди легко встановити є інформація достовірною чи помилковою, особливо якщо вона містить відомості про події, що ще не відбулися. Допускається два критерії, за якими можна судити про точність інформації: надійність джерела і самої інформації. Головним критерієм правдоподібності є пошук підтвердження в інших джерелах, якщо можливо, – незалежних. Рішення полягає в пошуку пов'язаних подій у різноманітних інформаціях. При відсутності надійності джерела інформації не варто її відкидати, особливо якщо вона справляє враження важливої. Необхідно просто відкласти про запас та чекати нових елементів, що дозволять її або підтвердити, або ні.

Значущість інформації. Інформація може бути важливою та точною й у той же час даремною, оскільки вона недостатня для розуміння і дії. Два тлумачення, наведені окремо або паралельно, дозволяють судити про значимість інформації. Перше називається «циркуляція». Воно складається у швидкій циркуляції інформації серед осіб, яких вона стосується, у надії на можливість встановлення зв'язку з іншою інформацією. Друге тлумачення називається «синтез». Воно полягає в об'єднанні всіх частин інформації, що схоже на складання головоломки для створення повного уявлення. Це не завжди легко, тому що часто не вистачає частин або вони непідходящої форми. Іноді навпаки, частини ідеально підходять, даючи зрозуміле уявлення про ситуацію. Частіше доводиться робити певний шлях при формуванні гіпотези: спробу синтезу, циркуляцію, пов'язати це з дослідженням допоміжної інформації для того, щоб отримати зрозуміле та повне уявлення.

Для визначення значимості інформації використовують два допоміжних підходи. Перший називається «розширення», а другий – «намір».

Підхід до методу розширення полягає в тому, що для даних, наявних у розпорядженні, шукається найбільш відповідне пояснення. Часто при завершенні різноманітних гіпотез виявляються протиріччя. У такому випадку важливо знайти всю інформацію, здатну підтвердити одну гіпотезу і відкинути інші.

Підхід до методу «намір» полягає у виявленні такої діючої особи, у наміри якої входять останні факти. Поставте себе на її місце, щоб зрозуміти, яку гру вона веде, щоб зробити висновок про її можливі дії. Виходячи з цього, будується безліч гіпотез щодо її намірів і, досліджується, як вони повинні були б пояснити факти. Нарешті, порівнявши імовірні факти з наявними даними, вибирається гіпотеза, що охоплює найбільший діапазон спостережень.

2.3.4. Цикл інформації

Щоб переконатися в корисності джерела інформації, необхідно здійснювати постійну перевірку джерел за двома простими критеріями: забезпечення і ефективність.

Перевірка забезпечення джерел полягає у визначенні цінності, корисності, своєчасної подачі інформації.

Ефективність джерел полягає в одержанні свіжої і конфіденційної інформації.

Таким чином, обробка інформації здійснюється за «малим» (рис. 2.1) і «великим» (рис. 2.2) циклами інформації [16,17].

«Малий» цикл інформації охоплює: джерела, збирання, обробку.

«Великий» цикл інформації містить у собі: мету, необхідність, обробку, дію.

Рис. 2.1. «Малий» цикл інформації

Рис. 2.2. «Великий» цикл інформації

2.3.5. Помилкова інформація

Помилкова інформація або дезінформація містить неправду про саму природу об’єкта, про ті чи інші його якості. Дезінформація залежить від точки зору адресата. Для нього це повідомлення повинно бути отримано як неправдива інформація, у протилежному випадку маневр зазнає невдачі. Отже, адресат повинен апріорі бути налаштований позитивно до помилкової інформації. У помилковій інформації є дві складові: сюжет, що підживлюється певною увагою,

і сюжет помилковий, що відповідає на цю увагу, пропагандуючи помилкову інформацію. На рис. 2.3 наведено шлях помилкової інформації [15,16].

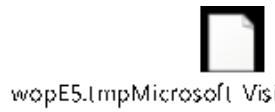


Рис. 2.3. Шлях помилкової інформації

Все мистецтво помилок складається з одержання відповіді, яка повинна бути близькою до реальної ймовірності й у той же самий час повинна містити щось віддалене, щоб ввести адресата в оману. Для того, щоб неправда була сприйнята, необхідно, насамперед, знати адресата і, особливо, привілейовані джерела інформації. Потім відправити повідомлення через визнані джерела.

При цьому дезінформація може потрапити до вас з джерела, яке ви вважаєте достовірнішим.

Існують два види дезінформаторів: дезінформатори випадкові й ті, що цим займаються професійно.

Дуже важко відстежити випадкову дезінформацію. Як чиста правда вона надходить занадто пізно, коли мета дезінформації вже досягнута. З професіоналами дезінформації справа набагато простіша. Спочатку через створення зіпсованих ефектів для маніпуляторів «дезінформація є такою досконалою, що її автори не можуть відрізнити правду від вигадки». Неможливо довго приховувати що-небудь. Коли зустрічаєшся з такими дезінформаторами, потрібно прив’язуватися до змісту інформації, щоб виявити мотиви, якими вони керуються. Скрізь зустрічаються факти з використанням техніки, яка має назву «білий шум». Ця техніка полягає у подачі такої кількості новин, що неможливо зробити сортування. Володіння циклами інформації в більшості випадків охороняє від маневрів помилки.

2.3.6. Витік інформації

Більша частина витоку інформації відбувається через недбалість. Тому захист інформації, насамперед, справа навчання. Необхідно знову і знову нагадувати всім (від простого службовця до керівного складу) про елементарні заходи безпеки. Уважність повинна починатися з голови і поширюватися по всьому організму доти, поки не стане рефлексом, що є природною дією, про яку ніхто не думає. Такий результат не досягається без зусиль, але, зрештою, вигода бере верх над невеликими незручностями на самому початку.

Ризиковані точки витоку інформації багаточисельні і важко піддаються контролю. Як приклад розглянемо невеликий перелік простих заходів витоку інформації [16,17].

Встановіть у бюро ріжучий апарат поблизу копіювального і виробіть у собі рефлекс знищувати всі непотрібні документи.

Керуючись конфіденційністю даних у пам'яті комп'ютера, прийміть якийсь код.

Контролюйте доступ до комп'ютера ззовні. Найпростіша процедура полягає в забороні користування протягом певного часу і оголошенні сигналу тривоги, якщо три введені слова помилкові. Це сприяє запобіганню крадіжки даних і захищає всю систему від руйнування.

Періодично робіть копії інформації, що охороняється, і зберігайте їх у надійному місці.

Обмежте вихід інформації до мінімуму.

Для того, щоб вводити помилку, інформацію можна піддати деякому упакуванню: підінформація – інформація подається правдива, але розрізнена або неповна, або занадто загальна; інформація помилкова; надінформація – подається велика кількість інформації, але частина її є даремною або помилковою, але все це подається так, щоб неможливо було виявити.

Обмежте місця прийому відвідувачів і не залишати їх самих.

Не зловживайте набором стажистів і тимчасових співробітників, що часто мають доступ до великої кількості інформації. Бійтеся особливо тих «студентів», яким під сорок.

Закривайте на ключ усі важливі документи наприкінці робочого дня. Це правило повинно застосовуватися з усією суворістю в усіх дослідницьких бюро, нічого ніде не повинно просто так лежати.

Телефони, телекси, телефакси повинні розглядатися з погляду безпеки передачі інформації особливо в певні країни, з якими необхідно звести контакти до мінімуму і застосувати код для повідомлення надважливої інформації.

Ці заходи ефективні, але не можна забувати, що берегти таємницю повинні самі люди.

Щоб уникнути витоку інформації, потрібно, насамперед, стежити за резервуарами її накопичення; за кранами, що управляють інформаційними потоками; за центрами розподілу інформації [18].

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

Що являє собою інформація? В якому випадку існує справжня інформація?

Які основні властивості інформації?

На які два класи поділяють інформацію і що вони собою являють?

Що є фундаментом для побудови інформації?

Що містять у собі стратегічні потреби?

Що необхідно для визначення стратегічних баз?

З якою метою роблять поділ сфери дії на галузі? Яка користь такого розподілу?

У чому полягає тактична мета?

Яку інформацію містять у собі тактичні бази першого і другого типу?

Що являють собою тактичні цілі, тактичні потреби і тактичні бази?

Що необхідно для одержання якісної інформації?

Простежте самостійно стежину інформації від запуску нової продукції до її зникнення.

Перерахуйте основні джерела отримання інформації.

Які канали інформації існують?

Перерахуйте методики пошуку джерел інформації.

Яка інформація є таємною?

У чому полягає операція синтезу?

У чому полягає важливість, точність і значущість інформації?

Які підходи використовують для визначення значущості інформації та у чому вони полягають?

РОЗДІЛ 3. СТРУКТУРА ІНФОРМАЦІЙНОГО ПРОЦЕСУ

3.1. Параметри інформаційного процесу і зв'язок між ними

Як відомо, будь-який інформаційний процес визначається зміною параметрів, які його задають, або приведенням одних параметрів (вихідних — $\Phi_1, \Phi_2, ..., \Phi_m$) у відповідність з іншими (вхідними — $x_1, x_2, ..., x_n$) за законом:

$$\begin{cases} \Phi_1 = \varphi_1(x_1, ..., x_n), \\ \Phi_2 = \varphi_2(x_1, ..., x_n), \\ \quad \vdots \\ \Phi_m = \varphi_m(x_1, ..., x_n), \end{cases} \tag{3.1}$$

де $(x_1, x_2, ..., x_n) \in D \subseteq R^n$.

Нехай $\varphi_i \in C^1(D),\ i = \overline{1,m}$. Припустимо, що значення одного з вихідних параметрів Φ_j однозначно визначається сукупністю значень інших $\Phi_1, ..., \Phi_{j-1}, \Phi_{j+1} ..., \Phi_m$, тобто, якщо $\Omega_0 \subseteq R^{m-1}$ є множина точок, що відповідають усіляким точкам $(x_1, x_2, ..., x_n) \in D$, то в Ω_0 буде мати місце функціональна залежність:

$$\Phi_j = f(\Phi_1, ..., \Phi_{j-1}, \Phi_{j+1}, ..., \Phi_m), \tag{3.2}$$

де $f \in C^1(\Omega),\ \Omega \subseteq R^{m-1},\ \Omega \supseteq \Omega_0,\ \Omega$ — відкрита множина, а при підстановці (3.1) в (3.2) виходить тотожність відносно $(x_1, x_2, ..., x_n) \in D$:

$$\varphi_j(x_1, ..., x_n) \equiv f\left(\varphi_1(x_1, ..., x_n), ..., \varphi_{j-1}(x_1, ..., x_n), \varphi_{j+1}(x_1, ..., x_n), ..., \varphi_m(x_1, ..., x_n)\right). \tag{3.3}$$

У цьому випадку будемо казати, що функція φ_j *залежить від функцій* $\varphi_1, ..., \varphi_{j-1}, \varphi_{j+1} ..., \varphi_m$ в області D [12]. У загальному випадку функції $\varphi_1, \varphi_2, ..., \varphi_m$ називаються *залежними* в області D, якщо одна з них залежить від інших.

Якщо ані в області D, ані в якій-небудь області $E \subseteq D$ не має місця тотожність (6.3), то функції $\varphi_1, \varphi_2, ..., \varphi_m$ називаються *незалежними* в D [12].

Визначення 3.1. Вихідні параметри інформаційного процесу будуть незалежними (залежними), якщо незалежними (залежними) в області D будуть функції (6.1), що їх визначають.

Зауваження 3.1. У випадку незалежності вихідних параметрів їх визначення відповідно до (3.1) може проводитися одночасно (паралельно), що значно скорочує при необхідності час реалізації й аналізу інформаційного процесу. Цей процес можна представити як сукупність не зв'язаних між собою «простих» процесів, результатом кожного з яких є отримання лише одного параметра Φ_i, а дослідження поданого інформаційного процесу зведеться до дослідження скінченної сукупності «простих».

Завдяки зауваженню 3.1 важливою є можливість визначення залежності (незалежності) вихідних параметрів (функцій (3.1)). Відповідь на це питання дається властивостями матриці частинних похідних функцій φ_i, $i=\overline{1,m}$, — матриці Якобі неперервного інформаційного процесу [12]:

$$\begin{pmatrix} \frac{\partial\varphi_1}{\partial x_1} & \frac{\partial\varphi_1}{\partial x_2} & \dots & \frac{\partial\varphi_1}{\partial x_n} \\ \frac{\partial\varphi_2}{\partial x_1} & \frac{\partial\varphi_2}{\partial x_2} & \dots & \frac{\partial\varphi_2}{\partial x_n} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \frac{\partial\varphi_m}{\partial x_1} & \frac{\partial\varphi_m}{\partial x_2} & \dots & \frac{\partial\varphi_m}{\partial x_n} \end{pmatrix}. \qquad (3.4)$$

Нехай $n \geq m$. Якщо хоч один визначник m-го порядку, складений з елементів матриці (2.4), відмінний від нуля в області D, то в цій області функції φ_i, $i=\overline{1,m}$, а тому і вихідні параметри інформаційного процесу, незалежні. Дійсно, припустимо, що

$$\det\begin{pmatrix} \frac{\partial\varphi_1}{\partial x_1} & \frac{\partial\varphi_1}{\partial x_2} & \dots & \frac{\partial\varphi_1}{\partial x_m} \\ \frac{\partial\varphi_2}{\partial x_1} & \frac{\partial\varphi_2}{\partial x_2} & \dots & \frac{\partial\varphi_2}{\partial x_m} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \frac{\partial\varphi_m}{\partial x_1} & \frac{\partial\varphi_m}{\partial x_2} & \dots & \frac{\partial\varphi_m}{\partial x_m} \end{pmatrix} \neq 0, \qquad (3.5)$$

але якась з функцій, наприклад, φ_m, визначається через інші:

$$\varphi_m = f(\varphi_1,...,\varphi_{m-1}) \qquad (3.6)$$

хоча б у деякій області $E \subseteq D$ (якби відмінним від нуля був інший визначник, то, змінивши нумерацію змінних, можна було б знову прийти до випадку (3.5)).

Продиференціюємо (3.6) по x_i, $i=\overline{1,m}$:

$$\frac{\partial\varphi_m}{\partial x_i}=\frac{\partial\varphi_m}{\partial\varphi_1}\frac{\partial\varphi_1}{\partial x_i}+\frac{\partial\varphi_m}{\partial\varphi_2}\frac{\partial\varphi_2}{\partial x_i}+...+\frac{\partial\varphi_m}{\partial\varphi_{m-1}}\frac{\partial\varphi_{m-1}}{\partial x_i},\quad i=\overline{1,m}. \tag{3.7}$$

З (3.7) випливає, що елементи останнього рядка матриці (3.5) отримуються шляхом додавання відповідних елементів перших $m-1$ рядків, помножених попередньо на множники $\frac{\partial\varphi_m}{\partial\varphi_1},...,\frac{\partial\varphi_m}{\partial\varphi_{m-1}}$. Але тоді визначник (3.5) дорівнює нулю. Отримали суперечність, тому припущення (3.6) хибне.

Розглянемо загальний випадок. Рангом матриці Якобі (3.4) в області D назвемо найвищий з порядків визначників, що складаються з елементів цієї матриці і не дорівнюють тотожно нулю в D. Кажуть, що *ранг r досягається* в деякій точці $M^0\left(x_1^0,x_2^0,...,x_n^0\right)$ області, якщо визначник r-го порядку в цій точці відмінний від нуля.

Теорема 3.1. Нехай ранг матриці Якобі інформаційного процесу (3.4) в області D є r і досягається в точці $M^0\left(x_1^0,x_2^0,...,x_n^0\right)\in D$, при цьому $r=m$. Тоді в D знайдеться така область зміни вхідних параметрів інформаційного процесу, де вихідні будуть незалежними.

Доведення. В умовах теореми існує окіл D_0 точки M^0, в якому r функцій з $\varphi_1,\varphi_2,...,\varphi_m$, похідні яких входять в визначник r-го порядку, який відрізняється від нуля в M^0, будуть незалежними, а інші будуть залежати від них [12], звідки при $r=m$ витікає висновок теореми.

3.2. Варіаційна матриця інформаційного процесу

Нехай тепер в області D вихідні параметри інформаційного процесу (функції φ_i, $i=\overline{1,m}$) можуть бути як залежними, так і незалежними. Для однаковості викладу всі параметри далі будемо позначати u_i, де $i=\overline{1,N}$, $N=n+m$ (для $i=\overline{1,n}$ u_i відповідають вхідним параметрам). Тоді реалізацію процесу можна формалізувати наступним чином:

$$u_k=F_k\left(u_{k_1},...,u_{k_{s_k}}\right),\quad n<k\le N,\ k_1,...,k_{s_k}<k, \tag{3.8}$$

де всі F_k є досить гладкими функціями своїх аргументів. Як результат процесу розглядається сукупність величин u_k (вихідні параметри). Не накладаючи серйозних обмежень, можна припускати, що результат — це величина u_N.

Співвідношення (3.8) визначають процес обчислення функції (3.2), що є загальною формалізацією інформаційного процесу:

$$\Phi(x_1,...,x_n)=(\Phi_1,\Phi_2,...,\Phi_m)^T,$$

чи в нових позначеннях

$$\Phi(u_1,...,u_n)=(u_{n+1},u_{n+2},...,u_N)^T. \qquad (3.9)$$

Якщо обчислення (3.9) спочатку задані за допомогою (3.8), то при великому N отримати явний вираз функції Φ (тобто функцій φ_i, $i=\overline{1,m}$) через вхідні дані ($u_i, i=\overline{1,n}$) важко й не завжди можливо. Для одержання достатньої умови такого представлення кожне рівняння системи (3.8) запишемо в еквівалентному виді:

$$F_k(u_{k_1},...,u_{k_{s_k}})-u_k = F_k(u_{k_1},...,u_{k_{s_k}})-u_k + 0\cdot\sum_{i\neq k,k_1,...,k_{s_k}} u_i = G_k(u_1,u_2,...,u_N)=$$

$$= G_k(x_1,...,x_n,\Phi_1,...,\Phi_m)=0$$

перетворивши (3.8) в еквівалентну систему рівнянь (у загальному випадку – нелінійну):

$$\begin{cases} G_1(x_1,...,x_n;\Phi_1,...,\Phi_m)=0,\\ G_2(x_1,...,x_n;\Phi_1,...,\Phi_m)=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ G_m(x_1,...,x_n,\Phi_1,...,\Phi_m)=0 \end{cases}. \qquad (3.10)$$

Якщо $G_i\in C^1(D)$, $i=\overline{1,m}$, де D — $n+m$-вимірний прямокутний паралелепіпед

$$D=[x_1^0-\Delta_1,x_1^0+\Delta_1]\times\ldots\times[x_n^0-\Delta_n,x_n^0+\Delta_n]\times[\Phi_1^0-\overline{\Delta}_1,\Phi_1^0+\overline{\Delta}_1]\times\ldots\times[\Phi_m^0-\overline{\Delta}_m,\Phi_m^0+\overline{\Delta}_m]$$

з центром в точці $(x_1^0,\ldots,x_n^0,\Phi_1^0,\ldots,\Phi_m^0)$, координати якої задовольняють системі (3.10), і визначник матриці Якобі для функцій G_i, $i=\overline{1,m}$, по змінним $\Phi_1,\ldots,\Phi_m$ відмінний від нуля, тобто

$$\det\begin{pmatrix} \frac{\partial G_1}{\partial \Phi_1} & \frac{\partial G_1}{\partial \Phi_2} & \cdots & \frac{\partial G_1}{\partial \Phi_m} \\ \frac{\partial G_2}{\partial \Phi_1} & \frac{\partial G_2}{\partial \Phi_2} & \cdots & \frac{\partial G_2}{\partial \Phi_m} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \frac{\partial G_m}{\partial \Phi_1} & \frac{\partial G_m}{\partial \Phi_2} & \cdots & \frac{\partial G_m}{\partial \Phi_m} \end{pmatrix} \neq 0,$$

тоді в деякому околі точки $\left(x_1^0,\ldots,x_n^0,\Phi_1^0,\ldots,\Phi_m^0\right)$ система (3.10) визначає $\Phi_1,\ldots,\Phi_m$ в виді (2.1), до того ж $\varphi_i \in C^1(D), \quad i=\overline{1,m}$.

Таким чином, інформаційний процес, який визначається за допомогою Φ, можна досліджувати через рекурентні співвідношення (3.8) [12,17]. Для цього система (2.8) для визначення величин u_k еквівалентно перетворюється:

$$F_k\left(u_{k_1},\ldots,u_{k_{s_k}}\right)-u_k=0\ ,\ \ n<k\le N;\ \ k_1,\ldots,k_{s_k}<k \qquad (3.11)$$

Аналіз інформаційного процесу (3.8) з метою встановлення його чутливості до збурних дій може бути формалізований за допомогою дослідження чутливості задачі про рішення системи (2.11). Для цього розглядається збурена система:

$$F_k\left(u_{k_1}+\Delta u_{k_1},\ldots,u_{k_{s_k}}+\Delta u_{k_{s_k}}\right)-\left(u_k+\Delta u_k\right)=0\ ,\ n<k\le N;\ \ k_1,\ldots,k_{s_k}<k \qquad (3.12)$$

де збурення Δu_k малі. Віднімаючи з (3.12) (3.11) і враховуючи представлення (3.4) для дійсної функції багатьох змінних, з точністю до нескінченно малих другого порядку, отримаємо систему лінійних алгебраїчних рівнянь відносно збурень Δu_k [12]:

$$\sum_{i=1}^{s_k}\frac{\partial F_k\left(u_{k_1},\ldots,u_{k_{s_k}}\right)}{\partial u_{k_i}}\ \Delta u_{k_i}-\Delta u_k=0\ , \qquad (3.13)$$

$$n<k\le N;\ \ k_1,\ldots,k_{s_k}<k$$

Матриця Ψ системи (3.13) — функціональна матриця Якобі функцій

$$y_k = F_k\left(u_{k_1},\ldots,u_{k_{s_k}}\right) - u_k = f_k(u_1,\ldots,u_N)$$

по змінним $u_1,\ldots,u_N$ розміром $m \times N$. Вона зазвичай сильно розріджена. Матриця Ψ має повний ранг, оскільки є нижньою трикутною відносно діагоналі, що проходить через правий нижній кут матриці, на діагоналі знаходяться елементи, які дорівнюють -1. Будемо називати Ψ *варіаційною матрицею інформаційного процесу* (ВМІП) (3.8). Її елементи ψ_{ij} у загальному випадку визначаються як

Варіаційна матриця відіграє важливу роль при аналізі структури й властивостей інформаційного процесу, зокрема, при дослідженні його міри чутливості до збурних дій (похибок вхідних даних).

$$\psi_{ij} = \begin{cases} -1, & \textit{якщо} \quad j = i+n, \\ \dfrac{\partial F_{i+n}}{\partial u_j}, & \textit{якщо} \quad j \ \textit{є одним з чисел} \ (i+n)_1,\ldots,(i+n)_{s_{i+n}} \\ 0, & \textit{в інших випадках} \end{cases}.$$

Як уже було відзначене, при визначенні $v = F(u)$ в реальних умовах точне значення v, загалом кажучи, отримати не можна. Замість v буде отриманий елемент $\bar{v} \neq v$. При проведенні прямого аналізу похибки [15,17], результатом якого є оцінка $\left\|\bar{v} - v\right\|$, стає зрозумілим, що якщо така оцінка виявиться великою, це може бути пов'язане з нестійкістю оператора F в околі u. У такій ситуації добре зарекомендував себе зворотний аналіз похибок [15,17], основна ідея якого полягає в спробі представити реально отриманий елемент $\bar{v}$ як точний результат перетворення F, але не елемента u, а елемента $\bar{u} \neq u$: $\bar{v} = F(\bar{u})$. Про це вже йшла мова вище. Якщо це вдається зробити, то вплив збурних дій оцінюється величиною $\left\|\bar{u} - u\right\|$, а $\bar{u} - u$ називається *еквівалентним збуренням*.

Розглянемо процес поширення похибок під час протікання інформаційного процесу (3.8), реалізація якого зводиться до обчислення функції (3.9) [12]. При реальних обчисленнях точних формул (3.8) мають місце співвідношення:

$$\bar{u}_k = \bar{F}_k\left(\bar{u}_{k_1},\ldots,\bar{u}_{k_{s_k}}\right), \quad n < k \le N, \ k_1,\ldots,k_{s_k} < k,$$

$$\Updownarrow \qquad (3.14)$$

$$\bar{u}_k = F_k\left(\bar{u}_{k_1},\ldots,\bar{u}_{k_{s_k}}\right) + \eta_k, \quad n < k \le N, \ k_1,\ldots,k_{s_k} < k,$$

де $\overline{F}_k$ — збурена «близька» до F_k функція, реальне обчислення якої здійснюється при реалізації інформаційного процесу (3.8), $\bar{u}_k$ — реально задана або обчислена величина u_k, η_k — еквівалентна абсолютна похибка (підсумковий результат збурної дії), яка вноситься в результат обчислення F_k.

Представимо (3.14) в виді:

$$\overline{u}_k+\varepsilon_k = F_k\left(\overline{u}_{k_1}+\varepsilon_{k_1},\ldots,\overline{u}_{k_{s_k}}+\varepsilon_{k_{s_k}}\right),\quad n<k\le N,\ k_1,\ldots,k_{s_k}<k, \qquad (3.15)$$

де ε_k — збурення $\bar{u}_k$ (ці збурення вносяться й у вхідні дані). Якщо взяти збурені вхідні дані $u_1+\varepsilon_1,\ldots,u_n+\varepsilon_n$ і провести з ними точний процес (3.8), то на кожному кроці цього процесу як точний результат виходить $\bar{u}_k+\varepsilon_k$.

Сукупність значень ε_k, в якій еквівалентні збурення вхідних даних дорівнюють 0, описує прямий аналіз похибок. Якщо в множині ε_k еквівалентні збурення вихідних даних дорівнюють 0, то маємо зворотний аналіз похибок. Інші варіанти ε_k описують мішаний аналіз похибок [12].

З (3.14), (3.15) отримуємо

$$\varepsilon_k = F_k\left(\overline{u}_{k_1}+\varepsilon_{k_1},\ldots,\overline{u}_{k_{s_k}}+\varepsilon_{k_{s_k}}\right)-F_k\left(\overline{u}_{k_1},\ldots,\overline{u}_{k_{s_k}}\right)-\eta_k,\ n<k\le N,\ k_1,\ldots,k_{s_k}<k. \qquad (3.16)$$

Якщо збурення вхідних даних $\varepsilon_1,\ldots,\varepsilon_n$ відомі, то за допомогою (3.16) можна визначити інші збурення $\varepsilon_k, k>n$ (значення u_k, збурення η_k визначаються реалізацією інформаційного процесу (3.14)), що дасть можливість для встановлення міри чутливості процесу до похибок вхідних даних (до збурних дій). Розглянемо (3.16) докладно.

Система (3.16) в загальному випадку є нелінійної відносно ε_k. Враховуючи представлення (3.4) для дійсної функції багатьох змінних, (3.16) можна замінити лінійною системою:

$$\varepsilon_k = \sum_{i=1}^{s_k}\frac{\partial F_k\left(\overline{u}_{k_1},\ldots,\overline{u}_{k_{s_k}}\right)}{\partial u_{k_i}}\varepsilon_{k_i}-\eta_k,\quad n<k\le N,\ k_1,\ldots,k_{s_k}<k,$$

Замінимо реально обчислені величини $\bar{u}_i, i=k_1,\ldots,k_{sk}$, на точні:

$$\sum_{i=1}^{s_k} \frac{\partial F_k\left(u_{k_1},\ldots,u_{k_{s_k}}\right)}{\partial u_{k_i}} \varepsilon_{k_i} - \varepsilon_k = \eta_k\,, \quad n < k \le N,\ k_1,\ldots,k_{s_k} < k \qquad (3.17)$$

Матриця системи (3.17) — це ВМІП (3.8), тому система завжди сумісна. Таким чином, величини збурень ε_k визначаються як рішення системи лінійних алгебраїчних рівнянь (3.17), властивості якої визначаються властивостями ВМІП.

Оскільки ε_k використовуються для аналізу інформаційного процеса з метою встановлення його чутливості до збурних дій, важливо, щоб ці значення були отримані якнайточніше, для чого матриця системи (3.17) — ВМІП (3.8) — повинна бути добре обумовленої.

ВМІП відіграє важливу роль не тільки при аналізі збурень параметрів, що визначають інформаційний процес.

3.3. Граф інформаційного процесу і його особливості

Довільному інформаційному процесу поставимо у відповідність орієнтований граф (орграф) наступним чином. Зіставимо k-й вершині графа отримання величини u_k. Перші n вершин будуть символізувати введення початкових даних $u_1,\ldots,u_n$ і називатися вхідними, а інші вершини — обчислення u_k як значень функцій F_k з (3.8). Будемо вважати, що дуга йде з i-ї вершини в j-у тоді й тільки тоді, коли при обчисленні величини u_j величина u_i використовується як аргумент. Відповідно до (3.8) дуги не будуть входити в k-у вершину, якщо $k \le n$. Якщо $k > n$, то в k-у вершину будуть входити дуги з вершин з номерами $k_1,\ldots,k_{sk}$.

Будемо називати орграф *дводольним*, якщо множина його вершин V може бути розбита на дві підмножини V_1 і V_2 так, що кожне ребро графа є впорядкованою парою виду $< v_1, v_2 >$, де $v_1 \in V_1$, а $v_2 \in V_2$.

Зі способу побудови графа стає очевидною істинність наступних тверджень.

Твердження 3.1. Граф інформаційного процесу є ациклічним.

Теорема 3.2. Вихідні параметри інформаційного процесу будуть незалежними тоді й тільки тоді, коли граф інформаційного процесу буде дводольним.

В графі, як моделі інформаційного процесу, наочно представлені відомості про те, як окремі перетворення при протіканні процесу пов'язані між собою

інформаційно, які перетворення в ході їх моделювання можуть виконуватися одночасно, які потрібно виконувати пізніше або раніше, чим інші і т.д. Граф інформаційного процесу описує всю картину поширення інформації при його протіканні, а тому може бути використаний для аналізу інформаційного процесу в цілому, його структури.

Отриманому графу ставиться в співвідношення матриця Ф розміром $m \times N$ з елементами φ_{ij}:

$$\varphi_{ij} = \begin{cases} -1, & \text{якщо } j = i + n, \\ 1, & \text{якщо } j \text{ є одним з чисел } (i+n)_1, \ldots, (i+n)_{s_{i+n}}, \\ 0, & \text{в інших випадках} \end{cases}.$$

Очевидно, k-ий стовпець матриці Ф відповідає параметру u_k, а k-ий рядок — параметру u_{k+n}. В k-ому рядку елемент -1 знаходиться в тому стовпці, номер якого відповідає номеру параметра, що обчислюється — u_{k+n}. Елементи +1 знаходяться у тих стовпцях, номери яких відповідають номерам аргументів параметра, що обчислюється — u_{k+n}. Матриця Ф описує зв'язок параметрів u_k між собою і називається *матрицею інформаційної зв'язності* інформаційного процесу (МІЗІП) (3.8). Очевидний зв'язок матриці зв'язності з ВМІП: структури ненульових елементів обох матриць повністю співпадають.

Для графа інформаційного процесу по МІЗІП заміною ненульових елементів якимись числами можна отримати нескінченну сукупність матриць, кожна з яких є *зваженою* МІЗІП. Будь-яка зважена МІЗІП, окремим випадком якої є й ВМІП, дозволяє однозначно відновити граф інформаційного процесу, а тому може використовуватися для його аналізу.

Для орієнтованого графа, що відповідає інформаційному процесу, стандартно визначається $N \times N$-матриця суміжності B з елементами b_{ij}

$$b_{ij} = \begin{cases} 1, & \text{якщо з } i-\text{ої вершини в } j-\text{у йде ребро}, \\ 0, & \text{в інших випадках} \end{cases},$$

і матриця інцидентності A з елементами a_{ij}

$$a_{ij} = \begin{cases} 1, & \text{якщо } j-е \text{ ребро виходить з } i-\text{ої вершини} \\ -1, & \text{якщо } j-е \text{ ребро входить в } i-\text{у вершину.} \\ 0, & \text{в інших випадках} \end{cases},$$

Матриця B тісно пов'язана з МІЗІП Φ: Φ — підматриця, яка складається з останніх m рядків матриці $B^T - I$, де I — одинична матриця відповідного розміру. У зв'язку з цим для приведення МІЗІП до більш «придатного» з погляду можливостей її обробки виду за рахунок перенумерації рядків і стовпців можна здійснювати відповідну перенумерацію для матриці суміжності.

До значного зменшення часових витрат, необхідних для дослідження властивостей інформаційного процесу, приводить виявлення й наступне використання його внутрішнього паралелізму на основі відповідного графа [12,17], тобто можливостей паралельного (одночасного) виконання вхідних до інформаційного процесу операцій.

3.4. Паралельні форми інформаційного процесу

Поява паралельних обчислювальних систем і впровадження їх у практику рішення великих прикладних задач привела до необхідності аналізу інформаційних процесів з метою визначення можливості їх математичної формалізації й обробки в паралельних обчислювальних системах. Результатом аналізу повинне стати виявлення таких частин процесу, які інформаційно між собою не пов'язані. Якщо такі частини знайдені, будемо говорити, що інформаційному процесу властивий *внутрішній паралелізм*.

Будемо використовувати граф $G = (V, E)$ інформаційного процесу, де V – множина вершин, а E – множина впорядкованих пар вершин (ребер), для аналізу його структури, не накладаючи ніяких обмежень на вид вхідних і вихідних параметрів. Граф інформаційного процесу не накладає, загалом кажучи, ніяких обмежень і на порядок виконання операцій, що входять до складу процесу, крім одного: до моменту початку реалізації будь-якої операції повинні закінчити своє виконання всі ті операції, які поставляють для неї параметри-аргументи. Таким чином граф інформаційного процесу визначає множину припустимих порядків виконання його операцій.

Будь-який інформаційний процес – це процес, що протікає в часі, будь-яка його реалізація породжує певне сортування вхідних до його складу операцій. Це сортування будує розбивку множини операцій (вершин відповідного графа) на

такі групи, які виконуються послідовно, а операції всередині групи можуть виконуватися одночасно.

Ототожнюючи інформаційний процес з його графом, будемо припускати, що в графі відображені операції отримання всіх параметрів і зв'язки, вплив яких на реалізацію процесу підлягає вивченню.

Нехай $G=(V,E)$ — довільний орієнтований ациклічний граф з n вершинами. Тоді [12] існує таке натуральне число $s \le n$, що всі вершини графа можна так помітити одним з індексів $1,2,...,s$, що якщо ребро йде з вершини з індексом i в вершину з індексом j, то

$$i < j . \qquad (3.18)$$

Така розмітка вершин називається *топологічним сортуванням* графа або *паралельною формою*. Очевидно, що ніякі дві вершини з однаковим індексом не є суміжними. Крім того, для будь-якого натурального $s \le n$, більшого довжини критичного шляху, існує топологічне сортування, при якому використовуються всі s індексів, тобто граф має не єдине топологічне сортування.

Якщо співвідношення (3.18) замінити на $i \le j$, то отримане сортування буде називатися *узагальненим топологічним сортуванням*.

Результатом топологічного сортування є виявлення можливостей паралельного (одночасного) виконання (аналізу) вхідних в інформаційний процес операцій. Ці операції будуть входити в одну групу сортування, яка називається *ярусом паралельної форми*. Сукупність всіх топологічних сортувань графа інформаційного процесу визначає його паралельні форми реалізації (обробки, аналізу). Операції, відповідні до вершин графа одного рівня топологічного сортування, є інформаційно незалежними, а тому можуть виконуватися паралельно. Групи операцій, що відповідають різним топологічним рівням, виконуються послідовно в порядку зростання номерів вершин графа, що входять у них.

Як правило, чим складніше граф, чим більший його розмір, тим важче побудувати його топологічне сортування. Зменшення необхідного часу для цього процесу може бути досягнуте за рахунок розбивки графа на підграфи меншого розміру з наступною побудовою топологічних сортувань підграфів і відновленням сортування всього графа по сортуваннях підграфів [12] (відповідний алгоритм наведено в додатку 3). Крім того, для скорочення часу для аналізу інформаційного процесу зменшити розмір графа можна за допомогою гомоморфної згортки його підграфів.

За допомогою перенумерації вершин графа інформаційного процесу можна спростити його опис. Отже, шляхом перенумерації операцій (3.8) можна спробувати привести МІЗІП і відповідно ВМІП до більш зручного виду.

Розглянемо довільне топологічне сортування вершин графа інформаційного процесу. Позначимо вершини наступним чином: спочатку нумеруються вершини, що потрапили в перший ярус, потім у другий і т.д., визначаючи тим самим порядок рядків МІЗІП. При впорядкуванні стовпців спочатку нумеруються стовпці, які відповідають аргументам F_1, потім стовпці, що відповідають лише тим аргументам F_2, які ще не були занумеровані, і т.д. При цьому нова нумерація стовпців, відповідних до обчислюваних величин, береться такою, щоб з точністю до викидання стовпців, відповідних до вхідних параметрів, вона збігалася з новою нумерацією рядків. Після описаного переставлення рядків і стовпців МІЗІП буде мати вигляд, представлений на рис.3.1. В кожному рядку P_i існує хоча б один ненульовий елемент, і всі її ненульові елементи дорівнюють 1. В кожному рядку зафарбованої частини знаходиться лише один ненульовий елемент — -1.

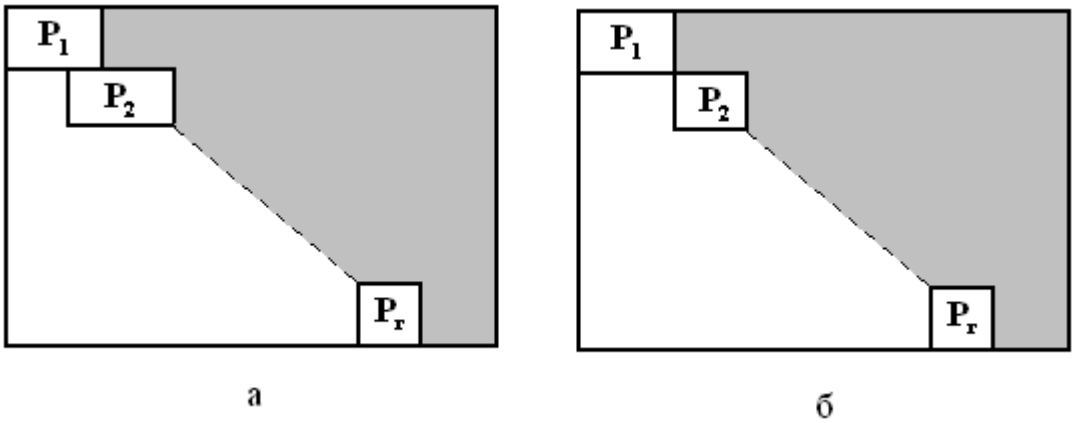


Рис.3.1. Структура МІЗІП, коли в інформаційному процесі розмноження інформації присутнє (а); відсутнє (б)

У загальному випадку в кожному стовпці МІЗІП може знаходитися більш однієї одиниці: в l-ому стовпці буде m_l одиниць, якщо m_l операцій, що входять в інформаційний процес, використовують параметр u_l як один з своїх аргументів, тобто якісь ребра, що виходять з деяких вершин графа інформаційного процесу, визначають перенесення одної інформації. У цьому випадку будемо говорити, що має місце *розмноження інформації*. Якщо розмноження інформації присутнє в інформаційному процесі, то деякі стовпці МІЗІП можуть мати непусті перетинання більш ніж з одним рядком. При будь-якому переставленні рядків і стовпців ця властивість зберігається. Отже, описані вище переставлення приведуть МІЗІП до виду, зображеного на рис.3.1(а), інакше її вид представлений на рис.3.1(б).

Для формалізації аналізу інформаційного процесу у відповідність його графу можна поставити не тільки одну з розглянутих вище двовимірних матриць, але й одновимірний вектор.

Однієї з характеристик протікання інформаційного процесу є час його виконання. При безпосередній реалізації визначені моменти виконання всіх операцій (3.8). Порушення певного часу виконання деякої операції в ході процесу є сигналом можливих збоїв, атак, спрямованих на засоби захисту, що забезпечують протікання процесу, і т.п.

Перенумеруємо вершини графа інформаційного процесу довільно й кожній i-й вершині поставимо в співвідношення час t_i закінчення виконання відповідної операції. Таким чином, з інформаційним процесом можна зв'язати вектор $t=(t_1,t_2,...,t_n)^T$, який будемо називати *вектором часового розгортання* процесу [12], який показує, як протікає процес у часі. Для елементів вектору t природно визначити деякі обмеження, наприклад, задати час h_j для реалізації j-ї операції. Якщо в графі інформаційного процесу існує ребро, що йде з i-ї вершини в j-у, то повинне виконуватися співвідношення: $t_j - t_i \geq h_j$.

Дійсно, час, що проходить від закінчення i-ї операції до закінчення j-ї, містить у собі не тільки час виконання j-ї операції, але й час, який затрачується на передачу інформації, необхідної для виконання j-ї операції. Невід'ємний вектор $h=(h_1,h_2,...,h_n)^T$ будемо називати *вектором реалізації інформаційного процесу*.

З кожним ребром графа можна зв'язати не тільки якусь інформацію, що передається від однієї вершини до іншої. Будь-яке часове розгортання однозначно визначає час t_i появи цієї інформації й час $t_j - t_i$ її існування, частково в незмінному, частково в перетвореному в j-й вершині виді. Можна вважати, що в момент t_j стара інформація повністю закінчує своє існування й народжується нова. Час $t_j - t_i$ — *час затримки інформації на дузі*, яка пов'язує i-у і j-у вершини. При реалізації інформаційних процесів на часи затримок накладаються обмеження знизу. Вони спричиняються часом передачі інформації по каналах і лініях зв'язку, часом зберігання інформації й іншими факторами. Ці обмеження можна задавати аксіоматично й вважати, що час затримки інформації на дузі, що зв'язує i-у і j-у вершини, не менше невід'ємного числа w_{ij}:

$$t_j - t_i \geq w_{ij}.$$

Вектор w з координатами w_{ij} називається *вектором затримок*.

Нехай інформаційний процес починає свою реалізацію в нульовий момент часу, і в кожний додатний цілочисловий момент виконується хоча б одна операція (3.8). Розглянемо відповідне часове розгортання. Згідно з розгортанням множина вершин графа розбивається на неперетинні підмножини, де в одну підмножину входять ті й тільки ті вершини, які відповідають операціям, що

виконуються одночасно. Кожній з побудованих підмножин приписується індекс, що дорівнює моменту виконання відповідних операцій. Очевидно, що отримана розбивка вершин графа інформаційного процесу визначає деяку паралельну форму його протікання. Вірно й те, що будь-яка паралельна форма інформаційного процесу породжує деяке часове розгортання.

Таким чином, очевидно, що аналіз часових розгортань є перспективним напрямком в галузі досліджень інформаційних процесів.

3.5. Введення у функціональне дослідження структури інформаційного процесу.

Представлення часових розгортань інформаційного процесу у вигляді векторів відповідає математичній формалізації процесу в виді (3.8), де виконувані операції ідентифікуються одним цілим параметром. Така ідентифікація при практичнім використанні (3.8) приводить до значних незручностей і труднощів.

Будемо вважати вершини графа інформаційного процесу точками скінченновимірного простору (з можливою в деякому розумінні «зручною» цілочисловою (хоча це необов'язково) фіксацією координат). Множина вершин буде знаходитися в деякій області D, а часові розгортання можна розглядати як функції, визначені на множині точок-вершин. Таким чином, якщо задане часове розгортання, то кожній з точок-вершин x ставиться у відповідність число, яке дорівнює часу виконання відповідної операції, тобто часове розгортання — це деяка функція

$$t(x) : D_d \to K, \tag{3.19}$$

де D_d — область визначення, що є дискретною множиною точок x з області D, $K \subseteq Z$ — область значень — дискретна множина, де Z — множина цілих чисел. Часові розгортання, представлені в такому виді, будемо називати *просторово-часовими*.

Будь-яка паралельна форма інформаційного процесу визначає деяку множину часових розгортань. При завданні розгортання у вигляді (3.19) яруси паралельної форми будуть мати явний геометричний зміст: вони визначаються поверхнями рівня (визначення 3.14) для $t(x)$ —

$$t(x) = const. \tag{3.20}$$

Дійсно, нехай множина точок (3.20) містить якісь вершини графа інформаційного процесу. Тоді відповідні вершинам операції виконуються в один момент, тобто утворюють ярус паралельної форми.

Для зручності подальшого аналізу, не обмежуючи значно спільності міркувань, продовжимо яким-небудь прийнятним способом просторово-часові розгортання (3.19) на всю область D. Позначимо відповідні функції $t_D(x)$. Будемо вважати, що функції $t_D(x)$ мають необхідну гладкість.

Нехай D — однозв'язна область. Поверхні рівня $t_D(x) = const$ можуть бути як одно- так і многозв'язними (рис.3.2 — цифрами відзначені поверхні рівнів, відповідні до послідовних значень t), однак, завдяки припущенням про

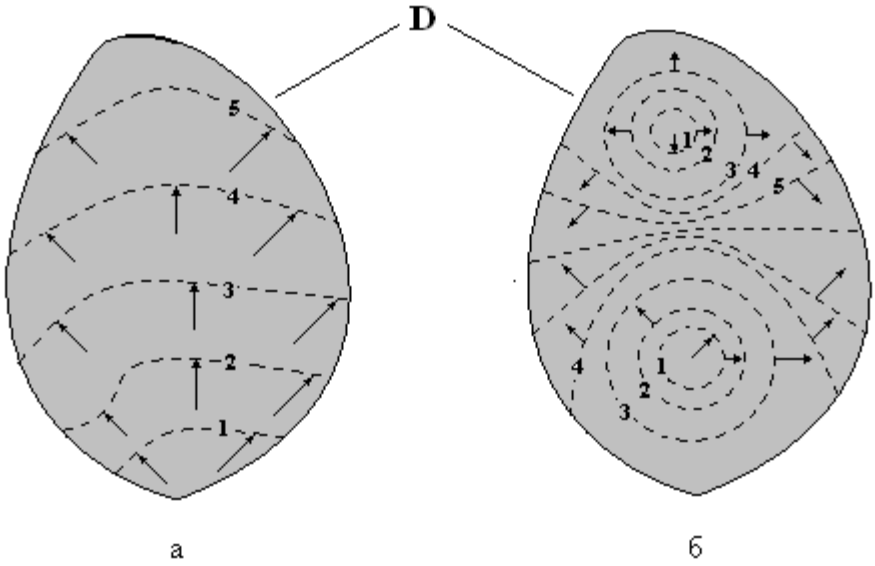


Рис.3.2. Системи поверхонь рівня: однозв'язні (а); многозв'язні (б)

гладкість функцій $t_D(x)$, з зміною t вони змінюються неперервно, тому по один бік від них завжди будуть знаходитися вершини, відповідні до операцій, що виконуються до часу t, а по інший — вершини, відповідні до операцій, що виконуються після часу t. Тоді перенесення інформації від вершин однієї групи до вершин іншої групи здійснюється лише тими ребрами графа інформаційного процесу, які для будь-якої поверхні рівня просторово-часового розгортання визначають орієнтований розріз графа процесу [12]. Поверхні рівнів показують розподіл потоків інформації в D.

Таким чином, опис паралельних форм інформаційного процесу зводиться до опису поверхонь рівня просторово-часових розгортань і дослідженню функцій, що їх визначають, і накреслює новий напрямок в області аналізу інформаційних процесів.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

3.1 Коли дійсні функції, що формалізують інформаційний процес, називаються залежними, незалежними?

3.2 Коли вихідні параметри інформаційного процесу будуть незалежними (залежними)?

3.3 За рахунок чого у випадку незалежності вихідних параметрів можна значно скоротити час реалізації й аналізу інформаційного процесу?

3.4 Як визначається матриця Якобі для неперервного інформаційного процесу?

3.5 Що є достатньою умовою незалежності вихідних параметрів неперервного інформаційного процесу?

3.6 Що таке варіаційна матриця інформаційного процесу? Яку роль при аналізі структури й властивостей інформаційного процесу відіграє варіаційна матриця?

3.7 Як варіаційна матриця інформаційного процесу пов'язана із чутливістю процесу до збурних дій?

3.8 Як інформаційному процесу можна поставити у відповідність орієнтований граф?

3.9 Які властивості має орієнтований граф, що відповідає інформаційному процесу? Що описує граф інформаційного процесу?

3.10 Критерій незалежності вихідних параметрів інформаційного процесу.

3.11 Що називається матрицею інформаційної зв’язності інформаційного процесу?

3.12 Як пов'язані між собою матриця інформаційної зв’язності й варіаційна матриця інформаційного процесу?

3.13 Чи можна по зваженій матриці інформаційної зв’язності однозначно відновити граф інформаційного процесу?

3.14 Коли інформаційному процесу властивий внутрішній паралелізм?

3.15 Які обмеження накладає на порядок виконання операцій, що входять до складу інформаційного процесу, граф процесу?

3.16 Що називається топологічним (узагальненим топологічним) сортуванням, або паралельною формою, графа інформаційного процесу? Що є результатом топологічного сортування?

3.17 Яка сукупність операцій інформаційного процесу називається ярусом паралельної форми?

3.18 За рахунок чого може бути досягнуте зменшення необхідного часу для побудови топологічного сортування графа інформаційного процесу?

3.19 Що називається вектором часового розгортання інформаційного процесу? Про що свідчить порушення певного часу виконання деякої операції в ході протікання процесу?

3.20 Який вектор називається вектором реалізації інформаційного процесу? Вектором затримок?

РОЗДІЛ 4. НЕОБХІДНІСТЬ КІБЕРЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ

4.1. Класифікація цілей кіберзахисту

Загальна класифікація цілей кіберзахисту інформації наведена на рис. 4.1 [12,19]. Аналіз класифікації показує, що друга мета захисту – попередження несанкціонованої модифікації інформації – в значній мірі є деякою комбінацією першої і третьої цілей. Дійсно, несанкціонована модифікація може бути випадковою або злочинною. Випадкова модифікація може бути наслідком перекручування деякої інформації. Злочинна ж модифікація є результатом злочинних дій.

Рис. 4.1. Загальна класифікація цілей кіберзахисту

Об’єктами захисту *є* [12,13,20]*:*

Вихідні дані, тобто дані, що надійшли від користувачів або абонентів.

Довільні дані, тобто дані, отримані в процесі обробки вихідних даних.

Нормативно-довідкові, службові і допоміжні дані, також дані системи захисту.

Постановка завдань та методів. Моделі, алгоритми і програми, які використовуються при обробці даних.

Технічна, технологічна, політична, військова й економічна документації.

Кіберзахист інформації повинен здійснюватися в таких зонах:

зона ресурсів, тобто зона функціонуючих технічних засобів;

зона помешкань, тобто сукупність помешкань, у яких розташовані технічні засоби і розміщуються люди, що мають відношення до них;

зона території, що охороняється, тобто та частина території, на якій розташовані будинки з зоною помешкань і на якій може повністю регулюватися доступ людей, а також можуть регулюватися і контролюватися всі дії і заходи, здійснювані на ній;

зона, що не охороняється, але контрольована територія, тобто та частина зовнішньої території, в якій може здійснюватися регулярний контроль її стану і зроблених на ній дій;

зовнішня зона, тобто та частина території, на якій можуть

здійснюватися дії і відбуватися події, що впливають на надійність інформації, тобто інформація, яка не може бути під постійним контролем.

Об'єктивна необхідність КЗ на сучасному етапі і при тій комплексно-системній постановці, як це сформульовано, обумовлена тими застосуваннями принципової значимості, що сталися в нижченаведених напрямках.

У концепціях застосування обчислювальної техніки в різноманітних сферах діяльності.

У розвитку самої обчислювальної техніки і її програмного забезпечення, а також у концепціях організації і використання ресурсів обчислювальної техніки.

У розвитку радіоелектроніки і елементної бази, що дозволило створити високоефективні засоби радіоелектронної розвідки.

Основні зміни в розвитку обчислювальної техніки і її програмне забезпечення можуть бути охарактеризовані таким чином:

Розширення типів ЕОМ, що випускаються.

Масовий випуск персональних ЕОМ.

Розширення номенклатури зовнішніх пристроїв.

Різке розширення об'єктів КЗ прямого доступу.

Масовий випуск машинних носіїв інформації великого обсягу персонального і групового використання – магнітних дисків.

Різке зниження об'ємів апаратури обчислювальної техніки за рахунок мікромініатюризації електронних пристроїв.

Різкий розвиток єдиного програмного забезпечення, призначеного для забезпечення програмування, забезпечення функціонування технічних засобів і виконання інших функцій.

Інтенсивний розвиток системного програмного забезпечення, призначеного для організації і забезпечення функціонування інформаційно-обчислювальних систем і мереж, також й автоматизованої передачі даних по мережах.

Інтенсивний розвиток і повсюдне впровадження систем управління базами даних, призначених для централізованого накопичення і збереження

великих масивів даних, пошуку і видачі їх користувачам та іншим, розв'язуваним у системі завданням.

Інтенсивний розвиток пакетів прикладних програм, що істотно полегшує розробку завдань функціональної обробки інформації.

Інтенсивний розвиток і удосконалювання засобів візуалізації, що розширює можливості і полегшує умови використання обчислювальної техніки.

Для сучасних концепцій організації і використання ресурсів обчислювальної техніки характерними є такі особливості [12,20,21]:

створення потужних обчислювальних центрів колективного користування (ОЦКК), призначених для промислової переробки інформації;тенденції об'єднання ОЦКК мережею передачі даних у мережу ОЦКК є прологом створення в державі організованої індустрії переробки інформації;

масове застосування автоматизованих робочих місць (АРМ), створюваних шляхом безпосереднього оснащення робочих місць засобами обчислювальної техніки;

значне поширення абонентських пунктів різноманітного призначення й інформаційно-обчислювальних пунктів групового використання оснащених малими і середніми ЕОМ;

об'єднання АРМ у локальні інформаційно-обчислювальні мережі;

поєднання АРМ, абонентських пунктів, групових інформаційно-обчислювальних пунктів і локальних мереж із ОЦКК і мережами ОЦКК.

Серйозні зміни, що мають принципове значення, відбуваються в концепціях застосування обчислювальної техніки в сфері управління. Причому, упровадження систем комплексної автоматизації породжує ряд проблем, пов'язаних із забезпеченням високої якості інформації, і, насамперед, її надійності в тій інтерпретації поняття надійності. Неважко помітити, що при реалізації комплексних АСУ характерними і типовими стають нижченаведені особливості [12,14]:

Все більша питома вага автоматизованих процедур у загальному обсязі процесів обробки інформації.

Всезростаюча важливість і відповідальність рішень, прийнятих в автоматизованому режимі і на основі автоматизованої обробки інформації.

Велика і всезростаюча концентрація в автоматизованих системах обробки даних (АСОД) інформаційно-обчислювальних ресурсів.

Велика територіальна поширеність компонентів АСОД і АСУ.

Складні режими функціонування технічних засобів АСОД.

Накопичення на технічних носіях величезних обсягів інформації, причому для багатьох видів цієї інформації усе більш важким стає виготовлення немашинних аналогів.

Інтенсивна циркуляція інформації між компонентами АСУ, у тому числі і розташованих на великих відстанях один від одного.

Інтеграція в єдиних базах даних інформації різноманітного призначення і різноманітної належності.

Довгострокове збереження великих масивів інформації на машинних носіях.

Безпосередній і одночасний доступ до ресурсів (у тому числі і до інформації) великої кількості користувачів різноманітних категорій і різноманітної належності.

Всезростаюча вартість ресурсів АСОД і АСУ.

У цих умовах різко зростає уразливість інформації, тобто її схильність до впливу різноманітних дестабілізувальних факторів, що може виявлятися в зниженні якості інформації. Результатом же зниження якості інформації буде висока ймовірність великомасштабних наслідків негативного характеру.

Оскільки інформаційні технології в основних сферах діяльності суспільства усе більше і більше стають автоматизованими, то зниження якості інформації в сучасних АСОД неминуче призведе до зниження ефективності відповідних сфер діяльності. Іншими словами, якість інформації в АСОД прямо і безпосередньо переноситься на якість функціонування тих сфер діяльності, в інтересах яких обробляється інформація.

Через те, що на машинних носіях накопичуються величезні масиви інформації, то порушення фізичної цілісності може призвести до великих втрат, а оскільки для дуже великих обсягів інформації усе меншими стають можливості створення і підтримки немашинних її аналогів, то й відновити порушену цілісність буде усе більш важкою і дорогою справою. Крім того, оскільки сучасні АСОД стають усе більш територіально розподіленими, обслуговують велику кількість різноманітних користувачів, функціонують у складних режимах, що різко збільшує можливості несанкціонованої модифікації і несанкціонованого одержання інформації, у тому числі й у злочинних цілях.

Отже, для забезпечення необхідної якості інформації повинні застосовуватися спеціальні заходи. Тобто, захист інформації об’єктивно набуває характеру завдання підвищеної актуальності.

Об’єктивні передумови вирішення проблеми ЗІ створюються нижчевказаними обставинами [14,16].

По-перше, до теперішнього часу практично повсюдно усвідомлена необхідність кіберзахисту.

По-друге, зараз вже розроблено достатньо розвинений арсенал засобів кіберзахисту.

По-третє, вже зараз накопичено деякий досвід з організації кіберзахисту.

4.2. Основні положення концепції кіберзахисту

У поняття системного підходу до КЗ входять такі положення [1,2,12,16]:

Дослідження і розробка з єдиних методологічних понять усієї сукупності питань, пов'язаних із КЗ.

Розгляд у єдиному комплексі усіх видів кіберзахисту інформації; забезпечення фізичної цілісності; попередження несанкціонованої модифікації, попередження несанкціонованого одержання.

Системне врахування всіх факторів, які впливають на захищеність інформації.

Комплексне використання всіх наявних засобів КЗ.

Концептуальність підходу означає, що вирішення всіх питань ЗІ здійснюється в рамках єдиної концепції, що об'єднує найбільш раціональним способом всі системні рішення захисту.

Центральним результатом, отриманим у рамках системно-концептуального підходу до проблеми захисту інформації, є висновок, що ефективний КЗ не може бути забезпечений простим застосуванням деяких механізмів роботи. КЗ необхідно управляти.

Управління КЗ являє собою складну сукупність взаємозалежних процесів безперервного створення й удосконалення механізмів КЗ. При цьому істотно важливою є та обставина, що зазначені питання повинні бути регулярними, тобто постійно керованими, причому управління повинне здійснюватися з метою досягнення необхідного рівня захисту при мінімальних затратах сил або з метою досягнення максимального рівня кіберзахисту при заданих затратах сил і засобів.

На підставі методології системно-концептуального підходу розглянемо узагальнену структуру уніфікованої концепції КЗ.

Конструктивними елементами концепції є функції, завдання, засоби і системи захисту.

Функція кіберзахисту – сукупність однорідних у функціональному відношенні заходів, регулярно здійснюваних з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного КЗ [7,9].

Засоби кіберзахисту – пристрої, програми та заходи, спеціально призначені для вирішення завдань кіберзахисту інформації.

Завдання кіберзахисту – організовані можливості засобів, методів і заходів з метою реалізації функцій кіберзахисту.

Система ЗІ – організована сукупність усіх засобів, методів і заходів, що передбачаються з метою КЗ.

Перераховані елементи концепції складають логічну і повну послідовність рішень, реалізація яких і створює об'єктивні передумови для надійного КЗ.

У суворій відповідності з основною передумовою про необхідність регулярного управління процесами КЗ, всі елементи зазначеної послідовності розділені на дві частини: створення механізмів захисту й управління механізмами захисту.

Важливим результатом системно-концептуального підходу до розглянутої проблеми є висновок про неможливість надійного ЗІ без дотримання при побудові цілого ряду достатньо специфічних умов. Ці умови повинні дотримуватися в процесі створення і функціонування інформації, в силу чого в концепції вони виступають як зворотний зв'язок від конструктивних елементів концепції захисту до концепцій побудови й організації функціонування інформації.

Дослідження в рамках системно-концептуального підходу до ЗІ показують, що концепція є уніфікованою в тому, що на її основі може бути реалізована раціональна система управління ЗІ практично будь-якої інформації. Для цього необхідно [7,8,9]:

Уніфікувати основні положення концепції ЗІ.

Вирішити організаційно-правові питання організації робіт зі створення систем захисту, організації і забезпечення їх функціонування.

Розробити робочий інструмент для створення організації і забезпечення систем ЗІ.

4.3. Визначення та аналіз поняття загрозикіберзахисту інформації

Під загрозою **інформації** будемо розуміти засіб виникнення на якому-небудь етапі життєдіяльності інформації такого явища або події, наслідком якого можуть бути небажані впливи на неї: порушення (або небезпека порушення) фізичної цілісності, несанкціонована модифікація (або загрози такої модифікації), несанкціоноване одержання (або загрози такого одержання) інформації. Ті чинники, наслідком яких можуть бути зазначені впливи на інформацію, назовемо дестабілізуючими.

Відповідно до технології і функціонування інформації, фактори або типи дестабілізуючими чинників такі [13,16]:

Кількісна недостатність.

Якісна недостатність.

Відмова.

Збої.

Помилки.

Стихійні лиха.

Побічні явища.

Названі типи дестабілізуючих чинників визначаються так [13,14]:

Кількісна недостатність – фізична недостача одного або декількох технічних компонентів для забезпечення необхідної КЗ інформації з розглянутих показників.

Якісна недостатність – недосконаліть конструкції або організації одного або декількох компонентів, у силу чого не забезпечується необхідний КЗ.

Відмова – порушення працездатності елемента, що призводить до неможливості виконання ним своїх функцій.

Збій – тимчасове порушення працездатності якогось елемента, наслідком чого може бути неправильне виконання ним у цей момент своїх функцій.

Стихійне лихо – спонтанно виникаюче неконтрольоване явище.

Злочинна дія – дія людей, спеціально спрямована на порушення КЗ інформації.

Помилка – неправильне (одноразове або систематичне) виконання однієї або декількох функцій, що відбуваються внаслідок специфічного (постійного або тимчасового) його стану.

Побічне явище – явище, що супроводжує виконання елементом своїх основних функцій, але наслідком якого може бути порушення КЗ інформації.

Джерелами дестабілізуючих чинників, тобто середовищем їхньої появи, можуть бути як компоненти технічних засобів, так і зовнішнє середовище. До повної множини джерел належать:

Люди, окремі особи або групи осіб, дії яких можуть бути причиною порушення КЗ. Технічні пристрої – технічні засоби.

Моделі, алгоритми і програми.

Технологія функціонування – сукупність засобів, прийомів, правил, заходів і угод, які використовуються у процесі опрацювання і передачі інформації.

Зовнішнє середовище – сукупність елементів, що можуть впливати на КЗ.

Оскільки в загальному вигляді кожний із типів може виявлятися в кожному з перерахованих джерел, то на підставі цього можна описати механізм формування причин порушення КЗ (рис. 4.2) [12,13].

Рисунок 4.2. Механізм формування причин порушення КЗ

Аналіз показує, що деякі типи чинників у певних джерелах не можуть з'являтися за своєю природою.

Таким чином, усі чинники, наслідком яких може бути порушення КЗ інформації, можна розділити на групи, кожна з якої містить деяку кількість однорідних чинників.

Як уже відзначалося раніше, розрізняються три види уразливості: порушення фізичної цілісності, несанкціонована модифікація і несанкціоноване одержання; причому, різноманітні дестабілізуючи чинники в загальному випадку по-різному можуть впливати на різноманітні види уразливості, то для конкретних і цілеспрямованих оцінок введемо поняття причин порушення захищеності для кожного виду уразливості. При цьому під причиною порушення захищеності будемо розуміти той конкретний прояв дестабілізуючого чинника, що безпосередньо впливає на КЗ.

Тоді, при системному розгляді проблем КЗ, повинні самостійно розглядатися причини порушення КЗ для кожного виду захисту. Причини порушення захищеності щодо фізичної цілісності інформації (ППЦІ) та несанкціонованого одержання інформації – канали несанкціонованого одержання інформації (КНОІ). Що стосується несанкціонованої модифікації, то вона може мати місце або внаслідок порушень цілісності (викривлень) інформації з якої-небудь причини, або внаслідок злочинних дій людей.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

Що розуміють під кіберзахистом інформації?

Що розуміють під надійністю інформації?

Які об'єкти захисту існують?

У яких зонах здійснюється кіберзахист інформації?

Чим характеризуються зміни в розвитку обчислювальної техніки?

До чого може призвести зниження якості інформації?

Наякі класи розділені шляхи несанкціонованого одержання інформації?

Перерахуйте групи можливих шляхів несанкціонованого одержання інформації.

Які положення містить у собі системний підхід до КЗ?

Який висновок був отриманий у рамках системно-концептуального підходу до проблем КЗ? Що випливає з цього висновку?

Які елементи визначають концепції КЗ? Дайте їхні означення.

На які дві частини розділені дані елементи?

Що необхідно для побудови уніфікованої концепції КЗ?

РОЗДІЛ 5. ЗАГАЛЬНІ ПИТАННЯ КІБЕРЗАХИСТУ

5.1 Задачі кіберзахисту

У сучасному світі інформація і її обробка відіграє ключову роль у керуванні й функціонуванні держав, організацій, компаній і підприємств. Маючи доступ до потрібної інформації, можна правильно оцінити поточну ситуацію, прийняти своєчасний розв'язок. Реалії сучасно світу такі, що ефективність роботи будь-якої структури (державної або приватної) прямо залежить від якості й оперативності керування всіма процесами.

Однак широке застосування інформаційних технологій неможливе без підвищення уваги до питань захисту інформації. Інформація повинна бути доступна тільки тим, кому вона призначена, і схована від сторонніх спостерігачів і несанкціонованого доступу. Тому створення систем, що забезпечують захист інформації й процедур над нею, оцінка якості проектування й експлуатації таких систем припускають розв'язок широкого кола різнопланових завдань. Розглянемо постановки деяких основних завдань захисту інформації від несанкціонованого доступу.

Визначимо наступні параметри для подальшого аналізу й дослідження завдань захисту інформації. Безліч об'єктів: W– кінцева безліч елементів $w_1,w_2,\ldots w_n$. J– безліч індексів об'єктів : $J(1,2,\ldots,n)$ і при цьому об'єкти - пасивні носії інформації. Кожний об'єкт має певний (базовий) рівень захисту $J_0(w_1)$, $\forall n \in$ J, тісно пов'язаний із цілісністю об'єкта w_1, т.е. рівень захисту об'єкта відповідає вартості $v(w_i)$ інформації, що втримується в ньому.

При цьому безліч методів захисту M- кінчена множина елементів $m_1,m_2,\ldots m_k$. Під «методами» слід розуміти всі можливі способи і засоби (організаційні, технічні, програмні, організаційно-правові, криптографічні тощо), які використовуються для захисту об'єктів $w_i \in W$, $i= 1,n$. Сукупність методів, застосовних для захисту об'єктів w_i назвемо їхнім об'єднанням і позначимо:

$$\bigcup_{J=1}^{K} m_j(w_i) = M(w_i),\ i = \overline{1,n}.$$

Позначимо через j – множину індексів усіх методів захисту об’єкта w_i утворюючих сукупність $M(w_i)$: $j= (1,2,\ldots,k)$.

Для розв'язку задач захисту інформації введемо множину підрівневого захисту L – кінцева множина елементів $l_1 l_2,,\ldots,l_k$. Кожен підрівень l_j, $1 \le j \le k$, забезпечується застосуванням m_j- -го методу захисту об'єкта $w_i \in W$, тобто

$$\forall w_i \in W \; l_j(w_i) \sim m_j(w_i),\; l_j \in L,\; m_j \in M,\; i \in J,\; i=\overline{1,k}.$$

Потужність множини L збігається з потужністю множини M. Сумарний рівень захисту, забезпечуваний сукупністю $M(w_i)$ методів захисту об'єкта повинен бути не менше базового рівня $J_0(w_i)$ захисту об'єкта w_i:

$$\forall i \in J: J(w_i) = \sum_{j \in J} l_j(w_i) \ge J_0(w_i) \qquad (5.1)$$

Підсумовування проводиться лише по тім методам, які належать об'єднанню $M(w_i)$, який використовується для захисту об'єкта w_i. Вираз (5.1) і зміст терміну «рівень захисту об'єкта» визначають принципову відмінність розглядаємих задач відмінних від задач утворення систем захисту.

Результатом з вище сказаного є те, що необхідно так саме оцінити множину вартості захисту $s_1, s_2, \ldots, s_k$. Елемент $s_j \in S,\; j=\overline{1,k}$ характеризує величину витрат при реалізації m_j -го методу захисту об'єкта, що $w_i \in W \; w_i \in W$ і забезпечующого l_j –й рівень захисту. Потужність множин $M,L,$S збігається: $\|M\|=\|L\|=\|S\|$.

Множину S можна розглядати як $S = \{S_j^i\}, i=\overline{1,n};\; j=1,k$, якщо припускати, що реалізація одного і того самого m -го методу для кожної пари різних об'єктів $w_{i1} \ne w_{i2} \ne i_2, \; w_{i1} \ne w_{i2} \ne i_2,$ має різну вартість:

$$S_j(w_{i1}) \ne S_j(w_{i2}).$$

У цьому випадку $\|M\| \cdot \|W\| = \|S\|$.

Введемо змінну:

$$x^j_{(wi)} = \begin{cases} 1, \text{ коли застосовується } m_j \text{ –й метод захисту об'єкта } w_i, \\ \text{який забезпечує } l_j \text{ підрівень захисту, } l \le j \le k \\ 0, \text{ в іншому випадку.} \end{cases}$$

відзначимо, що:

$$\sum_{j=1}^{k} \chi^j(w_i) \le k. \qquad (5.2)$$

Тоді вираз (1.1), що визначає рівень захисту об'єкта, який забезпечується сукупністю $M(w_i)$ методів, можна переписати у вигляді:

$$J(w_i) = \sum_{j \in J} l_j(w_i) \geq J_0(w_i), i = \overline{1,n}. \qquad (5.3)$$

Якщо рівень захисту суб'єкта (суб'єкти можуть переміщувати або змінювати зміст об'єктів) позначити через J_c то, з іншого боку, повинна також виконуватися умова:

$$J_c(w_i) \leq J_c.$$

Після визначення множин $w_i \in W, i = \overline{1,n}$ виділимо основні параметри систем захисту інформації. Захист об'єкта: $w_i \in W, i = \overline{1,n}$ визначається вибором сукупності $M(w_i)$ методів $m_{j(w_i)}, j = 1,k,$ які характеризуються підрівнем захисту $l_j(w_i)$. Друга характеристика забезпечення захисту об'єкта w_i - сумарна вартість реалізації обраних методів, яка не повинна перевищувати базової вартості $S_0(w_i)$ забезпечення захисту об'єкта. При цьому рівень захисту об'єкта, який забезпечується застосуванням обраної сукупності методів $M(w_i)$ захисту об'єкта w_i, не повинен бути менше базового рівня захисту об'єкта $w_i \in W$.

Злом системи або порушення системи захисту об'єкта w_i характеризується ймовірністю злому кожного методу захисту і усієї сукупності методів у цілому, сумарною вартістю злому всіх методів, а також тимчасовими витратами, необхідними для подолання всіх методів, застосовуваних для захисту об'єкта w_i.

Сумарна вартість злому всіх методів, які застосовуються для захисту об'єкта w_i, повинна бути більше вартості $v(w_i)$ самого об'єкта, тимчасові витрати злому системи захисту об'єкта повинні бути максимальні, принаймні, повинні бути більше $T_0(w_i)$ для базового обмеження тимчасових витрат нападу системи захисту об'єкта w_i.Тільки при цих умовах можна вважати за доцільне вибір даної сукупності методів захисту об'єкта w_i.

Наявність злому m_j -го методу, який застосовується для захисту об'єкта w_i, визначає величину втрат $\hbar_j(w_i)$ для об'єкта. Сумарна величина втрат при зломі всіх методів, які застосовуються для захисту об'єкта w_i, не повинна перевищувати вартості самого об'єкта $v(w_i)$, - вартості всієї інформації, що мається в об'єкті $w_i \in W$.

Ефективність захисту об'єкта, також як і системи в цілому, суттєво залежить від вартості реалізації обраних методів і засобів захисту. Природно

припустити, що чим менше вартість реалізації системи захисту (при рівності всіх інших якісних показників), тем менше її ефективність.

Вартість системи захисту об'єкта $w_i \in W$, $1 \le i \le n$, визначається сумою:

$$\sum_{j=1}^{k} S_j(w_i)\chi^j(w_i),$$

де кожний доданок $S_j(w_i)\chi^j(w_i)$,- вартість реалізації $m_j \in M(w_i)$ методу, який використовується для захисту об'єкта w_i. Якщо який-небудь $m_i(w_i)$ - й метод не був використаний для захисту об'єкта w_i, то $\chi^j(w_i) = 0$, отже, доданок суми дорівнює нулю.

Вартість захисту об'єкта повинна бути мінімізована, принаймні, вона не повинна перевищувати певної величини, скажемо $S(w_i)$:

$$S(w_i) = \sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) \le S_0(w_i), w_i \in W, i \in J. \qquad (5.4)$$

Для системи в цілому це можна записати :

$$S = \sum_{i=1}^{n} S(w_i) = \sum_{i=1}^{n}\sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) \le S_0(w_i) \qquad (5.5)$$

де S_0 - обмеження вартості для системи.

Узагальнимо через $S_j^n(w_i)$ і $S_j^э(w_i)$ відповідно вартості проектування і експлуатації m_j – го методу захисту об'єкта (w_i), через $S^n(w_i), S^э(w_i), S^n$, $S^э$ - відповідні вартості проектування і експлуатації захисту об'єкта w_i і системи в цілому.

Тоді вираження (1.4) і (1.5) буде мати вигляд:

$$S(w_i) = \sum_{j=1}^{k} S_j^n(w_i)\chi^j(w_i) + \max_{i\in 1} T_0(w_i)\sum_{j=1}^{k} S_j^э(w_i)\chi^j(w_i) = S^n(w_i) + \max_{i\in 1} T_0(w_i)\cdot S^э(w_i) \le S_0(w_i),$$
$$w_i \in W, i = \overline{1,n} \qquad (5.6)$$

$$S = S^n + \max_{i\in J} T_0(w_i)\cdot S^э = \sum_{i=1}^{n}\sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) + \max_{i\in J} T_0(w_i)\sum_{i=1}^{n}\sum_{j=1}^{k} S^э{}_j(w_i)\chi^j(w_i) \le S_0, \qquad (5.7)$$
$$w_i \in W, i = \overline{1,n}$$

де $T_0(w_i)$- максимальний час зберігання інформації обмеженого використання в об'єкті w_i, $\max_{i\in J} T_0(w_i)$- максимальний час знаходження закритої інформації в системі.

Вирази (5.6) і (5.7) дозволяють сформувати задачу оптимального вибору методів захисту для кожного конкретного об'єкта та для системи в цілому.

З іншого боку, вартість захисту об'єкта, обмеження на цю вартість і вартість самого об'єкта (вартість інформації, що міститься на об'єкті), повинні бути зв'язані між собою: вартість об'єкта $v(w_i)$ повинна бути більше обмеження на вартість захисту об'єкта, тобто можна записати:

$$v(w_i) \succ S_0(w_i) \geq S(w_i), \forall w_i \in W .$$

Для системи в цілому $V_c \succ S_0 \geq \sum_{i=1}^{n} S(w_i), \forall i \in J,$ (5.8)

де V_c - сумарна вартість інформації всіх об'єктів системи:

$$V_c = \sum_{i=1}^{n} v(w_i). \quad (5.9)$$

де різниця $v(w_i) - S(w_i)$ визначає ефективність системи захисту об'єкта, для системи вцелом ефективність визначається різницею: $V_c - \sum_{i=1}^{n} S(w_i)$.

Позначимо через $P_j(w_i), j = \overline{1,k}$, імовірність злому m_j-го методу, використаного для захисту об'єкта $w_i \in W$. Тоді сумарна ймовірність злому системи захисту об'єкта w_i, тобто ймовірність подолання всіх методів, застосованих для захисту об'єкта $w_i \in W$, має вигляд:

$$P(w_i) = 1 - \prod_{j=1}^{k} \left[1 - p_j(w_i)\right] \chi^j(w_i), \forall m_i \in W, \quad (5.10)$$

або для системи в цілому, тому що об'єкти системи на зв'язані між собою і представляють незалежні події,

$$P = \prod_{i=1}^{n} P(w_i) = \prod_{i=1}^{n} \left[1 - \prod_{j=1}^{k} (1 - p_j(w_i)) \chi^j(w_i) \right]. \quad (5.11)$$

Вирази (5.10) і (5.11), які визначають імовірності захисту об'єкту і системи в цілому, потрібно мінімізувати. Це і є *критерій вибору засобів і методів захисту*.

Тепер позначимо через $t_j(w_i)$ - тимчасові витрати, необхідні для злому m_j-го методу, застосовного для захисту об'єкта $w_i, i = \overline{1,n}$.

Тоді обмеження в зломі всіх методів, які використовуються для захисту об’єкта w_i, представляється у вигляді:

$$T_0(w_i) \le \sum_{j=1}^{k} t_j(w_i) p_i(w_i) \chi^j(w_i), \forall w_i \in W \qquad (5.12)$$

де $T_0(w_i)$ - максимальний час зберігання інформації обмеженого використання в об'єкті w_i.

Для системи, відповідно, маємо вираз :

$$T_0 = \sum_{i=1}^{n} \sum_{j=1}^{k} t_j(w_i) \chi^j(w_i) \qquad (5.13)$$

Якщо вартість продовження m_j-го методу ($m_j \in M$) захисту об'єкта w_i позначити через ${}_iC_j(w_i)$, то доцільність забезпечення захисту визначається наступними співвідношеннями:

$$C_j(w_i) = \sum_{j=1}^{k} c_j(w_i) p_i(w_i) \chi^j \succ v(w_i) \succ S(w_i), \forall w_i \in W \qquad (1.14)$$

А для системи повинне мати місце $C \succ V_c \succ S_o$,

де C – вартість подолання системи захисту усіх об'єктів $w_i \in W$. При цьому повинні бути враховані обмеження за часом подолання системи захисту.

Позначимо через $\pi_j(w_i)$.- величину втрат під час злому m_j - го методу, застосовуваного для захисту об'єкта w_i. Природно припускати, що захист об'єкта буде доцільним, якщо сумарна величина втрат при зломі всіх методів, які застосовані для захисту об'єкта, менше вартості самого злому цих методів:

$$\pi_j(w_i) = \sum_{j=1}^{k} \pi_j(w_i) p_i(w_i) \chi^j(w_i) \prec c(w_i) . \qquad (5.15)$$

З іншого боку, сумарна величина втрат при зломі всіх методів, застосованих для захисту об'єкта $w_i \in W$ не повинна перевищувати вартості самого об'єкта:

$$\pi_j(w_i) \le v(w_i), \forall w_i \in W . \qquad (5.16)$$

Якщо для системи в цілому $\pi_c \le V_{c,}$ де π_c- величина втрат при порушенні системи захисту всіх об'єктів $w_i \in W$, $i = \overline{1,n.}$

Тепер можна виділити $w_i \in W$ об'єкт інформаційної системи, що вимагає першочергових додаткових заходів по захисту інформації від несанкціонованого доступу.

Так як V - сумарна вартість інформації, що мається у всіх об'єктах системи, а $\pi_0(w_i)$ - величина втрат при порушенні системи захисту w_i, то мінімум різниці:

$$V_c - \pi_0(w_i), i = \overline{1,n} \text{ або}$$

$$\min_{w_i \in W} \left[\sum_{i=1}^{n} \sum_{j=1}^{k} S_j(w_i) \chi^j(w_i) - \sum_{j=1}^{k} \pi_j(w_i) p_i(w_i) \chi^j(w_i) \right], \qquad (1.17)$$

визначає номер об'єкта, втрати від злому методів захисту якого дають максимальну величину і, отже, вимагають застосування додаткових методів або засобів його захисту.

На підставі проведених досліджень сформулюємо *задачі системи захисту інформації*. Будемо розглядати множину елементів:

$$\{M_1(w_i), M_2(w_i), ..., M_\sigma(w_i)\}$$

де $M_\sigma(w_i) = \bigcup_{j=I_\tau} m_j(w_i) \subseteq M(w_i), \tau = \overline{1,\sigma}.$

Тут I_τ - підмножина індексів методів захисту об'єкта, що становлять об'єднання методів, застосованих для захисту об'єкта w_i і які забезпечують необхідний рівень його захисту $J(w_i): I_\tau \subseteq J, \forall \tau$.

Таким чином, кожний елемент $M_\tau(w_i)$ $(\tau = \overline{1,\sigma})$ являє собою об'єднання такої підмножини методів захисту об'єкта, практична реалізація яких забезпечує необхідний рівень захисту об'єкта $w_i \in W$.

Для створення системи захисту об'єкта $w_i \in W$ $(i = \overline{1,n})$ від несанкціонованого доступу до інформації і до процедур над нею, сформулюємо *задачі*, які припускають оптимізацію по всіх елементах:

$$M_\tau(w_i) \subseteq M(w_i), \tau = \overline{1,\sigma}.$$

Задача 1. Мінімізація вартості забезпечення захисту об'єкта $w_i \in W$, $i = \overline{1,n}$, тобто $S(w_i) = \sum_{j=1}^{k} S_j(w_i) \chi^j(w_i) \to \min_{M_\tau(w_i)}, \tau = \overline{1,\sigma},$ при наступних обмеженнях:

$$\sum_{j=1}^{k} \chi_{\tau}^{j}(w_i) \le k,$$

$$\sum_{j \in J} I_j(w_i)\chi_{\tau}^{j}(w_i) \ge J_0(w_i),$$

$$\sum_{j=1}^{k} S_j(w_i)\chi_{\tau}^{j}(w_i) \le S_0(w_i),$$

$$\chi_{\tau}^{j}(w_i) = \begin{cases} 1, \\ 0. \end{cases}$$

Більш точно задача формується з урахуванням нерівності (5.6), тобто з роздільним обліком вартості проектування і експлуатації засобів і методів, застосованих для захисту об'єкта.

Задача 2. Мінімізація ефективності систем захисту об'єкта $w_i \in W$:

$v(w_i) - S(w_i) \to \max\limits_{M_\tau(w_i)}$, при обмеженнях задачі 1.

Задача 3. Мінімізація ймовірності злому всіх методів, які використовуються для захисту об'єкта, при обмеженнях прийнятих при розв'язку задач 1 і 2:

$$P(w_i) = 1 - \prod_{j=1}^{k} (1 - p_j(w_i))\chi^j \to \min_{M\tau(w_i)}$$

Задача 4. Максимізація вартостіі злому усіх методів, які використовуються для захисту об'єкта $w_i \in W$:

$C(w_i) = \sum\limits_{j=1}^{k} c_j(w_i)p_j(w_i)\chi^j(w_i) \to \max\limits_{M\tau(w_i)}$, при обмеженнях задачі 1, а також наступних:

$$\sum_{j=1}^{k} t_j p_j(w_i)\chi^j(w_i) \ge T_0(w_i),$$

$$\sum_{j=1}^{k} c_j(w_i)p_j(w_i)\chi^j(w_i) \succ v(w_i).$$

Задача 5. Мінімізація величини втрат від злому всіх методів, які використовуються для захисту об'єкта $w_i \in W$:

$\pi(w_i) = \sum\limits_{j=1}^{k} \pi_j(w_i)p_j(w_i)\chi^j(w_i) \to \min\limits_{M\tau(w_i)}$, при обмеженнях прийнятих у задачі 4, а також обмеження на вартість злому системи захисту об'єкта:

$$\sum_{j=1}^{k} \pi_j(w_i)p_j(w_i)\chi^j(w_i) \prec c_o(w_i).$$

Розв'язок зазначених задач дозволить створити кращий варіант системи захисту об'єкта, а розв'язок відповідної сукупності задач для всієї множини об'єктів *W*- створити варіант системи захисту інформації для системи в цілому.

Вибір сукупності методів $m_j \in M$ захисту об'єкта повинен проводитися з урахуванням визначення усіх каналів витоку (за посередництвом каталогу каналів витоку інформації) для кожного конкретного об'єкта $w_j \in W$ з метою їх перекриття. Потім для кожного окремого методу захисту повинні бути визначені вартості проектування і експлуатації при реалізації цього методу, імовірність і вартість його злому. Наступні характеристики, досить важкі для визначення: оцінка вартості об'єкта, оцінки рівнів для кожного окремого методу захисту і рівня захисту самого об'єкта w_j, а також оцінки величини втрат у випадку злому кожного окремого методу захисту об'єкта. Тимчасові витрати, необхідні для злому всіх методів, застосованих для захисту об'єкта w_j,можуть бути отримані через імовірності подолання кожного з методів і часу, необхідного для реалізації однієї спроби подолання кожного методу захисту.

5.2 Вимоги до системи кіберзахисту інформації

Вимоги щодо ЗІ визначаються власником інформації і узгоджуються з виконавцем робіт з проектування і створення СЗІ.

Відповідно до ДСТУ 3396.0-96 і ДСТУ 3396.1-96 визначені основні положення і порядок робіт зі створення СЗІ. Ці стандарти встановлюють об’єкт захисту,мету, основні організаційно - технічні положення СЗІ, неправомірний доступ до якої може завдати збитку громадянам, організаціям, державі, а також категорії нормативних документів з СЗІ і вимоги до порядку проведення робіт з технічного захисту.

Виходячи з цих документів, метою СЗІ є запобігання витоку або порушенню цілісності інформації з обмеженим доступом (ІзОД).

Мета КСЗІ може бути досягнута побудовою СЗІ, яка є організованою сукупністю методів і засобів забезпечення СЗІ.

Зміст і послідовність робіт з протидії загрозам або їх нейтралізації повинні відповідати вказаним в ДСТУ 3396.0-96 етапи функціонування систем захисту інформації, відповідно до ДСТУ 3396.1-96, і полягати в:

проведенні обстеження об’єкту (підприємства, установи, організації);

розробці реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ;

прийому робіт з ТЗІ;

атестації засобів (систем) забезпечення інформаційної діяльності на відповідність вимогам нормативних документів системи ТЗІ.

У процесі формування вимог до СЗІ доцільно знайти відповіді на наступні питання:

які заходи безпеки пропонується використовувати?

яка вартість доступних програмних і технічних заходів захисту?

наскільки ефективні доступні заходи захисту?

наскільки уразливі підсистемі СЗІ?
чи є можливість провести аналіз ризику?
Сукупність вимог до СЗІ наведена на рис.5.1.

Рис. 5.1. Сукупність вимог до систем захисту інформації

У загальному випадку доцільно виділити наступні групи вимог до СЗІ:

– Загальні вимоги;
– Організаційні вимоги;
– Конкретні вимоги до підсистем захисту, технічного і програмного забезпечення, документування, способів і методів захисту.

Проведемо розробку і сформулюємо вимоги до систем ЗІ для широкого класу систем і об'єктів. Крім того розглянемо і врахуємо в цих вимогах вплив зовнішніх атак і дій зловмисників.

Загальні вимоги. Перш за все, необхідна повна ідентифікація користувачів, терміналів , програм, а також основних процесів і процедур, що відбуваються на об'єкті захисту. Крім того, слід обмежити доступ до інформацій, використовуючи сукупність наступних способів:

ієрархічна класифікація доступу;

класифікація інформації за важливістю і місцем виникнення;

вказівки обмежень до інформаційних об’єктів;

визначення програм і процедур, наданих тільки конкретнім користувачем

СЗІ повинна гарантувати, що будь - який рух інформації ідентифікується, авторизується, виявляється і документується.

Зазвичай формулюються загальні вимоги до СЗІ, які відповідають наступним характеристикам:

способам побудови СЗІ або її окремих компонентів;

архітектурі засобів обчислювальної техніки та інформаційних систем (до класу і мінімальної конфігурації ЕОМ, операційного середовища, орієнтації на ту або іншу програмну і апаратну(технічну) платформи);

застосуванню стратегії захисту;

витратам ресурсів на забезпечення СЗІ;

надійності і живучості функціонування СЗІ;

кількості ступенів секретності інформації, підтримуваних СЗІ;

забезпеченню швидкості обміну інформацією на об’єкті, у тому числі з урахуванням використовуваних криптографічних вимог;

кількості підтримуваних СЗІ рівнів повноважень;

можливості СЗІ обслуговувати певну кількість користувачів;

тривалість процедури генерації програмної версії СЗІ;

тривалість процедури підготовки СЗІ до роботи після подачі живлення на компоненти об’єкту;

можливість СЗІ реагувати на спроби несанкціонованого доступу або атаки ззовні;

наявності і забезпеченню автоматизованого робочого місця адміністратора ЗІ;

складу використовуваного програмного і лінгвістичного забезпечення , до його сумісності з іншими програмними платформами, до можливості модифікації і т.п.;

використовуваним компонентам СЗІ, що купуються (наявність ліцензії, сертифіката і тому подібне).

Організаційні вимоги до системі захисту передбачають реалізацію сукупності адміністративних і процедурних заходів.

Вимоги із забезпечення збереження повинні виконуватися вперш за все на адміністративному рівні. Організаційні заходи, що проводяться з метою підвищення ефективності ЗІ, повинні передбачати наступні процедури:

обмеження несупроводжуваного доступу до інформації;

здійснення контролю за зміною в системі програмного забезпечення;

виконання тестування і верифікація змін у системі програмного забезпечення і програмах захисту;

організацію і підтримку взаємного контролю за виконанням правил захисту інформації;

обмеження привілеїв персоналу, що обслуговує СЗІ;

здійснення запису протоколу про доступ до системи;

гарантію компетентності обслуговуючого персоналу;

розробку послідовного підходу до забезпечення збереження інформації для об'єкту , що захищається;

організацію чіткої роботи бібліотеки;

комплектування основного персоналу на базі інтегральних оцінок і твердих знань;

організацію системи навчання і підвищення кваліфікації обслуговуючого персоналу.

З погляду забезпечення доступу до інформації, що захищається, необхідно виконати наступні процедурні заходи:

розробити і затвердити інструкції на завантаження і зупинку роботи операційної системи;

контролювати використання магнітних носіїв і лістингів, порядок зміни програмного забезпечення і доведення цих змін до користувача;

розробити процедуру відновлення системи при відмовах;

встановити політику обмежень і визначити обсяг інформації, що видається;

розробити систему протоколювання використання ЕОМ СЗІ, введення інформації и виведення результатів;

забезпечити проведення періодичного чищення архівів для видалення і ліквідації не потрібної і застарілої інформації;

підтримувати документацію СЗІ відповідно до встановлених правил і стандартів.

Вимоги до підсистеми ЗІ в загальному випадку доцільно умовно розділити на:

підсистему управління доступу до інформації (включає також управління СЗІ в цілому);

підсистему реєстрації та обліку дій користувачів(процесів);

криптографічну підсистему;

підсистему забезпечення цілісності інформаційних ресурсів та їх конфігурацій.

Для кожної з підсистеми визначаються вимоги у вигляді:

- переліку забезпечуваних підсистемою функцій захисту;

- основних характеристик цих функцій;

Підсистема управління доступом повинна забезпечувати:

ідентифікацію, аутентифікацію і контроль за доступом користувачів до системи, терміналів, вузлів мережі, каналів зв'язку, зовнішніх пристроїв, програм, каталогів, файлів і т.п.;

очищення областей оперативної пам’яті і зовнішніх накопичувачів системи, що звільняються.

Підсистема реєстрації та обліку виконує:

- реєстрацію та облік доступу до ресурсів системи, видачі вихідних документів, запуску програм і процесів, доступу до файлів , що захищаються, передачу інформації по лініях і каналах зв’язку;
- реєстрацію зміни повноважень доступу, створення об’єктів доступу, що підлягають захисту;
- облік носії інформації;
- сповіщення про атаки і спроби порушення захисту об’єкту.

Криптографічна підсистема передбачає:

- шифрування конфіденційної інформації;
- шифрування інформації, що належить різним суб’єктам доступу (групам субєктів), з використанням різних ключів;
- використання сертифікованих і атестованих криптографічних засобів.

Підсистема забезпечення цілісності повинна здійснювати:

- забезпечення цілісності , програмних засобів і оброблюваної інформації;
- фізичну охорону засобів обробки інформації та її носіїв;
- наявність адміністратора і служби безпеки об’єкту;
- періодичне тестування СЗІ;
- наявність засобів відновлення СЗІ;
- використання сертифікованих засобів захисту;
- контроль за цілісністю: програмних засобів, ЗІ при завантаженні операційного середовища; операційного середовища перед виконанням різних процесів у системі;функціонального програмного забезпечення (ПЗ) та інформації;конфігурації СЗІ і об’єкту захисту;
- оперативне відновлення функцій СЗІ після збоїв;
- тестування засобів ЗІ
- виявлення і блокування дій зловмисників;
- контроль доступу до засобів обчислювальної техніки(ЗОТ)СЗІ, що дає упевненість в тому, що тільки авторизований користувач використовує наявні робочі програми та інформацію;
- контроль дій з персональною авторизацією, що забороняє операції, які роблять операційне середовище уразливим;
- захист програмного забезпечення, що виключає пошкодження програм;
- використання тільки ліцензованого продукту з метою забезпечення захисту від вбудованих програмних закладок і програм руйнування інформаційного середовища;
- захист комунікацій для забезпечення захисту інформації, що передається.

Вимоги до технічного забезпечення. У цій групі формуються вимоги до таких параметрів:

- місця застосування засобів захисту;

- способам використання засобів захисту;

- розмірам контрольованої зони;

- необхідній величині показників захищеності, що враховує реальну обстановку не об’єкті;

- застосуванню способів, методів і засобів досягнення заданого рівня захищеності;

- проведенню спец дослідження устаткування і технічних засобів на об’єкті захисту, метою якого є вимір електромагнітних випромінювань і виявлення небезпечних сигналів;

- проведення спец перевірки технічних засобів ЗІ, метою якої є визначення відповідності забезпечення необхідного рівня захищеності об’єкту.

Програмні засоби ЗІ повинні забезпечувати контроль доступу, безпеку інформації і захист самої СЗІ. Для цього необхідно виконати наступні умови:

- об’єкти захисту повинні ідентифікуватися в явному вигляді при використанні паролів і пропусків;

- система контролю доступу має бути достатньо гнучкою для забезпечення багатообразних обмежень і різних наборів об’єктів;

- кожен доступ до захищеного інформативного файлу і пристрою об’єкту або СЗІ повинен прослідживатися через систему контролю доступу для того, щоб фіксувати і документувати будь-яке звернення.

Безпека інформації може забезпечуватися наступною системою заходів:

- інформаційні об’єкти ідентифікуються і забезпечуються інформацією службою безпеки. Доцільно цю інформацію розміщувати не в окремому каталозі , а разом з інформацією, що має мітки;

- кодові слова захисту і паролі розміщуються усередині файлів, що значною мірою підвищує ефективність захисту;

- доступ до інформації доцільний за допомогою непрямих посилань, наприклад, списку користувачів, допущенних власником файлу до розміщеної в ньому інформації;

- інформація і програми можуть перетворюватися(кодуватися) внутрішнім способом або архівацією для зберігання.

СЗІ має бути захищена від дії навколишнього середовища. З цією метою виконується наступна сукупність заходів:

інформація по негативних запитах не відається;

повторні спроби доступу після невдалих звернень повинні кількісно обмежуватися;

при зміні конфігурації системи або при її тестуванні функції захисту зберігаються;

ніякі зміни таблиць безпеки, окрім зміни зі спеціально пристрою або пульта управління, не вирішуються.

У сучасних умовах у процесі взаємодії об’єкта і людини виникають події, процеси або явища, які можуть привести до знищення, втрати цілісності,

конфіденційності або доступності інформації. Проте до теперішнього часу,проектували СЗІ і розробляли вимоги до їх здійснюється без урахування відмінних особливостей систем «людина-обєкт інформації» або «засіб ЗІ-обєкт інформації».

Для вирішення завдань захисту інформації вводиться множина підрівневого захисту L - кінцева множина елементів $l_1, l_2, ..., l_k$.кожен підрівень $l_{i,1} \le j \le k$, забезпечується застосуванням m_j-го методу захисту об'єкту $W_i \in W$, тобто $\forall w_i \in W_i l_j(w_i), l_j \in L, m_j \in M, i \in J, j = \overline{1,k}$.

Сумарний рівень захисту, що забезпечується сукупністю $M(W_i)$ методів захисту об'єкту має бути не менше базового рівня $J_0(W_i)$ захисту об'єкту W_i:

$$\forall i \in J : J(w_i) = \sum_{j \in J} lj(w_i) \ge J_0(W_i) \qquad (5.18)$$

Підсумовування проводиться лише по тих методах, які належать об'єднанню $M(W_i)$, використовуваному для захисту об'єкту W_i.

Вираз (5.18) і зміст терміну «рівень захисту об'єкта» визначають принципову відмінність задач захисту об'єкта від задач створення систем захисту.

Виходячи зі сказаного , необхідно також оцінити множину вартостей захисту $s_1, s_2, ..., s_k$. Елемент $s_j \in S, j = \overline{1,k}$ характеризує величину затрат при реалізації m_j -го методу захисту об'єкту $w_i \in W$ і який забезпечує l_j-й рівень захисту. Потужність множин *M*,*L* та *S* збігаються.

Злом системи або порушення системи захисту об'єкту w_i характеризується вірогідністю злому кожного методу захисту і всієї сукупності методів в цілому, сумарною вартість злому або несанкціоноване проникнення через неї, а також тимчасовими витратами, необхідними для подолання всіх методів, вживаються для подолання системи захисту об'єкту w_i. Сумарна вартість несанкціонованих дій, що вживаються для подолання системи захисту має бути більше вартості засобів, що вживаються для захисту об'єкту і самого об'єкту. Тимчасові витрати об'єкту СЗІ на об'єкті мають бути максимальні, вони, принаймні, мають бути більш ніж для базового обмеження тимчасових витрат нападу системи захисту об'єкту . тільки за цих умов можна вважати за доцільне вибір даної сукупності методів захисту об'єкту і виконання вимог до СЗІ.

Будь-яка атака або несанкціонована дія, що діє на об'єкт, на кожному з них, що мають у розпорядженні СЗІ засобів захисту відіб'ється по різному:

- деякі із засобів можуть бути зруйновані повністю, деякі виведені з ладу частково, а для якихось засобів атака виявиться безпечною. Облік цих відмінностей у результатах дії атаки на засоби захисту є важливим при проектуванні, моделюванні будь-якої КСЗІ, а також при встановленні стійкості

СЗІ передбачуваному супротивникові. Для формування кожного обліку необхідно:

- визначити математичний параметр, що характеризує об'єкт при його використовуваному математичному представленні, якісне застосування якого буде відміни, залежно від характеру збурюючої дії;
- вибрати спосіб формального представлення атак СЗІ так, щоб він, будучи простим в обчислювальному сенсі, дозволяв відобразити безпосередню спрямованість атаки;
- вибрати простий в обчислювальному сенсі спосіб представлення результату атаки.

Вирішення поставлених завдань дає можливість для створення моделі СЗІ, що дозволяє максимально швидко визначити наслідки організованої атаки, виділяючи «постраждалі »і «незайняті» засоби захисту.

Традиційним шляхом для представлення групи людей з відображенням взаємних стосунків між ним є використання теорії графів. Це обумовлено рядом чинників, сереж яких наочність отримуваної моделі, можливість адекватного віддзеркалення за допомогою стандартних операцій на графах реальних дій над групами і подій у групах, існуванням розробленого математичного апарату для роботи з графами, включаючи велику кількість тих, що добре зарекомендували себе на практиці евристичних методів обробки.

Вибір сукупності методів захисту об'єкту повинен проводитися з урахуванням певних каналів витоку для кожного конкретного об'єкту з метою їх перекриття. Потім для кожного окремого методу захисту повинна бути визначена вартість проектування та експлуатації при реалізації цього методу, вірогідність і вартість його злому, атаки або несанкціонованої дії. Наступні характеристики досить складні для визначення:

- оцінка вартості об'єкту, оцінки рівнів для кожного окремого методу захисту і рівня захисту самого об'єкту, а також оцінки величини витрат у разі несанкціонованого одержання інформації, нейтралізувавши кожний окремий метод захисту інформації.

Тимчасові заборони необхідні для подолання кожного з методів і часу, необхідного для реалізації однєї спроби подолання кожного методу захисту.

Вказаним характеристиками є початкові дані, необхідні для створення і оцінки якості системи захисту об'єкта і всієї системи і об'єкта в цілому.

5.3. Підходи до створення систем кіберзахисту інформації

Для розгляду проблеми ЗІ в загальному вигляді виділимо в її предметній області три наступні ієрархії: структурну, причинно-наслідкову й функціональну.

Способи ЗІ залежать від типу інформації, форми її зберігання, обробки і передачі, типу носія інформації, а також передбачуваного способу нападу і наслідків його впливу на інформацію (копіювання, викривлення, знищення).

В основному власник інформації не знає де, коли і яким чином буде здійснений напад, тому йому необхідно виявити саме факт нападу.

Визначення потенційної цінності інформації дозволяє мислити в першу чергу про безпеку найбільш важливих секторів, витік яких здатний завдати шкоди. При цьому важливо встановити:

1. Яка інформація потребує захисту?
2. Кого вона може цікавити?
3. Які елементи інформації найцінніші?
4. Який «строк життя» цих секретів?
5. У вощо обійдеться їхній захист?

Досвід застосування СЗІ показує, що ефективної може бути лише **комплексна система захисту інформації (КСЗІ), що** поєднує наступні заходи:

1. Законодавчі. Використання законодавчих актів, що регламентують права і обов'язки фізичних і юридичних осіб, а також держави в області ЗІ.
2. Морально-етичні. Створення і підтримування на об'єкті такої моральної атмосфери, у якій порушення регламентованих правил поведінки оцінювалися б більшістю співробітників різко й негативно.
3. Фізичні. Створення фізичних перешкод для доступу сторонніх осіб до охорони інформації.
4. Адміністративні. Організація відповідного режиму серктности, перепускного і внутрішнього режиму.
5. Технічні. Застосування електронних та інших пристроїв для Зі.
6. Криптографічні. Застосування шифрування та кодування для приховування оброблюваної і переданої інформації від несанкціонованого доступу.
7. Програмні. Застосування програмних засобів розмежування доступу.

Обґрунтований вибір необхідного рівня захисту інформації є системотворчим завданням, оскільки як заниження, так і завищення рівня неминуче веде до втрат. При цьому останнім часом роль даного питання різко зросла у зв'язку з тим, що:

по-перше, тепер у число, що захищаються крім військових, державних і відомчих, включені також секрети промислові, комерційні й навіть особисті;

а по-друге, сама інформація усе більше стає товаром.

Таким чином, для оцінки необхідні показники двох видів, що характеризують інформацію як ресурс, що забезпечує діяльність суспільства та що характеризують інформацію як об'єкт праці.

Метою захисту інформації є виключення або істотне затруднення несанкціонованого одержання інформації. Для розв'язку проблеми ЗІ неоходимо

мати або одержувати відомості про параметри наведених сигналів на неінформаційні ланцюги, у тому числі і за межами контрольованої зони.

Підсистема вимірів і контролю повинна забезпечити оцінку параметрів полів і сигналів з достатньою точністю, методи оцінки параметрів, що визначають витік і захист інформації, повинні забезпечувати повторюваність і відтворюваність результатів. Контроль заходів ЗІ від витоку по технічних каналах у процесі експлуатації інформаційної системи з метою забезпечення пропонованих вимог, здійснюється з урахуванням різних факторів зовнішнього середовища і режимів функціонування.

Ефективність ЗІ контролюють в умовах складної обстановці при постановці завад, тому що контрольовані параметри повинні бути менше рівня ненавмисних (фонових) або, що маскуючих (спеціально організованих) перешкод.

Слід підкреслити, що оцінку ефективності заходів ЗІ бажано проводити в реальному масштабі часу, на основі автоматизації усіх процесів виміру і аналізу параметрів різних сигналів з необхідною точністю та вірогідністю.

Теорія і практика ЗІ розвивалася в рамках теорії і техніки зв'язки для забезпечення безпеки інформації в каналах зв'язку та потім поширювалася на побічні технічні канали витоку.

Сучасні досягнення в області ЗІ дозволяють по праву віднести її до наукового напрямку теорії інформатики. Систематизація знань по науковій проблемі ЗІ, узагальнення теоретичних і технічних розв'язків дасть можливість сформулювати сутність предметної області ЗІ:

1. Дослідження побічних фізичних явищ генерації і випромінювання, інформаційних полів різної фізичної природи в процесі взаємодії інформаційної системи та зовнішнього середовища;

2. Дослідження розсіювання фізичних полів, їх поширення і взаємного перетворення в різних фізичних середовищах, створення струмів і напруг у результаті впливу полів на різні інформаційні і неінформаційні ланцюги, які пов'язані з ланцюгами, що йдуть за межі обмеженого простору (зокрема контрольованих зон), а так саме перетворень струмів і напруг на неінформаційних ланцюгах у поля, що поширюються до развідприймачів. Ці поля, струми і напруги можуть нести признаковую (об'єкті) і семантичну інформацію при наявності фізичної доступності в точці перехоплення;

3. Дослідження процесів лінійних перетворювачів полів і сигналів на елементах інформаційної системи середовища, їх взаємодії з іншим полями (зокрема ВХ-Поля, ВХ - нав'язування, лазерного опромінювання тощо.);

4. Дослідження і розв'язок комплексу питань по обґрунтуванню нормативних параметрів і характеристик сигналів і перешкод і методів їх вимірів та автоматизованого контролю;

5. Розробка методологічних основ дослідження ЗІ, зокрема розробка методів оцінки ефективності заходів ЗІ в ІТС;

6. Дослідження і розробка різних способів ЗІ, а так саме шляхів переходу системи обстеження в бажаний стан на основі оптимальних алгоритмів і вимірів, контролю і керування;

7. Дослідження умов реалізації оптимальних методів ЗІ, развиток методів і засобів оптимізованого, автоматичного, оперативного, достовірного дієвого контролю заходів захисту і їх параметрів;

8. Теоретичне узагальнення, систематизування наукових завдань і прогнозування шляхів захисту інформації в різних інформаційних системах.

Основи захисту інформації технічними методами включають:

1. Аналіз інформаційних процесів в ІТС, включаючи пошук, збір, обробку і надання інформації, визначення та формування параметрів і характеристик інформаційного простору, що містять відомості і дані про об'єкт захисту, аналіз характеристик середовища поширення різних фізичних полів, аномальність фізичних полів, обумовлених неоднородностями;

2. Аналіз і оцінку можливості несанкціонованого доступу до ІТС всередині неконтрольованої зони з урахуванням особливостей об'єкта і характеристик можливих ІТС;

3. Класифікація і моделі можливих систем і засобів перехоплення та сигналів і полів різної фізичної природи та способів і засобів обробки сигналів в умовах низького співвідношення сигнал/перешкода.

Під час реалізації заходів ЗІ використовують:

1. Послаблення інформаційних фізичних полів розсіювання, їх наведень на неінформаційні ланцюги, на джерела випромінювання ВХ – коливань.

2. Послаблення взаємних перетворень інформаційних полів і їх превипромінювань і наведень на неінформативні ланцюги.

3. Зрив паразитних генерацій, переносників інформації.

4. Послаблення паразитних модульованих ВХ – коливань.

5. Локалізацію джерел інформаційних полів розсіювання.

6. Локалізацію зовнішніх ВХ - коливань, що поширюються у вигляді фізичних полів на інформаційних ланцюгах, що наводяться на інформаційні ланцюги.

7. Локалізацію випромінювань полів розсіювання сигналів з метою послаблення взаємодії із системами їх виявлення і перехоплення.

8. Руйнування ПЕМВН з метою забезпечення скритності функціонування інформаційних систем.

9.Формування інформаційних параметрів сигналів і маскуючих перешкод, що максимально ускладнюють перехоплення і обробку інформації (у тому числі кодове зашумлення).

10. Оцінку обмежуючих факторів і зв'язків між джерелом інформації і засобом виявлення та перехоплення.

13. Оцінку і контроль параметрів, що визначають ступінь ЗІ (апаратурними, програмними методами).

14. Автоматизований контроль параметрів, що захищаються.

Показники першого виду носять прагматичний характер. До них відносять:

- важливість, значимість із погляду тих завдань, для розв'язку яких використовується оцінювана інформація;

- повнота інформації для інформативного забезпечення розв'язуваних завдань;

- адекватність, тобто відповідність поточному стану відповідних об'єктів або процесів; релевантність інформації і її толерантність.

Показники другого виду повинні характеризувати інформацію як об'єкт праці, над якою здійснюються деякі процедури в процесі переробки її з метою інформаційного забезпечення завдань, які розв’язуються. До них відносяться:

- ефективність кодування інформації і її объем;

- методи визначення цих показників досить повно розроблені в теорії інформації.

Важливість інформації повинна оцінюватися по двом групам критеріїв (рис 5.2):

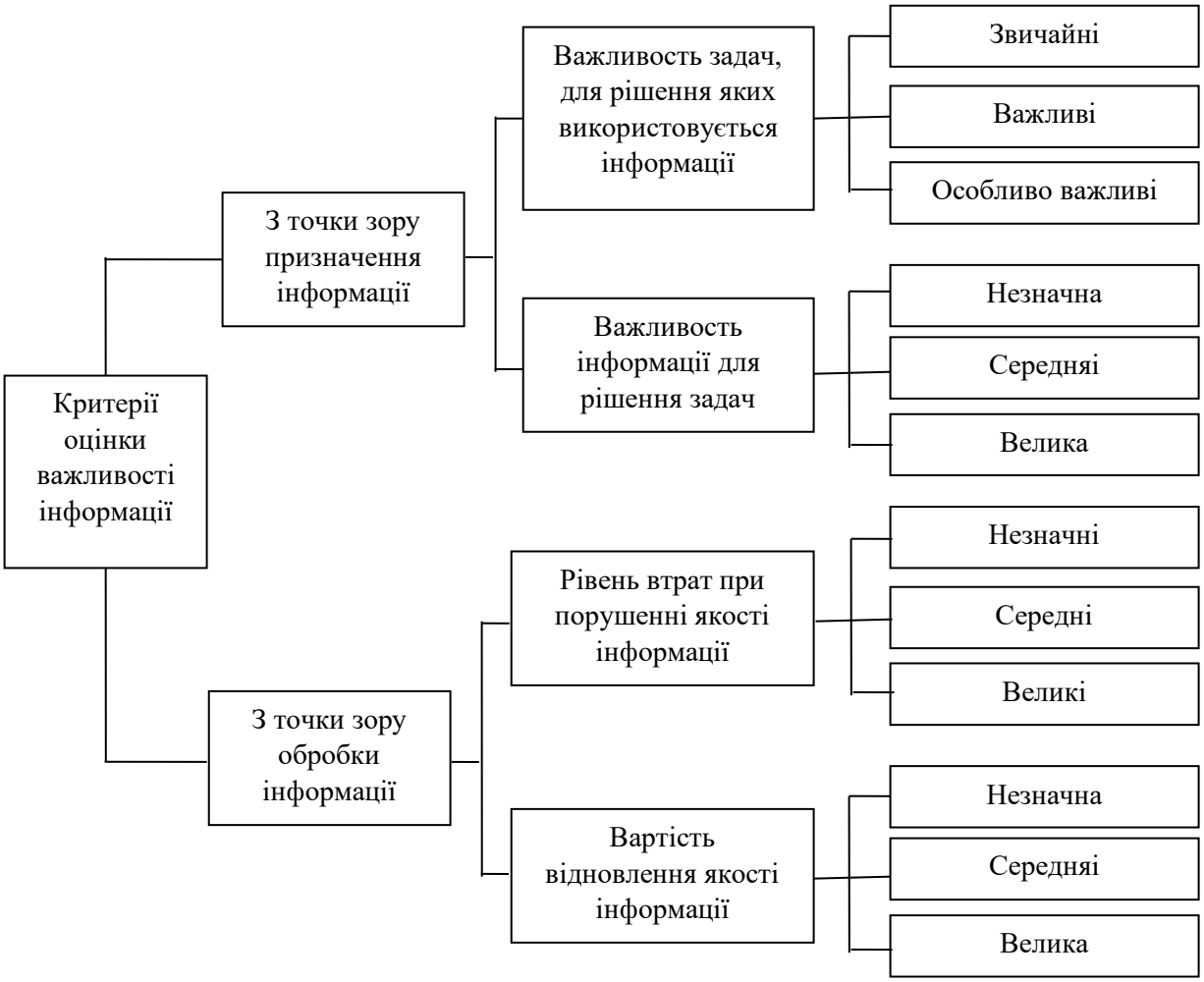


Рис. 5.2. Критерії оцінки важливості інформації

1. По призначенню інформації.
2. За умовами її обробки.

У першій групі слід виділити два критерії:

- Важливість самих завдань для забезпечення діяльності.
- Ступінь важливості інформації для ефективного розв'язку відповідного завдання.

У другій групі виділяються два складових критерію:

- Рівень втрат у випадку небажаних змін інформації в процесі обробки під впливом дестабілізуючих факторів.
- Рівень витрат на відновлення порушеної інформації.

Якщо позначити $K_{ВІ}$ – коефіцієнт важливості інформації; $K_{ВЗ}$ – коефіцієнт важливості тих задач, для забезпечення яких використовується інформація; $K_{ЕЗ}$ – коефіцієнт важливості оцінюваної інформації для ефективного розв'язку завдань; $K_{ВОІ}$ – коефіцієнт важливості оцінюваної інформації з погляду втрат при порушенні її якості; $K_{СВ}$ – коефіцієнт важливості оцінюваної інформації з погляду вартості відновлення її якості. Тоді одержимо:

$$K_{ВІ}=f(K_{ВЗ},K_{ЕЗ},K_{ВОІ},K_{СВ}). \qquad (5.19)$$

Тобто для оцінки важливості інформації необхідно вміти визначати значення перерахованих вище коефіцієнтів і знати вид функціональної залежності $K_{ВІ}$. Але на сьогоднішній день невідомі ні ті, ні інші, і є вагомі підстави стверджувати, що і у найближчім майбутньому ця проблема не буде вирішена, однак іноді для цих цілей для конкретної інформації і конкретних умов можна використовувати підхід, заснований на неформально-эврестических методах.

***Для оцінки захищеності інформації досліджують наступні її свойства*:**

Повнота інформації - це показник, що характеризує міру достатньості оцінюваної інформації для розв'язку відповідних завдань. Звідси випливає, що цей показник, є відносним: повнота інформації оцінюється відносно цілком конкретного завдання або групи завдань. Тому щоб мати можливість визначити показник повноти інформації, необхідно для кожного суттєво значимого завдання або групи завдань скласти перелік тих відомостей, які необхідні для їхнього розв'язку, Для надання таких відомостей зручно використовувати так звані об'єктивно - характерстичні таблиці, які уявляють собою двомірні матриці. У них по рядках наведений перелік найменувань тих об'єктів, процесів або явищ, які входять до кола інтересів відповідного завдання, а по стовпцях-найменування тих характеристик (параметрів) об'єктів, процесів або явищ, значення яких необхідні для розв'язку завдання. отже, саме значення характеристик будуть розташуються на перетинанні відповідних рядків і стовпців.

Адекватність інформації – ступінь її відповідності дійсному стану тих об'єктів, процесів, явищ, які відображає оцінювана інформація. У загальному випадку адекватність інформації визначається двома параметрами:

1. Об'єктивністю генерування (знімання, визначення, встановлення) інформації про об'єкт, процес або явище.

2. Тривалістю інтервалу часу між моментом генерування інформації і моментом її адекватності.

Об'єктивність генерування інформації залежить від способу одержання значень характеристик об'єкта, процесу, або явища і якості реалізації (використання) способу в процесі одержання цих значень. Класифікація характеристик по можливим способам отримання значень представлена на рис. 5.3.

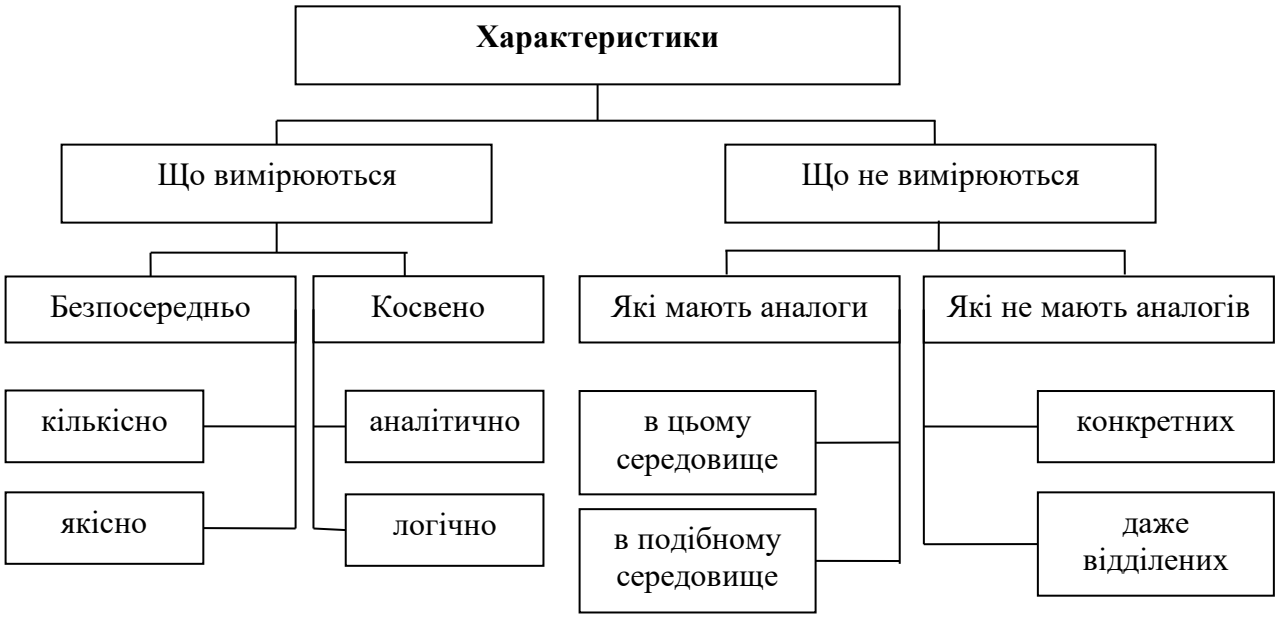


Рис. 5.3. Класифікація характеристик по способах отримання їх значень

Розглянемо тепер адекватність інформації із другого названого параметра – тривалості інтервалу часу між моментом генерування інформації і теперішнім моментом. Для оцінки адекватності по даному параметру цілком підходящим є відомий у теорії інформації так званий закон старіння інформації (рис. 5.4).

При цьому під t_0 – розуміється момент часу генерування (одержання) оцінюваної інформації; Δt_1 - тривалість часу, протягом якого оцінювана інформація повністю зберігає свою адекватність; Δt_2 - тривалість часу, протягом якого, адекватність інформації падає на 25%; Δt_3 - тривалість часу, протягом якого, адекватність інформації падає на половину; Δt_4 - тривалість часу, протягом якого, адекватність інформації падає на 75%.

Враховувая те, що обі дві складові адекватності інформації $K^{a'}$ і $K^{a''}$ залежать від великої кількості факторів, багато з яких носять випадковий характер, мається підстава стверджувати, що вони також носять випадковий характер і тому можуть інтерпретуватися як імовірності того, що інформація відповідного параметру є адекватною. Оскільки для переважної більшості теоретичних досліджень і практичних додатків важливо, щоб інформація була адекватної одночасно по обом параметрам, то відповідно до теореми множення ймовірностей загальний показник адекватності інформації може бути визначений як : $K^{a=}K^{a'} \cdot K^{a''}$. Незалежність значень a' і a'' представляється цілком природньою.

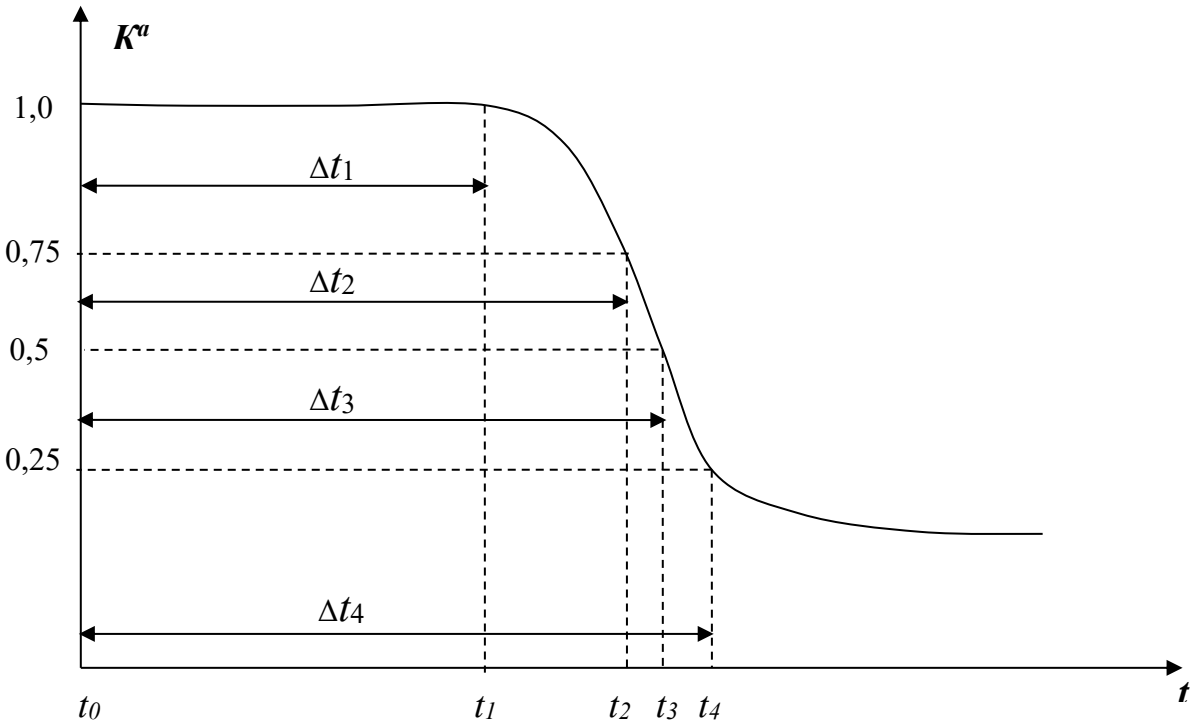


Рис. 5.4. Графічне представлення закону старіння інформації

Релевантність інформації - це показник, який характеризує відповідність її потребам розв'язуваного завдань. Для кількісного виразу цього показника використовують так званий коефіцієнт релевантності K_p - відношення обсягів релевантної інформації N_p до загального обсягу аналізованої інформації N_0, тобто

$$K_p = \frac{N_p}{N_0}. \qquad (5.20)$$

Сутність коефіцієнта релевантності зрозуміла, але труднощі практичного його використання пов’язані з кількісним виразом обсягу інформації. Тому завдання обчислення цього коефіцієнта на практиці ставиться до досить невизначеної і важкорозв'язної проблеми.

Толерантність інформації - це показник, що характеризує зручність сприйняття і використання інформації в процесах розв'язку того завдання, для розв'язку якого вона використовується. Вже з визначення зрозуміло, що поняття толерантності є дуже широким, значною мірою невизначеним і суб'єктивним. Тому не можна сподіватися на розробку строго формальної методики визначення толерантності інформації.

Необхідний рівень ЗІ повинен визначатися з урахуванням значень усіх розглянутих показників. Однак в цей час методика такого визначення відсутня і розробка її вимагає самостійних досліджень. У якості виходу цього положення можна використовувати наступну напівевристичну процедуру:

1. Усі показники інформації діляться на три категорії: визначальні, істотні і авторські, причому основним критерієм для такого розподілу повинна служити та мета, для досягнення якої здійснюється ЗІ.
2. Необхідний рівень захисту встановлюється за значеннями визначальних показників інформації.
3. Обраний рівень при необхідності може бути скорегований з урахуванням значення істотних показників. Значення другорядних показників при цьому можуть ігноруватися.

На підставі всього викладеного можна провести класифікацію методів і засобів ЗІ.

Методи захисту можна розділити на організаційні, технічні, криптографічні і програмні.

Засоби захисту у свою чергу можна розділити:

- постійно діючі;
- включаємі при виявленні спроб нападів.

По активності вони діляться на:

- пасивні;
- напівактивні;

- активні.

За рівнем забезпечення ЗІ засоби захисту підрозділяються на 4 класи:

- 1 клас: системи слабкого захисту;
- 2 клас: системи сильного захисту;
- 3 клас: системи дуже сильного захисту;
- 4 клас: системи особливого захисту.

Розглянемо предметну область ЗІ з позицій *структурної ієрархії.*

Вибір СЗІ (головна проблема) від передбачуваного способу нападу (зворотна проблема) і способів виявлення факту нападу (проміжна проблема).

Розв'язок завдання вибору залежить від форми надання інформації (відео, звукова, електромагнітний сигнал), а спосіб захисту - від передбачуваної форми впливу на інформацію (копіювання, знищення, викривлення), використовуваного носіями інформації (папір, магнітний диск і т.п), стану інформаційного масиву (перебуває в стані передачі, обробки або зберігання), від того, проводиться чи ЗІ безперервно або під час виявлення факту нападу. Даний тип ієрархії наглядно може бути представлений у вигляді семантичної схеми (рис. 5.5).

З погляду функціональної ієрархії СЗІ обмежує доступ, оперативно знищує носії інформації, і в тому числі ставить перешкоди для блокування активних дій порушників (рис. 5.6)

Рис. 5.5. Семантична схема проблеми захисту інформації за допомогою технічних засобів з позиції структурної ієрархії

З погляду *причинно - слідчої ієрархії* (рис. 5.7) у першому випадку СЗІ повинна виявити факт нападу. При виявленні факту нападу СЗІ реалізує деякий спосіб захисту. Виявлення факту нападу і реалізація конкретного способу захисту відбувається за умови, що заздалегідь відома кілька передбачуваних способів нападу. Сам спосіб нападу, у свою чергу, залежить від стану інформаційного масиву і форми надання інформації.

У другому випадку СЗІ працює безперервно, при цьому передбачається, що напад на інформацію може бути здійснений в будь-який час. СЗІ безперервно захищає інформаційний масив від декількох передбачуваних способів нападу з метою копіювання, викривлення знищення інформації шляхом її оперативного знищення, обмеження доступу, постановки перешкод і т.п.

Розглянемо деякі окремі випадки розв'язку проблеми ЗІ.

Спосіб захисту відеоінформації при її передачі залежить від способу передачі (оптоволоконний канал, телефонний канал, телевізійний канал,

провідний канал тощо), передбачуваного способу нападу, форми впливу на відеоінформацію.

Рис. 5.6. Семантична схема проблеми захисту інформації за допомогою технічних засобів з позиції функціональної ієрархії

Спосіб захисту *відеоінформації* при її зберіганні залежить від типу носія інформації, форм впливу на інформацію або її носій, передбачуваного способу нападу.

Спосіб *захисту звукової інформації* залежить: при *зберіганні* - від типу носія, форм впливу на інформацію або на носій, передбачуваного способу нападу: при *передачі* – від способу передачі, передбачуваного способу нападу, форм впливу на інформацію.

Спосіб захисту інформації, що існує у вигляді *електромагнітного сигналу*, який залежить від середовища поширення електромагнітного сигналу, довжини хвилі сигналу, наявності або відсутності спеціальної лінії зв'язку, передбачуваного способу нападу на інформацію.

Відповідно до вищевикладеного алгоритм проведення робіт із ЗІ повинен бути наступним.

1. Насамперед, необхідно визначити, чи є на об'єкті інформація, яку необхідно захищати, і який ступінь захисту повинен бути забезпечений. Крім того, слід визначити обсяг засобів, необхідних для забезпечення заданого рівня захисту.

2. Після оцінки доцільності створення СЗІ слід виявити або спрогнозувати, по можливості, усі загрози і можливі канали витоку інформації.

3. Наступним кроком є аналіз заходів щодо ЗІ об'єкта.

Для аналізу заходів щодо ЗІ на об'єкті необхідно оцінити напрямок діяльності системи захисту. Для побудови ефективної СЗІ доцільно виділити наступні напрямки:

Рис. 5.7. Семантична схема проблема захисту інформації за допомогою технічних засобів з позиції причинно-слідчої ієрархії

захист об'єкта;

захист процесів або процедур обробки і зберігання інформації, захист виробів;

захист каналів зв'язки;

придушення побічних електромагнітних лікувань;

контроль і керування СЗІ.

При цьому для захисту об'єктів необхідно виділити наступні функції, процедури і засоби захисту, незалежно від категорії об'єкта.

1. Мінімізація відомостей, доступних персоналу.
2. Мінімізація зв'язків персоналу.
3. Розподіл повноважень.

4. Мінімізація даних, які доступні персоналу.
5. Дублювання контролю.
6. Керування доступом.
7. Захист файлів і баз даних автоматизованих систем.
8. Ідентифікація захищеного об'єкта.
9. Надання повноважень.

Після визначень функцій ЗІ на об'єкті можна приступитися до аналізу вимог до КСЗІ.

Проектування систем захисту інформації поділяється на такі етапи:

- проектне обстеження, що формує базові вимоги до СЗІ;
- аналіз вимог до системи замовника;
- перетворення вимог на зрозумілі специфікації системи з подальшим проектуванням програмного та апаратного компонентів;
- виконання організаційно - технічних заходів, пов'язаних з розробкою та тестуванням компонентів системи;
- верифікація системи щодо вимог безпеки;
- Введення системи в експлуатацію.

Загальні принципи проектування:

- вартість побудови та експлуатації СЗІ має бути меншою за розміри збитків від будь-яких потенціальних загроз;
- програмний захист функціональних програм і даних має бути комплексним і багаторівневим, зорієнтованим на запобігання всім видам загроз з урахуванням відповідних можливих збитків;
- система повинна мати цільові, індивідуальні компоненти, що гарантують безпеку функціонування об'єкта з урахуванням його впливу на безпеку всієї системи;
- СЗІ не винна створювати перешкод і призводити до зниження ефективності інформаційної системи;

Процеси проектування СЗІ потребують аналізу конкретного завдання, даних тих факторів, що підтримують безпечне її функціонування. Передусім слід визначити:

- критерії якості та їх значення, що характеризують рівень безпеки інформаційної системи загалом та її основних систем і компонентів;
- перелік та характеристики можливих внутрішніх і зовнішніх дестабілізуючих факторів і загроз, що можуть вплинути на безпеку програмних засобів і баз даних;
- перелік завдань, необхідних для забезпечення захисту інформаційної системи із заданою ефективністю;
- необхідні та доступні ресурси;
- стандарти, нормативні документи та методики вимірювання показників безпеки;
- техніко-економічну оцінка проекту комплексу програм.

В основу формування вимог із захисту інформації потрібно покласти визначення переліку та характеристик потенціальних загроз інформаційної безпеки, а також встановлення можливих джерел їх виникнення (модель загроз).

5.4. Оцінка захищеності інформації

Інформація в сучасному світі набуває надзвичайної цінності, що зумовлено реальними прибутками, які отримують від її використання, або розмірами збитків унаслідок її втрати або несанкціонованого доступу до неї. Вирішення завдання оцінювання захищеності інформації від зловмисного вивчення технічних засобів захисту інформації з метою подальшого несанкціонованого доступу до інформації в засобах обчислювальної техніки та автоматизованих системах можливе завдяки використанню принципів системотехніки: досліджуваний процес описується на мовах теорій, які найбільш розвинені (результативні), і оцінюються за показниками ефективності підсистеми - людини, що визначає корисність створеної системи захисту інформації. При цьому використовується система математичних моделей, що має ієрархічну структуру, де математичні моделі «нижніх» рівнів уточнюють параметри «вищих» рівнів. Той факт, що системі захисту властива невизначеність (наскільки досконала створена система захисту інформації, а також яка її тимчасова стійкість в умовах «атак» зловмисника), дозволяє застосувати для оцінювання захищеності інформації показники ефективності ймовірнісно-тимчасової групи показників:

- середній час безпомилкового функціонування системи захисту;
- година безпомилкового функціонування системи захисту з імовірністю її спотворень вище заданим НСД;
- економічна ефективність створеної системи захисту інформації.

У нашому випадку завдання оцінювання стійкості системи захисту інформації від її зловмисного вивчення може бути сформульоване наступним чином:

- нехай мається система обробки даних, у якій реалізована КСЗІ на основі технічних засобів захисту інформації;
- до зловмисників потрапив примірник опису технічного засобу й розпочався процес його вивчення.

Тому потрібно оцінити стійкість КСЗІ до її злочинного вивчення за обраними показниками ефективності. Математична модель зловмисника повинна надати інформацію щодо чисельних характеристик ймовірностей виявлення спроб НСД на певному інтервалі години.

Вирішення завдання розробки моделі зловмисника, який вивчає технічний засіб захисту, передбачає пошук системи теорій:

- теорію, яка дозволила б пов'язати складність реалізованого розробником алгоритму захисту інформації, що знаходиться в конкретному технічному засобі, і час, необхідний зловмиснику для вивчення (розшифровки) цього алгоритму;

- теорію, яка могла б пов'язати знайдений час вивчення (розшифровки) алгоритму з імовірністю того, що зловмисник може виконати цю роботу за певний інтервал часу.

Аналіз показує, що перше завдання може бути вирішене через використання лінійної теорії алгоритмів відповідно.

Друге завдання може бути вирішене завдяки використанню теорії кадастрів, яка викладена у теорії масового обслуговування.

Розглянемо обидві теорії стосовно поставленої задачі.

Лінійна теорія алгоритмів у вирішенні завдання оцінки часу, необхідного зловмиснику для вивчення СЗІ – це завдання вивчення (розшифровки) програми довжиною N_1, яка написана на певній алгоритмічній мові, яку за складністю можна порівняти з написанням програми довжиною $N_{á³ð}$ тією ж мовою. Для його вирішення скористаємося апроксимацією рівняння часу, необхідного для написання програм - $N_{á³ð}$. У цьому випадку середній час вивчення (розшифровки) програми T можна знайти як:

$$T = \frac{N_2^2 \times \log_\tau}{4 \times S}[c], \tag{5.41}$$

де τ - алфавіт мови тексту програми; S - число Страуд ($S = 4 \div 20$ операцій за секунду, характеризує кількість об’єктів, яким може оперувати зловмисник одночасно); N- довжина тексту (команди + операнди) у бітах. За «Холстером», у разі якщо необхідно писати програму на машинній мові, то $TH \approx N^2(c)$.

Оскільки програми захисту інформації характеризуються великою довжиною, слід брати до уваги стомлюваність зловмисника. У цьому разі вираз для T буде мати вигляд:

$$T = 3N^2(c) \tag{5.42}$$

Теорія захисту інформації, керівні документи Державної служби спеціально зв'язку та захисту інформації України вимагають розглядати зловмисника як суб'єкт вищої кваліфікації, що дає можливість надати процесу зловмисного вивчення СЗІ – функцію розподілу розумного зловмисника - еспоненційний розподіл з параметром S=1/T(1/с), де T – середній час розшифровки (вивчення тексту програми.)

У цьому випадку ймовірність P_i не розшифровки тексту програми ща певний інтервал години (не настане катастрофа), розподіленому за

експоненціальним законом з параметром β, можна представити як перетворення Лапласа – функції розподілу інтервалу часу, на якому оцінюється ймовірність розшифровки (вивчення) тексту β(t):

$$Ð_i = 0\int^{\infty} å^{-st} dB(t) \frac{\beta}{\beta + S} \tag{5.43}$$

Таким чином, вдалося «плавно » перейти від довжини тексту програми *N*, написаної на певній алгоритмічний мові, яку передбачив для зловмисника розробник СЗІ, до ймовірності не розшифровки тексту програм захисту за певний інтервал часу, розподілений за експоненціальним законом.

Передбачається, що апаратні засоби СЗІ опускають «розгортання» у текст програми кінцевої довжини і текст програми захисту становить суму текстів програмної і апаратної частин.

Математична модель системи захисту інформації, системи обробки даних і зловмисника становить процес взаємодії:

- зловмисника, який вивчає СЗІ та оцінює успішність НСД;
- здатність СОД обробляти (зберігати) документи, що надійшли до неї, які підлягають захисту;
- документів, що надходять до СОД;
- створені розробником засоби захисту інформації характеризуються кінцевою нескінченністю можливих станів:

$$S = (S_1, S_2 ... S_r) \tag{5.44}$$

Процес у кожен момент часу t характеризується тільки одним з цих станів.

$$S_1 \left| n_{ij} \right| S_i \in S$$

$$m_j$$

$$T^* = \left\| t^* \right\| \lambda$$

$$N^* = \left\| n_{ij}^* \right\|;$$

$$N = (I - Q)^1$$

$$N = \left\| n_{ij}^* \right\|$$

$$D = C_1 \times P_{Í ÅÄ} - C_2 (1 - P_{Í ÅÄ})$$

Через деякі інтервали години відбуваються переходи з одного стану в інший (має місце крок процесу). Імовірність того, що на черговому кроці система перейде зі стану в стан S_j, у загальному випадку, залежить від

початкового стану системи і усіх проміжних станів аж до потокового. На сьогодні докладно вивчені ланцюги, що володіють харківською властивістю. У цьому випадку ймовірність переходу на черговому кроці зі стану S_i, у якому ланцюг виявився після попереднього кроку (поведінка системи в майбутньому залежить від її стану на цей момент і не залежить від того,яким чином вона перейшла в цей стан).

Отже, припустимо, що :

- імовірність одночасної зміни станів двох і більше елементів украй незначна;
- імовірність переходів з одного стану в інший не залежить від часу;
- за надзвичайно малий проміжок часу неможливий перехід у певний «сусідній» стан та повернення з нього .

За таких умов процес взаємодії математично характеризується напівмарківським процесом: з матрицею ймовірностей переходів, що поглинає ланцюг (поглинаючий стан характеризує тієї факт, що зловмисник, на його думку, вивчив (розшифрував) СЗІ і готовий на практиці реалізувати спробу НСД):

$$P = \begin{pmatrix} P_{11} & P_{12} \dots & P_{1r} \\ P_{21} & P_{22} \dots & P_{2r} \\ \dots & \dots\dots & \dots \\ P_{r1} & P_{r2} \dots & P_{rr} \end{pmatrix} i \qquad (5.45)$$

У загальному випадку розглянута система формально є СОД, на вхід якої надходити інформація, або документи,що підлягають захисту. Документи, що надійшли, характеризуються пуасонівським потоком з параметром β.

Документи, які надходять до СОД у певний час, який характеризуються партером γ.

Інтерес зловмисника до документів, що підлягають захисту, характеризується потоком спроб НСД з параметром НСД λ .

«за Холстедом» та використанням теорії катастроф отримаємо чисельні значення ймовірностей:

P_1- імовірність виявлення НСД у моменти часу, коли в системі немає інформації, що захищається;

P_2- імовірність виявлення спроби НСД на етапі аутентифікації прийнятого документа;

P_3- імовірність виявлення спроби НСД на етапі обробки (зберігання). документа, який отримано.

Крім цього відомі такі величини: дохід C_1 одиниць цінності отриманої, від обробки інформації, захищеного документа; збитки C_2 одиниць цінності від НСД до інформації захищеного документа.

Тоді завдання оцінювання ефективності захисту зводиться до оцінки середнього часу перебування напівмарковського процесу в безлічі незворотних станів до поглинання і використання його для отримання ймовірнісно-часових характеристик показників ефективності.

Оскільки розглянута система характеризується поглинаючим станом, коли зловмисник виявив, що для нього немає секретів і він готовий реалізувати свій задум, то математичний вираз середнього часу безпомилкового функціонування досліджуваної системи можна визначити як середній час пербування даної системи в безлічі незворотних станів, при цьому середній час t перебування досліджуваного процесу в безлічі незворотних станів може бути знайдено як добуток матриць:

$$\begin{aligned} t &= P(0)N^*E \\ P_{\text{Í ÅÄ}} &= \int_0^\infty e^{-\mu t} dS(t) \frac{S}{S+\mu} \\ D &> 0 \\ P_2 & \end{aligned} \qquad (5.46)$$

де $P(0)$ - матриця - вектор на початковому стані, з якого розпочався процес, що досліджується; $N^* = \left\| n_{ij}^* \right\|$ - матриця середнього часу n_{ij}^* перебування напівмарківського процесу в стані $S_i \in S$ до поглинання за умови, що початковим був стан $S_i \in S$.

$$N^* = \left\| n_{ij}^* m_{ij} \right\|;$$

де m_j - середній час одноразового перебування напівмарквського процесу в незворотних станах; $S_i \in S$; n_{ij} - елемент фундаментальної матриці $N = \left\| n_{ij} \right\|$, виходить з виразу $N = (I - Q)^{-1}$; Q- матриця переходів у кінцевій безлічі станів;

Таким чином, для того, щоб визначити середній час безпомилкового функціонування досліджуваної системи, необхідно:

- з матриці переходів досліджуваного процесу P отримати матрицю переходів у кінцевий безлічі станів Q і m_j - середній час одноразового перебування напівмарковського процесу в незворотних станах $S_i \in S$;

- отримати фундаментальну матрицю $N = \left\| n_{ij} \right\|$; згідно з виразом $N = (I - Q)^1$.

- отримати матрицю середніх часів n_{ij}^* перебування напівмарківського процесу в стані $S_i \in S$ до поглинання за умові, що початковим був стан S $S_i \in S$:

$$N^* = \left\| n_{ij}^* \right\|$$

- конкретизувати вектор-стовпець початкового стану, з якого розпочався процес, що досліджується;
- використовуючи вираз $t = P(0)N^*E$, отримати чисельне значення середнього часу безпомилкового функціонування системи захисту.

Вираз (1.46) дозволяє оцінити середній час безпомилкового функціонування системи захисту. Однак СЗІ повинна експлуатуватися. Експлуатація повинна включати перевірку несправності СЗІ за досягнення системою певного порога довіри - ймовірності включення НСД до інформації, що захищається нижче заданого.

Апроксимуємо функцію розподілу часу, на довіру до СЗІ не нижче заданого, а також функцію розподілу часу безпомилкового функціонування експоненціальними розподілами з параметрами S і μ відповідно:

$$\mu = 1/\mathrm{T}$$

Оскільки відповідно до теорії катастроф імовірність виключення НСД - $P_{Í ÀÄ}$ на інтервалі, розподіленому за експоненціальним законом з параметром s:

$$P_{Í ÀÄ} = \int_0^\infty e^{-\mu t} dS(t) \frac{S}{S+\mu} \tag{5.47}$$

Тоді середній час безпомилкового функціонування системи захисту з імовірністю виключення НСД не нижче $P_{Í ÀÄ}$ можна знайти як:

$$TO = \frac{1}{S} = \frac{t(1 - P_{Í ÀÄ})}{P_{Í ÀÄ}} \tag{5.48}$$

З виразу (5.48) випливає, що після закінчення часу для підтримки створеної СЗІ, необхідне проведення регламентних робіт. Формою повернень «довіри» до СЗІ може бути й впровадження чергової версії технічного засобу захисту інформації. Цим ми умовно ставимо зловмисника перед необхідністю освоєння щоразу більш нового технічного засобу захисту.

Таким чином, для того щоб обчислити середній час, що минав між проведеннями регламентних робіт, необхідно:

- відповідно до виразу (5.46) одержати середнє чисельне значення часу безвідмовної функціонування системи захисту;

- оцінити необхідний рівень захисту інформації нижнім порогом довіри до СЗІ- $P_{\text{Í ÄÄ}}$.

- використати значення інтервалу часу, протягом якого забезпечується захищеність інформації не нижче встановленого рівня.

Як уже зазначалося раніше, інформація в сучасному світі набуває надзвичайної цінності, що зумовлено реальними прибуткам, які отримують від її використання, або розмірами збитків унаслідок її втрати або несанкціонованого доступу (НСД) до неї.

Покладемо цей постулат в основу висновку математичного виразу оцінки доходу, отримуваного від використання СЗІ.

Оскільки процес функціонування досліджуваної системи через рівномірні інтервали включає проведення регламентних робіт (передбачається що досягнутий рівень довіри до СЗІ дорівнює нижньому порогу довіри $P_{\text{Í ÄÄ}}$), то обробка кожної інформаціє, що надійшла з імовірністю $P_{\text{Í ÄÄ}}$, приносить дохід в C_1 одиниць вартості, а з ймовірністю $(1-P_{\text{Í ÄÄ}})$ - збиток в C_2 одиниць вартості. У цьому випадку математичний вираз доходу *D*, принесеного кожною інформацією, що надійшла, складі дорівнює:

$$D = C_1 \times P_{\text{Í ÄÄ}} - C_2(1-P_{\text{Í ÄÄ}}) \qquad (5.49)$$

Природно вважати, що у випадку $D>0$ застосування технічного засобу захисту приносити дохід.

Оцінювання ймовірності розшифровки програмного модуля СЗІ між моментами надходження інформації в СОД може бути здійснене таким чином.

Визначимо:

P_1 - ймовірність розшифровки тексту програми модуля захисту інформації на етапі відсутності інформації в СОД (ймовірність не блокування системи захисту інформації для цього етапу);

P_2 - ймовірність не розшифровки програми модуля захисту інформації на етапі прийому (формування) інформації в СОД між сусідніми моментами надходження інформації в СОД (ймовірність не блокування системи захисту інформації для цього етапу);

P_3 - ймовірність не розшифровки тексту програм модуля захисту інформації в СОД між сусідніми моментами надходження інформації в СОД (ймовірність неблокуваняя системи захисту інформації цього етапу).

λ

$N_1 \gamma P_3 \approx 1$

$S_1, S_2, S_3, S_4, S_5 -$

$P_{11} = \lambda P1/(\lambda+\beta)$;

$P_{12} = \beta/(\lambda+\beta);$

$P_{13} = \lambda(1-P_1)/(\lambda+\beta);$

$P_{21} = \gamma/(\lambda+\gamma);$

$P_{22} = P_2\lambda(\lambda+\gamma);$

$P_{24} = (1-P_2)\lambda(\lambda+\gamma);$

$P_{32} = P_2; P_{34} = 1-P_{2;}$

$P_{41} = P_3; P_{45} = 1-P_3;$

$$M = \frac{1}{\lambda+\beta}\frac{1}{\lambda+(1-P_2)\gamma}\frac{1}{\beta}\frac{1}{\gamma}$$

Оскільки використовується Паусонівський закон надходження інформації програмного модуля довжиною $N_{1,}$ СЗІ між моментами надходження інформації в СОД оцінюється згідно з (5.43) як:

$$P_1 = P_2 = P_3 = 1 - \frac{1/T}{\beta + 1/T}$$

У СОД реалізована системана підставі технічних засобів захисту. Ці кошти забезпечують захист інформації на всіх етапах перебування й обробки в системі. Таким чином, досліджувана система характеризується:

- пуасонівським потоком подій, пов'язаних з НСД з параметром λ;
- пуасонівським потоком інформації, що підлягає захисту з партерами β;
- експоненціальним розподілом часу обробки (перебування)інформації в системі, що захищається, з параметром γ;

У СОД створено комплекс СЗІ, який забезпечує:

1) захист інформації на інтервалі часу, коли її немає в системі, що захищається, з імовірністю $P_1 \approx 1$;

2) захист інформації на інтервалі часу, коли повідомлення надійшло до системи захисту - на етапі попередньої обробки (аутентифікації) надійшло повідомлення $P_2 \approx 1$;

3) Захист інформації під час опрацювання надходження повідомлення (обробки інформації) - $P_3 \approx 1$.

Будемо виходити з того, що зловмисникові цікаве кожне повідомлення, що надійшло до системи.

Це робить можливим для цієї системи використання формалізму при пуасонівському потоці подій, пов'язаних з НСД, до повідомлень з параметром, що чисельно дорівнює параметру потоку інформації.

У нашому випадку процес функціонування системи захисту може бути представлений у вигляді графа переходів і матриці переходів отут S_1, S_2, S_3, S_4, S_5 – безліч станів;

Припустимо те, що процес преходів є марківським. У цьому разі зазаначений процес переходів описується матрицею преходів.

$$P_{11} = \lambda P1 / (\lambda + \beta) \ ;$$
$$P_{12} = \beta / (\lambda + \beta);$$
$$P_{13} = \lambda(1 - P_1) / (\lambda + \beta);$$
$$P_{21} = \gamma / (\lambda + \gamma);$$
$$P_{22} = P_2\lambda(\lambda + \gamma);$$
$$P_{24} = (1 - P_2)\lambda(\lambda + \gamma);$$
$$P_{32} = P_2; P_{34} = 1 - P_{2;}$$
$$P_{41} = P_3; P_{45} = 1 - P_3;$$

При цьому середній час одиничного пребування системи в одному з незворотніх станів складає:

$$M = \frac{1}{\lambda + \beta} \frac{1}{\lambda + (1 - P_2)\gamma} \frac{1}{\beta} \frac{1}{\gamma} \tag{5.50}$$

Оцінка середнього часу безвідмовного функціонування захищеної системи полягає в обчисленні середнього часу перебування процесу в безлічі неповоротних станів матрици.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

5.1 Що собою уявляе критерій вибору засобів і методів захисту.

5.2 Сформулювати задачу оптимального вибору методів захисту для кожного конкретного об’єкта і для системи в цілому.

5.3 Розкрити критерій вибору засобів і методів захисту.

5.4 Розкрити задачу мінімізації вартості забезпечення захисту об’єкта.

5.5 Розкрити задачу мінімізації ефективності систем захисту об’єкта.

5.6 Розкрити задачу мінімізації вірогідності злому усіх методів, які використовуються для захисту об’єкта.

5.7 Розкрити задачу мінімізації втрат від злому усіх механізмів захисту (методів захисту), які використовуються для захисту об’єкта.

5.8 Розкрити вимоги до СЗІ та пояснити їх.

5.9 Розкрити та пояснити задачі підсистеми управління доступом.

5.10 Розкрити та пояснити задачі підсистеми реєстрації та обліку.

5.11 Розкрити та пояснити задачі криптографічної підсистеми.

5.12 Розкрити та пояснити задачі підсистеми забезпечення цілісності.

5.13 Розкрити та пояснити заходи, які виконуються при створенні КСЗІ.

5.14 Розкрити та пояснити показники захисту інформаці.

5.15 Розкрити та пояснити напрямки побудови ефективної СЗІ.

5.16 Розкрити та пояснити загальні принципи проектування СЗІ.

5.17 Вивести імовірністні показники оцінки інформативності конфіденційної інформації щодо об'єкту захисту.

5.18 Вивести часові показники оцінки інформативності конфіденційної інформації щодо об'єкту захисту.

5.19 Розкрити порядок оцінки середнього часу вивчення програм захисту зловмисником.

5.20 Розкрити алгоритм визначення середнього часу безпечного функціонування системи захисту.

РОЗДІЛ 6. НАЙПОШИРЕНІШІ ЗАГРОЗИ ІНФОРМАЦІЇ

6.1. Основні означення і критерії загроз

Найчастіше загроза є наслідком наявності уразливих місць у кіберзахисті інформаційних систем (таких, наприклад, як можливість доступу сторонніх осіб до критично важливого устаткування або помилки в програмному забезпеченні).

Проміжок часу від моменту, коли з'являється можливість використати слабке місце, і до моменту, коли прогалина ліквідується, називається вікном небезпеки, асоційованим з даним уразливим місцем. Поки існує вікно небезпеки, можливі успішні атаки на ІС.

Якщо мова йде про помилки в ПЗ, то вікно небезпеки «відкривається» з появою засобів використання помилки й ліквідується при накладенні «латок», які її виправляють.

Для більшості уразливих місць вікно небезпеки існує порівняно довго (кілька днів, іноді – тижнів), оскільки за цей час повинні відбутися такі події [9,10]:

повинно стати відомо про засоби використання прогалини в кіберзахисті;

повинні бути випущені відповідні «латки»;

«латки» повинні бути встановлені в захищуваній ІС.

Ми вже вказували, що нові уразливі місця й засоби їхнього використання з'являються постійно; це значить, по-перше, що майже завжди існують вікна небезпеки й, по-друге, що відстеження таких вікон повинно проводитися постійно, а випуск і накладання «латок» – якомога оперативніше.

Відзначимо, що деякі загрози не можна вважати наслідком якихось помилок або прорахунків; вони існують у самій природі сучасних ІС. Наприклад, загроза відключення електрики або виходу її параметрів за припустимі межі існує внаслідок залежності апаратного забезпечення ІС від якісного електроживлення.

Розглянемо найпоширеніші загрози, яким піддаються сучасні інформаційні системи. Мати уявлення про можливі загрози, а також про уразливі місця, які ці загрози зазвичай експлуатують, необхідно для того, щоб вибирати найбільш економічні засоби забезпечення безпеки. Занадто багато міфів існує в сфері інформаційних технологій (згадаємо все ту ж «Проблему 2000»), тому незнання в цьому випадку веде до перевитрати коштів й, що ще гірше, до концентрації ресурсів там, де вони не дуже потрібні, за рахунок ослаблення дійсно уразливих напрямків. Підкреслимо, що саме поняття «загроза» у різних ситуаціях найчастіше трактується по-різному. Наприклад, для підкреслено відкритої організації загроз конфіденційності може просто не існувати – вся інформація вважається загальнодоступною; однак у більшості випадків нелегальний доступ є серйозною небезпекою. Іншими словами, загрози, як і все в ІБ, залежать від інтересів суб'єктів інформаційних відносин (і від того, який збиток є для них неприйнятним).

Ми спробуємо подивитися на предмет з точки зору типової (на наш погляд) організації. Втім, багато загроз небезпечні для всіх.

Загрози можна класифікувати за декількома критеріями [15,16]:

аспектом інформаційної безпеки (доступність, цілісність, конфіденційність), ещеиого загрози спрямовані в першу чергу;

компонентами інформаційних систем, на які загрози націлені (дані, програми, аппарат, підтримувальна інфраструктура);

способом здійснення (випадкові/навмисні дії природного/техно- генного характеру);

розташуванням джерела загроз (усередині/поза розглянутим ІС).

Як основний критерій ми будемо використовувати перший (за аспектом ІБ), залучаючи при необхідності інші.

6.2. Найпоширеніші загрози доступності

Найчастішими й найнебезпечнішими (з погляду розміру збитку) є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів й інших осіб, які обслуговують інформаційні системи.

Іноді такі помилки і є властиво загрозами (неправильно введені дані або помилка в програмі, що викликала крах системи), іноді вони створюють уразливі місця, якими можуть скористатися зловмисники (такими є помилки

адміністрування). За деякими даними, до 65% втрат – наслідок ненавмисних помилок.

Пожежі й повені не приносять стільки лих, скільки безграмотність і недбалість у роботі.

Очевидно, найрадикальніший засіб боротьби з ненавмисними помилками – максимальна автоматизація й строгий контроль.

Інші загрози доступності класифікуємо за компонентами ІС, на які націлені загрози [12,21]:

відмова користувачів;

внутрішня відмова інформаційної системи;

відмова підтримувальної інфраструктури.

Звичайно, стосовно користувачів розглядаються такі загрози:

небажання працювати з інформаційною системою (найчастіше проявляється при необхідності освоювати нові можливості й при розбіжності між запитами користувачів і фактичними можливостями та технічними характеристиками);

неможливість працювати з системою внаслідок відсутності відповідної підготовки (недостатня загальна комп'ютерна грамотність, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією й т. п.);

неможливість працювати з системою внаслідок відсутності технічної підтримки (неповнота документації, недостатньо довідкової інформації тощо).

Основними джерелами внутрішніх відмов є [12,21,22]:

відхід (випадковий або навмисний) від установлених правил експлуатації;

вихід системи зі штатного режиму експлуатації внаслідок випадкових або навмисних дій користувачів або обслуговувального персоналу (перевищення розрахункового числа запитів, надмірний обсяг оброблюваної інформації й т. п.);

помилки при переконфігуруванні системи;

відмови програмного й апаратного забезпечення;

руйнування даних;

руйнування або ушкодження апаратури.

Стосовно підтримувальної інфраструктури рекомендується розглядати такі загрози:

порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо- і/або теплопостачання, кондиціонування;

руйнування або ушкодження приміщень;

неможливість або небажання обслуговувального персоналу й/або користувачів виконувати свої обов'язки (цивільні безладдя, аварії на транспорті, терористичний акт або його загроза, страйк і т. п.).

Досить небезпечні так звані «скривджені» співробітники – нинішні й колишні. Як правило, вони прагнуть завдати шкоди організації-«кривднику», наприклад [12,22]:

зіпсувати устаткування;

вмонтувати логічну бомбу, що згодом зруйнує програми й/або дані;

видалити дані.

Скривджені співробітники, ще й знайомі з порядками в організації, здатні завдати чималої шкоди. Необхідно стежити за тим, щоб при звільненні співробітника його права доступу (логічного і фізичного) до інформаційних ресурсів анулювалися.

Небезпечні, зрозуміло, стихійні лиха й події, які сприймаються як стихійні лиха: пожежі, повені, землетруси, урагани. За статистикою, на частку вогню, води й тому подібних «зловмисників» (серед яких найнебезпечніший – перебій електроживлення) припадає 13% втрат, нанесених інформаційним системам.

6.3. Шкідливе програмне забезпечення

Одним з найнебезпечніших способів проведення атак є впровадження в системи, які атакують, шкідливого програмного забезпечення. Ми виділимо межі шкідливого ПЗ [21,22,23]:

шкідлива функція;

спосіб поширення;

зовнішнє подання.

Частину, що здійснює руйнівну функцію, будемо називати «бомбою» (хоча, можливо, більш вдалими термінами були б «заряд» або «боєголовка»). Загалом кажучи, спектр шкідливих функцій необмежений, оскільки «бомба», як і будь-яка інша програма, може мати яку завгодно складну логіку, але звичайно «бомби» призначаються для [21,22,23]:

впровадження іншого шкідливого ПЗ;

отримання контролю над системою, яку атакують;

агресивного споживання ресурсів;

зміни або руйнування програм й/або даних. За механізмом поширення розрізняють:

віруси – код, що має здатність до поширення (можливо, зі змінами) шляхом впровадження в інші програми;

«хробаки» – код, здатний самостійно, тобто без впровадження в інші програми, викликати поширення своїх копій по ІС й їхнє виконання (для активізації вірусу потрібен запуск зараженої програми).

Віруси звичайно поширюються локально, у межах вузла мережі; для передачі по мережі їм потрібна така зовнішня допомога, як пересилання зараженого файлу. «Хробаки», навпаки, орієнтовані, в першу чергу, на подорожі по мережі.

Іноді саме поширення шкідливого ПЗ викликає агресивне споживання ресурсів і, отже, є шкідливою функцією. Наприклад, «хробаки» «з'їдають» пропускні шляхи мережі й ресурси поштових систем. І з цієї причини для атак на доступність вони не мають потреби у вбудовуванні спеціальних «бомб».

Шкідливий код, що виглядає як функціонально корисна програма, називається троянським. Наприклад, звичайна програма, бувши ураженою вірусом, стає троянською; часом троянські програми виготовляють вручну й підсовують довірливим користувачам у якому-небудь привабливому пакунку.

Відзначимо, що дані нами означення й наведена класифікація шкідливого ПЗ відрізняються від загальноприйнятих.

Вікно небезпеки для шкідливого ПЗ з'являється з випуском нового різновиду «бомб», вірусів й/або «хробаків» і перестає існувати з відновленням бази даних антивірусних програм і накладенням інших необхідних «латок».

За традицією з усього шкідливого ПЗ найбільша увага громадськості зосереджується на частці вірусів. Однак до березня 1999 року з повним правом можна було стверджувати, що «незважаючи на експонентний ріст числа відомих вірусів, аналогічного росту кількості інцидентів, викликаних ними, не зареєстровано. Дотримання нескладних правил «комп'ютерної гігієни» практично зводить ризик зараження до нуля. Там, де працюють, а не грають, число заражених комп'ютерів становить лише частки відсотка».

У березні 1999 року, з появою вірусу «Melissa», ситуація кардинальним чином змінилася. «Melissa» – це макровірус для файлів MS-Word, що поширюється за допомогою електронної пошти в приєднаних файлах. Коли такий (заражений) приєднаний файл відкривають, він розсилає свої копії за першими 50 адресами з адресної книги Microsoft Outlook. У результаті поштові сервери піддаються атаці на доступність.

У цьому випадку нам хотілося б відзначити два моменти.

Як уже говорилося, пасивні об'єкти відходять у минуле; так званий активний уміст стає нормою. Файли, які за всіма ознаками повинні були б належати до даних (наприклад, документи у форматах MS-Word або Postscript, тексти поштових повідомлень), здатні містити інтерпретовані компоненти, які можуть запускатися неявним чином при відкритті файлу. Як

і будь-яке в цілому прогресивне явище, таке «підвищення активності даних» має свій зворотний бік (у розглянутому випадку – відставання в розробці механізмів безпеки й помилки в їхній реалізації). Пересічні користувачі ще не скоро навчаться застосовувати інтерпретовані компоненти «у мирних цілях» (або хоча б довідаються про їхнє існування), а перед зловмисниками відкрилося, власне кажучи, необмежене поле діяльності.

Інтеграція різних сервісів, наявність серед них мережевих, загальна зв'язність багаторазово збільшують потенціал для атак на доступність, полегшують поширення шкідливого ПЗ (вірус «Melissa» – класичний тому приклад). Образно кажучи, багато інформаційних систем, якщо не вжити захисних заходів, виявляються «в одному човні», так що досить однієї пробоїни, щоб «човен» відразу пішов на дно.

Як це часто буває, слідом за «Melissa» з'явилася на світ ціла серія вірусів, «хробаків» і їхніх комбінацій [8,12,14]: «Explorer.zip» (червень 1999), «Bubble Boy» (листопад 1999), «ILOVEYOU» (травень 2000) і т. д. Не те щоб від них був особливо великий збиток, але суспільний резонанс вони викликали чималий.

Активний вміст, крім інтерпретованих компонентів документів й інших файлів даних, має ще одне популярне обличчя – так звані мобільні агенти. Це програми, які завантажуються на інші комп'ютери й там виконуються. Найбільш відомі приклади мобільних агентів – Java-апплети, що завантажуються на комп'ютер користувача й інтерпретуються Internet-навігаторами. Виявилося, що розробити для них модель безпеки, яка залишає досить можливостей для корисних дій, не так вже й просто; ще складніше реалізувати таку модель без помилок. У серпні 1999 року стали відомі недоліки в реалізації технологій Active й Java у рамках Microsoft Internet Explorer, які давали можливість розміщати на Web-серверах шкідливі апплети, що дозволяють одержувати повний контроль над системою- візитером.

Для впровадження «бомб» часто використовуються помилки типу «переповнення буфера», коли програма, працюючи з областю пам'яті, виходить за межі припустимого й записує в потрібні зловмисникові місця певні дані. Так діяв ще в 1988 році знаменитий «хробак Моріса»; у червні 1999 року хакери знайшли спосіб використати аналогічний метод стосовно Microsoft Internet Information Server (IIS), щоб одержати контроль над Web-сервером. Вікно небезпеки охопило відразу біля півтора мільйона серверних систем.

Не забуті сучасними зловмисниками й випробовані троянські програми. Наприклад, «троянці» Back Orifice й Netbus дозволяють одержати контроль над системами користувачів з різними варіантами MS-Windows.

Таким чином, дія шкідливого ПЗ може бути спрямована не тільки проти доступності, але й проти інших основних аспектів інформаційної безпеки.

6.4. Основні загрози цілісності

На другому місці за масштабами збитків (після ненавмисних помилок і недоглядів) стоять крадіжки й підробки. За даними газети USA Today, ще в 1992 році в результаті подібних протиправних дій з використанням персональних комп'ютерів американським організаціям був нанесений загальний збиток у розмірі 882 мільйони доларів. Можна припустити, що реальний збиток був набагато більшим, оскільки багато організацій зі зрозумілих причин приховують такі інциденти; не викликає сумнівів, що в наші дні збиток від такого роду дій виріс багаторазово.

У більшості випадків винуватцями виявлялися штатні співробітники організацій, відмінно знайомі з режимом роботи й заходами захисту. еще раз підтверджує небезпеку внутрішніх загроз, хоча говорять і пишуть про них значно менше, ніж про зовнішні. Раніше ми відокремлювали поняття статичної й динамічної цілісностей. З метою порушення статичної цілісності зловмисник (як правило, штатний співробітник) може [22,24]:

ввести недостовірні дані;

змінити дані.

Іноді змінюються змістовні дані, іноді – службова інформація.

Можна зробити висновок, що існують не тільки загрози порушення цілісності, але й є небезпека сліпої довіри до комп'ютерної інформації. Заголовки електронного листа можуть бути підроблені; лист у цілому може бути фальсифікований особою, що знає пароль відправника (ми наводили відповідні приклади). Відзначимо, що останнє можливо навіть тоді, коли цілісність контролюється криптографічними засобами. Тут має місце взаємодія різних аспектів інформаційної безпеки: якщо порушено конфіденційність, може постраждати цілісність.

Ще один урок: загрозою цілісності є не тільки фальсифікація або зміна даних, але й відмова від зроблених дій. Якщо немає засобів забезпечити «безвідмовність», комп'ютерні дані не можуть розглядатися як доказ.

Потенційно уразливі, з погляду порушення цілісності, не тільки дані, але й програми. Впровадження розглянутого вище шкідливого ПЗ – приклад подібного порушення.

Загрозами динамічній цілісності є порушення атомарності транзакцій, перевпорядкування, крадіжка, дублювання даних або внесення додаткових повідомлень (мережевих пакетів і т. п.). Відповідні дії в мережевому середовищі називаються активним прослуховуванням.

6.5. Основні загрози конфіденційності

Конфіденційну інформацію можна розділити на предметну й службову. Службова інформація (наприклад, паролі користувачів) не належить до певної предметної області, в інформаційній системі вона відіграє технічну роль, але її розкриття особливо небезпечно, оскільки воно несе в собі одержання несанкціонованого доступу до всієї інформації, у тому числі предметної.

Навіть якщо інформація зберігається в комп'ютері або призначена для комп'ютерного використання, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер.

Багатьом людям доводиться виконувати ролі користувачів не однієї, а цілого ряду систем (інформаційних сервісів). Якщо для доступу до таких систем використовуються багаторазові паролі або інша конфіденційна інформація, то, напевно, ці дані будуть зберігатися не тільки в голові, але й у записній книжці або на листках паперу, які користувач часто залишає на робочому столі, а іноді просто губить. І справа тут не в неорганізованості людей, а в споконвічній непридатності парольної схеми. Неможливо пам'ятати багато різних паролів; рекомендації з їх регулярної (по можливості – частої) зміни тільки ускладнюють ситуацію, змушуючи застосовувати нескладні схеми чергування або взагалі намагатися звести справу до двох-трьох легких запам'ятовувань (і настільки ж легко вгадуваних) паролів.

Описаний клас уразливих місць можна назвати розміщенням конфіденційних даних у середовищі, де їм не забезпечений (найчастіше – і не може бути забезпечений) необхідний захист. Загроза ж полягає в тому, що хтось не відмовиться довідатися секрети, які самі просяться в руки. Крім паролів, що зберігаються в записних книжках користувачів, у цей клас потрапляє передача конфіденційних даних у відкритому вигляді (у розмові, у листі, по мережі), що уможливлює перехоплення даних. Для атаки можуть використовуватися різні технічні засоби (підслуховування або прослуховування розмов, пасивне прослуховування мережі й т. п.), але ідея одна – здійснити доступ до даних у той момент, коли вони найменш захищені.

Загрозу перехоплення даних варто брати до уваги не тільки при початковому конфігуруванні ІС, але й, що дуже важливо, при всіх змінах. Досить небезпечною загрозою є виставки, на які багато організацій, недовго думаючи, відправляє устаткування з виробничої мережі, з усіма даними, що зберігаються на ньому. Залишаються колишніми паролі, при вилученому доступі вони продовжують передаватися у відкритому вигляді. Це погано навіть у межах захищеної мережі організації; в об'єднаній мережі виставки – це занадто суворе випробування чесності всіх учасників.

Ще один приклад зміни, про яку часто забувають, – зберігання даних на резервних носіях. Для захисту даних на основних носіях застосовуються

розвинені системи керування доступом; копії ж нерідко просто лежать у шафах й одержати доступ до них може багато хто.

Перехоплення даних – дуже серйозна загроза, і якщо конфіденційність дійсно є критичною, а дані передаються по багатьох каналах, їхній захист може виявитися досить складним та дорогим. Технічні засоби перехоплення добре пророблені, доступні, прості в експлуатації, а встановити їх, наприклад на кабельну мережу, може будь-хто, так що цю загрозу потрібно брати до уваги стосовно не тільки зовнішніх, але й внутрішніх комунікацій.

Крадіжки устаткування є загрозою не тільки для резервних носіїв, але й для комп'ютерів, особливо портативних. Часто ноутбуки залишають без догляду на роботі або в автомобілі, іноді їх просто гублять.

Нетехнічною загрозою конфіденційності є також такі методи морально-психологічного впливу, як маскарад, тобто виконання дій під виглядом особи, що має повноваження доступу до даних.

До неприємних загроз, від яких важко захищатися, можна віднести зловживання повноваженнями. У багатьох типах систем привілейований користувач (наприклад, системний адміністратор) здатний прочитати кожен (незашифрований) файл, одержати доступ до пошти будь-якого користувача й т. д. Інший приклад – завдання збитків при сервісному обслуговуванні. Звичайно сервісний інженер одержує необмежений доступ до устаткування й має можливість діяти в обхід програмних захисних механізмів.

Такими є основні загрози, які завдають найбільшої шкоди суб'єктам інформаційних відносин.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

Назвіть найпоширеніші загрози.
Основні означення і критерії загроз.
Назвіть найпоширеніші загрози доступності.

Основні загрози цілісності.

Основні загрози конфіденційності.

Що таке вікно небезпеки?
Коли з'являється вікно небезпеки?

Коли перестає існувати вікно небезпеки?

Назвіть найнебезпечніші джерела внутрішніх загроз.

Яку загрозу несе агресивне споживання ресурсів?

РОЗДІЛ 7. КАНАЛИ НЕСАНКЦІОНОВАННОГО ОТРИМАННЯ ІНФОРМАЦІЇ

7.1. Структура і загальний зміст алгоритму формування відносно можливостей експертних методів

Структура і загальний зміст алгоритму формування відносно повної множини дестабілізувальних факторів, які мають вплив на КЗ, наведені на рисунку 7.1 [12,14.24].

Рис. 7.1. Структура загального алгоритму формування відносно повної множини дестабілізувальних факторів

7.2. Причини порушення цілісності інформації

На підставі проведеного аналізу літературних джерел сформулюємо відносно повну множину причин порушення цілісності інформації (ППЦІ). Нагадаємо, що під ППЦІ розуміють такі дестабілізувальні фактори, наслідком прояву яких може бути порушення фізичної цілісності інформації, тобто її викривлення або знищення.

Перелік класів і груп ППЦІ наведено в таблиці 7.1.

Таблиця 7.1. Класи ППЦІ і перелік потенційно можливих ППЦІ

Найменування групи ППЦІ	Найменування ППЦІ
ВІДМОВИ 1.1. Відмова основної апаратури	1.1.1. Повний вихід апаратури з ладу 1.1.2. Неправильне виконання функцій
1.2. Відмови програм	1.2.1. Викривлення коду операції 1.2.2. Викривлення адреси вибірки 1.2.3. Викривлення адреси відправлення 1.2.4. Викривлення адреси передачі

	керування 1.2.5. Знищення фрагментів програми 1.2.6. Неправильне розміщення програм у ЗП
1.3. Відмови людей	1.3.1. Повний вихід із ладу 1.3.2. Систематично неправильне виконання функцій
1.4. Відмови носіїв інформації	1.4.1. Фізичне порушення носія інформації 1.4.2. Погіршення характеристик носія
1.5. Відмови систем живлення	1.5.1. Аварійне відключення живлення 1.5.2. Ушкодження ліній електроживлення 1.5.3. Підвищення напруги, що не відновлюється 1.5.4. Зниження напруги, що не відновлюється
1.6. Відмови систем забезпечення нормальних умов роботи апаратури та персонал	1.6.1. Відключення систем кондиціонування 1.6.2. Зниження продуктивності систем контролю умов роботи кондиціонування апаратури 1.6.3. Незабезпечення персоналу системою кондиціонування 1.6.4. Відключення інших систем забезпечення нормальних умов роботи апаратури і персоналу
1.7. Відмови систем передачі даних	1.7.1. Повний вихід з ладу каналу зв’язку передачі даних 1.7.2. Повний вихід з ладу засобів зв’язку 1.7.3. Неправильне виконання функцій каналом зв’язку 1.7.4. Неправильне виконання функцій засобами зв’язку

1.8. Відмови допоміжних матеріалів	1.8.1. Дефекти паперу для пристрою друкування
ЗБОЇ 2.1. Збої основної апаратури	2.1.1. Неправильне виконання функцій
2.2. Збої програм	2.2.1. Неправильне виконання коду операції 2.2.2. Неправильне виконання адреси вибірки 2.2.3. Неправильне виконання адреси відправлення 2.2.4. Неправильне виконання адреси передачі керування
2.3. Збої людей	2.3.1. Тимчасовий вихід з ладу 2.3.2. Епізодичне неправильне виконання функцій
2.4. Збої носіїв	2.4.1. Погіршення характеристик носіїв інформації, що відновлюються
2.5. Збої систем живлення	2.5.1. Короткочасне вимикання 2.5.2. Короткочасне підвищення напруги 2.5.3. Короткочасне зниження напруги 2.5.4. Короткочасна зміна частоти струму
2.6. Збої системи забезпечення нормальних умов роботи	2.6.1. Короткочасне відключення систем забезпечення кондиціонування 2.6.2. Короткочасне зниження продуктивності систем кондиціонування 2.6.3. Короткочасне відключення інших систем забезпечення нормальних умов роботи апаратури і персоналу

2.7. Збої систем передачі даних	2.7.1. Неправильне виконання функцій передачі даних каналом зв’язку 2.7.2. Неправильне виконання функцій засобами зв’язку
2.8. Збої допоміжних матеріалів	2.8.1. Дефекти в пристроях друкування, що виправляються 2.8.2. Дефекти паперу, що виправляються
ПОМИЛКИ	
3.1. Помилки основної апаратури	3.1.1. Неправильний монтаж схеми процедури апаратури 3.1.2. Неправильний монтаж схеми переходу до процедури 3.1.3. Неправильний монтаж схеми адреси вибірки 3.1.4. Неправильний монтаж схеми адреси відправлення
3.2. Помилки програми	3.2.1. Неправильний код операції 3.2.2. Неправильна адреса вибірки 3.2.3. Неправильна адреса відправлення 3.2.4. Неправильна передача керування 3.2.5. Неправильне розташування елементів програм
3.3. Помилки людей	3.3.1. Неправильнеції 3.3.2. Неправильний набір інформації 3.3.3. Неправильний вибір процесу 3.3.4. Випадкове втручання в процес
3.4. Помилки системи передачі даних	3.4.2. Неправильна схема комутації в каналі 3.4.3. Неправильний монтаж схеми в пристроях зв’язку
СТИХІЙНІ ЛИХА	
4.1. Пожежа	4.1.2. Середня 4.1.3. Загальна (велика)

4.2. Повінь	4.2.2. Середня (у межах будинку) 4.2.3. Загальна (міська)
4.3. Землетрус	4.3.2. Середній 4.3.3. Сильний
4.4. Ураган	4.4.2. Середній 4.4.3. Сильний
4.5. Вибух	4.5.2. Середній 4.5.3. Сильний
4.6. Аварія	4.6.2. Середня 4.6.3. Значна
ЗЛОЧИННІ ДІЇ	
5.1. Запам’ятовування інформації	5.1.2. Запам’ятовування бланків з вихідними даними 5.1.3. Запам’ятовування вихідної документації
5.2. Копіювання	5.2.2. Виготовлення неврахованих копій документів 5.2.3. Друкування масивів
5.3. Розкрадання	5.3.2. Розкрадання магнітних носіїв 5.3.3. Розкрадання вихідних документів
5.4. Підміна	5.4.2. Підміна магнітних носіїв 5.4.3. Підміна вихідних документів 5.4.4. Підміна апаратури 5.4.5. Підміна елементів програм
5.5. Підключення	5.5.1. Підключення генератора завад 5.5.2. Підключення реєструвальної апаратури
5.6. Поломка	5.6.2. Ушкодження програм 5.6.3. Ушкодження елементів баз даних

	5.6.4. Ушкодження носіїв 5.6.5. Ушкодження документів
5.7. Диверсія	5.7.1. Створення пожежі 5.7.2. Організація повені 5.7.3. Організація вибуху 5.7.4. Ушкодження системи електроживлення 5.7.5. Ушкодження систем забезпечення нормальних умов роботи апаратури і персоналу
ПОБІЧНІ ЯВИЩА 6.1. Електромагнітні	6.1.2. Випромінювання процесорів ЕОМ 6.1.3. Випромінювання зовнішніх запам’ятовувальних пристроїв 6.1.4. Випромінювання друкувальних пристроїв 6.1.5. Випромінювання апаратури зв’язку 6.1.6. Випромінювання ліній зв’язку 6.1.7. Випромінювання допоміжної апаратури
6.2. Паразитні наводки	6.2.2. Наводки в слабкострумових ланцюгах 6.2.3. Наводки в мережах живлення
6.3. Зовнішні електромагнітні випромінювання	6.3.2. Випромінювання біля зовнішніх запам’ятовувальних пристроїв 6.3.3. Випромінювання біля друкувальних пристроїв 6.3.4. Випромінювання біля апаратури зв’язку 6.3.5. Випромінювання біля ліній зв’язку 6.3.6. Випромінювання біля допоміжних пристроїв 6.3.7. Випромінювання в сховищах носіїв інформації

6.4. Вібрація	6.4.1. Мала 6.4.2. Середня 6.4.3. Велика
6.5. Зовнішні атмосферні умови	6.5.1. Зміна температури 6.5.2. Підвищення вологості повітря 6.5.3. Підвищення запиленості повітря 6.5.4. Підвищення рівня радіації 6.5.5. Зараження повітря отруйними речовинами 6.5.6. Бактеріологічне зараження повітря

7.3. Канали несанкціонованого доступу до інформації

Під каналами несанкціонованого одержання інформації (КНОІ) розуміють такі дестабілізувальні фактори, під дією яких може бути одержання (або небезпека одержання) інформації, яка захищається, особами або процесами, що не мають на це законних повноважень. Об'єктивна необхідність формування повної множини потенційно можливих КНОІ така, як і для ППЦІ. У той же час, труднощі формування повної множини КНОІ значно більші, ніж при вирішенні аналогічної задачі для ППЦІ. Пояснюється це тим, що несанкціоноване одержання інформації пов'язано переважно зі злочинними діями людей, що дуже важко піддаються структуризації. Наведені структури множини і перелік КНОІ сформульовані з використанням методики, викладеної раніше [17,21].

Насамперед, було встановлено, що з метою формування більш повної множини КНОІ необхідно побудувати повну класифікаційну структуру. Така структура може бути побудована, якщо за критерії класифікації вибрати такі два показники: перший – що стосується стану інформації і ступінь взаємодії зловмисника з її елементами. Щодо першого критерію, то будуть розрізняти два стани: безвідносно обробки (несанкціоноване одержання інформації може мати місце навіть у тому випадку, якщо вона не обробляється, а просто зберігається) і в процесі безпосередньої обробки.

Повна структуризація другого критерію може бути здійснена виділенням таких його значень [12,14,24]:

перше – без доступу (тобто непряме одержання інформації);

друге – з доступом, але без зміни їхнього стану або змісту;

третє – з доступом і зі зміною змісту інформації або стану.

Отже, класифікаційна структура КНОІ буде мати вигляд (таблиця 7.2):

Повнота поданої класифікаційної структури гарантується тим, що обрані критерії класифікації охоплюють усі потенційно можливі варіанти взаємодії зловмисника з інформацією, а структуризація значень критеріїв здійснюється за методом розподілу цілого на частини.

Таблиця 7.2. Класифікаційна структура КНОІ

Ознака класифікації		***Відношення до стану інформації, що захищається***	
		безвідносно до обробки інформації ***А-канали***	*виявляються в процесі обробки* ***В-канали***
Без доступу	***К-канали***	*1-й КЛАС* *АК-канали*	*2-й КЛАС* *ВК-канали*
З доступом	*Без зміни* ***П-канали***	*3-й КЛАС* *АП-канали*	*4-й КЛАС* *ВП-канали*
	Зі зміною ***Пи-канали***	*5-й КЛАС* *Апи-канали*	*6-й КЛАС* *ВПи-канали*

Таким чином, уся множина потенційно можливих КНОІ може бути строго розділеною на шість класів.

Наступним кроком на шляху вирішення розглянутої задачі є обґрунтування більш повного переліку КНОІ в межах кожного з шести класів.

Отриманий перелік буде виглядати таким чином [12,23,24]:

КНОІ першого класу – канали, що виявляються безвідносно обробки інформації і без доступу зловмисника до інформації.

Розкрадання носіїв на заводах, де відбувається їхній ремонт.

Підслуховування розмов осіб, що стосуються інформації.

Провокування на розмови осіб, компетентних щодо інформації.

Використання зловмисником візуальних засобів.

Використання зловмисником оптичних засобів.

Використання зловмисником акустичних засобів.

КНОІ другого класу – канали, що виявляються в процесі обробки інформації без доступу зловмисника до неї [24,25].

Електромагнітні випромінювання пристроїв відображення.

Електромагнітні випромінювання процесорів.

Електромагнітні випромінювання зовнішніх запам’ятовувальних пристроїв.

Електромагнітні випромінювання апаратури зв’язку.

Електромагнітні випромінювання ліній зв’язку.

Електромагнітні випромінювання допоміжної апаратури.
Електромагнітні випромінювання пристроїв підготовки даних.

Паразитні наводки в комунікаціях електропостачання.

Паразитні наводки в системах водопостачання і каналізації.

Паразитні наводки в мережах теплопостачання і вентиляції.

Паразитні наводки в шинах заземлення.

Паразитні наводки в ланцюгах газифікації.
Паразитні наводки в ланцюгах радіофікації.

Паразитні наводки в ланцюгах телефонізації.

Паразитні наводки в мережах живлення по ланцюгу 50 Гц.

Паразитні наводки в мережах живлення по ланцюгу 400 Гц.

Підключення генератора завад.

Підключення реєструвальної апаратури.

Огляд відходів виробництва, що потрапляють за межі контрольованої зони.

КНОІ третього класу – канали, що виявляються безвідносно обробки інформації з доступом зловмисника до неї, але без зміни інформації.

Копіювання бланків із вихідними даними.

Копіювання першоносіїв.
Копіювання магнітних носіїв.

Копіювання пристроїв відображення інформації.

Копіювання вихідних документів.

Копіювання інших документів.

Розкрадання виробничих відходів.

КНОІ четвертого класу – канали, що виявляються в процесі обробки інформації з доступом зловмисника до неї, але без зміни останньої.

Запам’ятовування інформації на бланках із вихідними даними.

Запам’ятовування інформації з пристроїв відображення.

Запам’ятовування інформації на вихідних документах.

Запам’ятовування службових даних.

Копіювання в процесі обробки.
Виготовлення дублікатів масивів і вихідних документів.

Копіювання роздруківки масивів.

Використання програмних пасток.

Маскування під зареєстрованого користувача.

Використання недоліків операційних систем. Використання недоліків мов програмування.

Використання вразливості програмного забезпечення вірусом.

КНОІ п'ятого класу – канали, що виявляються безвідносно обробки інформації з доступом зловмисника до неї та зі зміною останньої.

Підміна бланків.

Підміна магнітних носіїв.

Підміна вихідних документів.

Підміна апаратури.

Підміна елементів програми.

Підміна елементів баз даних.

Розкрадання бланків із вихідними даними.

Розкрадання магнітних носіїв.

Розкрадання вихідних документів.

Розкрадання інших документів.

Внесення в програми блоків типу «троянський кінь», «бомба» і т. п.

Читання залишкової інформації в ОЗП після виконання санкціонованих запитів.

КНОІ шостого класу – канали, що виявляються в процесі обробки інформації з доступом зловмисника до інформації та застосуванням її.

Незаконне підключення до апаратури.

Незаконне підключення до ліній зв'язку.

Зняття інформації на шинах живлення пристроїв відображення.

Зняття інформації на шинах живлення процесорів.

Зняття інформації на шинах живлення апаратури зв'язку.

Зняття інформації на шинах живлення ліній зв'язку.

Зняття інформації на шинах живлення друкувальних пристроїв.

Зняття інформації на шинах живлення зовнішніх запам'ятовувальних пристроїв.

Зняття інформації на шинах живлення допоміжної апаратури.

7.4. Методи визначення значень показників уразливостіінформації

Для визначення значень показників уразливості інформації розроблений метод, що відповідає природі цих показників і враховує всі фактори, що впливають на значення показників.

У розділі «Система показників уразливості інформації» відзначалося, що з усієї сукупності показників особливе місце займають базові показники, тобто показники, що характеризують уразливість інформації в якому-небудь одному структурному компоненті інформаційної системи (ІС) в одному якому-небудь КНОІ, відносно якогось потенційного порушника. Тоді схему визначення показників уразливості в загальному вигляді можна уявити так (рис. 7.2) [24,25].

Рис. 7.2. Загальна схема визначення показників уразливості інформації

Цю схему можна покласти в основу розробки як методів, так і моделей визначення значень показників уразливості інформації.

Значення базових показників визначається архітектурою ІС (від чого залежить рівень захищеності кожного її структурного компонента), безліччю потенційно можливих КНОІ (від чого залежать потенційні можливості злочинних дій у структурному компоненті), а також чисельністю потенційних порушників і їхніх можливостей здійснювати злочинні дії.

Потенційно можливою є та обставина, що в сучасних ІС несанкціоноване одержання інформації можливо не тільки шляхом безпосереднього доступу до даних, але і багатьма шляхами, що не потребують такого доступу.

Структурну схему потенційно можливих злочинних дій в ІС для найзагальнішого випадку наведено на рис. 7.3.

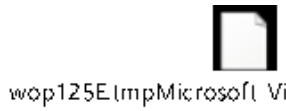


Рис. 7.3. Структурна схема потенційно можливих злочинних дій

Виділені зони характеризуються так [25,26,27].

Зовнішня зона, що не контролюється, – територія навколо ІС, на якій персоналом і засобами ІС не застосовуються ніякі засоби і не здійснюються ніякі заходи для ЗІ.

Зона території, **що контролюється,** – територія навколо приміщень ІС, що постійно контролюється персоналом або технічними засобами.

Зона приміщень ІС – внутрішній простір тих приміщень, у яких розташовані засоби системи.

Зона ресурсів ІС – та частина приміщень, звідки можливий безпосередній доступ до ресурсів системи.

Зона даних – та частина ресурсів системи, з якої можливий безпосередній доступ до захищуваної інформації.

Злочинні дії з метою несанкціонованого одержання інформації в загальному випадку можливі в кожній із перерахованих зон. При цьому для несанкціонованого одержання інформації необхідне одночасне настання таких подій.

Порушник повинен одержати доступ у відповідну зону.

Під час перебування порушника в зоні у ній повинен з'явитися відповідний КНОІ.

Відповідний КНОІ повинен бути доступний порушнику.

У КНОІ в момент доступу до нього порушника повинна знаходитися інформація, що захищається.

Зробимо висновок щодо загальних залежностей для визначення значень базових показників уразливості. Введемо такі позначення змінних індексів.

Тоді, відповідно до теореми можливостей, можливість несанкціонованого одержання інформації порушником *k*-ї категорії в *j*-му КНОІ в *l*-й зоні і-го структурного компонента ІС визначається такою залежністю [28,29]:

$$P_{ijkl}^{(n,l)} = P_{ikl}^{(n,d)} * P_{ijl}^{(n,k)} * P_{ijkl}^{(j,n)} * P_{ijl}^{(n,u)}, \qquad (7.1)$$

де *i* – поточний ідентифікатор структурного компонента ІС;

j – те ж для КНОІ;

k – те ж для категорії потенційних порушників;

l – те ж для зони злочинних дій.

Введемо такі позначення:

P_{ikl} – можливість доступу порушника *k-ї* категорії в *l-у* зону *і-го* компонента ІС;

P_{ijl} – можливість появи *j*-го КНОІ в *l*-й зоні *i*-го компонента ІС; P_{ijkl} – можливість доступу порушника *k*-ї категорії до *j*-го КНОІ в *l*-й зоні *i*-го компонента за умови доступу порушника в зону;

P_{ijl} – можливість наявності захищуваної інформації в *j*-ому КНОІ в *1*-й зоні *i*-го компонента в момент доступу туди порушника.

Наведена залежність буде справедлива в тому випадку, коли всі події, відображені в правій частині формули, є незалежними одна від одної, тобто коли поява будь-якої з них впливає на можливість появи інших. В іншому випадку необхідно враховувати коефіцієнти між можливостями залежних подій.

Для базової можливості несанкціонованого одержання інформації байдуже, в якій зоні це одержання інформації мало місце, вона раніше визначена як можливість несанкціонованого одержання інформації в одному компоненті ІС одним порушником якоїсь категорії і в одному КНОІ. Позначимо базову можливість як P_{ijk}, запишемо її в такому вигляді [28,29]:

$$P_{ijk}^{(n,b)} = 1 - \Pi_{l-1}^{5}\left[1 - P_{ijkl}^{(n,b)}\right] = 1 - \Pi_{l=1}^{5}\left[1 - P_{ikl}^{(n,d)} * P_{ijl}^{(j,k)} * P_{ijkl}^{(j,n)} * P_{ijl}^{(n,u)}\right]. \qquad (7.2)$$

Значення частково узагальнених показників можуть визначатися таким чином. Нехай *{k*}* є підмножиною з повної множини потенційно можливих порушників. Тоді можливість несанкціонованого одержання інформації зазначеною підмножиною порушників в *j-му* КНОІ в *i-ому* компоненті ІС

$P^{(r)}\{k^*\}$ визначається виразом:

$$P_{ij}^{(r)}\{k*\} = 1 - \prod_{\forall k*}\left[1 - P_{ijk}^{(b)}\right],$$

де $\forall k*$ – множення в дужках для усіх k, що входять в підмножину.

Аналогічно, якщо *{j*}* – підмножина структурних компонент ІС, що викликають інтерес, то уразливість інформаційного компонента даної підмножини КНОІ щодо *k-го* порушника визначається так:

$$P_{i}^{(r)}\{j*\}k = 1 - \prod_{\forall j*}\left[1 - P_{ijk}^{(b)}\right].$$

Якщо ж *{i*}* – підмножина структурних компонент ІС, що викликають інтерес, то уразливість інформації в них у *j*-му КНОІ щодо *k*-го порушника визначається так:

$$P^{(r)}\{i*\}jk = 1 - \prod_{\forall i*}\left[1 - P_{ijk}^{(b)}\right].$$

Кожен з наведених виразів дозволяє робити узагальнення щодо одного якогось параметра.

Для одержання узагальненого виразу необхідно врахувати одночасно підмножини *{i*}*, *{j*}*,*{k*}*.Очевидно, загальний показник уразливості чином:

$$P^{(r)} = 1 - \prod_{\forall i}\left[1 - P_{ijk}^{(b)}\right]\prod_{\forall j}\left[1 - P_{ijk}^{(b)}\right]\prod_{\forall k}\left[1 - P_{ijk}^{(b)}\right].$$

Тепер визначимо вирази, що описують екстремальні показники уразливості. Як уже відзначалося раніше, екстремальними названі показники, які характеризують найбільш несприятливі умови захищеності інформації: найуразливіший структурний компонент ІС, КНОІ, найнебезпечнішу категорію порушників. Позначимо:

i – найбільш уразливий структурний компонент ІС;

j – найбільш небезпечний КНОІ;

k – найнебезпечніша категорія порушників.

Тоді очевидно:

$$\bar{i} = iEp^{y} \to \max \forall i,$$

де *i* – є таке *i*, для якого заданий показник уразливості p^{y} приймає максимальне значення для всіх *i*.

Аналогічно:

$$\bar{j} = jEp^{y} \to \max \forall j;$$

$$\bar{k} = jEp^{y} \to \max \forall k.$$

На підставі проведених досліджень розроблені методи розрахунку показників уразливості інформації з урахуванням інтервалу часу, в якому оцінюється уразливість.

Неважко помітити, що наведені вище вирази є адекватними для таких інтервалів часу, що названі малими. Для інших інтервалів отримані вирази не будуть адекватними, тому що чим більший інтервал часу, тим більше можливостей у порушника для дій і тим більша можливість зміни стану ІС і умов обробки інформації.

Можливі такі підходи для вирішення цієї задачі [30,31].

Малими називають інтервали, які не можна зводити до точки, але процеси, що відбуваються на них, відносно уразливості інформації можна вважати однорідними. Тоді природно можна розділити малий інтервал на дуже малі інтервали і на кожному з них визначати уразливість інформації. А оскільки процеси, що відбуваються на малому інтервалі часу, однорідні, то на кожному інтервалі уразливість буде визначатися однозначно за такою залежністю [29,30,31]

$$P^M = 1 - \prod_{t-1}^{Nt} \left(1 - P^T\right),$$

де P^T – уразливість у точці (на дуже малому інтервалі);

P^M – показник уразливості на малому інтервалі;

t – змінний індекс дуже малих інтервалів, на які розбитий малий інтервал;
N_t – загальне число інтервалів.

Неважко помітити, що розглянутий підхід може поширюватися і на інші види інтервалів: великий інтервал уявити деякою послідовністю малих і т. п.

Проте наведені вирази будуть справедливими лише в тому випадку, якщо на всьому розглянутому інтервалі часу умови для злочинних дій залишаються незмінними. У реальних умовах вони можуть змінюватися, причому найбільш важливим фактором, що впливає на можливості злочинних дій, є активні дії системи ЗІ. Технологія функціонування системи ЗІ повинна бути тим сильнішою та активнішою, чим вища уразливість інформації.

З урахуванням цього запишемо [31]:

$$P^T(t) = \int \left[P^T(t-1) \right], \qquad (7.3)$$

тобто значення показника в кожній точці розглянутого інтервалу є деяка функція значення цього показника в попередній точці. Тоді вираз (7.3) можна записати в такому вигляді:

$$P^M = 1 - \prod_{t-1}^{Nt} \left\{ 1 - \int \left[P^T\left(t-1\right) \right] \right\}.$$

Функціональну залежність зумовлюють використовувані засоби захисту і технології функціонування систем ЗІ.

Розглянуті моделі є аналітичними, оскільки вони дозволяють визначати необхідні значення показників уразливості шляхом аналітичних обчислень.

Проте в багатьох практичних ситуаціях конкретні значення вихідних розмірів для визначення базового показника уразливості інформації можуть змінюватися залежно від конкретних ситуацій у ІС і в зовнішньому середовищі і не виражатися у вигляді конкретних формул унаслідок складності вихідних моделей. В той же час часто можна структурувати системи, що моделюються, та процеси до такого ступеня, що задача може бути вирішена методом моделювання.

Для складних ІС і слабоструктурованих схем функціонування систем обробки найбільш адекватним методом прогнозування показників уразливості буде статистика. Проте для того, щоб статистичним шляхом безпосередньо прогнозувати значення показників уразливості, необхідні багатопараметричні статистичні дані передісторії. В даний час статистичні дані практично відсутні, і одержання їх являє собою дуже складну проблему.

З метою спрощення задачі будемо прогнозувати не безпосередні показники уразливості, а складові величини, що входять у вираз для показників якості. Як випливає з моделей оцінювання показників якості, такими величинами є нижченаведені.

Можливість прояву дестабілізувальних факторів (наявності КНОІ).

Можливість наявності захищуваної інформації в місці і під час прояву дестабілізувальних факторів.

Можливість несанкціонованого одержання інформації під впливом дестабілізувальних факторів, незважаючи на застосування ЗІ.

Розглянемо можливі підходи до прогнозування перерахованих величин.

Можливість прояву дестабілізувальних факторів – P_{ijz}.

При сталому процесі функціонування системи обробки інформації прояв дестабілізувальних факторів можна вважати випадковим пуассоновим процесом. Позначивши *ijz* як інтенсивність потоку *i*-го фактора в *j*-му технічному засобі (ТЗ), що знаходиться в *z-му* стані, то, відповідно до властивостей пуассонового процесу, запишемо [29,30]:

$$P_{ijk} = f_{\text{tijk}} * \sigma_t,$$

де σ_t – інтервал часу, істотно менший того інтервалу, відносно якого визначена величина.

Оскільки для загального випадку інтервал прогнозування цю умову не буде задовольняти, то величину P_{ijk} запишемо в такому вигляді:

$$P_{ijk} = 1-(1-\rho_{\text{ijk}}) * ((\Delta t)/(\sigma_t)),$$

де Δt – інтервал прогнозування.

Отже, можна розділити весь період прогнозування Δt на менші інтервали тривалістю σ_t і записати, що

$$\bar{j} = jEp^y \rightarrow \max \forall j.$$

Тоді за умови, що $\Delta t >> \sigma_t$, можна записати

$$P_j^M = \frac{\sum_\theta \gamma_{t\theta} \Delta t}{\frac{\Delta t}{\sigma t}} = \frac{\sigma t}{\Delta t} \sum \gamma_{j\theta}$$

.

Значення функції визначаються з технологічного графіка обробки інформації в прогнозований період часу.

Аналогічно аналізу попереднього параметра період прогнозування будемо здійснювати на малих інтервалах часу. Введемо функцію N_{in}^{Q}, що є [31,32]:

1 – якщо *j*-ий засіб захисту на *k*-му інтервалі часу активно використовується в *i*-ому ТЗ;

0 – не враховується.

З урахуванням того, що $\Delta t >> \sigma_t$, можна записати

$$P_{ij}^{НП} = \prod_{\forall \eta} \left(1 - P_{шо}^{\eta}\right) * \frac{\sigma}{\Delta e} * \sum N_{от}^{\theta},$$

де $P^{НП}$ – можливість того, що при використанні η-го засобу захисту в *j*-му ТЗ несанкціоноване одержання інформації не буде мати місця навіть при появі *i*-го дестабілізувального фактора.

Виходячи з концепції захисту інформації як сукупності взаємозалежних організаційних заходів і технічних систем, синтезованих на основі обраних критеріїв оптимізація з урахуванням обмежень і спрямованих на захист інформації при її формуванні, передаванні, прийомі, обробці та зберіганні з метою збереження її цілісності, формується поняття захищеності інформації в ІС. Поняття захищеності є центральним у силу нижченаведених причин.

Сама мета створення системи (моделі) ЗІ є досягненням науково-технічного рівня захищеності інформації в ІС. Таким чином, методологія оцінювання захищеності інформації є, за суттю, методологією наукового обґрунтування кількісних показників досягнення мети системи захисту.

Методологія оцінювання захищеності інформації в ІС є, насамперед, методологією наукового обґрунтування норм ефективності ЗІ. Оптимальний або раціональний вибір одиниць виміру і кількісних значень норм ефективності визначає категорії якості системи захисту, структуру і математичний аппарат синтезу, аналізу та оптимізації моделі захисту і саму якість захисту. Дійсно, завищені норми ефективності ведуть до підвищення витрат на створення системи захисту, а занижені норми просто не дозволяють досягти цілей захисту.

Методологія оцінювання захищеності інформації в ІС є основою для реального рівня захисту інформації в конкретних системах і його порівняння з нормами ефективності захисту, а, отже, є основою для вирішення питань про методи і засоби досягнення системи захисту.

Визначаючи критерії якості захисту, структуру і математичний апарат синтезу, аналізу й оптимізації моделі системи захисту, методологія оцінювання захищеності інформації визначає цілі, засоби і методологію інженерного аналізу, спрямованого на виявлення потенційних стратегій нападу на інформацію в ІС і основні характеристики стратегій нападу, визначення можливих заходів захисту і вимог до їхніх параметрів.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

Що розуміють під загрозою інформації?

Які фактори складають систему дестабілізувальних факторів, як їх визначають?

Які існують джерела дестабілізувальних факторів?

У яких ситуаціях необхідно оцінювати уразливість інформації?

Чим обумовлюється уразливість у процесі функціонування системи?

Як виражають кількісну міру уразливості?

Що позначають показники, зображені в таблиці 7.2? З якою метою використовують експертні помилки?

Що розуміють під КНОІ?

Які два показники вибирають за критерії класифікації КНОІ?

У чому полягає повнота класифікаційної структури, наведеної на рисунку 7.1?

На які 6 класів класифікується КНОІ?

Що характеризують базові показники і чим визначаються їхні значення?

Чим характеризуються зони, подані на рис. 7.3?

Які умови необхідні для несанкціонованого одержання інформації?

РОЗДІЛ 8. КЛЕПТОГРАФІЯ ТА ПРИХОВАНІ КАНАЛИ У КІБЕРБЕЗПЕЦІ

8.1. Клептографія

Тайнопис, яким займаються криптографія чи стеганографія, з давніх часів був переважно прерогативою держави та військових (у середні віки – ще й церкви). Усі розробки технологій захисту інформації та відповідні наукові

дослідження проводились у надрах спецслужб за завісою таємничості. Однак розвиток технологій та потреби суспільства у захисті зростаючих об’ємів інформації, що передаються або зберігаються, спонукало повільне перетікання накоплених спецслужбами знань і технологій у відкрите середовище із розгортанням подальших досліджень в різних наукових центрах.

Так, початком становлення *криптографії* як науки можна рахувати 1949 рік, коли була опублікована розсекречена робота Клода Шеннона «Теорія зв'язку в таємних системах». Під час Другої світової війни Шеннон займався зломом ворожих шифрів і саме він почав першим вивчати криптографію, використовуючи системний підхід. Наприклад, він дав визначення «цілком стійкого шифру» (шифру, який не можна зламати, маючи лише зашифроване повідомлення) та довів, що такі шифри можуть існувати (шифр Вернама).

На сьогоднішній день, з розвитком сучасних технологій, переважна більшість людей у повсякденному житті так чи інакше користується так званою “*цивільною криптографією*” – тобто криптографією, яка, на відміну від державної чи військової криптографії, покликана задовольняти потреби приватних осіб та організацій. Цивільна криптографія присутня у мобільному зв'язку, у банківських картах, в інтернет-браузерах при передачі інформації протоколом SSL/TLS тощо. З'явились навіть побутові прилади, які підключені до Інтернету (технологія IoT, Internet-of-Things), – і звичайно ж, комунікації таких пристроїв між собою та їх власником мають бути захищені. Навіть автомобілі стали частиною IoT (концепція Connected Car) – а це питання безпеки не тільки особистої інформації водія, але і його життя.

За такою ж схемою у 90-х роках минулого сторіччя у відкритому просторі почала формуватися наука *стеганографія*. Незважаючи на те, що стеганографія як спосіб приховування секретних даних відома вже протягом тисячоліть, роком становлення сучасної стеганографії як науки можна вважати 1996 рік, коли на міжнародному семінарі InfoHiding-96 була введена єдина термінологія. Методи “*цивільної стеганографії*” також зайняли своє місце у повсякденному житті суспільства, наприклад у таких технологіях, як цифрові водяні знаки (digital watermark) – для захисту авторських прав на цифровий об’єкт або цифрові відбитки пальців (digital fingerprinting) – для захисту виключного права на цифровий об’єкт.

Водночас користувачами цивільної криптографії або стеганографії стають не лише законослухняні громадяни, а й злочинці, шахраї чи терористи, які використовують сучасні технології для підготовки, скоєння та приховування злочинів. З погляду правоохоронних органів, криптографія (стеганографія) в їхніх руках безумовно дуже зручна та небезпечна зброя.

У зв'язку зі зростанням терористичних загроз суспільство вимагає вжити заходів, у тому числі найжорсткіших. Держава, як правило, із задоволенням йде назустріч таким побажанням і антитерористичні заходи, які проводять з боку держави, стали стосуватися також криптографії та стеганографії. Тому посилення вторгнення держави у цивільну криптографію – цілком очікувана та неминуча реакція державних інституцій і, насамперед, законодавців та спецслужб.

З широким впровадженням сучасних інформаційних технологій у повсякденне життя все більше офіційних осіб стали заявляти, що для боротьби з тероризмом необхідно прийняти рішення на офіційному державному рівні про впровадження відповідних лазівок в інформаційні системи, мережі та засоби захисту, у тому числі у криптоалгоритми, які є державними стандартами. Не впадаючи в пафос слів про свободи та права людини, варто усвідомити, що ми стоїмо перед непростим вибором – гарантоване обмеження свобод чи можлива загроза десяткам, сотням, а то й тисячам життів. На жаль, однозначного рішення немає. Лазівки, призначені для захисту від тероризму, можуть стати зброєю для терористів у разі витоку конфіденційних даних про них (наприклад, лазівка в Connected Car дозволяє дистанційно керувати автомобілем). А чи існують надійні способи забезпечення ексклюзивного доступу спецслужб до інформації користувача при збереженні достатнього рівня стійкості до сторонніх зловмисників? Цим питанням опікується наука *клептографія.*

Будь-яка держава намагається контролювати принаймні свій сегмент кіберпростору. Це можливо різними способами. Наприклад, за рахунок колаборації державних структур (насамперед спецслужб США, Китаю та Росії) з великими фірмами-виробниками мікроелектроніки, обчислювальної та телекомунікаційної техніки з метою створення можливості збирання інформації про користувачів та доступу до їх інформації. До публікацій Едварда Сноудена і оприлюднення конкретних прикладів ніхто не був упевнений, що це відбувається насправді.

На даний час у ЗМІ неодноразово з'являлися дані про співпрацю зі спецслужбами відомих виробників засобів телекомунікацій (Cisco, Huaway), шифраторів (Crypto AG, Omnisec, Mils Electronic), програмного забезпечення (Microsoft), соціальних мереж (Facebook, Вконтакте, Однокласники), антивірусних систем (Касперский, Radware, McAfee), постачальників послуг електронної пошти та мережевих Інтернет-гігантів (Google, Yahoo, AT&T, CenturyLink, Verizon). Така співпраця включає розробку та вбудовування необхідних «бекдорів» з подальшою передачею спецслужбам таємних відомостей про вразливості в апаратному та програмному забезпеченні, в тому числі і про ключі шифрування, що діють.

Але така співпраця зі спецслужбами інколи може зіграти згубну роль для виробника. Яркою ілюстрацією цієї тези може служити 70-річна історія відомої швейцарської компанії Crypto AG, яка була заснована Б. Хагеліном у 1952 році та спеціалізувалася на комунікаційній та інформаційній безпеці.

Шифрувальну машину М-209 розміром із мильницю Борис Хагелін розробив ще перед Другою світовою війною. Через свої габарити вона була цілком придатна для використання у польових умовах, тому США закупили ліцензією та виробили більше 140 000 таких шифраторів. Першу шифрувальну машинку, яку Б. Хагелін виробив після закінчення війни у Швейцарії, просто шокувала американців - вона була занадто надійна. Тому за їх наполегливою вимогою компанія Crypto AG стала випускати шифратори з керованою стійкістю. Фактично це стало початком операції «Рубікон», однією з найбільших розвідувальних операцій з часів Другої світової війни.

У 1970 році компанія Crypto AG була викуплена через посередників у спільну власність ЦРУ США та БНД (федеральної служби розвідки) Німеччини. З того часу спецслужби (США, Німеччини та Великобританії) могли давати розробникам прямі вказівки та читати секретні телеграми як можливих супротивників, так і дружніх країн. Шифратори Crypto AG купувалась багатьма країнами світу для організації зв'язку у військових відомствах та зі своїми дипломатичними представництвами. При цьому випускалися два типи машин: з якісними криптографічними алгоритмами (їх отримували Швейцарія, Швеція та деякі країни НАТО) та варіанти машин з вбудованим «бекдором», які дуже легко зламувалися тими, хто знав, як це можна зробити. Таку техніку отримували інші держави. Усього дешифрувалися секретні шифртелеграми понад ста країн, включаючи Іспанію, Італію, Пакистан, Аргентину, Іран, Лівію та інші арабські країни. Тому ЦРУ і БНД мали у своєму розпорядженні, наприклад, всю повноту інформації про Фолклендську війну 1982 року, про теракт у берлінській дискотеці «Ла Бель» у 1986 році або про захоплення заручників в Ірані в 1979 році — і все завдяки невеликій швейцарській компанії в кантоні Цуг.

В останніх лінійках шифраторів Grypto AG (Cryptomatic, Cryptofax, Cryptovox тощо) були реалізовані складні криптоалгоритми та нові криптографічні конструкції, які враховували зростання обчислювальних потужностей у світі. Усі вони були електронними пристроями, реалізованими на сучасній елементній базі, багатошарових друкованих платах із захищеними спеціалізованими процесорами для виконання криптографічних перетворень й захищеною пам'яттю, де зберігалися специфічні криптографічні параметри. У цих засобах була реалізована багатоступенева система ключів:

- структурні ключі, які були згенеровані виробником для кожного конкретного клієнта (відомства, країни);
- змінні довгострокові ключі, що змінювалися з певною періодичністю;
- сеансові ключі для кожного конкретного повідомлення.

При чому, структурні ключі були відомі виробнику, довгострокові ключі генерувалися по відомому виробнику алгоритму і мали деякі особливості. Крім того, структура самого шифрованого повідомлення включала також низку синхронізуючих елементів, що були отримані шляхом певних математичних перетворень над елементами ключів, криптографічними параметрами, мітками часу тощо. У разі потокового шифрування, синхропакети для початкової і автоматичної повторної синхронізації також формувалися специфічним чином. Кожен такий елемент ніс в собі певні відомості, які дозволяли будувати додаткові рівняння відносно елементів ключів і параметрів криптоперетвореня, що загалом суттєво полегшувало задачу криптоаналітику.

У 2018 році після скандалів Crypto AG була ліквідована, а Федеральна прокуратура Швейцарії, яка проводила розслідування діяльності компанії, зробила висновок, що операція «Рубікон», що проводилася у рамках співпраці «дружніх спецслужб», була цілком легальною і не суперечила як тодішнім, так і нинішнім правовим засадам та положенням.

Цей приклад показує, що спецслужби завжди приділяли увагу забезпеченню контролю чуттєвих технологій, що з’являлися на ринку. В їх надрах накоплено відповідний науково обґрунтований досвід для вирішення таких проблем. І це стосується на тільки криптографії, а й телекомунікаційних технологій та програмного забезпечення (у першу чергу операційних та антивірусних систем).

З широким впровадження сучасних інформаційних технологій в повсякдення життя все більше і більше офіційних осіб стали заявляти про необхідність ухвалення на офіційному державному рівні рішення про впровадження вразливостей в інформаційні системи, мережі та пристрої, а також про обов'язкове впровадження лазівок у криптоалгоритми, які є державними стандартами. На даний час відомо як мінімум про два алгоритми, які були затверджені в США як федеральні стандарти і мають відповідні «бекдори».

Перший випадок - це стандарт криптографії з депонуванням ключів (проект Skipjack), де бекдор передбачався на апаратному рівні. На початку дев'яностих уряд США ініціював масовий випуск мікросхеми Clipper chip (VLSO MYK-78). Передбачалося, що вона встановлюватиметься у всі телефони і шифруватиме голосовий зв'язок, залишаючи АНБ можливість простого розшифровування за рахунок вбудованого бекдору. У центрі концепції Clipper була система

депонування ключів (key escrow). На кожному пристрої з шифрувальним чіпом встановлювався криптоключ, який передавався уряду для депонування.

Депонований ключ складався з двох частин, що окремо зберігалися в уповноважених урядових відомствах. Мікросхема генерувала сеансовий ключ, за допомогою якого шифрувала відкрите текстове повідомлення. Отриманий ключ шифрувався за допомогою ключа, що депонується. Після цього в зашифрованому вигляді, разом з ідентифікаційним номером мікросхеми, він приєднувався до шифрованого тексту. Якщо потрібно було побачити вміст повідомлення, зашифрованого з Clipper Chip, правоохоронці запитували депонований ключ у відповідних відомств. І вже використовуючи його, розшифровували сеансовий ключ і читали відкритий текст повідомлення. Тільки виняткова дорожнеча проекту Skipjack не дозволила перетворити його на життя.

Другий випадок – це криптографічний генератор псевдовипадкових чисел NIST SP 800-90A, який використовує криптографію з еліптичною кривою (Dual_EC_DRBG, Dual Elliptic Curve Deterministic Random Bit Generator). Вважається, що АНБ США зберігає закритий ключ, який разом з помилками зміщення Dual_EC_DRBG дозволяє розшифровувати трафік SSL між комп'ютерами. Більш того, цей стандарт був успішно просунутий у міжнародні стандарти.

На даний час розгортається скандал щодо створення стандартів постквантової криптографії (PQC). Деніел Бернштейн, експерт з університету Чикаго, вважає, що NIST при участі АНБ припустився навмисних або випадкових помилок у розрахунках безпеки нових стандартів типу Kyber512. Цілком ймовірно, що бекдори закладено при розробці інших стандартів шифрування і не тільки у США. Фахівці жартують, що на ринку завжди присутні лише два типи криптографічних продуктів: з відомими лазівками та ще не виявленими. Причому непомітними ці бекдори можуть залишатися роками.

Постає питання: а чи взагалі існують надійні методи забезпечення ексклюзивного доступу спецслужб до інформації користувача при збереженні достатнього рівня стійкості від стороннього порушника?

І тут на вирішення цього питання з надр спецслужб у повсякденне життя виринає та формується ще одна наука - ***клептографія*** (англ. keptography), яка вивчає теорію і практику побудови інформаційних систем, що містять безпечні та приховані штучні канали витоку секретної інформації шляхом впровадження вразливостей у систему захисту інформації.

Термін клептографія з'явився у 1998 році завдяки роботі відомих фахівців з криптографії А. Янга та М. Юнга. Спочатку вони називали клептографією впровадження бекдора, що важко виявляється, виключно в схемах асиметричної

криптографії. Такий бекдор давав можливість обчислити секретний ключ користувача за його відкритим ключем, але тільки тим, хто знав секрет. Згодом, вони розширили межі клептографії на інші види криптоалгоритмів, включаючи криптографічні протоколи.

Клептографія, як напрямок інформаційної безпеки, тісно пов'язана з криптографією та стегенографією (рис.8.1).

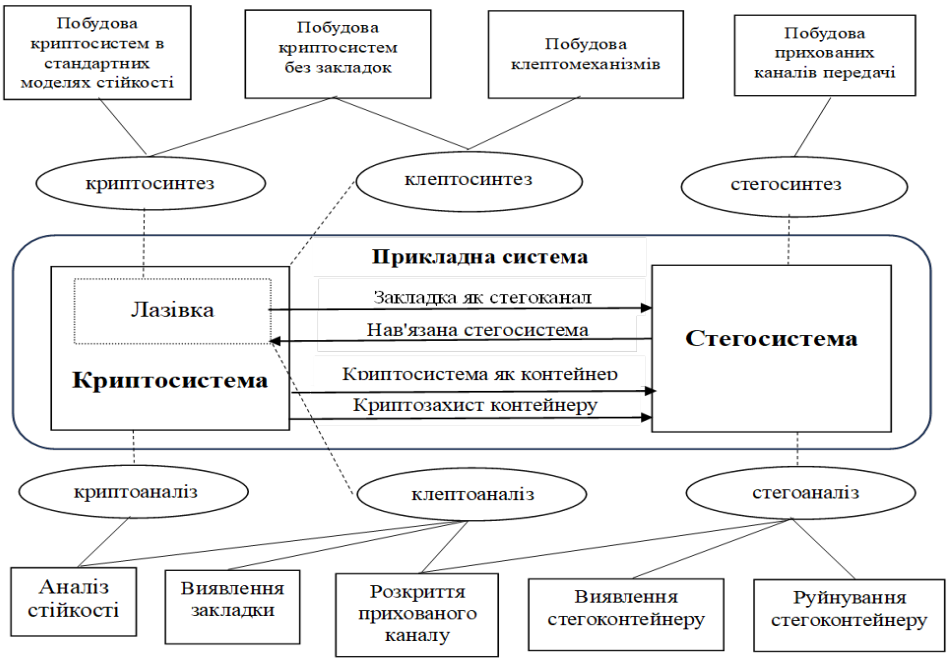


Рис.8.1. Зв’язок клептографії з криптографією та стеганографією

Зв'язок клептографії з криптографією обумовлено тим, що об'єктом її досліджень є клептографічна закладка, яка є частиною криптосистеми. Методи криптоаналізу часто використовуються для виявлення клептозакладок, тобто одночасно є інструментами клептоаналізу.

Клептографія близька також до стеганографії: їх базовим елементом є прихований канал (анг. subliminal channel, підсвідомий канал), який вперше запропонував Симмонс. Будь-яка клептографічна атака ґрунтується на прихованому каналі передачі інформації. Саме вони у поєднанні з додатковими криптографічними методами забезпечують не виявлення цих атак.

Таблиця 8.1. Відмінність методів клептографії та стеганографії

Критерій порівняння	Клептографія	Стеганографія
Мета	Корекція роботи системи	Приховування факту передачі інформації між

	в інтересах розробника чи спецслужби	користувачами
Рівень абстракції	На рівні крипто протоколу	На рівні передачі даних (залежить від типу даних та параметрів мережі)
Спосіб застосування	Таємна модифікація системи або впровадження лазівки на етапі розробки	Попереднє узгодження між користувачами стегосистеми
Спосіб впровадження	Інтегрується реалізацію системи	Сторонній модуль, програма, плагін
Щільність передачі	Відносно висока	Відносно низька
Вектор протидії	Збереження захисних властивостей системи користувача	Унеможливлення обміну прихованою інформацією
Протидія передачі	Стійкий клептомеханізм не може бути виявлений чи отфільтрований без порушення роботи системи	Псування контейнеру без порушення загальної роботи системи

Клептографічні методи дозволяють довести до досконалості приховування факту передачі додаткової інформації. У цьому сенсі простежується подібність до стеганографії, але є і відмінності (табл.8.1). Приховані клептографічні канали є частиною криптоалгоритму і дозволяють непомітно передавати інформацію з криптографічної системи або, навпаки, до криптографічної системи. Наприклад, додаткова інформація може міститись у цифровому підписі або у відкритому ключі шифрування.

Терміни клептографії лише формуються, наведемо деякі з них:

- *клептографічний механізм (закладка, клептографічна лазівка)* -особливість дизайну системи захисту, що дозволяє розробнику, який впровадив даний механізм, створювати канал витоку секретних даних;

- *клептографічна атака* – можливі зловмисні сценарії, що можуть виконуватися розробником закладки: клептографічна модифікація системи захисту, побудова системи захисту з закладкою, використання можливостей закладок тощо;
- *стійкість до клептографічних атак* – властивість системи, що полягає у неможливості побудови непомітної закладки або каналу витоку.
- *клептографічний канал витоку* – канал непомітного витоку секрету (прихований канал, subliminal channel), який практично може отримати розробник закладки і не можуть отримати інші учасники системи.

Надійний клептографічний канал передачі даних повинен володіти наступними властивостями:

- *невиявленістю* - що означає неможливість виявлення клептографічної атаки виключно за зовнішніми ознаками, якщо система захисту (криптосистема в узькому сексі) є «чорною скринькою»;
- *стійкості до злому без проведення реінжинірингу* – неможливість перехоплення інформації без знання внутрішнього устрою системи захисту, тобто у рамках моделі «чорної скриньки»;
- *стійкості до злому групи пристроїв у результаті успішного реінжинірингу одного з них* - якщо група пристроїв працює за однаковим алгоритмом і з тими самими даними, то визначення в результаті реінжинірингу внутрішньої структури і стану одного з пристроїв не дозволяє визначити стан інших пристроїв групи, отже, і їх вихідні значення;
- *непередбачуваності вліво* - говорять, що послідовність непередбачувана вліво, якщо за довільною кількістю елементів послідовності неможливо визначити її попередні елементи. Тобто йдеться про непередбачуваність вліво для внутрішнього стану криптосистеми. Це актуально, наприклад, для недеструктивного зворотного проектування. Атака називається стійкою до цього виду аналізу, якщо навіть при повному знанні внутрішньої схеми пристрою та її поточного стану неможливо дізнатися про її попередній стан;
- *повної непередбачуваності* - мається на увазі непередбачуваність вліво, а також неможливість визначення наступних станів системи захисту (непередбачуваність вправо). Очевидно, що якщо нападнику вдається визначити внутрішній стан системи і значення усіх змінних, то для повної непередбачуваності системи потрібна наявність у ній джерела ентропії.

Зауважимо, деякі властивості є залежними, наприклад: друга властивість може виконуватися лише у тому випадку, якщо виконується перша. Третя властивість має сенс, лише якщо виконується друга, а п'ята – лише якщо виконується четверта. Інші властивості незалежні.

Для відповіді на питання чи існує клептографічний канал та аналізу його властивостей необхідно, як правило, провести реінжиніринг (англ. reverse engineering) - процес дослідження деякого готового пристрою, програми,

системи, а також документації з метою визначення внутрішнього устрою апарата чи програми для відтворення принципу роботи. Існують дві моделі реінжинірингу:

- *недеструктивний реінжиніринг*, який дозволяє використовувати пристрій після проведення процедури реінжинірингу. Така модель найчастіше застосовується до програмних систем та, інколи, до апаратних систем, якщо атакуюча сторона володіє відповідними неруйнівними технологіями;
- *деструктивний реінжиніринг*, який дозволяє визначити внутрішню схему системи, але проте подальше функціонування даного екземпляру системи стає неможливим.

Реінжиніринг може виявити встановлену закладку і навіть інколи використовувати її.

При аналізі роботи клептографічних систем зазвичай виділяють наступних трьох учасників:

- *розробник* – володіє інформацією про лазівку I_l, володіє секретним ключем до лазівки K_l, але не володіє секретним ключем користувача K_k;
- *користувач* – володіє секретним ключем користувача K_k, у разі успішного реверс інжинірингу має інформацію про лазівку, але не володіє її секретним ключем K_l;
- *зловмисник* – у разі успішного реверс-інжинірингу володіє інформацією про лазівку I_l, але не володіє її секретним ключем K_l, а також секретним ключем користувача K_k.

Передбачається, що зловмисник успішно провів реверс-інжиніринг до одного або кількох подібних пристроїв та отримав інформацію про лазівку I_l: код і вміст енергонезалежної пам'яті. Передбачається також, що зловмисник має доступ до всієї публічної інформації, включаючи загальнодоступні алгоритми, відкриті ключі, зашифровані тексти, підписи тощо. При цьому можна виділити два типи зловмисника:

- *зловмисник-відрізняльник* – мета якого полягає в тому, щоб відрізнити чесну реалізацію від нечесної;
- *зловмисник-криптоаналітик* – його мета полягає в тому, щоб зламати безпеку даного пристрою, який ніколи не піддавався реверс-інженірингу (це може включати знаходження закритого ключа користувача, дешифрування інформації, зашифрованих з відкритим ключем, підробку підпису тощо).

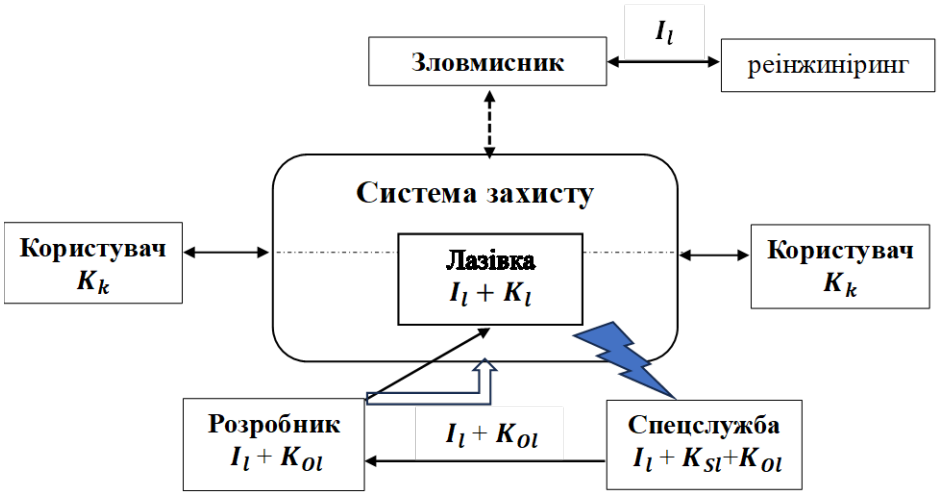


Рис.8.2. Механізм взаємодії учасників клептографічної системи

Зважаючи на тенденції останніх років, рольову модель можна видозмінити, додавши ще одного учасника – *спецслужбу* – та обмежити рівень знання розробника (рис.8.2). У цій новій моделі разом із «користувачем» та «зловмисником» діють:

- *спецслужба* - має інформацію про лазівку I_l, володіє секретним ключем до лазівки K_{Sl}, не володіє секретним ключем користувача K_k;
- *розробник* - має інформацію про лазівку I_l, володіє відкритим ключем лазівки K_{Ol}, не володіє секретним ключем до лазівки K_{Sl}, не володіє секретним ключем користувача K_k.

Спецслужба видає розробнику інструкції з реалізації лазівки та відкритий ключ K_{Ol}, за допомогою якого шифруватимуться дані, що видаються через лазівку. Розробник знає весь механізм роботи I_l, але не знає секретного ключа K_{Sl}, тому при використанні не зможе отримати доступ до даних користувача (тобто користувач захищений не тільки від стороннього порушника, але і від розробника).

Зловмисник до проведення реверс-інжинірингу має менші можливості, ніж розробник, а після його проведення він може отримати механізм роботи лазівки I_l. Крім того, у зловмисника, якщо у нього є відповідні спроможності, є можливість вивчити архітектуру побудови системи захисту, розробити та впровадити свою закладку для створення клептографічного каналу.

На даний час існує тільки загальні рекомендації щодо захисту від клептографічних атак в криптосистемах, такі як проведення комплексного аналізу структури криптосистеми із залученням фахівців у галузі криптографії або композиція (каскадування) криптоперетворень, що мають походження з різних джерел:

1. Перед використанням криптографічного примітиву, його структура має бути ретельно вивчена та оцінена. Не можна беззастережно довіряти апаратним компонентам із заданою специфікацією (необхідна перевірка реалізації на відповідність специфікації, а також вивчення самої специфікації). Навіть програмні реалізації можуть бути небезпечні, особливо якщо вихідний код і документація розробника недоступні для перевірки.

2. Проходження тестів за формальними критеріями не гарантує відсутності прихованих лазівок. Зокрема, не можна приймати рішення про довіру лише виходячи з великого статистичного дослідження. Очевидно, для будь-якого фіксованого набору критеріїв можна побудувати криптосистему з лазівкою, яка задовольнятиме цим критеріям.

3. Непоганий захист від наявності прихованих лазівок у криптоалгоритмах дає композиція (каскадування) криптоперетворень, що мають походження з різних джерел.

4. Важливим є контроль за випадковістю. Цілком необхідно, щоб алгоритми генерації випадкових величин, що використовуються в криптографічних примітивах, були відкриті для користувача. Якщо є програмне забезпечення для вироблення ключів – воно має бути абсолютно надійним та довіреним. Добре щоб була можливість використовувати стороннє джерело випадкових чисел.

5. Краще якщо джерело випадковості, генератор ключів та алгоритм, що їх використовує – були три роздільні компоненти. При цьому має бути виключена можливість їхнього обходу, самі вони – з надійного джерела, а канали, що їх пов'язують, не допускають витоку інформації.

Поки що можна констатувати, що ліцензування систем захисту є єдиним способом боротьби з клептографією (якщо не враховувати інтереси спецслужб).

Загалом, можна виділити подальші напрямки клептографічних досліджень:

- побудова клептографічного каналу витоку шляхом модифікації стандартної системи захисту;
- створення нових систем захисту з вбудованим клептографічним каналом;
- виявлення клептографічних закладок як у загальній схемі системи захисту, так і у її конкретній реалізації;
- побудова системи захисту з гарантованою відсутністю клептограічного каналу витоку;
- побудова системи захисту із мінімізацією можливостей вбудовування клептозакладки.

У ході дослідження за даними напрямками виникає ще ряд пов’язаних проблем:

- відсутність достатньої формалізації клептографії (не зважаючи на те, що наразі вже відомі чисельні практичні та теоретичні клептографічні системи, досі не сформована більш-менш загальна теорія);

- неадекватність наявних моделей надійності систем захисту у контексті клептографічних задач;
- відсутність методів оцінки ризиків, пов’язаних з клептографічними атаками;
- відсутність методів побудови елементів захисту з доведеною відсутністю клептозакладок;
- відсутність критеріїв оцінки потенційних клептографічних можливостей систем захисту та інші.

8.2. Приховані канали

Спроби зберегти у таємниці сам факт передачі інформації має давню історію, а наука, яка вивчає методи створення, виявлення та використання каналів прихованої передачі інформації, отримала назву ***стеганографії***.

Відомі згадки про методи приховування інформації вже у стародавньому світі. Так, за однією з версій, шумери одними з перших використовували стеганографію: було знайдено безліч глиняних клинописних табличок, в яких один запис покривався шаром глини, на якому писалася інша інформація. Таким чином приховувалася первинна інформація.

Історично одним із найпоширеніших методів класичної стеганографії було використання симпатичних (невидимих) чорнил. Текст, записаний таким чорнилом, проявляється лише за певних умов (нагрів, освітлення, хімічний проявник тощо).

Нині, у зв'язку з бурхливим розвитком обчислювальної техніки, методи приховування інформації отримали друге життя. У стеганографії з'явився новий напрямок – ***цифрова стеганографія***, в основі якої лежать методи приховування чи впровадження додаткової інформації у цифрові об'єкти (контейнери) з можливим спотворенням цих об'єктів. Як правило, такі об'єкти є мультимедіа-об'єктами (аудіо, відео, зображення), призначеними для сприйняття такими сенсорними органами людини, як зір або слух. Внесення невеликих спотворень нижче за поріг чутливості середньостатистичної людини, не призводить до значних змін сприйняття цих об'єктів. Більш того, в оцифрованих об'єктах, які мають аналогову природу, завжди присутній шум квантування, а при

відтворенні таких об'єктів з'являється ще додатковий аналоговий шум та нелінійні спотворення апаратури. Тому все це сприяє ще більшій непомітності прихованої інформації.

З другого боку, методи цифрової стеганографії дають також можливість зловмисникам обмінюватися таємною інформацією без розкриття факту передачі. Так, наприклад, якщо одному з них стала відома інформація, відкрита передача якої небажана, то для її прихованої передачі він може підібрати відповідний контейнер (мультимедіа-файл), вбудувати в нього цю інформацію і спокійно передати результат спільнику по відкритому (небезпечному) каналу зв'язку. І це буде виглядати як звичайний обмін мультимедіа-файлами й не викличе підозру.

У наведеному прикладі зловмисники обмінюються інформацією по відкритому каналу зв'язку, тобто у межах певної моделі, для якої існує політика безпеки, що дозволяє такий зв'язок. Насправді це не завжди так. В ідеалі, для забезпечення належного рівня захисту суб'єкту безпеки має бути заборонено будь-яку діяльність, результат якої може призвести до небажаного розкриття конфіденційної інформації. Вказаного у прикладі витоку інформації можна було уникнути, якби адміністратор безпеки врахував можливість такого розвитку подій і заборонив цим суб'єктам обмінюватися даними.

До певного часу вважалося, що якщо у системі реалізована якась недискреційна модель безпеки й у межах цієї моделі безпеки кожному суб'єкту визначена чітка безпекова політика, яка виключає можливість передачі небажаної інформації, то ця система безпечна.

Але чи є так насправді? А якщо впроваджена модель безпеки не повністю відповідає реальності? А якщо адміністратором безпеки не було враховано якийсь неочевидний, але потенційно можливий взаємозв'язок суб'єктів? Тоді можна припустити наявність комунікаційних каналів, які деякі суб'єкти безпеки можуть використовувати для обміну інформацією. І у випадку, якщо

взаємозв'язок даних суб'єктів був заборонений, обмін інформацією відбуватиметься в рамках чинної моделі безпеки, але в обхід існуючих безпекових політик.

Механізми, що дозволяють передавати неавторизовану інформацію за допомогою методів, які вважаються авторизованими, отримали назву ***прихованих каналів*** (covert channels).

Вивчення прихованих каналів є теоретичною та практичною базою, окрім стеганографії, ще для одного наукового напрямку – ***клептографії***, яка займається проблемою існування лазівок (бекдорів) у криптографічних системах. Клептографія, у свою чергу, стала теоретичною базою ***криптовірології*** - методів розробки шкідливого програмного забезпечення, що шифрує свій код та/або трафік. Близько до клептографії примикають класичні програмні та апаратні закладки, які часто встановлюють самі розробники або їх контрагенти. Більш детально методи стеганографії та клептографії будуть розглянуті у наступних розділах.

8.2.1. Теорія прихованих каналів

Прийнято вважати, що вперше поняття прихованого каналу було введено у 1973 р. Батлер Лемпсоном, який у своїй роботі "A Note on the Confinement Problem", розглядає таке завдання: нехай клієнт викликає деякий сервіс, передаючи йому у якості параметру деяку конфіденційну інформацію, витік якої небажаний. Як слід обмежити поведінку цього сервісу?

Щоб визначити область можливих обмежень, Лемпсон розглядає різні потенційно можливі канали витоку інформації. І хоча їх кількість велика, автор пропонує кожен із них пронумерувати, а потім заблокувати. Намагаючись дати певну класифікацію каналів витоку інформації, Лемпсон виділяє окремий клас - *приховані канали* - і дає таке визначення: *комунікаційний канал називається прихованим, якщо він не призначався для передачі даних*.

Ідея додаткового обмеження дій, які дозволяється виконувати програмі (крім застосування наявних в ОС механізмів контролю доступу), є виключно важливою та глибокою, що випередила свій час.

Розмірковуючи про заходи боротьби з прихованими каналами, Лемпсон формулює наступне правило: *для ефективної протидії необхідно забезпечити зашумлення усіх можливих прихованих каналів шляхом виконання дій, що імітують дії обмежувальної програми в моменти передачі даних у прихований канал*.

Звичайно, таке рішення може бути далеко не оптимальним і у багатьох випадках його застосування неможливе. Більш практичною альтернативою є обмеження пропускної спроможності прихованих каналів. Але слід розуміти, що зниження пропускної спроможності каналу зовсім не означає неможливості передачі даних.

У 1976 р. Боб Міллен продемонстрував своїм колегам реалізований ним прихований канал. Два процеси взаємодіяли між собою, використовуючи "*помилки відмови сторінок*" (page fault). Процес відправника звертався на читання до певних сторінок файлу загальної бібліотеки. Процес отримувача звертався до тих самих сторінок, вимірюючи час, витрачений на цю операцію. Таким чином, за часом звернення можна було визначити, перебуває дана сторінка в пам'яті чи ні, що дозволяло кодувати інформацію та здійснювати передачу даних. Ця історія була першим описаним фактом організації прихованих каналів за часом.

Продовжуючи вивчати позначену Лемпсоном проблему обмеження та попутно розвиваючи тему прихованих каналів, в 1977 р. Марвін Шойфер приходить до наступного визначення прихованих каналів: *«Комунікаційний канал є прихованим (непрямим), якщо він заснований на передачі, що використовує зміни станів ресурсу»*.

До проблеми обмеження Шойфер, на відміну Лемпсона, підійшов з практичної сторони. У своїх дослідженнях він використав систему KVM/370 – одну з перших ОС із багаторівневою моделлю безпеки. Тому його визначення прихованого каналу мало суто практичний прикладний характер. Вводиться поняття ресурсу, що необхідний для організації прихованої взаємодії. Зміна стану загального ресурсу, з одного боку, і спостереження за станом цього ресурсу, з іншого, – ось основний спосіб організації прихованої взаємодії, на думку Шойфера.

У 1978 р. виходить у світ технічний звіт, що розглядає питання існування прихованих каналів у системах з розподілом часу. Його автор Джон Хаскемп наводить опис кількох потенційно можливих сценаріїв організації прихованих каналів. Він дотримується наступної думки. Так як у системах з управлінням доступом до ресурсів завжди існують політики розподілу ресурсів, що працюють в рамках будь-якої реалізації, то приховані канали слід визначати як *«канали, які є результатом дії політик розподілу ресурсів та управління ресурсами»*.

Протягом усього того часу, що пройшло з моменту публікації Лемпсоном його замітки, всі матеріали по темі прихованих каналів носили або теоретичний, або вузько-прикладний, дослідницький характер. Наукова громадськість розуміла, що тема прихованих каналів досить актуальна при розгляді питань безпеки, проте перша спроба використати науковий підхід у створенні методів протидії прихованим каналам була зроблена лише 1983 року.

Саме тоді Кеммерер публікує свої наукові роботи, присвячені питанням виявлення прихованих каналів. *По-перше*, він пропонує використовувати матриці сумісних ресурсів як спосіб виявлення потенційно можливих зв'язків між суб'єктами. *По-друге*, він першим дає визначення прихованим каналам *пам'яті* (storage) і прихованим каналам *часу* (timing) – двом принципово різним класам прихованих каналів. Так, прихованим каналом пам'яті називається такий

канал, в якому інформація передається за допомогою доступу відправника на запис та отримувача на читання до одних й тих самих ресурсів або об'єктів. Прихований канал за часом характеризується доступом відправника та отримувача до одного й того самого процесу чи атрибуту, який змінюється у часі.

Під прихованими каналами Кеммерер має на увазі ті канали, *«які використовують сутності, які зазвичай не відображаються як об'єкти даних для передачі інформації від одного суб'єкта до іншого»*.

Кульмінацією першої хвилі досліджень є видання в 1985 р. Міністерством Оборони США так званої «помаранчевої книги» — збірки керівних документів, присвячених критеріям оцінки захищеності комп'ютерних систем (TCSEC). У ньому, починаючи з класу захищеності B2, присутні вимоги аналізу системи щодо наявності прихованих каналів. Особливим пунктом виділено «Посібник із прихованих каналів». Так, згідно з TCSEC, *«прихований канал – це будь-який комунікаційний канал, який може бути використаний процесом з метою передачі інформації у спосіб, що порушує політику безпеки системи»*.

Вводяться також два типи прихованих каналів – приховані канали пам'яті та приховані канали за часом:

• *«Приховані канали пам'яті включають всі засоби, що дозволяють прямий або непрямий запис в комірку зберігання одним процесом і пряме або опосередковане читання цієї комірки іншим.*

• *Приховані канали за часом включають всі засоби, що дозволяють одному процесу сигналізувати іншому процесу за допомогою модуляції використання системних ресурсів таким чином, що відстеження зміни часу відповіді дає інформацію іншому процесу».*

З точки зору безпеки, приховані канали становлять тим більшу загрозу, чим більша їхня пропускна здатність. Однак методи зниження пропускної спроможності таких каналів до певної величини (залежної від архітектури

системи та механізму функціонування самого каналу) можуть призводити до зниження продуктивності системи в цілому, що неминуче торкнеться звичайних користувачів. Тому завжди слід дотримуватися балансу між зниженням пропускної здатності прихованого каналу і падінням загальносистемної продуктивності. Очевидно, що у випадку, якщо в системі відбувається обробка закритої інформації, розголошення якої небажане, така система не повинна містити прихованих каналів з високою пропускною здатністю.

У TCSEC стверджується, що прихований канал має високу пропускну здатність, якщо він здатний передавати інформацію зі швидкістю більше 100 біт в секунду. Така швидкість приблизно дорівнює швидкості роботи багатьох терміналів. Тому не можна назвати систему захищеною, якщо інформація витікає із системи зі швидкістю виведення звичайного термінального пристрою.

Взагалі немає нічого дивного в тому, що в багаторівневих комп'ютерних системах може існувати велика кількість низькошвидкісних прихованих каналів, і зниження їх пропускної спроможності вестиме до значних втрат у продуктивності. Тому, згідно з керівними документами TCSEC, у багатьох випадках допускається існування таких каналів, пропускна здатність яких не перевищує 1 біта в секунду. У деяких випадках, з метою збереження системної продуктивності, допускається не вживати заходів щодо протидії прихованим каналам з пропускною здатністю більше 1 біта в секунду, а натомість відстежувати спроби передачі по них інформації без значного зниження продуктивності.

Згідно з TCSEC, аналіз прихованих каналів повинен включати:

- виявлення прихованих каналів;
- визначення максимально досяжної пропускної спроможності виявлених прихованих каналів;
- вжиття заходів протидії виявленим прихованим каналам;

- підтвердження того, що вжиті заходи щодо протидії виявленим прихованим каналам є ефективними.

З ухваленням TCSEC закінчується перша хвиля досліджень прихованих каналів. Подальше зростання інтересу до цієї проблеми зумовлене, *по-перше*, визнанням фахівцями високого рівня загроз, що становлять існування прихованих каналів, *по-друге*, включенням до складу керівних документів Міністерства Оборони США положень, пов'язаних з аналізом прихованих каналів, і, *по-третє*, бурхливим розвитком обчислювальної техніки та появою глобальних мереж, зокрема мережі Інтернет.

З середини 80-х минулого сторіччя ведуться роботи з вивчення механізмів створення прихованих каналів та методів протидії їм. Інструментами таких досліджень є *теорія інформації Шеннона, теорія ланцюгів Маркова, теорія кодування інформації*. Більшість досліджень орієнтована на побудову моделей прихованих каналів, вивчення їх якостей і параметрів. З'являються роботи, що описують методи виявлення прихованих каналів у програмах шляхом аналізу їх вихідних кодів.

Розвиток мереж та технологій пакетної передачі даних, особливо TCP/IP, також відбивається на кількості робіт, присвячених прихованим каналам. Так, зростає частка практичних досліджень, присвячених розробці нових типів прихованих каналів на основі популярних протоколів зв'язку. Пропорційно до цього збільшується кількість наукових праць, пов'язаних із виявленням та протидією цим прихованим каналам.

Традиційним стає таке визначення прихованого каналу: «*Нехай дана модель недискреційної політики безпеки M та її реалізація I(M) у певній системі. Потенційний зв'язок між суб'єктами I(S) і I(R) в I(M) називається прихованим каналом тоді і тільки тоді, коли зв'язок між S і R в моделі M не дозволений*».

З одного боку, порівняно з роботою Лемпсона, поняття прихованого каналу тут трактується ширше. Фактично до прихованих каналів віднесено всі види передачі інформації, що порушують політику безпеки. З іншого боку, накладено обмеження на дисципліну розмежування доступу, що реалізується. Вона не повинна зводитися до довільного управління доступом.

Дискреційні механізми не можуть протистояти недбалості або злому наміру, оскільки переносять весь тягар забезпечення безпеки на користувача, неакуратність якого в будь-який момент часу може призвести до порушення політики.

Якщо використовуються лише дискреційні механізми безпеки, зловмисник, який має доступ до конфіденційної інформації та додатків, може розкрити закриту інформацію безпосередньо, порушивши політику безпеки. Дії авторизованого, але неакуратного користувача також можуть стати причиною витоку конфіденційної інформації, при цьому канал витоку може не зачіпати комп'ютерну систему, можливість використання комп'ютерних каналів витоку інформації може збільшити розміри витоку і зменшити ефективність її виявлення та відстеження. За наявності ж мандатних чи інших недискреційних механізмів захисту виток конфіденційної інформації можлива лише через приховані канали, що обмежує розміри витоку та забезпечує контроль за нею за умови аудиту прихованих каналів.

Таким чином, коло систем звужується до вельми нечисленних, хоча і критично важливих, режимних конфігурацій, що використовують багаторівневу безпекову політику і примусове (мандатне) управління доступом.

Початкові дослідження прихованих каналів мали суто практичний характе, у яких пропонувалися методи організації нових типів прихованих каналів, що у своє чергу привело до появи нових робіт, які були відповіддю на загрозу, тоді як теоретичним дослідженням було присвячено лише невелика частина робіт. В

даний час чітко намітилися такі основні тенденції у питаннях дослідження прихованих каналів:

- дослідження методів організації та механізмів функціонування прихованих каналів;
- визначення характеристик прихованих каналів;
- розробка способів протидії.

Перед розглядом методів організації та механізмів функціонування прихованих каналів у системах обробки інформації розглянемо питання, пов'язані з характеристиками таких каналів.

8.2.2. Характеристики прихованих каналів

У роботах, присвячених дослідженню характеристик прихованих каналів, приховані канали зазвичай розглядаються з погляду теорії інформації Шеннона (Шеннон К. Математична теорія зв'язку. // Шеннон К. Роботи з теорії інформації та кібернетиці. М., 1963). І це невипадково, враховуючи те, що головна відмінність прихованого комунікаційного каналу від звичайного у тому, що прихований канал не проектувався і не передбачався для передачі даних. При розгляді характеристик прихованих каналів ця відмінність вважається несуттєвою.

У вводяться різні параметри прихованих каналів, які покликані описати їх властивості. Так, крім поділу прихованих каналів по пам'яті та за часом, вводяться такі характеристики:

- шумність;
- ємність / пропускна здатність;
- синхронізація;
- агрегація.

Як і будь-який комунікаційний канал, прихований канал може бути *з шумом* або *безшумним*. Під безшумним каналом мається на увазі такий канал, у якому символи, що приймаються отримувачем, завжди збігаються із символами,

які передані відправником. Зазвичай, у разі прихованих каналів, кожен символ являє собою 1 біт інформації. Тому, незалежно ні від чого, в безшумному каналі отримувач гарантовано отримує кожен біт, що передається відправником.

У разі наявності у каналі шумів, отримувач не завжди приймає саме те, що надсилав відправник. Тому для забезпечення надійної передачі інформації необхідно використовувати завадостійке кодування.

Теорія інформації Шеннона дозволяє отримати відповідь на питання існування способу надійної передачі у каналі з заданими характеристиками шуму. Теорія кодування дозволяє побудувати оптимальні для конкретного випадку коригуючі коди, що підвищують надійність передачі інформації.

Ємність відноситься до характеристик комунікаційного каналу. Під ємністю каналу мається на увазі максимально можлива швидкість надійної передачі через канал. Очевидно, що ємність каналу може вимірюватися як у кількості біт на величину завантаження каналу C_u, так й у кількості біт на одиницю часу C_t. У випадку, якщо на передачу кожного символу витрачається однакова кількість часу φ, співвідношення між C_t та C_u набуває форми:

$$C_t = \varphi^{-1} \cdot C_u.$$

Відповідно до TCSEC, до характеристик прихованих каналів належить їхня *пропускна здатність* – швидкість, з якою здійснюється надійна передача інформації. Очевидно, що пропускна здатність каналу та його ємність пов'язані між собою. Так, ємність є максимально досяжною пропускною здатністю.

Одним із найважливіших результатів теорії інформації Шеннона є те, що вона дозволяє дати оцінку ємності як верхньої межі швидкості передачі інформації через комунікаційний канал за наявності перешкод (теорема Шеннона). Міллен вперше застосував теорію інформації Шеннона для визначення ємності прихованих каналів.

Цей напрямок отримав подальший розвиток. Так, Московиць дослідив у своїх роботах *дискретні комунікаційні канали без пам'яті* (discrete memoryless channels, DMC). Це, *по-перше*, означає, що як відправник, так і отримувач у процесі передачі інформації використовують дискретні алфавіти, вибір яких багато в чому залежить від реальних фізичних процесів, що відбуваються під час передачі (як було зазначено вище, у разі відсутності шумів у каналі, алфавіти відправника та отримувача збігатимуться). *По-друге*, процес передачі у поточний час не залежить від переданої раніше інформації. Але, на думку автора досліджень, для визначення характеристик прихованих каналів ці обмеження несуттєві. Для такого класу каналів, названих *простими часовими каналами* (simple timing channels, STC), були визначені значення ємності, а також отримані значення верхньої та нижніх її меж.

Для визначення ємності зазвичай використовується теорія інформації. Нехай дана якась випадкова дискретна величина X, $X = x_i$. Нехай $H(X)$ є ентропія величини X. Ентропія наразі визначає «невизначеність» значень X. Для деякого значення x його невизначеність є $-logP(x)$, де $P(x)$ – функція розподілу ймовірності. Ентропія у цьому випадку дорівнюватиме

$$H(X) = -\sum_i [P(x_i) \cdot \log P(x_i)].$$

Тобто ентропія величини X є сумою з протилежним знаком усіх добутків відносних частот появи події x_i, помножених на їх логарифми (для зручності роботи з інформацією зазвичай використовується логарифму за основою 2).

Нехай X визначає дані на вході каналу, а Y – дані на виході. Тоді умовну ентропію $H(X|Y)$ можна визначити як

$$H(X|Y) = \sum_i [H(X|y_i) \cdot P(y_i)] = H(X) = -\sum_i [P(y_i) \cdot P(x_i|y_i) \cdot \log P(x_i|y_i)].$$

Якщо X та Y незалежні, то $H(X|X) = 0$ та $H(X|Y) = H(X)$.

Для будь-яких дискретних випадкових величин X і Y можна визначити величину взаємної інформації як статистичну функцію двох випадкових

величин, що описує кількість інформації, що міститься в одній випадковій величині щодо іншої:

$$I(X;\ Y) = H(X) - H(X|Y),$$

де $H(X)$ – ентропія, $H(X|Y)$ – умовна ентропія.

Для дискретного комунікаційного каналу без пам'яті, передавач якого представлений дискретною випадковою величиною X, а приймач – величиною Y, значення ємності каналу буде визначено як

$$C_u = \max I(X;\ Y) \text{ [біт/завантаження каналу]}$$

$$C_t = \max [I(X;\ Y) / E(X)] \text{ [біт/одиниця часу]},$$

де $I(X;\ Y)$ – взаємна інформація між X і Y, $E(X)$ – очікуваний час передачі X, а максимізація проводиться X.

Необхідно відзначити важливий момент щодо нульового значення ємності каналу. А саме, нульова ємність каналу не означає неможливість передачі повідомлення цим каналом. Так, у роботі наведено приклад теоретичного комунікаційного каналу з нульовою ємністю, що дозволяє надсилати невеликі повідомлення. Основний висновок, який із цього випливає, полягає в тому, що *для визначення ступеня захищеності системи недостатньо отримати значення ємності прихованого каналу*.

Наприклад, нехай існує якийсь канал, здатний передати 100 біт лише за початковий відрізок часу. У такого каналу буде нульова ємність, проте все ж таки він дозволить передати якусь інформацію. Необхідно розуміти, що ємність каналу є асимптотична величина і її застосування найбільше підходить до випадків передачі великих обсягів даних за тривалі періоди часу. Розрахункове значення ємності може дати лише верхню оцінку пропускної спроможності каналу. Насправді, як показує практика, ця величина виявляється набагато меншою.

Нехай безпека системи залежить від конфіденційності інформації. Розглядаючи характеристики прихованих каналів і торкаючись питання визначення ступеня небезпеки даного каналу, можна визначити ступінь припустимої загрози, що виходить від прихованого каналу. Для оцінки ступеня загрози безпеці системи можна використовувати наступну трійку параметрів (*n, p, t*):

- мінімальна довжина *n* повідомлення, витік якого ставить під загрозу безпеку системи;
- мінімально допустима точність *p* передачі повідомлення;
- максимально допустимий час *t* надсилання повідомлення.

Таким чином, можна сформулювати критерій оцінки безпеки системи з точки зору захищеності від прихованих каналів: *якщо існуючий в системі прихований канал дозволяє передати інформацію довжини n з точністю не гірше за p за час не більше t, то такий канал вважається можливим для витоку інформації.*

Повертаючись до характеристик прихованих каналів, необхідно торкнутися питань організації передачі даних за допомогою прихованих каналів. І хоча мова про методи організації прихованих каналів піде пізніше, зараз необхідно висвітлити важливий момент створення прихованого з'єднання – синхронізацію та агрегацію.

У визначено, що *синхронізація* між сторонами комунікаційного каналу дозволяє одній стороні інформувати іншу про те, що вона завершила читання або запис даних. Це важливий момент, що дозволяє організувати синхронну взаємодію у випадку, якщо відправник та отримувач діють асинхронно. Проте, зазвичай, використання механізмів синхронізації веде до зниження пропускної спроможності каналу.

Для підвищення швидкості передачі можна використовувати *агрегацію* різних прихованих комунікаційних каналів. Тобто можна, наприклад, групувати

існуючі канали з метою збільшення загальної пропускної спроможності за рахунок розпаралелювання потоків даних.

Таким чином, розглянуті характеристики прихованих каналів дозволяють дати їх кількісний опис, сприяючи застосуванню формальних підходів для дослідження прихованих каналів.

8.2.3. Сучасний погляд на приховані канали

Як правило, базові концепції аналізу прихованих каналів були сформовані досить давно. Частина з них вірна в даний час, проте все частіше у сучасних роботах з'являються новаторські ідеї та методи. Так, у роботі запропоновано новий підхід до моделювання прихованих каналів та їх класифікації.

Згідно з основною ідеєю, викладеною в роботі, для передачі інформації відправник повинен мати можливість зробити щось, що отримувач здатний «побачити». Під словом "бачити" тут маються на увазі будь-які методи, за допомогою яких спостерігач зможе вивчити стан або отримати значення об'єкту спостереження. Однак одночасний розгляд усіх можливих механізмів на всіх можливих рівнях системи в загальному випадку важко реалізувати. Натомість, використовуючи загальні принципи, пропонується аналізувати один рівень абстракції в одиницю часу.

Таким чином, пропонується розглядати сукупність методів даного рівня абстракції, які дають змогу спостерігачеві вивчати стан об'єкту. Сукупність усіх видимих спостерігачем об'єктів називається *видимим простором спостерігача V*.

Не важливо, які фізичні механізми використовує відправник передачі інформації. Зрештою, зроблені зміни відображаються у видимому просторі спостерігача даного рівня абстракції. Навпаки, механізми, які можуть викликати зміни у видимому просторі, неспроможні передавати інформацію на цьому рівні, хоча можуть бути використані інших. Це дає можливість обмежити аналіз одним рівнем абстракцій за одиницю часу.

Нехай дана якась обчислювальна система. Вона може бути розглянута як кінцевий автомат, що містить активні суб'єкти (наприклад, виконувані програми) та пасивні об'єкти (наприклад, дані цих програм). Пасивні об'єкти формують стан автомата, а активні суб'єкти змінюють його. *Суб'єкт є послідовністю атомарних операцій, що змінюють стан одних об'єктів (вихід) залежно від стану інших (вхід)* (вважається, що операція є атомарною, якщо процес зміни стану, що виробляється цією операцією, неподільний).

Усі програми в системі суть суб'єкти. Частина апаратного забезпечення, що генерує дані, також може бути представлена як суб'єкт на відповідному рівні абстракції. Відправник і отримувач – також суб'єкти, кожен із яких може складатися з багатьох інших суб'єктів. Однак у процесі взаємодії окрім відправника та отримувача завжди існує «третя особа», здатна вносити непередбачувані зміни у процес передачі. Тому *під «стороннім» розуміється якась третя особа, яка має можливість проводити зміни у видимому просторі отримувача*.

Відправник немає контролю над стороннім суб’єктом (третьою особою), який може взагалі нічого не підозрювати про взаємодію відправника та отримувача. Поняття «стороннього» введено, оскільки він відіграє важливу роль у встановленні прихованого каналу, у разі, коли відправник не має доступу для запису у видимому для отримувача просторі.

Наведені вище припущення дозволяють сформулювати мінімальні вимоги для встановлення прихованого каналу.

Теорема 1. *Прихований канал може існувати, якщо відправник може викликати зміни у видимому просторі отримувача*.

Доказ. Нехай отримувач та його видимий простір є кінцевим автоматом. Якщо наявність відправника здатна впливати на хід роботи отримувача, то можна показати, що отримувач може отримувати інформацію від відправника, тобто можливий прихований канал. У даному випадку, у зв’язку з тим, що

відправник здатний змінювати видиме оточення отримувача, яке є станом кінцевого автомата, то в хід роботи отримувача можуть бути внесені зміни. Тобто допустиме існування прихованого каналу.

Теорема 2. Прихований канал може існувати, якщо відправник здатний керувати моментом оновлення об'єкту, що спостерігається отримувачем.

Доказ. Нехай OP_n означає *n*-е дію отримувача. OP_n отримує об'єкт OBJ_i на вході та перетворює його на OBJ_o на виході. Нехай $OBJ_i(k)$ відповідає *k*-му перетворенню об'єкта OBJ_i. Якщо відправник може контролювати час модифікації об'єкта OBJ_i так, що оновлення об'єкта може відбуватися як до, так і після виконання OP_n, тобто передавати OP_n або $OBJ_i(k)$ або $OBJ_i(k\text{-}1)$ як вхідні дані, то результат дії OP_n буде змінюватися під контролем відправника. Таким чином, прихований канал може існувати.

Теорема 3. Необхідною та достатньою умовою встановлення прихованого каналу є наявність однієї або обох можливостей відправника, описаних у теоремах 1-2.

Доказ цієї теореми наведено у роботі.

З основних механізмів організації прихованих каналів, запропонованих вище, пропонується підхід до класифікації прихованих каналів (табл. 8.2). Так, перший механізм утворення прихованого каналу (Теорема 1) передбачає внесення змін до видимого простору отримувача, що може бути охарактеризовано як просторова інформація, утворюючи *просторовий канал* (spatial channel). Другий механізм утворення прихованого каналу (Теорема 2) передбачає внесення змін до послідовності подій, що може бути охарактеризовано як інформація події, утворюючи *часовий канал* (temporal channel).

Таким чином, вводяться такі типи прихованих каналів:

— VBSC – параметричний просторовий канал;

— TBSC – просторовий канал подій;

— VBTC – параметричний часовий канал;

— TBTC – часовий канал подій.

У понятті параметричний просторовий канал немає нічого нового, це звичайні приховані канали пам'яті. Введення поняття просторових каналів подій проливає світло на можливість створення прихованого каналу по пам'яті непрямим чином, без необхідності контролю відправником значення об'єкта. Наприклад, відправнику не потрібно мати доступ на запис до об'єкту видимого простору отримувача. Часові канали подій за своєю суттю також не становлять нічого нового. Однак введення параметричних часових каналів (VBTC) дозволило описати новий клас каналів, який раніше не розглядався.

Таблиця 8.2

Класифікація прихованих каналів

Клас каналу	Механізм організації каналу
Value-based spatial channel (VBSC)	Відправник змінює значення об'єктів, за якими може спостерігати отримувач. На підставі цих значень отримувач має необхідну інформацію.
Transition-based spatial channel (TBSC)	Відправник визначає, які з об'єктів, що спостерігаються, будуть змінені. Отримувач має інформацію шляхом визначення наявності або відсутності факту модифікації об'єктів.
Value-based temporal channel (VBTC)	Відправник знає майбутнє значення об'єкта, що спостерігається, і може керувати моментами спостереження даного об'єкта отримувачем. З появою необхідного значення він дає можливість отримувачу здійснити спостереження. Отримувач має інформацію на підставі значень, що спостерігаються.
Transition-based temporal channel (TBTC)	Відправник може керувати порядком зміни об'єктів відносно спостережень, що здійснюються отримувачем. Отримувач має інформацію з порядку появи цих подій замість

	аналізу значень об'єктів.

Як відомо, визначення ємності прихованого каналу пов'язане з моделлю, якою описується цей канал. Різноманітність різних моделей веде до безлічі різних методів визначення ємностей. Наприклад, припускаючи, що деякі приховані канали є каналами стеганографічними, можна використовувати результати досліджень в області стеганографії. Однак, всі традиційні методи визначення ємності зазвичай розраховують її значення, виходячи з припущення, що канал синхронний або існують механізми, які можуть бути використані для синхронізації передачі.

У роботі представлений новий підхід до визначення ємності прихованого каналу. Припускаючи, що прихований канал фактично є синхронними, автори пропонують отримувати оцінку ємності з урахуванням «витрат» на організацію синхронної передачі. Ґрунтуючись на тому факті, що перешкоди та несинхронні операції з різних боків каналу можуть призводити як до втрати корисної інформації, так і до вставок помилкових символів, приховані канали подаються у вигляді *двійкових ID-каналів* (binary insertion-deletion channel) - каналів, які визначаються параметрами P_d, P_i, P_t, P_s - відповідно ймовірностями видалення (deletion), вставок (insertion), передачі (transmission) і заміщень (substitute).

Фізично, такий канал є двійковою чергою (FIFO), потрапляючи в яку з одного боку біти даних очікують своєї відправки з іншого. Щоразу при зверненні до каналу відбувається одна з наступних подій: з ймовірністю P_d черговий символ видаляється з черги; з ймовірністю P_i до черги додається додатковий біт; із ймовірністю P_t черговий біт передається, тобто приймається отримувачем; із ймовірністю P_s виникає помилка заміщення. На рис. 8.3 схематично подано граф переходів такого каналу.

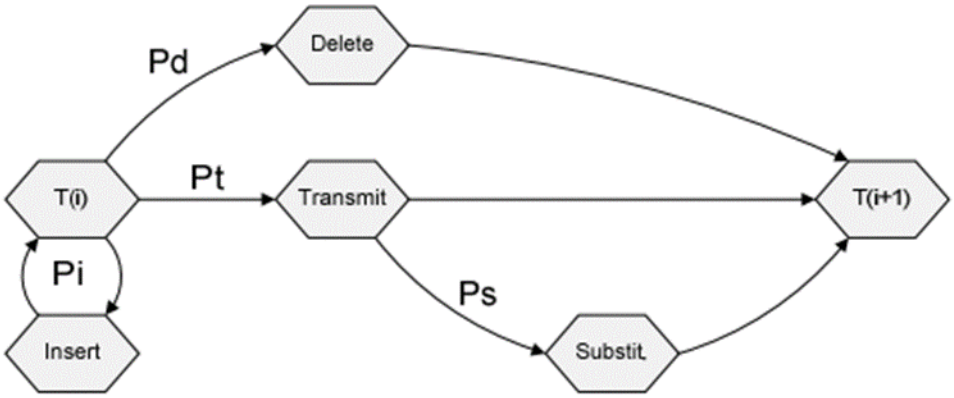


Рис. 8.3. Ілюстрація роботи двійкового ID-каналу

Такий підхід до моделювання прихованих каналів дозволяє визначити ємність каналу з більшою точністю, ніж раніше, оскільки представлена модель враховує необхідність синхронізації. На жаль, через складність моделі, а також її відносну новизну, точне значення ємності двійкових ID-каналів дотепер так і не отримано. Необхідно відзначити, що хоча такі канали досі повністю не вивчені, все ж таки існують методи організації надійної передачі даних.

Верхню межу ємності двійкового ID-каналу можна визначити як

$$C_{max} = N(1 - P_d),$$

де N – кількість бітів на символ, а P_d – ймовірність видалень.

У випадку, якщо синхронізація відправника та отримувача забезпечується за допомогою зворотного зв'язку, маршрут якого існує незалежно від прихованого каналу, верхня та нижня межі ємності будуть відповідно рівні

$$C_{\text{upper-bound}} = N(1 - P_d),$$

$$C_{\text{lower-bound}} = [(1 - P_d) / (1 - P_i)]\, C_{conv},$$

де $C_{conv} = N - \beta P_i \log_2(2^N - 1) - H(\beta P_i)$,

$\beta = 1 - (1/2^N)$,

$H(p) = - p \cdot \log_2 p - (1 - p) \log_2(1 - p)$.

Для ілюстрації асимптотичної збіжності верхньої та нижньої меж необхідно покласти рівними ймовірності P_i та P_d, а N спрямувати до нескінченності, тоді

$$C_{\text{lower-bound}} = C_{conv} \approx N(1 - P_d) - H(P_d),$$

$$\lim_{n \to \infty} (C_{\text{lower-bound}} - C_{\text{upper-bound}}) = [(N(1 - P_d) - H(P_d)) / (N(1 - P_d)] = 1.$$

Таким чином, можна відзначити, що організація передачі інформації за допомогою несинхронних каналів можлива, проте така взаємодія буде менш ефективною порівняно з синхронним обміном і може вимагати складної схеми кодування. Витрати на організацію синхронізації знижують ємність каналу, причому верхня межа ємності пропорційна ймовірності видалень P_d.

8.2.4. Потайні та побічні канали

На практиці приховані канали трактуються ширше, ніж у теорії. Розширення відбувається за чотирма напрямками:

- розглядаються системи з довільною дисципліною керування доступом (а не лише з багаторівневою безпековою політикою);
- розглядаються не лише нестандартні канали передачі інформації, а й нестандартні способи передачі інформації легальними каналами (потайні канали);
- розглядаються загрози не лише конфіденційності, а й цілісності інформації;
- розглядаються як односпрямовані, а й двоспрямовані канали.

Насправді приховані канали найчастіше виникають через можливість доступу до даних декількома способами. Наприклад, якщо в кореневому каталозі файлової системи розташовується TFTP-сервер, він дозволить отримати всім користувачам доступ до всіх файлів, незалежно від встановлених прав доступу. Очевидно, кількість подібних прикладів можна множити до безкінечності.

Нестандартні способи передачі інформації легальними каналами отримали назву *потайних каналів* (subliminal channels). Потайні канали використовують тоді, коли є легальний комунікаційний канал, але щось (наприклад, політика безпеки) забороняє передавати певну інформацію. Потайні канали лежать в основі більшості методів сучасної стеганографії та клептографії.

Між прихованими та потаємними каналами є дві важливі відмінності. *По-перше*, всупереч назві ніхто не намагається приховати існування прихованих каналів, просто для передачі інформації використовують сутності, які з самого спочатку для цього не були призначені, я створені для інших цілей. Навпаки, потайний канал існує тільки доти, доки про нього не дізнався супротивник. *По-друге*, вважається, що час передачі інформації прихованим каналом не обмежений. На противагу цьому, час передачі по потайному каналу визначається характеристиками обгортаючого каналу. Наприклад, якщо для таємної передачі інформації застосовується графічний образ, то можна передати тільки те, що вдається помістити в цей образ, не порушуючи скритності.

У цілому, потайні канали набагато практичніше, ніж приховані, оскільки у них є легальна основа – обгортаючий канал. *Потайні (а не приховані) канали - найбільш підходящий засіб для управління ворожою системою*. Але їх потребують не тільки зловмисники. Потайні канали можуть ефективно використовуватися постачальниками інформаційного контенту, які вбудовують у нього приховані «цифрові водяні знаки» і можуть контролювати його розповсюдження та дотримання споживачами цифрових прав.

Зрозуміло, що якщо не формалізувати структуру даних, що передаються програмами по легальним каналам, останні завжди можна використовувати для прихованої передачі інформації.

Класичним прикладом є застосування потайного каналу прем'єр-міністром Великобританії Маргарет Тетчер, яка, щоб з'ясувати, хто з її міністрів винен у витоках інформації, роздала їм варіанти одного документа з різними

проміжками між словами. За документом, що надійшов до друку, однозначно визначався власник цього екземпляра.

Побічні канали (side channel) вважаються окремим випадком прихованих каналів. У ролі передавачів у подібних каналах мимоволі виступають штатні компоненти інформаційних систем, а у ролі приймачів – зовнішні спостерігачі, які застосовують відповідне устаткування. Найчастіше за допомогою побічних каналів вимірюється час видимих операцій (для здійснення часових атак на двоключові криптоалгоритми), їх енергоспоживання та/або побічні електромагнітні випромінювання та наведення. Докладніше про побічні канали можна дізнатися у роботах.

8.2.5. Приховані канали у системах обробки інформації

Як було зазначено, необхідною і достатньою умовою організації прихованого каналу взаємодії двох суб'єктів є можливість відправнику проводити зміни у видимому просторі отримувача. У такому разі кажуть, що існує прихований канал від відправника до отримувача.

У загальному випадку організацію прихованого каналу у системі обробки інформації можна уявити як послідовність взаємодії суб'єктів на різних логічних рівнях. Враховуючи той факт, що склад сучасних систем обробки інформації досить одноманітний, можна умовно виділити два рівні абстракції, які здатні забезпечити приховану взаємодію: локальний та мережевий.

На першому, локальному рівні, розглядається взаємодія суб'єктів, що відбувається в рамках однієї робочої станції. У якості суб'єктів тут зазвичай виступають різні системні процеси. Метою організації прихованого каналу на даному рівні є забезпечення взаємодії між процесами в обхід чинних безпекових політик, контрольованих системами розмежування доступу.

Другий, мережевий рівень, має на увазі взаємодію суб'єктів, представлених як вузли одного або різних сегментів мережі. Суб'єктами цього рівня можуть бути робочі місця користувачів, різні мережеві сервери тощо. Організація

прихованого каналу у даному випадку передбачає організацію прихованої мережевої взаємодії в обхід існуючих засобів мережевого контролю (міжмережевих екранів, систем аналізу трафіку та інших.).

Розглядаючи локальні приховані канали, необхідно мати уявлення про засоби забезпечення захисту на локальному рівні. В даний час існує неправильне припущення про те, що адекватний ступінь захисту може бути досягнутий на прикладному рівні (за допомогою додатків) спільно з механізмами захисту, що існують в основних сучасних операційних системах. Як би там не було, основою захисту ресурсів є механізми контролю доступу, що забезпечують розмежування доступу суб'єктів до інформаційних та технічних ресурсів, що захищаються, — об'єктів.

Існує безліч моделей, які забезпечують керування доступом. Загальним підходом всім таких моделей є поділ множини сутностей, з яких складається система, на множини об'єктів і суб'єктів. Безпека обробки інформації забезпечується шляхом вирішення завдання управління доступом суб'єктів до об'єктів відповідно до заданого набору правил та обмежень, що утворюють безпекову політику. Можна виділити три основні моделі керування доступом до об'єктів: *мандатну*, *дискреційну* та *рольову*.

Ці моделі є основою більшості існуючих систем контролю доступу (rwx-UNIX, SELinux, SMACK, AppArmor, RSBAC, grsecurity тощо). Кожна з таких систем відповідно до реалізованої моделі повністю вирішує завдання розмежування доступу між суб'єктами та об'єктами. Відмінності між ними полягають лише в деяких аспектах, що стосуються ідеології побудови системи та складності адміністрування. Таким чином можна стверджувати, що в рамках сучасних інформаційних систем повністю вирішено завдання розмежування доступу.

З іншого боку, будь-яка система побудована на основі певної моделі взаємодії. І враховуються в ній лише ті суб'єкти та об'єкти, які передбачені

реалізованою моделлю. Очевидно, що не існує моделей, що повністю відповідають реальності. Тому можна стверджувати наявність таких сутностей, взаємодія між якими не контролюватиметься системою контролю доступу. Наприклад, у моделях розмежування доступу немає поняття часу, що дозволяє використовувати часові послідовності різних подій як кодові послідовності. Завданням побудови прихованого каналу у даному випадку є пошук таких сутностей і організація взаємодії між ними.

Використання загальних ресурсів для організації прихованих каналів є основним напрямом розвитку даної предметної області. Наявність загальних ресурсів означає те, що суб'єкти мають можливість організувати взаємодію. У сучасних системах обробки інформації у якості загальних системних ресурсів на локальному рівні виступають апаратне та програмне забезпечення.

Дійсно, апаратне забезпечення конкретного комп'ютера є загальним ресурсом для встановленого ПЗ. Програмне забезпечення, у свою чергу, також може бути спільним ресурсом для користувачів, що працюють в системі (наприклад, ядро ОС). Найважливішою функцією операційної системи є організація раціонального використання апаратних та програмних ресурсів інформаційної системи. Знання механізмів управління ресурсами, реалізованими в операційних системах, дозволяє проводити порівняльний аналіз та оцінку їх характеристик.

Працюючи у системі, кожен користувач представлений відповідним процесом (процесами). Процес - частина операційної системи, що функціонує під керуванням апаратного забезпечення. Функціонально операційну систему можна вважати складним недетермінованим кінцевим автоматом, майбутнє стан якого залежить від поточного стану і вхідних даних - дій користувача і реакцій на різні апаратні винятки.

Таким чином, майбутній внутрішній стан операційної системи залежить у тому числі від поточних дій користувача (тобто якогось процесу). Маючи

здатність отримувати необхідну інформацію про поточний внутрішній стан операційної системи, зловмисник може використовувати таку можливість для побудови прихованого каналу. Те саме можна припустити щодо апаратного забезпечення.

Таким чином, можна виділити такі базові механізми організації прихованих локальних каналів:

- використання загальних апаратних ресурсів;
- використання загальних програмних ресурсів.

В основі мережевих прихованих каналів лежить прихована мережна взаємодія суб'єктів. Приховані мережеві канали дозволяють обходити різні мережеві системи контролю доступу, моніторингу і збору статистики, так як подібні системи часто не можуть оцінити внутрішню природу потоків даних, що проходять через них.

Більшість мережевих прихованих каналів базуються на концепції тунелювання. Це механізм, що дозволяє інкапсулювати один протокол усередині іншого. Таким чином, довільні дані можуть передаватися усередині авторизованих потоків даних. Однак такий метод організації мережевих прихованих каналів є найпоширенішим, але не єдиним.

Так як в основі сучасних обчислювальних мереж лежить технологія комутації пакетів, використання пакетної мережі даних для організації прихованих каналів накладає очевидні обмеження. Тому інструментарій суб'єктів, які намагаються налагодити приховану взаємодію, включає засоби маніпулювання пакетами даних, а саме:

- можливість керування вмістом пакетів;
- можливість управління статистичними характеристиками інформаційного потоку (частота проходження пакетів, розподіл довжин пакетів тощо).

У разі керування вмістом пакетів даних самі пакети виступають у ролі контейнерів. Передача даних є впровадження додаткової інформації у певні

місця пакетів, спотворюючи певним чином їх. Але зазвичай ці спотворення не впливають на передачу вихідних даних. По суті цей спосіб є аналогом *цифрової стеганографії*. Впровадження додаткової інформації в пакети даних найчастіше можливе завдяки існуванню невизначеності в описах мережевих протоколів, а також наявності надмірності.

Управління статистичними характеристиками інформаційного потоку дозволяє організовувати приховану передачу даних у вигляді впливу на різні властивості потоку даних. Передача даних у такому випадку є процес організації певних впливів з одного боку та їх детектування з іншого.

При передачі даних по прихованому мережевому каналу може бути використаний існуючий інформаційний потік. У разі, якщо прихована передача не пов'язана з генерацією трафіку, такий канал називають пасивним. Якщо ж у процесі передачі даних відбувається генерація трафіку, такий канал буде активним.

Запитання для самоконтролю

1. Клептографія, що це?
2. Методи пошуку у клептографії.
3. Історія клептографії.
4. Характеристики прихованих каналів.
5. Потайні канали, їх особливості.
6. Побічні канали, їх особливості.
7. Особливості прихованих каналів у системі.
8. Як працюють приховані канали?

РОЗДІЛ 9. АТАКИ ЗА ПОБІЧНИМИ КАНАЛАМИ

9.1. Класифікація побічних каналів

При аналізі безпеки криптопроцесорів корисно здійснювати систематичний огляд предмету атак – сукупності фізичних, електричних та логічних інтерфейсів, які можуть піддаватися впливу потенційного супротивника, тобто способу його можливого доступу до криптомодуля. Також системно важливими є такі фактори, як можливість контролю над обчислювальним

процесом в криптомодулі та методи аналізу отриманих даних побічного каналу, що можуть бути застосовані.

9.1.1. Спосіб доступу до системи

Залежно від рівня доступу (фізичний, електричний або логічний рівень інтерфейсів, що доступні для криптоаналітика) до апаратного модуля можна виділити чотири класи атак:

Агресивні (Invasive) атаки пов'язані з безпосереднім електромонтажним доступом до внутрішніх компонентів криптопроцесора. Наприклад, зловмисник може розкрити корпус і зробити отвір в пасивації (захисному шарі) чипу мікроконтролера і помістити голку мікрозонду на шину даних з метою захоплення сигналу. Таким чином можливо отримати ключ шифрування і, навіть, відновити невідомий алгоритм шифрування.

До **напівагресивних** (Semi-invasive) відносяться атаки, які забезпечують доступ до пристрою, але без пошкодження пасивації чипу або встановлення безпосереднього електричного контакту, а тільки за допомогою легального інтерфейсу. Наприклад, зловмисник може використовувати лазерний промінь для іонізації відповідного транзистора і, таким чином, змінити стан тригера, який визначає в пристрої режим «захист пам'яті від читання».

Можливо, найбільш потужною технологією в цієї області нападу є диференційний електромагнітний аналіз (Differential Electromagnetic Analysis – DEA). Він ґрунтується на використанні крихітної котушки або іншого магнітного датчика, який може позиціонуватися з великою точністю в будь-якій точці безпосередньо на поверхні чипу. В результаті зловмисник може аналізувати не тільки сумарну потужність електроспоживання, яка є складовою потужністю, струмів споживаних усіма ланцюгами чипу, але і зміни локальної потужності струму, який споживається деякими цільовими ланцюгами чипу. Це може давати значно більше інформації.

Локальні неагресивні (Local non-invasiv) атаки полягають у безпосередньому спостереженні або маніпулюванні процесом виконання пристроєм операцій. Першим представником цього класу є атаки по часу, так звані локальні таймінг-атаки. Такі операції як обчислення цифрового підпису включає в себе безліч модульних множень і час, витрачений на виконання операції, сильно залежить від вхідних значень. При відповідному аналізі, час, що витрачається криптопроцесором для виконання таких операцій, видає значення відповідних елементів його закритого ключа.

Іншим прикладом є атаки з аналізу споживаної потужності: з високою точністю вимірюється струм, споживаний процесором, і співвідноситься це з тими обчисленнями, які виконує пристрій над значеннями криптографічного ключа, для того, щоб вгадати ці значення.

Дистанційні (Remote) атаки полягають в спостереженні або маніпуляції вхідними та вихідними даними пристрою. Прикладами є атаки з аналізу часу виконання (якщо виконуються дистанційно), криптоаналіз, аналіз протоколів і атаки на інтерфейси прикладного програмування.

Слід зауважити, що криптомодулі зазвичай обладнуються захисними механізмами, які захищають від НСД (агресивних атак). Неагресивні ж атаки помітити і запобігти практично неможливо. Неагресивні атаки також більш вигідні з економічної точки зору: вони, звичайно, не потребують дорогого обладнання.

9.1.2. Контроль над обчислювальним процесом

Кожна з цих атак може також бути активною або пасивною. В ході останньої зловмисник працює з пристроєм так, як це робить легальний користувач, в той час як в ході активної атаки зловмисник може маніпулювати пристроєм, його входами або його оточенням таким чином, щоб викликати відхилення в роботі.

Залежно від ступеня впливу на обчислювальний процес кожна з цих атак може також бути активною або пасивною.

В ході пасивної атаки атакуючий працює з пристроєм, як це робить легальний користувач, але таким чином, щоб отримати необхідну інформацію без помітного впливу на криптомодуль, який при цьому продовжує функціонувати у штатному режимі.

Під час активної атаки атакуючий може маніпулювати криптомодулем, його входами або його оточенням таким чином, щоб викликати відхилення в роботі. Така зміна може бути і непомітною для криптомодуля, але криптоаналітик в змозі виявити і використати інформацію щодо змін роботи.

Слід відзначити, що відмінність між активними і пасивними атаками більше лежить в площині внутрішньої природи атаки, ніж в реалізації фізичного втручання:

- активна агресивна атака може включати ін'єкцію сигналів в пристрій фізично, використовуючи відповідні зонди;

– в ході активної напівагресивної атаки може використовуватися лазерний або сильний електромагнітний імпульс, щоб викликати неадекватну поведінку деяких внутрішніх компонентів чипу;
– активна локальна неагресивна атака може виконуватися шляхом маніпуляції напругою електроживлення або тактовою частотою, щоб викликати часткову відмову пристрою, що тестується;
– при реалізації активної віддаленої неагресивної атаки зловмисник може надавати криптопроцесору ретельно підібрані послідовності даних для того, щоб викликати поведінку, яке не була передбачена розробником пристрою.

9.1.3. Застосовані методи аналізу

Залежно від методів, використаних в процесі аналізу оцифрованих даних, SCA-атаки можна розділити на **прості** (Simple side channel attack, надалі – SSCA) і **диференційні** атаки (Differential side channel attack, надалі – DSCA).

У **SSCA** атаці використовується інформація побічного каналу, яка, в основному, залежить від операцій, що виконується пристроєм. Звичайно, в SSCA аналізі використовується одне трасування і припускається, що секретний ключ може бути безпосередньо вилучений з інформації трасування. Очевидно, що інформація побічного каналу, яка пов'язана з «корисними» інструкціями (сигналом) повинна бути більше, ніж інформація побічного каналу, пов'язана з «непотрібними» командами (шумом). SSCA експлуатує взаємозв'язок між інструкціями, що виконуються, та інформацією побічного каналу.

З іншого боку, коли використання SSCA не представляється можливим через занадто велику кількість шуму в вимірах, застосовується **DSCA**. Звичайно, в DSCA аналізі використовується багато трасувань і застосовуються статистичні методи для обчислення можливих секретних ключів. З огляду на це можна стверджувати, що DSCA є більш потужною, ніж SSCA.

Диференційні атаки за побічними каналами експлуатують кореляцію між даними та миттєвим витоком з криптографічного пристрої по побічному каналу. Оскільки ця кореляція, як правило, дуже мала, повинні бути використані статистичні методи, щоб її ефективно експлуатувати. У DSCA-атаці атакуючий використовує гіпотетичну модель пристрою, що атакується. Якість цієї моделі залежить від можливостей атакуючого.

Гіпотетична модель (рис. 9.1) використовується для прогнозування вихідної інформації з побічного каналу пристрою; такою вихідною інформацією можуть бути декілька величин. Це можуть бути як величини, що описують один тип витоку інформації протягом декількох часових інтервалів, або це можуть

бути величини, що прогнозують виток з різних побічних каналів. У разі, якщо тільки одна єдина вихідна величина використовується для атаки, – ця атака називається атакою першого роду. Якщо дві або більше вихідні величини з одного і того ж бокового каналу використовуються для атаки, то вона називається атакою другого порядку і атакою вищого порядку, відповідно.

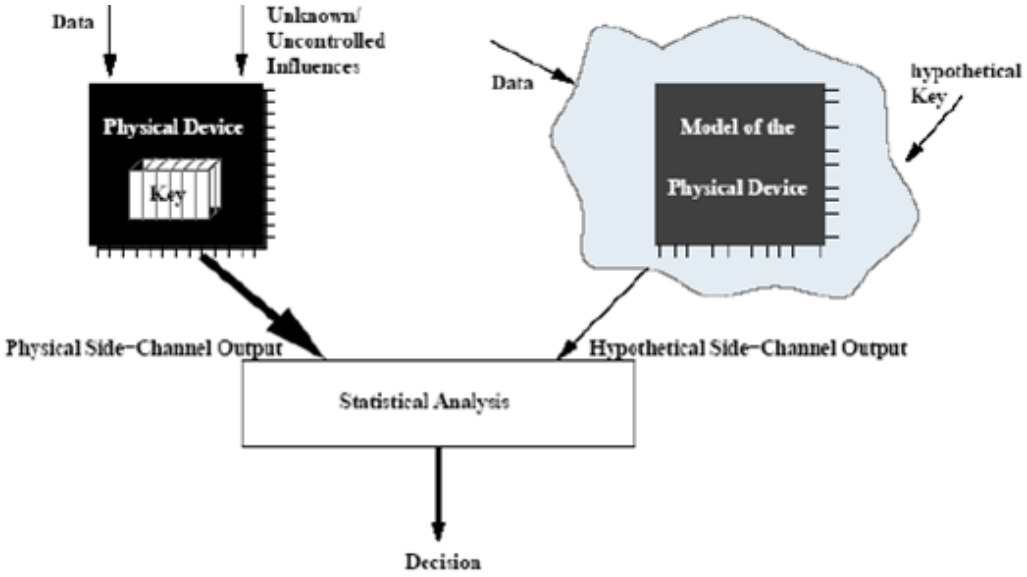


Рис 9.1. Загальна ідея DSCA

9.2. Атаки за часом виконання операцій

Атака за часом (Timing attack) – перша з широко відомих атак за побічними каналами, запропонована Полом Кохером в 1996 році і застосована на практиці проти алгоритму RSA в 1998 році. Атака заснована на припущенні, що різні операції виконуються в пристрої за різний час, в залежності від вхідних даних. Таким чином, вимірюючи час обчислень і проводячи статистичний аналіз даних, можна отримати повну інформацію про секретний ключ.

Виділяються декілька ступенів вразливості алгоритмів стосовно даного типу атак:

• Атака неможлива на алгоритми, операції яких виконуються за однакове число тактів на всіх платформах: інвертування, зсув і інші бітові операції над фіксованим числом біт.

• Можлива атака на алгоритми, що використовують додавання і віднімання.

• Особливо схильні до атак за часом алгоритми, що використовують множення, ділення, піднесення до степеня і бітові операції над довільним числом біт.

Атаки за часом також можуть застосовуватися віддалено. Так, наприклад, відомі атаки по мережі на сервер, де використовуються OpenSSL.

З поширених алгоритмів до атаки за часом вразливі DES, AES, IDEA, RC5.

9.2.1. Причина вразливості в алгоритмі зведення у ступінь

Піднесення до степеня за модулем в публічній криптографії часто реалізується за допомогою наступного псевдокоду.

Алгоритм 1. Піднесення до степеня за модулем

Обчислюється $M^{Secret\ Key} \bmod N$:

```
Result = 1

for ( every bit of the secret key- from right to left )

{

    if ( the secret key bit = '1' )

        Result = Result * M % N

    M = M * M % N;

}

return Result
```

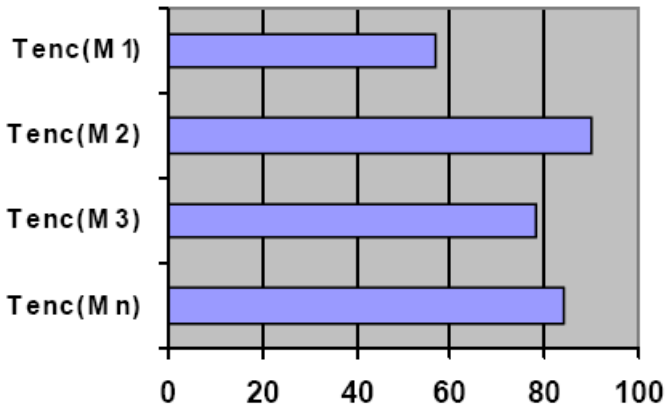
де M – це повідомлення, яке шифрується/розшифровується, а N – це модуль.

Виділена інструкція «***Result = Result*M%N***» в алгоритмі 1 виконується тільки тоді, коли біт секретного ключа дорівнює '1'. Отже час виконання залежить не тільки від повідомлення (всі обчислення містять *M*), але також від секретного ключа.

Математично це записується так:

$$\text{Time} = f(\text{SecretKey}, M).$$

Атака по часу реалізується в тому випадку, коли зловмисник може отримати серію повідомлень і відповідні їм часи шифрування, тоді він буде мати можливість відновити секретний ключ. Для цього зловмисник повинен мати можливість точного таймінгу процесу модульного піднесення до степеня на рівні біт. На рис. 9.2 показано, що зловмисникові повинно бути відомо.



Час шифрування

$T_{enc}(M_i)$ = Час шифрування/розшифрування повідомлення № i

Рис. 9.2. Приклади шифрування повідомлень

Об'єднання всіх часів шифрування повідомлень дає розподіл, для якого може бути отримана оцінка стандартного відхилення. Якщо часи шифрування для повідомлень дещо схожі, то стандартне відхилення буде менше, ніж коли часи шифрування дещо різні. На рис. 9.3 показаний типовий профіль розподілу.

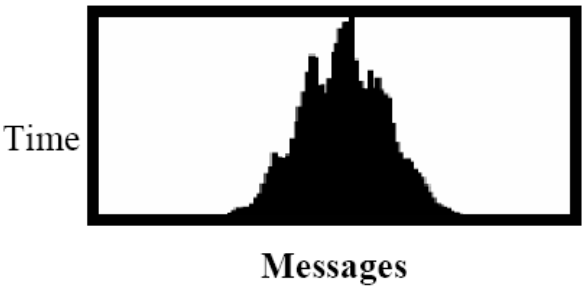


Рис. 9.3. Приклад розподілу часу для набору повідомлень

Атака по часу експлуатує таку вразливість: час обробки для модульного піднесення до степені різних повідомлень є змінний і в такому випадку дисперсія частково залежить від значень біт секретного ключа. Ретельні вимірювання зловмисником часу шифрування/розшифрування повідомлень можуть привести до витоку вмісту ключа.

9.2.2. Алгоритм проведення атаки

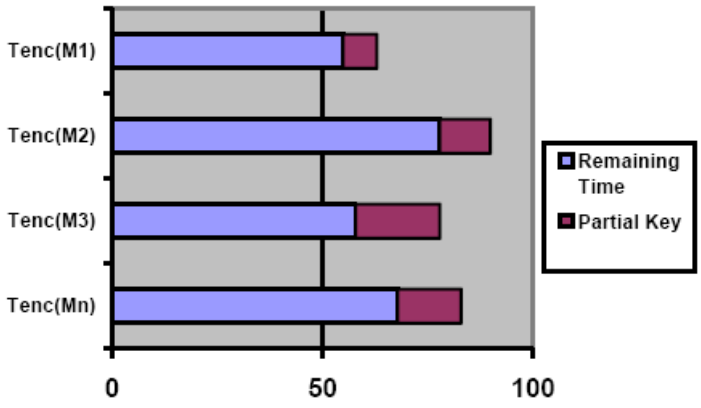
Атака починається з першого біту ключа. Наприклад, справа-наліво, тобто першим бітом буде найменш значущий біт ключа. Використовуються два комплекти вимірювань: в першому комплекті буде вимірюватися, скільки часу потрібно, щоб зашифрувати кожне повідомлення на окремому біті ключа '0', а в іншому комплекті буде вимірюватися, скільки часу потрібно, щоб зашифрувати

кожне повідомлення на окремому біті ключа '1'. Ці два набори вимірювань часу потім віднімаються з відомих загальних часів шифрування для отримання двох різних розподілів. Один розподіл відображає загальний час мінус час для окремого біту ключа '0', інший розподіл відображає загальний час мінус час для окремого біту ключа '1'. З причин, які будуть розглянуті пізніше, розподіл, що має найменше стандартне відхилення, швидше за все, буде відповідати правильному значенню для біту ключа.

Атака продовжується по 2-му біту. З огляду на припущення для першого біту (припустимо, це '1'), обчислюється інший набір часів для варіантів 2-го біту 0/1, щоб вгадати другий біт. Ці часи додаються до часу попереднього припущення для двох таймінгів: один таймінг для "01" і інший таймінг для "11" (при руху з праворуч на ліворуч). Ці 2-бітові розподіли віднімаються з відомих повних часів шифрування. Знову розглядаються два розподіли: один розподіл загального часу мінус значення для "01" перших двох біт, а інший розподіл загального часу мінус значення для "11" перших двох біт. Розподіл з найменшим стандартним відхиленням обирається в якості найбільш ймовірного кандидата, відповідного першим двом бітам.

Атака триває по 3-му біту. З огляду на припущення для перших двох біт (припустимо, що це "01"), обчислюється третій набір часів для варіантів 3-го біту 0/1: знаходяться часи для "001" і "101". Ці 3-бітові розподіли віднімаються з відомих повних часів шифрування. Як і в попередніх раундах, розподіл з найменшим стандартним відхиленням вибирається в якості найбільш ймовірного кандидата.

Далі атака проводиться по всіх позиціях біт ключа.



$T_{enc}(M_i)$ – час шифрування повідомлення №i після віднімання часу обробки вгаданих біт

Рис. 9.4. Відображення процесу атаки

На наведеному вище рисунку показаний процес атаки. Права частина діаграми часу обробки кожного повідомлення є розрахунковий час обробки вгаданої частини ключа (для перших 1,2,3, .. біт). Зафарбована синім ліва частина діаграми часу обробки кожного повідомлення – це кількість часу, який залишився після видалення часу обробки вгаданої частини ключа. Цей час для кожного повідомлення, що залишився, використовується для обчислення стандартного відхилення розподілу часів. Якщо віднімання часу для припущення чергового біту ключа '0' дає менше стандартне відхилення, ніж при припущенні цього біту ключа '1', то біт "0" покладається значенням даного біту ключа, і навпаки.

9.2.3. Як алгоритм атаки працює

Час, необхідний для шифрування повідомлення можна розглядати як послідовність випадкових величин. Кожна випадкова величина являє собою інтервал часу, необхідний для шифрування повідомлення з залученням певного біту ключа.

$$X_0 + X_1 + X_2 + \dots X_n$$

n – число біт ключа,

X_i *– випадковий час, необхідний для шифрування на і-му біті ключа.*

Якщо значення біта, відповідного X_n вгадано правильно, і час обчислення – X_n для кожного повідомлення точно відомий, то час шифрування кожного повідомлення зменшується на час X_n. Насправді одна з випадкових величин, які використовуються для отримання загального часу, видаляється. Новий розподіл після вирахування правильного припущення є результатом суми (n-1) випадкових величин.

$$X_0 + X_1 + X_2 + \dots X_{n\text{-}1}$$

З іншого боку, якщо X_n вгадано неправильно, час шифрування кожного повідомлення зменшується на незалежну (некорельовану) випадкову величину (X_z). Новий розподіл є тоді сумою (n+1) випадкових величин.

$$X_0 + X_1 + X_2 + \dots X_n - X_z$$

Теоретична основа атаки полягає в тому, що правильне вгадування з більшою ймовірністю призводить до меншої дисперсії, ніж неправильне

припущення, тому що розподіл суми меншого числа випадкових величин з більшою ймовірністю має меншу дисперсію, ніж розподіл суми більшої кількості випадкових величин.

9.2.4. Приклад моделювання атаки за часом на комп'ютері

Головною проблемою при моделюванні є розрахунок часу виконання операцій, оскільки на ПК він не дуже точний. Перемикання задач операційною системою, свопи віртуальної пам'яті та різний час доступу до диску ускладнюють точний таймінг виконання. Тому для моделювання атаки по часу розроблено сценарій «Середовища ідеального таймінгу» за допомогою написання спеціальної процедури модульного піднесення до степеня при виконанні шифрування.

Процедура повертає однакові характеристики часу виконання незалежно від того, скільки разів ця атака була запущена. Ця процедура сама вираховує час виконання операцій (в умовних одиницях) за наступною схемою (див. Алгоритм 2):

Бітовий зсув виконується за 1 одиницю часу;

Додавання – за 1 одиницю часу;

Множення – за 1 одиницю часу;

Модульна операція – за 1 одиницю часу.

Algorithm 2. Псевдокод модульної процедури піднесення до степеня в «Середовищі ідеального таймінгу».

```
int MyModExp( Key, Message, Modulus)
{
  TimeSlots = 0;
  z = 1;
  for (each bit of the key )
  {
        if( the key bit value = '1' )
        {
              determine time for modular multiplication routine
              MultTime = MyMult(z, Message)
              Add time for multiplication and modulation routine to Timeslots
              TimeSlots += MultTime + 1;
        }
```

```
        Message = Message * Message % Modulus;
        increase time for above multiplication and mod operations
        TimeSlots += 2
  }
  return TimeSlots
}

int MyMult ( Mult1, Mult2)
{
  answer = 0
  MultTime = 0;
  while (Mult1 != 0)
  {
        if (Mult1 & 1 )
        {
              answer += Mult1;
              increase time for above addition
              MultTime++
        }
        Mult2 = Mult2<< 1;
        Mult1 = Mult12 >> 1;
        increase time for above shifts
        MultTime += 2;
  }
  return MultTime;
}
```

В результаті ця процедура має передбачуваний механізм часу виконання модульного піднесення до степеня в умовних одиницях часу.

Класична атака часу атакує ключ біт за бітом по черзі. Однак атаку можна здійснити будь-якими кроками розміром по 2^n біт (2,4,8,16 ...). При перебиранні ключа групами по k біт, в кожній ітерації потрібно проводити більше тестів і виправлення невірної здогадки є більш складним з точки зору обчислень, але вірно вгадані k біт ключа дають більш стабільну статистику. В розглянутому прикладі використовується значення приросту ключа k=4 біти.

Виконувалось шифрування 10 000 повідомлень (кожне повідомлення 16 біт завдовжки) з використанням 16-бітного ключа «859A» та тестуванням одного шістнадцяткового символу (4-х біт) одночасно в умовах «ідеального таймінгу». Результати представлені як пара чисел. Ліве число – це шістнадцяткове

значення шаблону біт, а праві числа – це упорядковані значення стандартних відхилень (у десятковому вигляді) розподілу часу, після відніманий часу, відповідного шаблону біт, від загального часу шифрування.

Ітерація 1: Перевіряються всі 16-ть комбінацій для найменш значущого шістнадцяткового символу та порівнюються стандартні відхилення:

A 9.667300
E 10.073498
B 10.428452
8 10.735512
2 10.807549
F 10.811693
C 10.917827
6 10.985436
9 11.416848
3 11.488290
D 11.593687
7 11.661000
4 11.880611
0 11.888783
5 12.499812
1 12.502725

"A" або "1010" має найнижче стандартне відхилення, тому припускається, що молодшим шістнадцятковим символом секретного ключа є "A".

Ітерація 2: Припускаючи, що 'A' є першим шістнадцятковим символом, перевіряються всі комбінації для 2-го шістнадцяткового символу і порівнюються стандартні відхилення:

9 7.047491
D 7.570274
B 7.791618
8 8.338350
1 8.505963
F 8.528599
C 8.644474
5 8.711277
A 8.748246
3 8.994066
E 9.279894

7 9.424113
0 9.667300
4 9.723608
2 9.897477
6 10.170431

"9" або "1001" має найнижче стандартне відхилення, тому припускається, що другим шістнадцятковим символом секретного ключа є "9".

Ітерація 3: Припускаючи, що '9A' є першими двома шістнадцятковими символами, перевіряються всі комбінації для 3-ого шістнадцяткового символу та порівнюються стандартні відхилення:

5 3.893773
D 5.336799
7 5.469493
1 5.564645
4 5.579840
9 6.332458
3 6.441206
6 6.470513
C 6.564324
F 6.786015
0 7.047491
B 7.310170
2 7.494667
E 7.525820
8 7.578764
A 8.170389

"5" або "0101" має найнижче стандартне відхилення, тому припускається, що 3-ім шістнадцятковим символом секретного ключа є "5".

Ітерація 4: Припускаючи, що '59A' є першими трьома шістнадцятковими символами, перевіряються всі комбінації для 4-го шістнадцяткового символу та порівнюються стандартні відхилення:

8 0.000000
9 3.893365
0 3.893773
A 3.896687
C 3.898579
4 5.109091

2 5.271112
1 5.386519
D 5.739522
B 5.861718
E 5.866206
5 6.522335
6 6.538750
3 6.756850
F 7.494855
7 7.950508

"8" або "1000" має найменше стандартне відхилення, тому припускається, що четвертим шістнадцятковим символом є "8".

Шістнадцятирозрядний ключ має 2^{16} або 65,536 можливих комбінацій. Це моделювання атаки по часу в умовах «ідеального таймінгу» визначило ключ на одному пробігу без помилок!!!

9.2.5. Передумови реалізації атаки за часом та її складність

Необхідними умовами для успішної реалізації атаки по часу є:

1) Здатність точно вимірювати загальний час перетворення;

2) Можливість отримання багатьох відкритих чи шифрованих повідомлень;

3) Детальні знання про HW/SW реалізацію перетворення;

4) Можливість вимірювати часові характеристики кожної ітерації;

5) Час перетворення повинен бути залежним від секретного ключа та повідомлення;

6) Криптографічний процес не повинен використовувати китайську теорему про лишки.

Наведений в параграфі 3.4 приклад моделювання атаки по часу створює враження легкості її реалізації. Але в реальних умовах неправильні припущення символів ключа є неминучими. Кількість раундів, необхідних для відновлення після неправильного вгадування символу, включає в себе всі тести, необхідні для повернення до точки атаки, де було зроблено некоректне припущення. Тобто необхідно вивчити всі можливі комбінації, починаючи з моменту виявлення помилки до точки некоректного припущення. Це є відомою дискретною математичною задачею з визначення числа вузлів у бінарному

дереві висоти h. Число вузлів такого дерева (проведених тестів) становить $(2^{h+1}-1)$. Ця формула безпосередньо впливає на складність атаки.

Зважаючи на вказану формулу і враховуючі, що висота дерева h залежить від *розподілу часу* виконання операцій піднесення до степеня і не залежить від довжини ключа, отримуємо, що складність атаки по часу є пропорційною довжині ключа.

Цей факт робить атаку серйозною загрозою. При використанні атаки грубої сили, число комбінації ключа, які необхідно тестувати, експоненційно збільшується завдяки довжині ключа. Атака по часу перетворює пошук ключа на процес тестування зі складністю, пропорційною довжині ключа. Це зниження ставить атаку в область можливого, з урахуванням обчислювальної потужності, доступної нападникам сьогодні.

Разом з тим, атака по часу не є тривіальною і нападнику дійсно потребується докладне знання про криптографічну реалізацію. Загальновизнано, що атака по часу не є серйозною загрозою від випадкового нападника. Однак обізнаний супротивник може витратити необхідні ресурси для здійснення атаки часу, якщо винагорода за таку атаку буде досить високою.

9.2.6. «Сліпий» захист від атаки за часом

Хорошим захистом від атаки часу є введення випадкового часового компонента до процесу криптографічних обчислень. Впровадження випадкового компонента робить інформацію про часові дані непридатними для використання нападником, оскільки випадкове число спотворює розрахунок часу виконання операцій. Використання рандомізованих значень для захисту відомий як «сліпий» захист.

Незахищене піднесення до степеня за модулем задається рівнянням

$$M = C^d \bmod N,$$

де M – повідомлення, C – шифртекст, d – секретний ключ, N – модуль.

При застосуванні сліпого захисту до рівняння додається рандомізована змінна R, така, що $R = R^{ed} \bmod N$, таким чином:

$$M = R^{-1}(C*R^e)^d \bmod N \text{ (blinded)}$$

При кожному дешифруванні результати є такими самими, як і у незахищеному рівнянні. Однак, з огляду на те, що R є випадковим, – час обробки також стає випадковим, і, отже, не буде витоку інформації про таймінг

операцій піднесення. Витрати продуктивності при застосуванні «сліпого» захисту складають від 2% до 10%.

Розробник модуля шифрування повинен визначитися, чи варті додаткової безпеки вказані витрати на такий захист.

9.3. Напівагресивні атаки

Між агресивними і неагресивними атаками лежить третій клас локальних атак, які називаються напівагресивними атаками. Ці атаки передбачають доступ до поверхні чипу, але не вимагають проникнення через пасивуючий шар або прямого електричного контакту з топологією чипу.

Перший напрямок напівагресивних атак пов'язаний з використанням ультрафіолетового світла для скидання біта захисту на мікроконтролерах, щоб можна було вичитати вміст пам'яті.

Одною з перших також було використання технології LIVA/LECIVA тестування напівпровідників, розробленої компанією Sandia. LECIVA (Low energy charge-induced voltage alteration) – технологія скануючої електронної мікроскопії, яка дає швидку локалізацію відкритих з'єднань. LIVA (Light-induced voltage change) – метод оптичної скануючої мікроскопії, який дає швидке виявлення пошкоджених напівпровідникових з'єднань і визначає стан транзисторної логіки. Використання цих технологій для підсвічування непроводящих КМОП транзисторів призводить до відчутного струму витоку, який може бути зареєстрованим на контактах мікросхеми, що тестується. Це надає можливість вичитування змісту комірок пам’яті, побудованої на транзисторних вентилях.

Перспективним напрямком є виконання атак за допомогою індукування несправностей, – відповідним чином влаштовані несправності (наприклад, імпульсами мікрохвильового випромінювання) можуть викликати необхідні порушення роботи криптографічних механізмів. Наприклад, можна видалити матеріал криптографічного ключа, послідовно встановлюючи біти ключа в 0. В конкретних системах часто можна обійти криптографію взагалі, наприклад, втручаючись в послідовність команд процесора таким чином, щоб криптографічні обчислення не виконувалися, або їх результати ігнорувалися. На практиці такі атаки виконувалися з використанням оптичних методів зондування для порушення захисту в цифрових схемах. Ідея полягає в тому, щоб висвітлюючи цільовий транзистор змінити його поведінку, тим самим викликаючи тимчасовий збій. Така атака може бути здійснена за допомогою простого, недорогого обладнання: наприклад шляхом установки фото- спалаху

на порт камери мікроскопа в станції ручного зондування. Використовуючи це, можливо встановлювати або скидати будь-який окремий біт ОЗП в мікроконтролері.

Набагато кращі результати можуть бути отримані з використанням лазерного зондуючого обладнання. На додаток до можливості заносити в комірки оперативної пам'яті потрібні значення, лазерне зондування може бути пристосоване для зчитування вмісту пам'яті, побудованої на інших технологіях, таких як Flash і EEPROM, а також щоб втручатися в логіку управління безпосередньо.

Крім виконання атак шляхом індукування збоїв, лазерне зондування може бути використано для пасивного читання з пам'яті. Тут хитрість полягає в тому, щоб одномоментно висвітлити комірку пам'яті на транзисторах. В результаті іонізація призводить до вимірюваного збільшення струму витоку, якщо транзистор вимкнений. Такі атаки не обов'язково вимагають дорогих лазерів і можуть бути здійснені за допомогою адаптованої лазерної указки.

Ще одним перспективним, але дорогим напрямком реалізації напівагресивних атак є застосування електронно-променевих тестерів (Electron Beam Prober – EBP).

Електронно-променевий тестер – це скануючий електронний мікроскоп (SEM) з функцією контролю контрастності електронного променя (сигналу тестування). Типові напруги прискорення і струми пучка для первинних електронів 2.5 kV і 5 nA. Число і енергія вторинних електронів є індикацією локального електричного поля на поверхні чипу, що дозволяє спостерігати сигнальні лінії (шини) чипу з субмікронною роздільною здатністю. Сигнал, що генерується під час тестування електронним променем, по суті, являє собою результат низькочастотної фільтрації струму пучка, помножений на функцію напруги сигналу на лінії плюс шум. ЕВТ можуть вимірювати зразки сигналів з пропускною здатністю кілька Ггц, але тільки періодичних сигналів, де можуть бути використані стробоскопічні методи і періодичне усереднення. Якщо використовувати контрастний режим в реальному часі, де промінь безперервно направляється в одну точку і записується сигнал від реєстрації зашумленого потоку вторинних електронів, то ширина смуги частот сигналу обмежується декількома мегагерцами. Хоча така пропускна здатність може бути просто достатньою для спостереження за однією сигнальною лінією смарт-картки з тактовою частотою 3,5 МГц, вона занадто мала, щоб спостерігати всю шину з частотою дискретизації кілька мегагерц для кожної лінії.

Програмне забезпечення EBP обробляє вказаний сигнал і таким чином виявляє відхилення напруги на шинах чипу і відображає їх як зображення різної контрастності (рис. 9.5). За допомогою цієї технології також можливо вичитувати інформацію з комірок пам'яті типу Flash ROM.

Електронно-променеві тестери дуже зручні інструменти атаки, якщо тактова частота процесора, що аналізується, може бути зменшена нижче 100 кГц, щоб в масштабі реального часу записувати все лінії шини або, якщо процесор може бути змушений генерувати періодичні сигнали, безперервно повторюючи ту ж саму операцію під час вимірювання.

Стандартний EBT має такі режими роботи:

• Стробоскопічний режим з усередненням – призначений для вимірювання періодичного сигналу зі смугою до декількох Ггц.

• Режим реального часу – здатний вимірювати довільні сигнали зі смугою в кілька Мгц.

• Одночасний контроль всіх сигналів чипу – при зниженні тактування процесора чипу до 100 кГц.

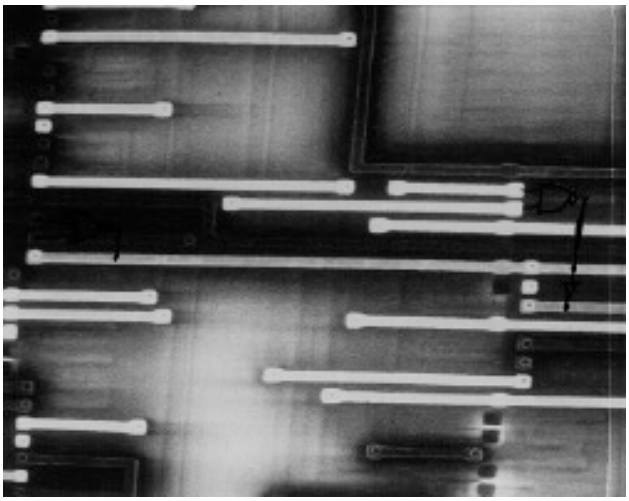


Рис. 9.5. Отримане на EBT зображення проходження сигналів по послідовній шині чипу (на зображенні – найбільша за довжиною)

9.3.1. Приклади атак з безпосереднього вичитування даних з пам’яті

Метою такої напівагресивної атаки є відновлення інформації з пам'яті смарт-карток та інших криптопроцесорів без використання легальних операцій читання, тобто шляхом обходу будь-яких елементів керування доступом і захисту від безпосереднього зчитування секретних даних.

Традиційний спосіб зчитування даних з пам'яті смарт-карток включає агресивну атаку за допомогою механічного зондування, як правило, шини процесора. Такі атаки пов'язані з фізичним вилученням чипу та зчитуванням його внутрішнього стану шляхом прямого електричного підключення до внутрішніх компонентів, використовуючи мікрозонди. Це стає все важче з ряду причин, починаючи від зменшення розмірів топології компонент чипу до використання схем керування доступом до пам'яті на чипі.

Останнім часом для цього використовуються напівагресивні атаки, в яких мікросхема декапсулюється, але не створюється прямого електричного контакту і пасивація чипу залишається незмінною. Приклади таких атак включають оптичне зондування, в якому лазер використовується для індукування тимчасових збоїв в одному або декількох транзисторах таким чином, щоб викликати виток інформації, і атаки вихровим струмом, в яких подібний ефект досягається шляхом розміщення невеликої котушки на поверхні мікросхеми та індукування потужного імпульсу магнітного поля.

Оптичне вичитування CMOS RAM

Структура типової комірки SRAM показана на рисунку 9.6. Два інвертори побудовані з пар p- і n-канальних транзисторів (T1 і T5; T2 і T6). Вихід першого інвертора підключений до входу другого, і навпаки ($\mathbf{x}$ і $\overline{\mathbf{x}}$). Два n-канальних транзистори використовуються для зчитування даних з комірки та запису даних в неї (T3 та T4). Доступ для читання комірки забезпечує підсилювач на основі диференційної структури (рис. 7.3).

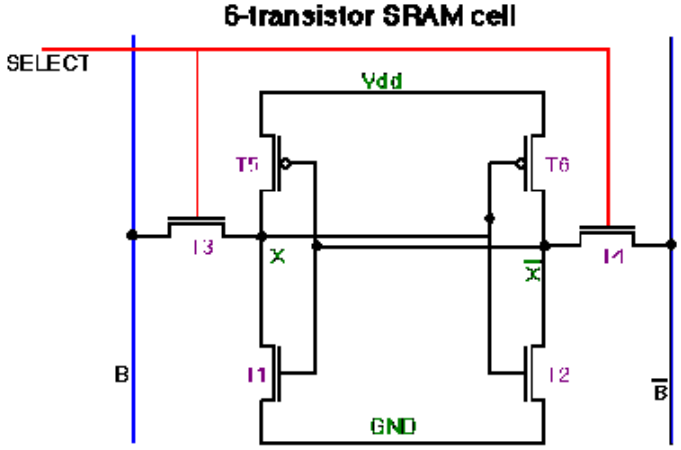


Рис. 9.6. Архітектура комірки SRAM

Для аналізу структури пам'яті SRAM використовувався червоний лазер, сфокусований на поверхні чипу за допомогою мікроскопа. Оскільки фотони з червоного лазера (довжина хвилі 650 нм) мають енергію, більшу ніж

заборонений проміжок зони кремнію, вони будуть іонізувати активні області усередині чипу. Якщо фотони досягають області біля p-n переходів, то буде продукуватися фотострум через фотоелектричний ефект. Коли фотони потраплять в область p- або n-каналу, це зменшить опір каналу внаслідок введення вільних носіїв. У кожному CMOS-інверторі є шість p-n переходів, а також два резистори, що відповідають n- і p-каналам.

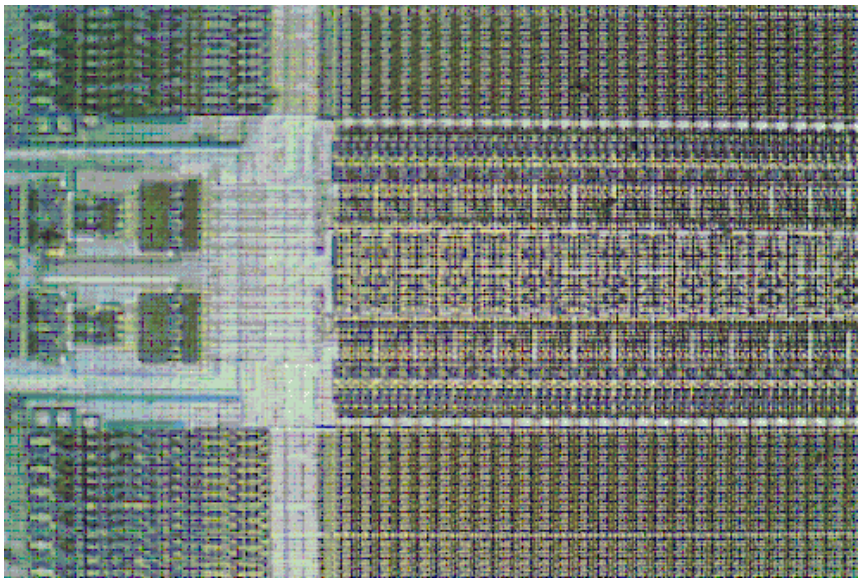


Рис. 9.7. Вигляд внутрішньої структура ОЗП (підсилювачі та комірки).

Прочитати стан комірки пам'яті дозволяє той факт, що зменшення опору помітно для замкнених каналів і майже незначне для відкритих каналів. Таким чином, шляхом націлювання лазерного променя на відповідний транзистор або транзистори, ми можемо розрізняти два можливих стани пам'яті. Аналогічна методика може бути використана для перемикання стану бітів пам'яті, але в цьому випадку необхідне використання лазера з більшою потужністю, у порівнянні з неруйнівним зчитуванням.

Прикладом застосування цієї методики є експеримент з побудови карти активних областей в мікроконтролері шляхом вимірювання фотоструму, індукованого лазерним скануванням поверхні чипу. Чип, на який не подане живлення, був встановлений на дослідницький стенд, що може рухатися в координатах X-Y з роздільною здатністю 0,1мкм. Результат сканування показано на рис. 9.8. Можна побачити активні області, оскільки вони виробляють більший струм. Але більша частина чипу покрита металевими шарами, крізь які лазерний промінь не може проникнути, тому ці ділянки не виробляють струму.

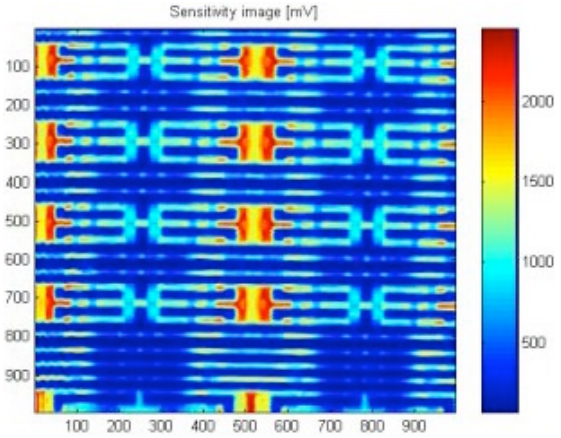


Рис. 9.8. Лазерне сканування пам'яті без подавання живлення

Наступний експеримент зроблений з чипом під напругою. Чип було запрограмовано таким чином, щоб завантажувати будь-які значення у його оперативну пам'ять, а потім зупиняти роботу чипу. Результат сканування комірок пам'яті, що завантажені випадковими даними, показаний на рис. 9.9. Видно, що комірки пам'яті мають різні стани: там, де в комірці є "1", верхня частина яскравіше, а де "0" – має меншу інтенсивність.

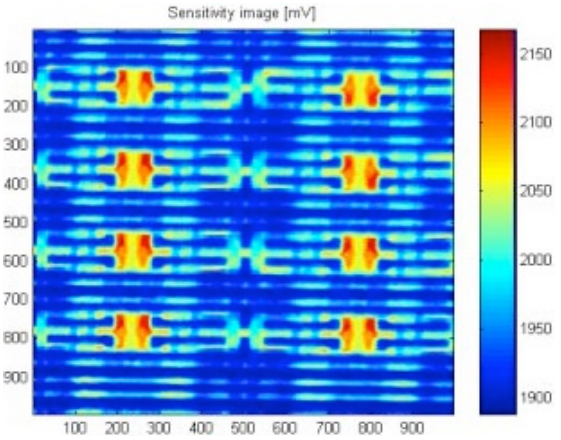


Рис. 9.9. Лазерне сканування пам'яті під напругою, у статичному стані

Таким чином встановлено, що шістнадцять біт, які розташовані у відсканованих комірках, мають значення, наведені в таблиці 9.1.

Таблиця 9.1

Отриманий вміст комірок памяті

1	1	0	0
1	1	1	0

1	1	1	1
1	1	1	1

Електромагнітна атака

Для сканування топології чипу мікросхеми може бути застосована електромагнітна індукція. Використовуючи спалах від фотокамери, мікрозондову голку та тонкий провід можливо реалізувати недорогу атаку, щоб визвати збої в криптографічному процесорі. Можна зробити мініатюрну індуктивність шляхом обгортання кількох сотень витків тонкого дроту навколо кінчика мікрозондової голки. При пропусканні електричного струму через цю котушку – створюється магнітне поле і голка концентрує лінії цього поля. Підключивши котушку до камери замість спалаху можна подавати на неї потужні імпульси струму. Якщо випробувальний зонд переміщувати на відстані кілька мікрон над поверхнею цільового процесора і подавати на зонд імпульси струму, тоді імпульсне магнітне поле створить імпульси вихрового струму у мікросхемі, які можна зареєструвати, щоб побудувати карту топології чипу (рис. 9.10).

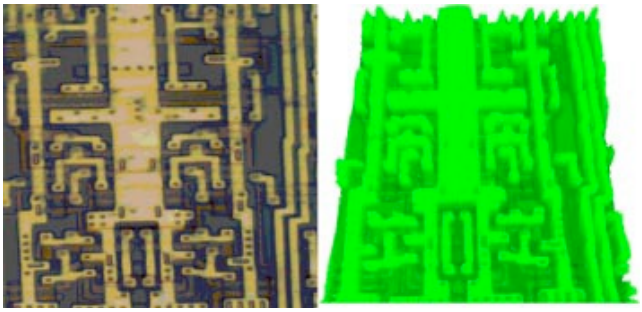


Рис. 9.10. Побудова карти топології чипу за допомогою техніки вихрового струму

Ця методика індукції збою також може бути використана для неруйнівного зчитування вмісту пам’яті. За допомогою такого ж зонду, який використовувався для сканування чипу, створюється невелике збурення в комірці пам'яті. Ідея становить у тому, щоб на дуже короткий час зміщувати точку поляризації транзисторів. Оскільки точки поляризації будуть повертатися до початкового стану з різними швидкостями для випадків, коли транзистор знаходиться у стані "0" або "1", – це може бути використане для встановлення дійсного стану транзистора. Наприклад, шляхом вимірювання часу повернення. На практиці виявилося, що відмінності часу недостатні для розрізнення станів пам'яті. Однак інтенсивність струму, необхідного для відновлення початкового

значення точки поляризації, помітно відрізнялася для випадків стану транзистора «0» і стану «1».

Безумовно, що з подібним недосконалим обладнанням досить важко створити достатній струм на чипі, не порушуючи вмісту будь-яких комірок пам'яті поряд. Проблема в тому, що підсилювачі читання-запису є досить чутливими, і навіть невелике перевищення граничного рівня струму призведе до скидання цілого рядка або стовпця пам’яті до фіксованого значення.

Проте з певним комплектом кращого обладнання, застосовуючи більш складну обробку сигналів, можна використовувати електромагнітну технологію, засновану на вимірюванні різниці струмів, для читання пам'яті статичної RAM та FLASH.

Заморожування та зондування

Описані вище методи прямого читання пам'яті є ефективними, але повільними. Вони є достатніми для зчитування даних з чипів, стан пам’яті яких у певний момент часу може бути зафіксований; проте, чипи смарт-карток, як правило, мають захист від зупинки тактування, наприклад, шляхом скидання схеми у неробочій стан.

У випадку статичної оперативної пам'яті можливо застосування заморожування для збереження цілісності даних після вимкнення живлення. Для цього можна використати, наприклад, охолоджувальний спрій або рідкий азот. Заморожений ОЗП зберігає свій вміст значно довше – від хвилин до годин. Цей метод придатний для підтримки даних у SRAM, щоб прочитати його вміст після виключення живлення. Після заморозки дані вичитуються за допомогою того чи іншого методу.

В цілому, якщо цінні дані присутні у відкритому вигляді хоча б під час одного циклу у місці пам'яті, який зловмисник може встановити і зможе заморозити його стан (фізично, використовуючи низьку температуру або іншим способом, наприклад, зупинити тактування) тоді цілком можливо для зловмисника прочитати ці дані за допомогою оптичних або електромагнітних методів зондування. Витрати на розробку та обладнання, що необхідні для проведення таких атак, значно нижчі, ніж ті, що необхідні для повномасштабних агресивних атак. Апаратні контрзаходи будуть необхідні для будь-яких процесорів, які повинні протистояти атакам на реалізацію криптографічних механізмів.

9.3.2. Технології захисту від напівагресивних атак

Механізми захисту включають в себе технології програмного захисту, щоб виявляти активні атаки і виконувати деяку відповідну тривожну функцію, таку як стирання ключового матеріалу. Непрозорі металізовані сітки та екрани також піднімають планку для зловмисників за витратами часу і вартості обладнання – зловмисник тепер може бути змушений діяти через тильну частину чипу, що, як правило, пов'язане із залученням обладнання іонного травлення для стоншення підкладки чипу та інфрачервоного лазера, щоб проникнути через кремнієву підкладку.

Жодна дешева технологія захисту не може захистити чип криптопроцесора від нападу. Існуючі високоефективні технології, такі як захисна металізація верхнього шару, шифрування шини даних і рандомізаційна криптографія, роблять атаки більш складними. Але витончений зловмисник може подолати захисну металізацію, використовуючи інфрачервоне опромінення з тильного боку або рентгенівські промені, в той час як шифрування шини даних можна обійти, атакуючи регістри безпосередньо.

Для захисту від оптичного вичитування пам’яті достатньо використовувати непрозору пасивацію чипу смарт-картки, але цього недостатньо для її захисту від електромагнітних атак. В останньому випадку потрібно мати безперервний металевий шар, хоча навіть це не блокує атаки на основі використання інфрачервоних лазерів через задню частину чипу або використання рентгенівських променів. Для реального захисту необхідні більш ефективні контрзаходи.

В сучасних смарт-картках високого рівня захисту топологія процесора реалізується з використанням технології заплутування – транзистори, що складають регістри, «розкидаються» по різних місцях чипу таким чином, щоб утруднити розпізнавання регістрів процесора (звичайно, з міркувань продуктивності вони не можуть бути розкидані занадто широко). Також може використовуватися певний вид шифрування пам'яті: під час запису та читання даних з масиву комірок пам'яті – вони певним чином шифруються (але використання складного шифру призводить до падіння продуктивності). Проте в реальних конструкціях процесора не вся пам'ять може бути зашифрована; завантажувальний код і основний ключ повинні десь зберігатися. Також, коли використовується обмін з пам'яттю великими блоками, прості технічні прийоми шифрування можуть бути вразливими.

Багато уваги приділяється техніці захисту з використанням логіки вбудованого сигналу тривоги. Принаймні, доцільно включати в смарт-картки

низькотемпературні сигнальні датчики, а також датчики для різних видів іонізуючого випромінювання від інфрачервоного до рентгенівських променів.

Оскільки в нових технологіях виробництва мікросхем розміри елементів топології чипу зменшуються, зростає можливість застосування більш стійкого шифрування пам'яті, в межах дозволеної затримки операцій запису-читання. Також збільшенню безпеки сприяє використання самосинхронізуючих схем, оскільки це ускладнює зловмисникові визначення моменту, коли можливо заморозити схему для аналізу.

В цілому, ефективність захисту залежить від того, наскільки добре захисні механізми працюють разом. Часто це не так, оскільки апаратні засоби, операційна система, крипто- бібліотеки і програмне забезпечення створюються різними командами, які мінімізують обмін інформацією з міркувань "безпеки".

9.4. Віддалені атаки

Є кілька видів атак, що не залежать від відстані між атакуючим і криптопроцесором, тому об’єднуються за цієї ознакою в один клас – віддалених атак. Атакуючий може знаходитися на іншому боці земної кулі, – йому просто потрібен доступ до трафіку транзакцій з криптопроцесором. Ці атаки можуть бути пасивними або активними: в першому випадку потік транзакцій тільки спостерігається і аналізується, в той час як в останньому – атакуючий може вставляти транзакції і спостерігати відповіді.

Один з видів віддаленої атаки, специфічний для криптографічних процесорів – це атаки на API криптопроцесора. Такі API-атаки розроблені вперше в кінці 80-х років, коли виявилося, що деякі HSM компанії Eracom, які в даний час називаються криптопроцесорами, мають API-вразливості. Хоча з тих пір виробники криптопроцесорів постійно випускають патчі для ліквідації відомих вразливостей, нові API-вразливості продовжують знаходити.

В загальному, ідея активної API-атаки полягає у *застосуванні несподіваної послідовності операцій, яка б змусила криптомодуль розкрити секрет наперекір вимогам політики безпеки пристрою*.

Зазвичай, атаки на API розглядаються на прикладі HSM, що використовуються для захисту банкоматів на основі PIN-коду. API-вразливості також зустрічаються в інших додатках, таких як токени, торгові автомати, але захист на основі PIN-коду є хорошим прикладом для розгляду підходів, що лежать в основі API-атак.

Різниця між захищеним API і криптографічним API

Захищений API є програмним прикладним інтерфейсом, який використовує криптографію для забезпечення політики безпеки при взаємодії двох суб'єктів, – по суті це інтерактивна програмна компонента ПЗ криптопроцесора, яка управляє його взаємодією з зовнішнім світом.

Ця програмна компонента відрізняється від *криптографічного* API тим, що крім надання криптографічних служб (наприклад, реалізації DES, RSA, підтримки PKCS), вона також стежить за дотриманням політики безпеки в області взаємодії з криптопроцесором.

Дизайнер *криптографічного* API покладається на приєднаний host-комп'ютер (далі – host) в плані політики використання ключів, в той час як дизайнер *захищеного* API більш песимістичний, і робить деякі припущення про зовнішній світ. Він, як правило, передбачає, що host, з яким взаємодіє криптопроцесор, знаходиться під контролем супротивника.

9.4.1. Приклади атак на криптографічні API

Важливими для розгляду є API-атаки, що відносяться до слабкостей архітектури управління ключами в фінансових HSM.

Приклад API-атаки шляхом заміни особистого рахунку клієнта

Загальною банківської практикою було обчислення PIN-коду клієнта шляхом шифрування номера особистого рахунку клієнта (Personal Account Number – *PAN*) за допомогою секретного ключа, а потім перетворення отриманого шифртексту в чотиризначний номер. Якщо клієнт змінив свій PIN-код, то банк зберігає зсув між старим і новим PIN-ми у своїй основній базі даних. Наприклад, оригінальний PIN-код 3566 змінений на 3690, дає зміщення 0134, яке буде відніматися під час перевірки.

Одному з банків було необхідно впорядкувати базу основних рахунків (*PANs*) своїх клієнтів. На жаль, зміна *PAN*-ів змінювала початкові PIN-коди, видані для клієнтів, а банк не бажав примушувати всіх своїх клієнтів отримувати нові PIN-коди. Тому банк замовив у розробника HSM таку транзакцію для налаштування всіх збережених зміщень в базі даних (рис. 9.11), яка могла б змінити *PAN*-и без необхідності перевидання PIN-ів. Розробник підготував потрібну транзакцію, попереджаючи, що це небезпечно і повинно бути використано тільки для виконання пакетного перетворення, а потім видалено з API. Тепер і далі – $U \rightarrow C$ позначає команду користувача криптопроцесору, а $C \rightarrow U$ відповідь.

$$U \rightarrow C: \text{ old } PAN, \text{ new } PAN, offset$$

$$C \rightarrow U: \text{ new } offset$$

Рис. 9.11. Транзакція налаштування зміщень

Ці попередження були забуті і транзакція не була відключена. Пізніше один з програмістів зауважив, як можна було б зловжити цією транзакцією. Якщо він задасть в транзакції свій власний номер рахунку в якості нового *PAN*, то команда належним чином визначить і поверне різницю між виданим PIN-ом будь-якого клієнта і його власним оригінальним PIN-кодом!

У той час це було охарактеризовано як помилка протоколу, але стало приводом для постановки більш складного питання: «*Чи можна бути впевненим, що не існує деякий ланцюжок з 17 транзакцій, який призведе до витоку ключа у відкритому вигляді?*».

Атака на криптомодуль VISA з вилучення PIN-коду клієнта Криптомодуль VISA (Visa Security Modul – VSM) був одним з найбільш ранніх конструкцій фінансових HSM, що використовувався для забезпечення безпеки в банківських АТМ мережах на основі PIN-коду. Криптомодулю VSM доводилося взаємодіяти з автономними банкоматами (через погану надійність телефонної мережі в деяких країнах). Тому, коли банки створили нові АТМ-банкомати, їм знадобився спосіб, щоб надійно передавати похідні від PIN ключі з VSM в банкомати. У системі VISA використовується подвійний контроль: кожен з двох сервісних інженерів повинен взяти один з компонентів головного ключа до банкомату, і ввести його в банкомат. Після того, як обидві компоненти були введені, банкомат може об'єднати компоненти за допомогою функції XOR. Отриманий «Майстер-ключ терміналу» (*TMK*), завантажений в VSM може використовуватися для передачі всіх інших ключів. Транзакція спочатку запускається двічі в VSM для створення двох компонентів, рис. 9.12.

$$C \rightarrow Printer: \ TMK1 \qquad C \rightarrow Printer: \ TMK2$$

$$C \rightarrow U: \ \{TMK1\}_{Km} \qquad C \rightarrow U: \ \{TMK2\}_{Km}$$

Рис. 9.12. Генерація компонентів ×2

Криптомодулі VSM мали дуже обмежену внутрішню пам'ять, проте може бути багато різних банкоматів, ключі яких потрібно підтримувати. Тому використовувалася така парадигма роботи з зашифрованими ключами: замість того щоб зберігати ключі всередині, VSM зберігає тільки кілька майстер-ключів (Km_1, ...,Km_n), а інші ключі, зашифровані на одному з цих майстер ключів, виступають в якості аргументів для потрібної транзакції (наприклад, $\{K1\}_{Km}$). Таким чином, у відповідь на зазначену вище транзакцію, VSM повертає на хост-

комп'ютер зашифровану на ключі *Km* копію компоненти майстер-ключа (а також друкує відкриту копію на спеціальному запечатаному контейнері для сервісного інженера).

Для створення майстер-ключа АТМ-банкомату VSM використовує команду, щоб об'єднати дві зашифровані компоненти разом. Але ця транзакція може бути використана для атаки, як показано на рис. 9.13.

$U \rightarrow C: \{TMK1\}_{Km}, \{TMK2\}_{Km}$ $\quad$ $U \rightarrow C: \{TMK1\}_{Km}, \{TMK1\}_{Km}$

$C \rightarrow U: \{TMK1 \oplus TMK2\}_{Km}$ $\quad$ $C \rightarrow U: \{TMK1 \oplus TMK1\}_{Km}$

Рис. 9.13. Зліва звичайна операція; справа – атака за 0-вим ключем

Сутність полягає в наступному: якщо той же самий компонент подається два рази, то потім, завдяки використанню XOR, це призведе до відомого ключу ($TMK1 \oplus TMK1=0$). Цей відомий ключ може потім використовуватися для експорту ключа отримання PIN-коду (*PDK*) в незашифрованому вигляді.

Пізніше в наборі транзакцій VSM було виявлено ще більше вразливостей, через неадекватний поділ функцій ключів. Майстер-ключі терміналів використовуються для передачі інших ключів в банкомати, а ключі *PDK*, які використовуються для розрахунку PIN-кодів клієнтів, – розглядаються VSM як ключі того ж типу (оскільки VSM зберігає їх в зашифрованому вигляді на тому ж майстер-ключі *Km*).

Два приклади операцій з використанням цих ключів наведені нижче, де *PDK*1 – це ключ отримання PIN-коду, а *TMK*1 є майстер-ключем терміналу.

Перша транзакція шифрує *PAN* клієнта за допомогою ключа *PDK*, але посилає PIN-код на захищений принтер (для подальшого розсилання замовнику); друга шифрує *PDK* на *TMK*, що належить банкомату. Хоча вони виконують абсолютно різні функції, які не пов'язані, їх вхідні аргументи шифруються одним і тим же майстер-ключем (рис. 9.14).

$U \rightarrow C: PAN, \{PDK1\}_{Km}$ $\quad$ $U \rightarrow C: \{PDK1\}_{Km}, \{TMK1\}_{Km}$

$C \rightarrow Printer: \{PAN\}_{PDK1}$ $\quad$ $C \rightarrow U: \{PDK1\}_{TMK1}$

Рис. 9.14. Зліва печатання конверту з PIN; справа – пересилання *PDK* в АТМ банкомат

Разом з тим, в VSM чітко розрізняються ключі «Для зв'язку з терміналом» (Terminal communication – *TC*) та ключі *PDK* або *TMK*. Вони зберігаються окремо, тому що ключі зв'язку терміналів не рахуються такими ж цінним як *PDK*. Якщо *TC*1 є ключем зв'язку з терміналом № 1, то для шифрування ключів

цього типу і зберігання їх окремо від інших використовується інший майстер-ключ $Km1$, а для завантаження у відкритому вигляді обраного ключа $TC1$ використовується спеціальна транзакція (рис. 9.15, зліва).

$U \rightarrow C:\ TC1$ $\qquad$ $U \rightarrow C:\ \{TC1\}_{Km1},\ \{TMK1\}_{Km}$

$C \rightarrow U:\ \{TC1\}_{Km1}$ $\qquad$ $C \rightarrow U:\ \{TC1\}_{TMK1}$

Рис. 9.15. Зліва завантаження ключа $TC1$; справа – пересилання $TC1$ в АТМ банкомат

Ключі TC повинні бути передані до банкоматів таким же чином, як і ключі PDK, тому існує команда, яка працює дуже схожим чином, шифруючи обраний $TC1$ відповідно до обраного $TMK1$, що відповідає конкретному банкомату (рис. 9.15, справа).

Якщо ці дві транзакції використати разом, з огляду на відсутність поділу між ключами PDK і ключами TMK, тоді можлива наступна проста атака: необхідно увійти в PAN клієнта, проголошуючи, що це ключ TC (рис. 9.16, зліва)., і замінити ключ PDK на TMK в транзакції «відправити ключ TC АТМ банкомату» (рис. 9.16, справа).

$U \rightarrow C:\ PAN$ $\qquad$ $U \rightarrow C:\ \{PAN\}_{Km1},\ \{PDK1\}_{Km}$

$C \rightarrow U:\ \{PAN\}_{Km1}$ $\qquad$ $C \rightarrow U:\ \{PAN\}_{PDK1}$

Рис. 9.16. Зліва завантаження «ключа TC»; справа – пересилання «ключа TC» в АТМ банкомат

За результатами буде отримано $\{PAN\}_{PDK1}$, тобто просто PIN-код клієнта.

Атака типу «Зустріч-по-середині» на реалізацію алгоритму DES

API криптомодуля VSM і API Common Cryptographic Architecture (CCA) криптомодуля IBM 4758 для мали операції для генерації ідентифікаторів ключів – «перевірочних значень» (Check Value) для ключів. Вони вираховуються шляхом шифрування фіксованого рядка на кожному ключі (рис. 9.17). Ці перевірочні значення використовувалися для виявлення помилок під час введення ключа і для налагодження. Типове перевірочне значення отримувалось шляхом шифрування блоку бінарних нулів.

$$U \rightarrow C:\ \{TMK1\}_{Km}$$

$$C \rightarrow U:\ \{0000000000000000\}_{TMK1}$$

Рис. 9.17. Генерація Check Value

Архітектура HSM, зазвичай, дозволяє користувачу генерувати практично необмежену кількість звичайних ключів певного типу, наприклад *TMK*. Проектувальники усвідомлювали, що перевірочні значення можуть бути використані в якості відомого відкритого тексту для здійснення атаки перебором з метою знаходження ключа. Було зроблено багато оцінок складності розкриття DES, за результатами яких вважалося, що пошук в 56-бітному просторі ключів DES занадто витратний. Однак, через вказані особливості архітектури HSM, будь-який великий набір ключів можна використовувати для випробування з метою вилучення значущих ключів. Таким чином можливо здійснити атаку «Зустріч-по-середині». Алгоритм наступний:

1. Генерування великої кількості майстер-ключів терміналу і збір їх перевірочних значень.

2. Збереження всіх перевірочних значень в упорядкованій геш-таблиці.

3. Перебирання ключів, зашифрування тестового зразку на кожному, і порівняння отриманих перевірочних значень з усіма збереженими перевірочними значеннями шляхом пошуку в геш-таблиці.

При розмірах простору всіх ключів 2^{56} і кількості цільових ключів 2^{16}, цільовий ключ знаходиться, в середньому, за $2^{56}/2^{16} = 2^{40}$ випробувань. Ця технологія атаки може бути застосованою до багатьох HSM зі старими архітектурами API.

Атака реалізації двохключового 3DES пов'язаними ключами

В низці API фінансових HSM використовується криптоалгоритм Triple-DES (3DES). У свій час CCA від IBM була розширена для підтримки двохключового 3DES, зі зберіганням кожної половини ключа 3DES (лівої і правої) окремо, зашифрованої на майстер-ключі. Один з варіантів використання одного майстер-ключа для зберігання лівої і правої половин – це застосування XOR констант, що представляють з майстер-ключем *Km* ключі зберігання для лівої і правої половин. У такому випадку транзакція шифрування даних має вигляд, зображений на рис. 9.18.

$$U \rightarrow C: \ \{KL\}_{Km \oplus left}, \{KR\}_{Km \oplus right}, data$$

$$C \rightarrow U: \ \{data\}_{KL|KR}$$

Рис. 9.18. Транзакція шифрування

Інтерфейс CCA підтримує звичайний DES в спеціальному застарілому режимі, для чого може бути згенерований «реплікований» ключ 3DES з однаковими обома половинами, тобто *KL=KR=X* (рис. 9.19). Тоді 3DES – це

шифрування на ключі X, з подальшим розшифрування на X, потім з шифруванням на X, тобто E(X, D(X, E(X, *data*))) = E(X, *data*) і реплікація ключа виконує таку ж в точності роль, як застосування одноключевого DES.

$$C \rightarrow U: \ \{X\}_{Km \oplus left}, \ \{X\}_{Km \oplus right}$$

Рис. 9.19. Генерація реплікату

Недолік у тому, що дві половини ключа 3DES не були зв'язані один з одним належним чином, тільки розділені на ліву і праву частини. Може бути згенеровано багато реплікованих ключів (рис. 9.20) і можуть бути два розкриті за допомогою паралельного пошуку ключів.

$$C \rightarrow U: \ \{X\}_{Km \oplus left}, \ \{X\}_{Km \oplus right}$$

$$C \rightarrow U: \ \{Y\}_{Km \oplus left}, \ \{Y\}_{Km \oplus right}$$

Рис. 9.20. Генерація реплікату ×2

Перестановка половинок двох розкритих реплікованих ключів призводить потім до отримання відомого справжнього 3DES ключа $\{X\}_{Km \oplus left}, \{Y\}_{Km \oplus right}$, який може бути використаний для експорту інших за своєю природою цінних ключів.

Ця атака пов'язаними ключами знижує складність розкриття 3DES в реалізації CCA з 2^{112} до 2^{57} (тільки в два рази складніше, ніж звичайний DES).

9.4.2. Приклади атак на захищені API

Однак, виявляється, що існують атаки по витоку інформації на рівні API, які обумовлені конкретною фінансовою функціональністю.

Атака на формат PIN

Відома класична атака проти стандарту ISO-0 блочного шифрування PIN. Згідно ISO-0 PIN-код представляється у вигляді шістнадцяти шістнадцяткових цифр, що містять PIN-код, інформацію контролю і заповнення. Цей буфер потім складається XOR з номером рахунку клієнта перед шифруванням на відповідному ключі. Це представляється як $\{P \oplus A\}_{PEK}$, де PEK є ключем, P – відформатований буфер PIN, а A – номер рахунку.

$$U \rightarrow C: X, \ \{P \oplus A\}_{\text{PEK}}$$

$$C \rightarrow U: ((P \oplus A) \oplus X) < 10$$

Рис. 9.21. Протокол контролю цілісності PIN

Коли зашифрований PIN-код перевіряється або повторно зашифровується на іншому ключі, – він повинен бути розшифрований, тому його треба витягти з формату, що вимагає від користувача надати номер рахунку клієнта, позначений через *X*. PIN-код витягується і здійснюється перевірка цілісності. Оскільки кожна цифра PIN-коду – це десяткова цифра в діапазоні від 0 до 9, то перевірка просто тестує, що кожна шістнадцяткова цифра PIN-коду, яку вилучають із розшифрованого буфера становить менше десяти («перевірка PIN на здоровий глузд»). Якщо цей тест не проходить, то це означає, що номер рахунку або ключ або зашифрований PIN невірний або пошкоджений.

На перший погляд, перевірка цілісності здається достатньою, і дійсно виявляє ненавмисні помилки. Однак, повторення виконання цього протоколу з різними значеннями заявленого номера рахунку *X*, швидко призводить до ідентифікації PIN-коду. Це ясно видно з таблиці 9.2. Задане значення $P \oplus A$ призводить до унікальної комбінації дозволів і помилок, ідентифікуючи кожну цифру PIN з точністю до множини $\{P, P \oplus 1\}$.

Таблиця 9.2

Ідентифікація PIN шляхом використання перевірки його на цілісність

		$P \oplus A$				
		0, 1	2. 3	4, 5	6, 7	8, 9
	0, 1	Pass	Pass	Pass	Pass	Pass
	2, 3	Pass	Pass	Pass	Pass	Fail
	4, 5	Pass	Pass	Pass	Pass	Fail
X	6, 7	Pass	Pass	Pass	Pass	Fail
	8, 9	Pass	Fail	Fail	Fail	Pass
	A, B	Fail	Pass	Fail	Fail	Pass
	C, D	Fail	Fail	Pass	Fail	Pass
	E, F	Fail	Fail	Fail	Pass	Pass

На практиці атака трохи складніша, вимагає додаткових заходів, щоб розкрити всі цифри PIN-коду і визначити точні значення з множини $\{P, P \oplus 1\}$ [16].

Диференційна атака на протокол веріфікації PIN-коду

Атака заснована на тому способі, як PIN-коди генеруються і перевіряються. Номер рахунку клієнта шифрується за допомогою ключа отримання PIN-коду (*PDK*), в результаті отримується по суті випадковий рядок з 16 шістнадцяткових цифр (один 64-бітний блок DES). Вибираються перші чотири цифри, які перетворюються в десяткові цифри для використання в якості PIN-коду. Це відображення здійснюється за допомогою функції користувача – таблиці перетворення в десятковий вигляд (dectab), що має вигляд, подібний до таблиці 9.3. У цьому прикладі шістнадцятковий символ 0 відображається в 0, а символ A також відображається в 0. Нижній рядок цієї таблиці записується у вигляді 0123456789012345.

Таблиця 9.3

Приклад таблиці перетворення в десятковий вигляд

Hexadecimal Digit	0123	4567	89AB	CDEF
Mapped Decimal Digit	0123	4567	8901	2345

PIN-код, отриманий таким способом, ніколи не повертається на host у відкритому вигляді; він відправляються або на захищений принтер або повертається в зашифрованому вигляді на ключі шифрування PIN (*PEK*) для подальшого друку в іншому місці.

$$U \rightarrow C : A, \text{dectab}$$

$$C \rightarrow U : \{P \oplus A\}_{PEK} \text{ где } P = \text{dectab}(\{A\}_{PDK})$$

Рис. 9.22. Генерація PIN на основі номера рахунку

Проблема полягає в тому, що таблиця перетворення в десятковий вигляд відкрита для шкідливих маніпуляцій. Якщо встановити таблицю з усіх нулів (тобто 0000000000000000), то повинен бути згенерований PIN-код «0000» і він повертається в зашифрованому вигляді. Потім повторюється виклик, використовуючи злегка модифіковану таблицю 1000000000000000. Якщо результат шифрування номера рахунку (тобто $(\{A\}_{PDK})$ не містить нульову шістнадцяткову цифру серед перших чотирьох шістнадцяткових цифр, то PIN-код буде незмінним і буде повернений той же самий зашифрований PIN-блок

$\{P \oplus A\}_{PEK}$. Ця техніка аналогічним чином може повторюватися з різними таблицями для визначення складових цифр PIN-коду. Оскільки метод експлуатує порівняння повторюваних (злегка змінених) виконань одного і того ж протоколу, – цей тип атаки відноситься до «Диференційного аналізу протоколу». Точний PIN-код можна розкрити за рахунок експлуатації функції HSM щодо зміни PIN-коду клієнтом. Змінені PIN-коди зберігаються як зміщення між згенерованим PIN і новим PIN, що обраний клієнтом (зміщення = клієнтський PIN – згенерований PIN (mod10)). Цей зсув зберігається в основній базі даних банку. Перевірка зсувів проводиться відповідно до рис. 9.23.

$$U \rightarrow C : \{P \oplus A\}_{PEK}, A, \text{dectab}, offset$$

$$C \rightarrow U : \text{true якщо } P = \text{dectab}(\{A\}_{PDK}) + offset$$

Рис. 9.23. Протокол веріфікації PIN-коду

Транзакція, що представлена на рис. 9.23 є вразливою до попередньої атаки. Маючи дійсний зашифрований PIN-блок і відповідний рахунок, можна маніпулювати таблицею перетворення в десятковий вигляд, щоб дізнатися PIN-код. Припустимо, що змінено звичайну таблицю (0123456789012345) на 1123456789012345, зберігаючи при цьому інші входи: A, $\{P \oplus A\}_{PEK}$ і зміщення – постійними. Якщо PIN-и не збігаються і перевірка зазнає невдачі, то це означає, що $\{A\}_{PDK}$ містить принаймні один випадок модифікації цифри. Завдяки простому арифметичному взаємозв'язку між клієнтськими PIN-кодами, згенерованими PIN-кодами і зсувами, визначається, які конкретні цифри порушені шляхом повторення виклику з відповідними обраними значеннями зсуву. Таким чином встановлюються як значення складових цифр PIN-коду, так і їх позиції.

Статистична атака на шифровані дані PIN-блоків

Наслідком процесу перетворення в десятковий вигляд є те, що спотворюється вихідний рівномірний розподіл згенерованих цифр PIN-коду, що призводить до можливості статистичних атак. Розглянемо певну слабкість, яка при цьому виникає: припустимо, що команда генерації PIN-коду на рис. 9.24 багаторазово виконується, вибираючи багато випадкових *PD*K при постійному A і зміщенні. PIN-коди будуть створюватися відповідно до розподілу частот цифр в таблиці перетворення в десятковий вигляд, і цей розподіл буде відображатися у відповідній частоті зашифрованих PIN-блоків, що повертаються. Це саме по собі ще не досить, щоб однозначно визначити PIN-код, оскільки багато хто буде мати ту ж очікувану частоту.

$$U \rightarrow C : A, \text{dectab}, offset$$

$$C \rightarrow U : \{P \oplus A\}_{PEK}, \text{ де } P = \text{dectab}(\{A\}_{PDK}) + offset$$

Рис. 9.24. Протокол для генерації PIN-кодів зі зміщеннями

Однак, маніпулювання параметром зсуву, дозволяє зашифровані PIN-коди розташувати по порядку. Для цього генеруються зашифровані PIN-коди для фіксованих вхідних значень *A*, dectab і *PDK*, але варіюючи зміщення, починаючи з 0000. Збільшуючи зміщення на 1 (за модулем 10) і повторюючи виклик, отримується таким чином зашифрований PIN-блок, відповідний суміжному PIN- коду в просторі можливих PIN-кодів. Після того, як співвідношення між усіма зашифрованими PIN-блоками відомі, в поєднанні зі знанням частоти виникнення кожного блоку, можливо ідентифікувати конкретний блок (і таким чином всі блоки) однозначно.

Атака колізією на формат ISO-0

Сам по собі формат ISO-0, що описаний вище, створює канал витоку інформації незалежно від алгоритму, який використовується для генерації PIN-кодів. Якщо розглянути фіксований номер рахунку *A* і таблицю перетворення в десятковий вигляд dectab, то всі можливі зашифровані PIN-блоки – $\{P \oplus A\}_{PEK}$ – можуть бути отримані шляхом маніпулювання зміщенням, як описано вище. Оскільки і цифри PIN-коду *P* і цифри рахунку *A* – десяткові, буде спостерігатися неповний набір можливих шістнадцятирічних значень $P \oplus A$. Дублюючи цей процес з іншим номером рахунку *A*', отримаємо другий неповний набір зашифрованих PIN-блоків. Атакуючий може тепер порівняти набори зашифрованих PIN-блоків, отримані в результаті двох серій. Обидві серії містять всі PIN-коди. Однак, дві серії використовують різні номери рахунків, які впливають на те, як множина PIN-кодів шифрується і зберігається. Тоді PIN-коди першої серії, складені XOR з номером рахунку *A*, можна порівняти з PIN-кодами другої серії, складеними XOR з іншим номером рахунку *A*'. Коли це робиться, зіставляються також і зашифровані блоки (тобто, мають ті ж значення). З іншого боку, кожен зашифрований PIN-блок, який існує тільки в одному зі списків (без обмеження загальності, припустимо, що список з першої серії), відповідає значенню $P \oplus A$, яке не досяжне в другій серії. Це дозволяє атакуючому визначити множину можливих значень для $P \oplus A$, і, отже, варіантів PIN-коду.

Цю техніку можна проілюструвати на прикладі PIN-коду, який використовує одну цифру. Атакуючий будує два списки всіх можливих зашифрованих блоків для номерів рахунків з PAN-ами 7 і 0, як показано в таблиці 9.4.

Таблиця 9.4

Множини зашифрованих PIN-блоків для номерів рахунків з *PAN*-ами 7 і 0

A	*P*	(*P*⊕*A*)	*block*	*A'*	*P*	(*P*⊕*A'*)	*block*
7	0	7	2F2C	0	0	0	21A0
7	1	6	345A	0	1	1	73D2
7	2	5	0321	0	2	2	536A
7	3	4	FF3A	0	3	3	FA2A
7	4	3	FA2A	0	4	4	FF3A
7	5	2	536A	0	5	5	0321
7	6	1	73D2	0	6	6	345A
7	7	0	21A0	0	7	7	2F2C
7	8	F	AC42	0	8	8	4D0D
7	9	E	9A91	0	9	9	21CC

Зашифрований блок AC42 з лівого списку не міститься в правому списку, і аналогічно для зашифрованого блоку 9A91. Отже, ці блоки повинні мати шістнадцяткові значення, які не можуть вийти в результаті XOR номера рахунку 0 з десятковою цифрою PIN: існують дві можливості 8 і 9.

Запитання для самоконтролю

1. Класифікація атак.
2. Спосіб доступу до системи
3. Контроль обчислювального процесу.
4. Метод аналізу та його застосування.
5. Алгоритм проведення атаки за часом.
6. Предумови реалізації атаки за часом.
7. Захист від атак.
8. Електромагнітна атака.
9. Технології захисту від напівагресивних атак.
10. На криптографічні API.
11. Атаки на захищені API.

РОЗДІЛ 10. КОНЦЕПЦІЇ ТА МОДЕЛІ КІБЕРБЕЗПЕКИ

10.1. Концепція керування кібербезпекою інформаційних технологій

Сприйняття концепцій, що відповідають мікрополітиці й оточенню, у яких працює організація, може дати значний ефект у створенні підходів до КЗ в цілому. Крім того, вони можуть вплинути на окремі підрозділи організації, відповідальні за кіберзахист. У деяких випадках уряд встановлює чи скасовує відповідальність уведенням у дію відповідних законів. В інших випадках відповідальність призначає власник чи керівник.

Підхід

Для визначання необхідних умов КБ інформаційних технологій у межах організації потрібно застосовувати системний підхід. Цей підхід також застосовують для організації захисту в інформаційних технологіях і наступному керуванні ним. Процес керування КБ інформаційних технологій містить такі дії [33,34,35]:

1. Розробка стратегії КЗ інформаційних технологій;
2. Ідентифікація ролей і обов'язків у межах організації;
3. Керування ризиком, ідентифікацією й оцінюванням:

активів, що будуть захищені,

загроз,

подразнень,

уражень,
ризиків,

засобів КЗ,

залишкових ризиків,

обмежень;

Керування конфігурацією;

Керування змінами;

Планування випадкових процесів і планування відновлення у випадку непередбачених ситуацій;

Вибір засобів КЗ та їхнє застосування;

Встановлення компетентності щодо КЗ разом з:

експлуатацією,

контролем безпеки,

перевіркою,

переглядом,

обробкою інцидентів.

Цілі кібербезпеки, стратегії і методики

Цілі безпеки, стратегії і методики треба брати за основу для здійснення ефективного КЗ інформаційних технологій в організації. Вони супроводжують діяльність організації й сукупно гарантують стабільність усіх засобів захисту та їхніх взаємозв'язків.

Цілі визначають, чого потрібно досягнути, стратегії визначають, як досягти цих цілей, методики визначають, як виконувати конкретні заходи. Цілі, стратегії і методики можуть бути розроблені за рівнями підпорядкованості організації. Вони мають відображати організаційні вимоги і брати до уваги будь-які зв'язки, вони також мають гарантувати незмінність КБ на кожному рівні зокрема і на всіх рівнях разом. Безпека – це відповідальність усіх рівнів керівництва організації протягом усіх фаз життєвого циклу системи. Цілі, стратегія і методики мають бути підтримані й модифіковані на підставі результатів періодичного перегляду безпеки (наприклад, аналізу ризику, аудиту захищеності) і змін в цілях підвищення ділової активності.

Методика кіберзахисту по суті містить принцип КЗ і директиви для організації в цілому. Методики КЗ мають детально відображати методики, охоплюючи ті, які стосуються індивідуальних прав, вимог законодавства і стандартів.

Методика кіберзахисту інформаційних технологій має відображати істотні принципи безпеки і директиви, застосовувані до корпоративної методики захисту, та загальне використання систем інформаційних технологій в організації.

Методика кіберзахисту системи інформаційних технологій має відображати принципи захисту і директиви у межах методики КБ інформаційних технологій. Вона має також містити детальний опис специфічних вимог безпеки і засобів захисту, які будуть застосовані, а також метод, використаний для забезпечення відповідного КЗ. В усіх випадках важливим є вибір ефективного підходу до потреб діяльності організації.

Цілі, стратегії й методики систем КЗ в інформаційних технологіях описують з позиції КБ. Їх звичайно описують природною мовою, однак системи КЗ можуть бути формалізовані з використанням математичної мови. Системи КЗ призначені для забезпечення таких критеріїв КБ інформаційних технологій, як [24,25]:

конфіденційність;

цілісність;

доступність;

обліковість;

достовірність;

надійність.

Цілі, стратегії й методики визначають рівень безпеки в організації, а також допустимий рівень ризику і непередбачуваних обставин в організації.

10.2. Елементи кібербезпеки

Наведені положення на високому рівні описують головні елементи, задіяні в процесі керування КЗ. Кожен з елементів визначений і наведені його основні супутні чинники.

Активи

Наявність відповідного керування активами важлива для забезпечення успіху організації і є головною рисою всіх рівнів керування. До активів організації належать [36-40]:

фізичні об’єкти (апаратне забезпечення, засоби зв’язку, будівлі тощо);
інформація/дані (наприклад, документи, бази даних);
програмне забезпечення;
здатність виробляти деяку продукцію чи надавати послуги;
людські ресурси;
нематеріальна власність (наприклад, імідж, символіка).

Більшість із цих активів має потребу в певному захисті. У випадку, коли активи не мають належного рівня захищеності, необхідно застосовувати до них механізми оцінювання ризиків.

Якщо йдеться про перспективність програми КБ організації, то немає сенсу забезпечувати захист і здійснювати його подальшу підтримку, якщо чітко не визначені активи організації. У більшості випадків процес ідентифікації активів і визначення їхніх розмірів можна виконати на досить високому рівні і без дорогого, детального і тривалого аналізу. Рівень деталізації для цього аналізу визначають значенням часу і вартістю аналізу стосовно цінності активів, виходячи з цілей КЗ. Зокрема, ці підходи можна застосовувати до груп активів.

Розглядають такі характеристики активів, як їхня цінність і (або) критичність і різноманітність застосовуваних засобів КЗ. Необхідність застосування засобів захисту до активів визначають також їхньою вразливістю до впливу специфічних загроз. Якщо ці аспекти очевидні для власника активів, їх треба зафіксувати на початкових стадіях. Оточення і мікрополітика, у яких діє організація, можуть впливати на активи та їхні характеристики.

Загрози

Активи є об'єктами для багатьох видів загроз. Загроза потенційно є причиною небажаного інциденту, що здатний заподіяти шкоду системі чи організації та її активам. Ця шкода є результатом прямої чи непрямої атаки на інформацію, якою оперує система чи служба інформаційних технологій, наприклад, її несанкціоноване знищення, розкриття, зміна, перекручування, втрата доступності чи втрату взагалі. Загроза може здійснитися, заподіяти шкоду у випадку наявності в активах уразливих місць. Загрози, причиною яких є людина, розділяють на випадкові й навмисні. І випадкові, і навмисні загрози повинні бути ідентифіковані й визначені їхні рівні й імовірність.

Статистичні дані накопичуються збиранням інформації про різні типи загроз із довкілля. Ці дані повинні бути отримані і використовуватися організацією в процесі виявляння загрози. Деякі загрози мають спрямовану дію на окремі елементи організації, наприклад, викликають збої інформаційних систем. Загрози можуть мати специфічне територіальне походження, наприклад ушкодження будівель від ураганів чи спалахів блискавки. Загроза може діяти зсередини організації, наприклад, саботаж службовців, чи зовні, наприклад, навмисний злом чи промислове шпигунство. Шкода, викликана небажаним інцидентом, може мати тимчасовий, легко відновлюваний характер чи остаточний і безповоротний, як у випадку знищення активів.

Обсяги шкоди, заподіяної загрозою, можуть варіюватися в широких межах для кожного конкретного випадку. Наприклад [42-44]:

програмний вірус може заподіяти різні обсяги шкоди залежно від його впливу;

землетрус у зоні специфічного територіального розташування може мати різну силу в кожному конкретному випадку.

Такі загрози часто характеризуються обсягами заподіюваної ними шкоди. Наприклад:

вірус можна охарактеризувати як такий, що руйнує чи не руйнує;

силу землетрусу можна виміряти за шкалою Ріхтера.

Прояви загроз можуть впливати на більш ніж один вид активів. У цьому випадку вони ведуть до різних конфліктів, що впливають на активи. Наприклад, програмний вірус може вразити єдину інформаційну систему. Однак той самий програмний вірус, потрапивши на основний мережний файл-сервер, може поширитися на декілька інформаційних систем. Різноманітні загрози чи їх прояв у різних місцях можуть постійно завдавати великої шкоди. Якщо шкода, заподіяна загрозою, є постійною, то можна використовувати універсальний визначений підхід. Однак якщо обсяги заподіяної шкоди змінюються в широких межах, необхідно використовувати конкретизований підхід, що відповідає локалізації загрози.

Загрози характеризуються даними, що містять корисну інформацію.

Приклади такої інформації [41-43]:

джерело (внутрішнє чи зовнішнє);

мотивація, наприклад збагачення, конкуренція;

частота появи;

серйозність загрози.

Оточення й мікрополітика організації можуть мати істотне значення й обумовлювати вплив загроз на організацію.

У критичних ситуаціях деякі загрози в певних мікрополітичних середовищах не розглядають і вважають безпечними. Всі аспекти щодо оточення й діяльності треба розглядати стосовно загроз.

Вразливості

Вразливості звичайно пов'язані зі слабкими місцями в активах, а саме: у розташуванні організації, процесах, персоналі, керуванні, адмініструванні, апаратному та програмному забезпеченні, в інформації. Їх використовують як потенційну загрозу для заподіяння шкоди системі інформаційних технологій чи діловій активності в цілому. Вразливість сама по собі не є причиною шкоди; вразливість є тільки умовою чи множиною умов, які можуть допустити вплив загрози на активи. Вразливість, що виникає з різних джерел, наприклад від активів, повинна братися до уваги. Вразливість може зникнути чи втратити актуальність, якщо відбудуться зміни в активах.

Вразливість послаблює експлуатовану систему і може призводити до небажаних наслідків. Вразливість – непряма причина шкоди, заподіюваної загрозою. Наприклад, відсутність механізмів контролювання за доступом до службових і гостьових приміщень – вразливість, що може дати змогу загрозі з легкістю впливати на активи і призводити до їхньої втрати. Специфіка конкретної системи чи організації обумовлює те, що не всі вразливості чутливі до загроз. Треба негайно приділяти увагу вразливості, що має відповідну загрозу. Оскільки оточення може змінюватися динамічно, всі вразливості потрібно постійно перевіряти щодо відкритості до старих і нових загроз.

Аналіз вразливості – це експертиза слабких місць, вразливих до ідентифікованих загроз. Цей аналіз повинен брати до уваги середовище й наявні засоби захисту. Вразливість специфічної системи чи активів до загрози описує способи, якими система чи активи можуть бути ушкоджені.

Ураження

Ураження – наслідок небажаного інциденту, спричинений навмисним чи випадковим впливом на активи. Наслідки можуть бути згубними для деяких активів, нанести ушкодження системі інформаційних технологій, призвести до втрати конфіденційності, цілісності, доступності, обліковості,

достовірності чи надійності. Можливі також і такі побічні наслідки, як фінансові втрати частки чи всього ринку, іміджу компанії. Уведення кількісних характеристик уражень дає можливість знаходити компромісне рішення між втратами в результаті небажаного інциденту і витратами на засоби захисту, які страхують від небажаного інциденту. Необхідно враховувати також і частоту появи небажаних інцидентів. Це особливо важливо, коли заподіяна шкода в кожному окремому випадку незначна, проте сумарні втрати як наслідок багатьох випадків протягом періоду часу будуть дуже великими. Запобігання ураженням є важливим складником у зменшенні ризику і виборі засобів захисту.

Кількісні і якісні характеристики ураження можна отримати через [44-47]:

визначення фінансових витрат;

надання емпіричного рангу серйозності ураження, наприклад, від одного до десяти;

використовування залежностей, обраних із заздалегідь визначеного списку, наприклад: низько, середньо, високо.

Ризик

Ризик – імовірність того, що дана загроза, впливаючи через вразливість організації, заподіє втрати чи пошкодження активів, а значить прямим чи опосередкованим шляхом заподіє збитки організації. Разові чи численні загрози, що повторюються, можуть скористатися окремою чи множинною вразливістю.

Сценарій ризику описує, як специфічна загроза чи група загроз може скористатися конкретною вразливістю чи групою вразливостей, що шкодять активам. Ризик характеризується комбінацією двох чинників: імовірністю появи небажаного інциденту і його ураженням. Будь-яка зміна стану активів, загроз, вразливостей і засобів захисту може вплинути на ризики. Чим раніше будуть виявлені зміни в самій системі чи в її оточенні, тим більше можливостей для дій, що зменшують ризик.

Засоби кіберзахисту

Засоби кіберзахисту – засоби, процедури чи механізми, що можуть захистити від загроз, зменшити вразливість, обмежити ураження внаслідок небажаного інциденту, виявити небажані інциденти і полегшити процес відновлення. Ефективний захист звичайно потребує комбінації різних засобів захисту для забезпечення багаторівневого захисту активів. Наприклад, механізми контролю доступу, що їх застосовують у інформаційних системах, повинні супроводжуватися засобами керування аудитом, увагою і навчанням персоналу, безпекою фізичних засобів. Деякі засоби КЗ вже існують як

частина оточення чи як властивий аспект активів, або вже існують в системі чи організації.

Засоби КЗ можуть виконувати одну чи кілька таких функцій: виявляння, стримування, запобігання, обмеження, корекція, відновлювання, контроль й усвідомлення. Відповідний добір засобів КЗ – невід'ємна частина правильно виконаної програми захисту. Багато засобів КЗ можуть виконувати декілька функцій. Часто вигідніше і дешевше вибрати засоби КЗ, що реалізують декілька функцій. Деякі приклади ділянок, де використовують засоби захисту [43-47]:

фізичне оточення;

технічне оточення (апаратні засоби, програмне забезпечення і зв'язок);
персонал;

адміністрація.

Поняття КБ – засоби захисту та їхній взаємозв'язок з персоналом. Оточення і внутрішні умови, в яких діє організація, часто впливають на вибір засобів КЗ і на розуміння безпеки організації в цілому. Деякі засоби КЗ посилають суворе і чітке повідомлення про тривогу відкритим текстом до підрозділу організації, яка займається захистом. Реагуючи на це повідомлення, важливо точно визначити засоби КЗ, що не суперечать мікрополітиці та (або) оточенню, у якому діє організація.

Приклади засобів захисту [48-50]:

файрволи в мережі;

моніторинг і аналіз мережі;

шифрування з метою забезпечення конфіденційності;

цифрові підписи;

програми антивірусів;
резервні копії інформації;
безперебійні джерела живлення;

механізми контролю доступу.

Залишковий ризик

Ризики, зазвичай, лише частково зменшуються за допомогою засобів КЗ. Часткове зменшення – єдине, що найчастіше може бути досягнуто, подальші зменшення спричиняють невиправданий ріст вартості. Це показує, що завжди наявні так звані залишкові ризики. Частина оцінок з безпеки або відповідає потребам організації, або допускає залишковий ризик. Цей процес відомий як допускання ризику.

Керування треба здійснювати з урахуванням усіх залишкових ризиків в умовах уражень та імовірності їхньої появи. Рішення про допустимість

залишкового ризику повинні приймати ті, хто приймає рішення у разі появи небажаного інциденту і хто уповноважений застосовувати додаткові засоби захисту, якщо рівень залишкового ризику є неприйнятним.

Обмеження

Обмеження звичайно встановлює чи визнає керівництво організації з урахуванням чинників оточення, в якому діє організація. Розглядають, наприклад, такі обмеження [54-62]:

- організаційні;
- фінансові;
- навколишні;
- персональні;
- часові;
- юридичні;
- технічні;
- мікрополітичні/соціальні.

Усі ці чинники треба враховувати під час вибору і застосування засобів КЗ. Періодично наявні та нові обмеження треба переглядати, фіксуючи будь-які зміни. Необхідно також відзначити, що обмеження можуть змінюватися з часом, географією та соціальною еволюцією, а також з мікрополітикою організації. Оточення і мікрополітика, у яких діє організація, можуть негативно впливати на різні елементи безпеки, особливо на загрози, ризики і засоби захисту.

10.3. Процес керування безпекою інформаційних технологій

Керування КБ інформаційних технологій – тривалий процес, що складається з багатьох інших процесів. Деякі процеси, як керування конфігурацією настроювання і керування змінами, застосовуються не тільки до питань безпеки. Як показує досвід, один із процесів є дуже корисним у керуванні безпекою інформаційних технологій – це керування ризиком і його підпроцес – аналіз ризику. Деякі аспекти керування КБ інформаційних технологій охоплюють керування ризиком, аналіз ризику, керування змінами і організацією системи.

Налаштування системи

Налаштування системи – процес фіксації тенденції змін у системі, який виконують формально чи неформально. Первинною метою керування налаштуванням, з погляду КБ, є гарантування того, що зміни в системі не знизять ефективність засобів КЗ і загальну безпеку організації.

Метою налаштування, з погляду безпеки, є розпізнання змін, щоб вони не впливали на безпеку засобів шляхом проведених запобіжних змін у системі інформаційних технологій. У деяких випадках можуть з'явитися причини для змін, що призводять до зниження захищеності. У таких ситуаціях привнесене в захист зниження має бути оцінено, й у відповідь мають бути визначені також керівні рішення на підставі всіх залежних чинників. Іншими словами, усі зміни в системі повинні спричинити відповідні зміни у захисті. Ще одна мета керування налаштуванням полягає в гарантуванні, що зміни в системі відображені в інших документах, а саме: відновлювання після нещасних випадків і плани непередбачених обставин. Якщо зміна дуже важлива, то необхідно проаналізувати деякі чи всі системні засоби захисту.

Керування змінами

Керування змінами – процес визначання потреб в нових засобах КЗ у випадках, коли відбуваються зміни в системі інформаційних технологій [28,36].

Системи інформаційних технологій і оточення, у якому вони працюють, постійно змінюються. Ці зміни – результат надання нових можливостей інформаційних технологій і послуг чи результат виявлення нових загроз і уражень. Зміни в системах інформаційних технологій містять [26,28]:

нові процедури;

нові можливості;

модернізацію програмного забезпечення;

переробку апаратного забезпечення;

появу нових користувачів у зовнішніх чи анонімних групах;

додаткову роботу з мережами і зв'язками.

Коли відбувається чи планується зміна в системі інформаційних технологій, важливо визначити ураження в захисті системи, якщо вони були. Якщо в системі є відділ керування конфігурацією чи інша організаційна структура, то повинен бути призначений відповідальний за безпеку інформаційних технологій у відділ для керування спеціальними змінами в системі, а також визначена відповідальність за прийняття рішень залежно від того, чи призведе зміна до уражень у захисті, і якщо так, то яким чином. Для важливіших змін, що охоплюють придбання нових апаратних засобів, програмного забезпечення чи створення послуг, також потрібен аналіз, що визначає необхідні нові вимоги КБ. З іншого боку, багато змін у системах насправді незначні і не потребують широкого аналізу, необхідного для важливіших змін. Для обох типів змін повинна бути оцінена величина ризику, виходячи з

користі і витрат. Для незначних змін рішення можуть бути прийняті неформально, на зустрічах, але результати і рішення керівництва повинні бути задокументовані.

Керування ризиком

Дії з керування ризиком найбільш ефективні, якщо вони виконуються в процесі всього життєвого циклу системи. Процес керування ризиком сам по собі є важливим циклом активності. У той час, як нові системи можна супроводжувати повним циклом, для успадкованих систем це може бути ініційовано з будь-якого моменту всього життєвого циклу системи. Стратегія може вимагати робити ревізію у певних інтервалах життєвого циклу системи чи у певні часові інтервали. Наступними можуть бути дії з попереднього розгляду-перевірки застосування засобів КЗ. Також може виявитися необхідність керування ризиком у процесі створення і розробки системи, це гарантуватиме, що безпека розроблена і реалізована з максимальною ефективністю щодо вартості та часу.

Незалежно від того, які методи чи технічні засоби використовують у керуванні ризиком, важливо забезпечити прийнятний компроміс у зменшенні часових витрат і витрат ресурсів, задіяних у визначанні і застосуванні засобів КЗ, поки існує впевненість у відповідному захисті всіх систем.

Керування ризиком – процес порівняння оцінки ризиків з вигодами і (або) витратами на засоби захисту та забезпечення стратегії їхнього застосування й методики КБ системи, створеної з урахуванням корпоративної методики КБ інформаційних технологій і завдань бізнесу. Треба розглядати різні типи засобів захисту і проводити аналіз вартості та (або) вигоди. Засоби захисту вибирають з урахуванням ризиків і потенційних уражень. Також треба брати до уваги рівень прийнятного залишкового ризику.

Засоби КЗ безпосередньо можуть містити уразливості і призводити до нових ризиків. Тому потрібно з обережністю вибирати відповідні засоби захисту, щоб не тільки знижувати ризики, але і не створювати потенційно нові.

Нижченаведені положення описують додаткові особливості процесів керування ризиком.

Аналіз ризику

Аналіз ризику ідентифікує ризики, що потребують керування чи врахування. З погляду КБ інформаційних технологій аналіз ризику для систем інформаційних технологій охоплює аналіз номінальної вартості загроз і уражень. Ризики оцінюють відносно потенційного ураження, що може бути викликано порушенням конфіденційності, цілісності, доступності, обліковості, достовірності чи надійності. Результат оглядового аналізу ризику – положення про найбільш ймовірні ризики стосовно активів.

Аналіз ризику є частиною керування ризиком і може бути виконаний без додаткових витрат часу і ресурсів після оглядового короткого аналізу всіх систем. Це дозволяє встановити, які системи можуть бути адекватно захищені за допомогою практичних вказівок чи базовими засобами керування, і ті системи, що їх можна використовувати після детальнішого аналізу ризику. Це питання практично охоплює комплект інструкцій і базових настанов, які можуть бути використані як базис для домовленості щодо задоволення основних потреб захисту.

Обліковість

Забезпечення ефективного захисту потребує обліковості (звітності) точно визначених завдань і розподілу обов'язків у питаннях безпеки. Обов'язки і обліковість мають бути доручені власникам активів, постачальникам і користувачам ресурсів систем інформаційних технологій. Отже, володіння активами і пов'язані з ними обов'язки щодо захисту з подальшим перевірянням реалізованого захисту є важливими чинниками для ефективного захисту.

Компетентність у захисті

Компетентність у захисті – це істотний елемент ефективного захисту. Відсутність компетентності в захисті і недостатність досвіду в захисті персоналу організації можуть призвести до значного зниження ефективності системи захисту. Людей в організації вважають однією з найслабших ланок захисту. Щоб бути упевненим у належному рівні компетентності в захисті організації, важливо дотримуватися і розвивати програму компетентності захисту. Метою програми компетентності захисту є пояснення робітникам, компаньйонам і компаніям-постачальникам [26,27]:

- цілей, стратегій і методик захисту;
- потреб у захисті і пов'язаних з ними функцій та обов'язків.

Крім того, має бути розроблена програма, що гарантує розподіл обов'язків із захисту між співробітниками, компаньйонами і компаніями-постачальниками.

Програма компетентності захисту повинна виконуватися на всіх рівнях організації: від вищого керівництва до найнижчої ланки. Необхідно часто розробляти документи, що стосуються підвищення компетентності людей у різних ролях і обов'язках у різних підрозділах організації. Всебічне розуміння програми безпеки розвивається і передається поступово. Кожна стадія формується на основі попередньої, починаючи з концепцій захисту і до обов'язків з виконання і контролю безпеки.

Програми компетентності захисту в межах організації мають ряд етапів. Один з таких етапів – розробка і розподіл документації щодо компетентності в захисті (наприклад, плакатів, бюлетенів, брошур чи документів). Призначення

цих матеріалів – збільшити загальну компетенцію службовців і контрактників. Наступний етап – організація курсів для навчання службовців з питань захисту. Також необхідні поглиблені курси професійного рівня для специфічних аспектів захисту.

У деяких випадках є ефективним об'єднати всі повідомлення з безпеки в окремі навчальні програми. Цей підхід є альтернативою чи повноцінною заміною програми компетентності захисту. Для розвитку програми компетентності захисту, що взаємозалежна з необхідними мікрополітичними й адміністративними умовами даної організації, треба розглядати такі аспекти [34,35]:

аналіз потреб;

програма забезпечення;

контроль;

зміст програми компетентності.

Контроль

Використання засобів захисту треба постійно контролювати для гарантії, що вони функціонують правильно, що зміни в оточенні не нейтралізували їхню ефективність і що обліковість активізована і функціонує. Автоматичний перегляд й аналіз системних журналів – ефективний спосіб, що допомагає забезпечити контроль. Цей спосіб також можна використовувати для пошуку небажаних подій, що допоможе перешкодити виникненню цих подій.

Ефективність засобів захисту системи безпеки треба періодично перевіряти. Це здійснюють контролем і гнучкою перевіркою для гарантії, що засоби захисту функціонують і використовуються передбачуваним способом. Вихідні дані багатьох засобів захисту треба перевіряти на наявність вагомих для безпеки подій, наприклад, журналів, які є сигнальною звітною документацією. Загальна система функцій аудиту може надати корисну інформацію про перспективність захисту. Цю інформацію можна відповідно використовувати.

Плани відновлювання після уражень

Таке планування інформує щодо того, як поводитися й виконувати роботу, коли супровідні процеси, разом з системами інформаційних технологій, руйнуються чи стають недоступними.

Ці плани можуть передбачати звернення до можливих комбінацій з численних сценаріїв, що охоплюють:

- різноманітність періодів переривання;
- втрати різних типів засобів;
- повну втрату фізичного доступу до приміщень;

• що необхідно зробити для повернення до стану, що передував порушенню.

Плани відновлювання після нещасних випадків описують як відновити функціювання системи інформаційних технологій після небажаного інциденту та охоплюють:

критерії, за яких відбуваються катастрофи;

обов'язки щодо активізації дій з відновлювання;

відповідальність за різні дії відновлювання;

опис дій відновлювання.

10.4. Керування кібернетичною безпекою інформації

Результати аналізу об'єктів, які досліджуються, мають конструктивний характер, коли на їхній основі створюються теоретичні фізичні і математичні моделі об'єкта.

Теоретична модель об'єкта, який досліджується, – це сукупність знань, припущень і гіпотез, побудованих у вигляді цілісної логічно витриманої структури, яка відображає основні властивості та характеристики досліджуваного об'єкта, сформульована у термінах і символах, властивих цій науці і необхідних для вирішення цілого класу конкретних завдань.

Таким чином, фізична модель відображає взаємозв'язок і взаємодію фізичних складових з урахуванням фізичних законів досліджуваного об'єкта, а його математична модель – математичний компонент (функції, оператори).

Відомо, що, залежно від постановки завдань досліджень об'єкта, можуть використовуватися різні моделі. Разом з тим, одна математична модель може описувати певне коло досліджуваних об'єктів, різних за своєю фізичною природою.

Фізична модель досліджуваного об'єкта має задовольняти такі вимоги [16,17]:

• параметри моделі повинні мати реальний фізичний зміст, а їхні основні значення можуть бути отримані шляхом прямих або непрямих вимірів;

• має бути отримана і розроблена методика визначення характеристик параметрів моделі за даними вимірювань, спостережень;

• для математичних об'єктів моделі має бути вказаний клас допустимих операцій і відношень.

Аргументами фізичних і математичних моделей є просторові координати і час.

Відомо, що існує багато моделей для керування КБ інформаційних технологій. Моделі презентують концепції, необхідні для розуміння процесів керування захистом в інформаційних технологіях. Описувані моделі [19]:

залежності елементів КЗ;

залежності керування ризиком;

керування процесом КЗ інформаційних технологій.

Концепції, що їх попередньо презентують, і бізнесові цілі організації спільно формують плани, стратегії і методики для убезпечування інформаційних технологій організації. Зміна цілей має гарантувати, що організація буде здатна до ділової активності з допустимими рівнями ризику. Будь-який захист не може бути цілком ефективним, і тому важливо наперед планувати дії з відновлювання після небажаного інциденту і структурувати захист, щоб обмежити ступінь ушкодженості.

КБ системи інформаційних технологій є багатовимірною проблемою, яку розглядають у різних аспектах. Тому, щоб визначити і реалізувати загальну й чітку стратегію та методики КЗ інформаційних технологій, організація має брати до уваги всі доречні аспекти.

Іноді потрібно декілька засобів захисту, щоб звести залишковий ризик до припустимого рівня. У деяких випадках, коли ризик допустимий, немає потреби застосовувати засоби захисту, навіть якщо є загрози. В інших випадках уразливість може існувати, але не обов'язкова наявність відомих загроз щодо неї. Засоби захисту можуть забезпечувати контроль наявності загроз в оточенні, щоб запобігти ураженню у разі прояву загрози.

Обмеження впливають на вибір засобів КЗ.

Рисунок 8.1 ілюструє залежність між елементами захисту, тісно пов'язаними з керуванням ризиком. Для наочності відображені тільки основні залежності.

wop36AE.tmpMicrosoft Visio Drawing7.vsdx

Рис. 8.1. Залежність у керуванні ризиком.

(Напис на стрілці між будь-якими полями вказує на залежність між ними)

Рисунки 8.2, 8.3 та 8.4 відображають залежності між необхідними умовами захисту і загрозами, уразливостями і вартістю активів відповідно. На цих рисунках проілюстровано перспективи деяких підходів до керування захистом інформаційних технологій. Однак такі підходи можуть не враховувати деякі важливі аспекти.

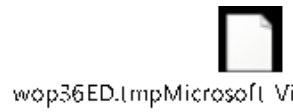


Рисунок 8.2. Залежності у керуванні ризиком у аспекті загроз

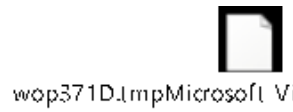


Рисунок 8.3. Залежності у керуванні ризиком у аспекті вразливостей

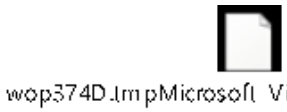


Рисунок 8.4. Залежності у керуванні ризиком у аспекті ураження

Керування КБ інформаційних технологій є тривалим процесом, що має враховувати весь життєвий цикл системи безпеки (рис. 8.5).

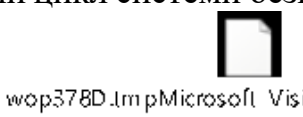


Рисунок 8.5. Керування процесом КЗ інформаційних технологій

Отже, вибір моделі залежить від конкретних вимог організації в цілому та інформаційної системи зокрема.

10.5. Архітектура систем кібернетичної безпеки інформації

Використання поняття «сутність» означає, що взаємодія в мережі може здійснюватися не тільки між людиною і інформаційною системою, але і між програмами, як такі виступають інтелектуальні агенти або віруси. При цьому [20,21]:

конфіденційність – властивість інформації бути недоступною або нерозкривною для неуповноважених осіб, сутностей або процесів;

аутентифікація – визначення джерела даних, тобто підтвердження того, що джерелом прийнятих даних є вказане в них джерело, а також як

визначення взаємодійної сутності, тобто підтвердження того, що взаємодійна сутність є тим, за кого вона себе видає (peer-entity);

цілісність – визначається як виявлення будь-яких модифікацій, вставок або видалень, що впливають на коректність інформації, зосередженої в інформаційному ресурсі та подаваної у двох формах – без встановлення мережного з'єднання і зі встановленням мережного з'єднання;

управління доступом – визначається як захист від неавторизованого використовування ресурсу, також як захист від використання ресурсу неавторизованим способом (цей рівень іноді плутають з рівнем аутентифікації);

контроль учасників взаємодії – визначається як захист від відмови однієї з сутностей, що беруть участь у взаємодії, від участі у всій взаємодії або її частині і зводиться до контролю учасників з перевіркою джерела, а також контролю даних з перевіркою доставки інформації.

Рисунок 8.6. Система кібернетичної безпеки

Прогрес у сфері ІКТ і глобальних комп'ютерних мереж привів до появи нових методів забезпечення інформаційної безпеки, які, враховуючи природні неточності пристроїв оцифровування і надмірність аналогового відео або аудіосигналу, дозволяють приховувати повідомлення в комп'ютерних файлах (контейнерах) або, на відміну від криптографії, приховувати сам факт передачі інформації.

Методи шифрування діляться на симетричні і асиметричні [21,22]:

- симетричні (з секретним ключем), використовується один і той же ключ як для шифрування, так і для дешифрування;
- асиметричні методи шифрування з відкритим ключем (public keys, PKI) припускають загальнодоступність ключа шифрування і закритість ключа дешифрування, який неможливо розкрити за ключем шифрування.

Найбільше розповсюдження отримали [23,24,25]:

- розроблена Циммерманом (Philip Zimmerman) безкоштовна (freeware) програма PGP (Pretty Good Privacy) для різних платформ, яка забезпечує шифрування пошти і файлів на основі існуючих криптосистем і криптографічних протоколів;
- алгоритми RSA (абревіатура від перших букв імен авторів – Rivest, Shamir і Alderman, 1977 р.) – це система з відкритим ключем, призначена як для шифрування, так і для аутентифікації, заснована на складності розкладання дуже великих цілих чисел на прості співмножники;

• алгоритми IDEA (International Data Encryption Algorithm, автори До. Lai і D. Massey, – шифр з 64-бітових блоків, що повторюються, з 128-бітовим ключем і вісьмома проходами (rounds), дешифрування якого виконується за тим же принципом, що і шифрування (безпека IDEA ґрунтується на використанні трьох несумісних типів арифметичних операцій над 16-бітовими словами);

• алгоритми DES (Data Encryption Standart) – розроблена IBM і затверджена у США в 1977 р. як офіційний стандарт система шифрування з симетричними ключами і 16-кратною перестановкою даних;

• MD5 (Message Digest Algorithm 5) – алгоритм хешування, розроблений компанією RSA Data Security, Inc., що використовується для хешування рядка байтів довільної довжини у 128-бітове значення.

В даний час методи шифрування активно використовуються при створенні електронного цифрового підпису.

Цифровий підпис (digital signature) – це блок даних, що згенерований з використанням деякого секретного ключа. Зараз використовуються три варіанти визначення цифрового підпису [22,25]:

1) перший варіант передбачає, що всі електронні підписи повинні відповідати законодавчим вимогам про підпис;

2) другий варіант передбачає, що електронний підпис має юридичну силу тільки в тому випадку, якщо він:

• дійсно належить особі, яка користується ним;

• може бути перевірений;

• знаходиться винятково під контролем особи, яка користується ним (електронні цифрові підписи, виготовлені з використанням шифрувальної криптографічної технології);

• пов’язаний з інформацією таким чином, що у разі зміни інформації, підпис втрачає силу;

3) третій варіант пов’язаний із загальною тенденцією міжнародного законодавства з питань цифрового підпису, направленою на ухвалення більш широкого і всеосяжного визначення електронного підпису на основі другого варіанта як більш нейтрального з технологічної точки зору, не унеможливлює застосування досконаліших технологій в майбутньому і не обмежує виконання підпису з використанням сучасної технології криптографії.

В Директиві ЄС використовується другий варіант і поняття «кваліфікованого електронного підпису», в якому говориться, що такий підпис, якщо він сертифікований і створений надійним способом, відповідає

законодавчим вимогам як і поставлений вручну підпис, може використовуватися як доказ у суді.

Не дивлячись на достатньо прозоре загальне означення, розвинуті країни світу дають цьому феномену своє визначення:

- у ФРН електронний підпис визначають як «створена за допомогою приватного ключа печатка до цифрових даних, яка за допомогою відповідного відкритого ключа, забезпеченого сертифікатом ключа підпису, виданим центром сертифікації або державною установою, дозволяє визначити власника ключа підпису і автентичність даних»;
- в Австрії – це «електронні дані, які додані до інших електронних даних або логічно сполучені з останніми і слугують для аутентифікації останніх або для ідентифікації особи, що поставила підпис» (закон локальної дії прийнятий 1 січня 2000 року);
- в США електронний підпис визначають як «електронний звук, символ або процес, приєднаний або логічно сполучений з контрактом або іншим документом (записом) і вироблений або прийнятий особою з метою підписання документа (запису)», а під «особою» розуміється «фізична особа, корпорація, комерційний траст, маєток, траст, партнерство, товариство з обмеженою відповідальністю, асоціація, спільне підприємство, урядове агентство, публічна корпорація, або будь-яка інша юридична або комерційна особа» (закон E-SIGN Act, діє з 30 червня 2000 року і розповсюджується на міжнародні транзакції);
- в російському законі електронний цифровий підпис розуміється як «послідовність символів, отримана в результаті криптографічного перетворення початкової інформації з використанням закритого ключа, що дозволяє користувачу відкритого ключа встановити цілісність і незмінність цієї інформації, а також власника закритого ключа»;
- в українському законі дано таке означення: «електронний цифровий підпис – сукупність даних, отриманих в результаті певного криптографічного перетворення якого-небудь набору даних, яка додається або логічно сполучена з цим набором даних і дає можливість підтвердити його цілісність, а також належність підпису особі, що його підписала». При цьому в українському законі не розкривається значення поняття «криптографічний» або «криптографія», що робить означення недостатньо чітким.

У зв’язку з цим відзначимо, що в Директиві ЄС виражений тільки намір підвищити надійність цифрового підпису без обмеження її рамками криптографії. Проте на практиці цифровий підпис документа звичайно створюється генерацією дайджесту повідомлення (message digest) з додаванням до нього службової інформації (кореспондент, адресат, час), а

потім шифрується секретним ключем того, хто підписує, з використанням того або іншого алгоритму. Зашифрований бітовий стек, що вийшов, і є цифровим підписом.

В цифрових підписах використовуються стандарти RSA для підпису і MD5 для обчислення дайджесту. Крім того, для генерації дайджесту повідомлення при створенні цифрового підпису використовуються криптографічні хеш- функції для відображення повідомлення у фіксований розмір (128 і більше бітів) хеш-значення (hash value) таким чином, що вся множина можливих повідомлень розподіляється рівномірно по множині хеш-значень. PGP також може забезпечувати шифрування повідомлень і цифрові підписи, використовуючи ZIP компресію, а також маскуючи координати і дані відправника, що трохи ускладнює процес аналізу трафіку.

Методи стеганографії (steganos – секрет, graphy – запис) забезпечують обмін інформацією з приховання самого факту комунікацій і є не альтернативою, а доповненням до криптографії. Суть стеганографічних методів полягає у вкладанні одних інформаційних об’єктів в інші інформаційні об’єкти (контейнери) таким чином, що б операція вкладання не спотворювала приховану інформаційну сутність і об’єкт-контейнер.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

- Які дії містить процес керування безпекою?
- Цілі безпеки, стратегії і методики.
- Перелічіть головні елементи, задіяні в процесі керуванням захистом.
- Охарактеризуйте поняття «залишковий ризик».
- Охарактеризуйте поняття «обмеження».
- Що собою являє налаштування системи?
- Які вимоги повинна задовольняти фізична модель об’єкта?
- Охарактеризуйте рисунки 8.2, 8.3, 8.4.
- Який основний документ визначає рівні архітектури інформаційної безпеки?
- Проаналізуйте основні моделі моніторингу.

РОЗДІЛ 11. АНАЛІЗ РИЗИКІВ У КІБЕРБЕЗПЕЦІ

11.1. Підходи до аналізування ризиків

Перед початком будь-якої діяльності, пов'язаної з аналізуванням ризи- організація повинна мати стратегію щодо здійснення цього аналізування, та її складові частини (методи, технології тощо) мусять бути відображені в методиці безпеки інформаційних технологій. Засоби і критерії для вибору методу аналізування ризиків потрібно погодити з вимогами організації. Стратегія аналізування ризиків має гарантувати, що обраний підхід відповідає оточенню і що він зосереджує зусилля захисту там, де вони необхідні.

Ефективне використання або звернення до детального аналізу всіх систем не є ефективними без врахування серйозності ризиків. Підхід, який забезпечує рівновагу між цими екстремальними показниками, передбачає аналіз посадовцями високих рівнів для встановлення потреб в захисті системи інформаційних технологій, а потім проведення докладного дослідження з урахуванням цих потреб. Потреби в захисті будь-якої організації будуть залежати від її розміру, виду ділової активності, який вона здійснює, її оточення і мікрополітики.

У деяких ситуаціях організація вирішує питання відносно застосування засобів захисту або призупинення їхньої дії на даному етапі. Таке рішення потрібно приймати тільки після того, як організація ретельно здійснить всі аналізи. Якщо таке рішення прийняте, адміністрація повинна знати всі потенціальні. Ризики і несприятливі ситуації й імовірність виникнення небажаного інциденту. Без цих відомостей організація може ненавмисно порушити закони або правила і може довести свою ділову активність до потенційного збитку. Рішення про пасивність або відкладання застосування засобів Хисту повинні бути прийняті тільки після того, як зроблено докладний розгляд цих та інших можливих несприятливих наслідків.

Між можливістю бездіяльності та визнанням множини ризиків невідомої величини і серйозності можна виділити чотири основних варіанти методики аналізування ризику:

- використання однакового основного підходу для всіх систем незалежно від ризиків, що стоять перед системами, і прийняття того, що рівень захисту ніколи не може бути відповідним;

- використання неформального підходу для аналізування кожного;.

- використання змішаного підходу для застосування початкового аналізу ризику високого рівня, щоб визначити системи інформаційних технологій з високим рівнем ризику і є критичними для ділової активності, з детальним аналізом ризику для цих систем і застосуванням основного підходу до всіх інших систем.

Ці різні можливості щодо напрямків ризиків безпеки обговорюються з подальшими рекомендаціями щодо переваги кожного підходу.

Якщо організація вирішує нічого не робити щодо захисту чи вкласти в реалізацію заходів захисту, адміністрація повинна знати можливі наслідки такого рішення. Хоча це не вимагає ні часу, ні грошей, ні персоналу, ні інших ресурсів, така пасивність все-таки має безліч недоліків. Якщо організація впевнена у безпечності своїх систем, вона може тривалий бути відкритою для серйозних впливів. Організація може бути в конфлікті законами та розпорядженнями, і її репутація може постраждати, якщо цей конфлікт спричинить порушення у захисті і це покаже, що не було ніякої попереджувальної роботи. Якщо організація мало турбується про захист, не має інших робочих перевіряючих систем, тоді це може бути життєвою стратегією. Однак така організація не знає, наскільки добрий чи поганий поточний стан безпеки, і для більшості організацій це навряд чи буде прийнятним рішенням.

Перший підхід полягає в тому, що організація за основу безпеки всіх інформаційних технологій систем вибирає стандартні засоби захисту.

Мета основного захисту полягає в тому щоб установити мінімальну кількість засобів захисту і захистити всі чи деякі системи організації. Використовуючи цей підхід, можна застосувати основний захист у всій організації, і, як відзначено вище, додатково використовувати докладний аналіз ризику для захисту систем з високими рівнями ризику чи систем, вирішальних для справи.

Відповідний основний захист можна забезпечити, використавши засоби захисту, які застосовуються для системи інформаційних технологій від найзагальніших загроз. Рівень основного захисту може бути відкоригований відповідно до потреб організації. Докладне оцінювання загроз, вразливостей і ризиків не потрібне. Усе, що треба зробити для здійснення основного захисту, - вибрати ті засоби захисту, що стосуються розглянутої системи інформаційних технологій. Після визначення засобів захисту основного у кожному місці можуть бути визначені засоби захисту, які потрібно конкретно використовувати.

Організація може, звичайно, також створити власну основу, установлюючи відповідність із типовим оточенням і з діловими цілями.

Є такі переваги використання цього підходу:

- потрібний мінімум витрат для детального аналізування ризику і керування під час забезпечення засобами захисту і менше часу і зусиль на вибір засобів захисту;

- основні засоби захисту є рентабельні, ті самі або подібні основні засоби захисту можуть бути легко пристосовані до багатьох систем, якщо багато систем організацій працюють у спільному оточенні і якщо потреби захисту порівнянні.

Може виникнути ускладнення в керуванні змінами, що залежать від захисту. Наприклад, якщо система модернізована, можуть виникнути труднощі у визначенні, чи є первинні основні засоби захисту, як і раніше, ефективними.

Недоліки цього підходу: якщо базовий рівень захисту визначено як дуже високий, то це може або занадто дорого коштувати, або не забезпечувати необхідного захисту деяких систем, а якщо основний рівень дуже низький, то може виявитися, що для деяких систем немає достатнього рівня захисту.

Якщо всі системи інформаційних технологій організації мають низький рівень необхідних вимог захисту, тоді це - найрентабельніша стратегія. У цьому випадку основа повинна бути відповідною рівню захисту, необхідному більшості систем інформаційних технологій. Більшість організацій завжди повинна буде вибирати деяку мінімальну кількість стандартів, щоб захистити секретні дані й узгодити із законами та розпорядженнями, наприклад, із законом захисту даних. Однак там, де системи організації відрізняються в діловій активності, розмірі і складності, цей підхід нелогічний і не рентабельно застосовувати загальний стандарт до всіх систем.

Другий підхід полягає в неформальному, прагматичному аналізуванні ризику всіх систем. Неформальний підхід базується не на структурованих методах, а на обізнаності і досвіді осіб. Якщо експертизу захисту не можна провести своїми силами, то залучають зовнішніх консультантів.

Перевага цього підходу - ефективність щодо вартості і часу. Немає потреби навчати виконувати неформальне аналізування і його проводять значно швидше, ніж детальне аналізування ризику. Отже, цей підхід ефективний з точки зору вартості і найбільше підходить для малих організацій.

Є, однак, ряд недоліків такого підходу:

- відсутність структурованого підходу збільшує імовірність неврахування деяких ризиків і сфер їхнього впливу;

- існує лише незначне мотивування вибору засобів захисту, отже, складно визначити витрати на них.

- може виникнути складність у керуванні безпекою під час змін без частого аналізування;

- відсутність формального підходу або вичерпного переліку ризиків збільшує імовірність пропустити деякі важливі деталі:

- підтвердження застосування засобів захисту від ризиків у цьому випадку ускладнюється;

- особи, що мають незначний досвід в аналізуванні ризиків, можуть мати мало інструкцій, які б допомогли їм у виконанні завдань;

- частина пропозицій у минулому керувалася уразливістю, тобто реалізовані засоби захисту ґрунтувалися на певній вразливості, без врахування можливості використання загрозою цієї вразливості, тобто без реальної потреби в засобах захисту;

- оскільки підхід є неформальним, результатам властива суб'єктивність поглядів і упередженість консультанта:

- виникають проблеми, якщо особа, що проводить неформальне аналізування ризику, іде з організації.

Ґрунтуючись на вищевикладених недоліках, цей підхід не вважається ефективним щодо виконання аналізування ризику для багатьох організацій.

Третій підхід полягає в докладних оцінках аналізування ризику всіх систем інформаційних технологій організації. Докладне аналізування ризику охоплює визначання та оцінювання активів, а також оцінювання рівнів загроз щодо інформації та її вразливості. Цю інформацію використовують ця визначання ризиків. Виконання цього аналізу ризику сприяє ідентифікуванню, вибору і впровадженню засобів захисту, скоригованих ідентифікованими ризиками стосовно інформації, а також знижує ці ризики до прийнятного визначеного рівня керування. Докладне аналізування ризику може бути ресурсомістким процесом і тому вимагає чіткого визначення меж і постійної уваги адміністрації.

Переваги цього підходу:

- визначають рівень захисту відповідно до вимог безпеки для кожної системи;

- додаткова інформація, отримана з детального аналізування ризику сприяє керуванню змінами, пов'язаними із захистом;

- висока імовірність того, що для всіх систем визначені відповідні засоби захисту;

Недоліки цього підходу:

- він вимагає багато часу, зусиль і спеціальних знань для одержана результатів;

- є ймовірність, що вимоги захисту небезпечної системи будуть враховані надто пізно;

- усі системи інформаційних технологій треба розглядати докладно, і буде потрібно багато часу, щоб завершити аналізування.

Четвертий підхід насамперед ідентифікує ті системи, які мають підвищений ризик або є критичними щодо ділової активності, і передбачає високорівневе аналізування ризику. Ґрунтуючись на отриманих при цьому результатах, системи поділяються на ті, які потребують докладного аналізування ризику для досягнення відповідного захисту, і ті, для яких є достатнім базовий захист.

Цей підхід - комбінація кращих положень, описаних вище підходів. **Таким** чином він забезпечує рівновагу та мінімізацію часу і зусиль, що їх витрачають на ідентифікацію засобів захисту, щоб гарантувати відповідну захищеність усіх систем.

Додаткові переваги цього підходу:

- поєднання на початку швидкості і простоти підходу підвищує імовірність приймання програми аналізування ризиків;

- можливість швидко отримати уявлення про стратегію програми захисту в організації, що може сприяти покращенню планування;

- є можливість побудови безпосередньої стратегічної картини програми безпеки організації, яку можна використовувати під час планування;

- ресурси і кошти можуть бути спрямовані на одержання максимальної вигоди, і системи з імовірно найбільшою потребою в захисті можуть бути враховані на ранніх стадіях;

- наступні дії будуть успішнішими.

Недоліки цього підходу: якщо високорівневий аналіз ризику дає неточні результати, то деяким системам, для яких необхідне докладне аналізування ризику, не буде приділено належної уваги. Звичайно, така ситуація малоймовірна, якщо результати аналізування ризику відповідно перевірені, але в будь-якому випадку такі системи все ж повинні додатково підтримуватися базовими засобами захисту.

У більшості випадків цей підхід є найрентабельнішим рішенням, і його Рекомендовано до застосування більшістю організацій.

11.2. Аналіз активів організацій

Докладне аналізування ризику для системи інформаційних технологій містить визначення структури ризиків і оцінку їхніх величин. Необхідність у докладному аналізуванні ризику може бути визначена без зайвих витрат часу і коштів, коли огляди високого рівня проводять для всіх систем, які супроводжуються докладним аналізом ризику тільки високого рівня чи вирішальних систем.

Аналізують ризик визначанням потенційних несприятливих уражень, небажаних подій і ймовірності їхньої появи. Небажані події можуть впливати на ділову активність службовців чи на будь-який цінний об'єкт організації. Несприятливе ураження в результаті небажаного випадку - складова частина можливих збитків, пов'язаних із значенням активів і їхніх ризиків. Імовірність появи уражень залежить від того, наскільки привабливі активи для потенційного нападника, від імовірності появи загроз і легкості, з яким уразливість можна використати. Привабливими активами організації можуть бути:

- програмне забезпечення, в тому числі прикладне (наприклад, програми обробки тексту, програми, розроблені для спеціальних цілей);

- апаратура зв'язку (наприклад, телефони, мідний кабель, скловолокно);

- програмно-апаратне забезпечення (наприклад, гнучкі диски, стійка пам'ять на компакт-диску (CD ROM), програмовані ROM);

- документи (наприклад, контракти);

- виготовлені товари;

- служби (наприклад, інформаційні служби, обчислювальні ресурси);

- оточення;

- персонал;

- імідж організації.

Всі активи у встановлених межах огляду повинні бути зафіксовані і навпаки, будь-які активи, що їх вилучають з огляду за будь-якої причини повинні бути вміщені в інший огляд, для впевненості, що їх не забудуть і пропустять.

Наявність відповідного керування активами важлива для забезпечення успіху організації і є головною рисою всіх рівнів керування. До активів організації належать:

- фізичні об'єкти (апаратне забезпечення, засоби зв'язку, будівлі

- інформація або дані (документи, бази даних);

- програмне забезпечення;

- здатність виробляти деяку продукцію чи надавати послуги;

- людські ресурси;

- нематеріальна власність (символіка).

Більшість із цих активів мають потребу в захисті. У випадку, коли активи не мають належного рівня захищеності, необхідно застосовувати до них механізми оцінювання ризиків.

Якщо йдеться про перспективність програми безпеки організації, має сенсу забезпечувати захист і здійснювати його подальшу підтримку, чітко не визначені активи організації. У більшості випадків процес ідентифікації активів і визначання їхніх розмірів можна виконати на досить високому рівні і без дорогого, детального і тривалого аналізу. Рівень деталізації для аналізу визначають значеннями часу і вартості аналізу стосовно цінності вів. У будь-якому випадку рівень деталізації визначають, виходячи з цілей хисту. Зокрема, ці підходи можна застосовувати до груп активів.

Розглядають такі характеристики активів, як їхня цінність або критичність і різноманітність застосовуваних засобів захисту. Необхідність застосування засобів захисту до активів визначають також їхньою вразливістю до впливу специфічних загроз. Якщо ці аспекти очевидні для власника активів їх треба зафіксувати на початкових стадіях. Оточення і мікрополітика, у яких діє організація, можуть впливати на активи та їхні характеристики. Наприклад - мікрополітика організації може розглядати як дуже важливі завдання захисту особистої інформації. У діяльності міжнародних організацій і їхніх систем інформаційних технологій вагому роль відіграють оточення і мікрополітика.

Активи є об'єктами для багатьох видів загроз.Різноманітні загрози чи їхній прояв у різних місцях можуть постійно завдавати великої шкоди. Якщо шкода, заподіяна загрозою, є постійною, то можна використовувати універсальний, визначений підхід. Однак якщо обсяги заподіяної шкоди змінюються в широких межах, необхідно використовував конкретизований підхід, що відповідає локалізації загрози.

Вихідні дані для оцінювання загрози треба отримувати від власників чи користувачів, від фахівців із планування і фахівців інформаційних технологій, від фахівців, відповідальних за захист в організації. Перелік можливих загроз може виявитися корисним під час оцінювання загрози. Перелік наведено нижче.

У разі використання переліків загроз чи більш ранніх оцінювань загроз потрібно знати, що загрози постійно модифікуються, особливо якщо ділове оточення чи інформаційні технології змінюються. Наприклад, сьогоднішні віруси значно складніші ніж були декілька років тому. Цікаво, що реалізація засобів захисту, таких як перевірка на наявність вірусу, майже завжди веде до розробки нових вірусів, що мають імунітет до поточних засобів захисту. Після визначення джерела загрози (хто і що викликало загрозу її спрямованості (тобто на які елементи системи може вплинути загроза, необхідно визначити імовірність виникнення загрози. У цьому випадку потрібно брати до уваги:

- частоту загроз (як часто вони можуть виникати, спираючись на довідкові - статистичні дослідження та інше), якщо статистичні дослідження існують;

- мотивацію, усвідомлені можливості і здатності, ресурси, доступні потенційним нападникам, і привабливі моменти та вразливості активів системи інформаційних технологій для потенційного нападника і навмисних джерел загрози;

- географічні чинники, такі як близькість до хімічних чи нафтових заводів, можливість появи критичних метеорологічних умов, і чинники, що можуть впливати на людські помилки і несправність устаткування, випадкові джерела загрози.

Залежно від ступеня точності може виникнути необхідність розбивати активи на складові і установлювати зв'язки загроз із складовими. Наприклад, у фізичних активах можуть спочатку розглядати «центральні сервери даних», а коли визначено, що ці сервери перебувають у різних місцях, то розглядають окремо «центральний сервер даних 1» і «центральний сервер даних 2», тому що можуть бути дещо різні загрози і з різними впливами. Так само програмні активи можна спочатку розцінювати як «прикладне програмне забезпечення», а пізніше розбити на кілька видів «прикладного програмного забезпечення». Прикладом стосовно активів даних може слугувати початкове визначення як

«кримінального досьє», а пізніше поділ на «текст кримінального досьє» і «зараження до кримінального досьє».

У разі завершення оцінювання загроз буде отримано перелік ідентифікованих загроз, активів чи груп активів, на які загрози можуть впливати, і оцінок ймовірностей появи загроз у градації «високо», «середньо» чи «низько».

11.3. Побудова моделей загроз

Необхідно здійснити аналіз об'єктів захисту, ситуаційний план умов функціонування організації, оцінити ймовірність прояву загроз та очікувану шкоду від їхньої реалізації, підготувати засадні дані для побудови окремої моделі загроз.

Обстеження має бути проведено комісією, склад якої визначається відповідальною за технічний захист інформації особою і затверджується наказом керівника організації.

У ході обстеження необхідно:

- провести аналіз умов функціонування організації, її розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;

- дослідити засоби забезпечення інформаційної діяльності, які мають вихід за межі контрольованої території;

- визначення схеми і системи життєзабезпечення організації (електроживлення, заземлення, пожежної та охоронної сигналізації тощо), а також інженерних комунікацій та металоконструкцій;

- дослідити інформаційні потоки та технологічні процеси обробки інформації;

- визначення наявності та технічний стан засобів забезпечення технічного захисту інформації;

- перевірити наявність в організації нормативних документів, які забезпечують функціонування системи захисту інформації з обмеженим доступом, організацію проектування будівельних робіт з урахуванням вимог

технічного захисту інформації, а також нормативної та експлуатаційної документації яка забезпечує інформаційну діяльність;

- виявлення наявності транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, проводів тощо;

- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтажу;

- визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів технічного захисту інформації.

Матеріали обстеження необхідно використовувати під час розробки окремої моделі загроз, яка має включати:

- генеральний та ситуаційний план організації, схеми розташування засобів і систем забезпечення інформаційної діяльності, а також інженерних комунікацій, які виходять за межі контрольованої території;

- схему та опис каналів витоку інформації, каналів спеціального впливу і шляхи несанкціонованого доступу до інформації з обмеженим доступом;

- оцінку шкоди, яка передбачається від реалізації загроз.

Розглянемо приклад, коли джерелами загроз можуть бути навмисні або ненавмисні дії юридичних і фізичних осіб. Загрози можуть здійснюватися:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали:

• побічними електромагнітними випромінюваннями і наводками (електромагнітні випромінювання, що утворюються під час роботи засобів забезпечення інформаційної діяльності під впливом електричних і магнітних полів, на випадкові антени у процесі акусто-електричних перетворень, під час виконання азитивної високочастотної генерації та паразитної модуляції шляхом взаємного впливу кіл технічних засобів, призначених і не призначених для обробки інформації з обмеженим доступом, і кіл електроживлення,

електроосвітлення, сигналізації та управління, під час хибних комутацій і несанкціонованих дій користувачів);

• акустичними, лазерно-акустичними каналами (випромінювання звукового та ультраразвукового діапазонів частот);

• оптичними (електромагнітні випромінювання інфрачервоного, видимого та ультрафіолетового діапазонів частот);

• радіо-, радіотехнічними (електромагнітні випромінювання в діапазоні радіочастот);

• хімічними (хімічні речовини різної природи, що використовуються як сировина, утворюються в нових технологічних процесах, під час розробки нових матеріалів, проведення випробувань спеціальної техніки та виробів і містяться у навколишньому середовищі);

• іншими (радіаційними, магнітометричними тощо);

- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

- несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування підкладних пристроїв чи програм та вкорінення вірусів (рис. 11.1).

В деяких випадках в якості носія інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або змін фізичних властивостей носія.

Опис загроз і схематичне подання шляхів їхнього здійснення становлять окрему модель загроз. При аналізі загроз використовуються три терміни: загрози, вразливі місця і захист інформації.

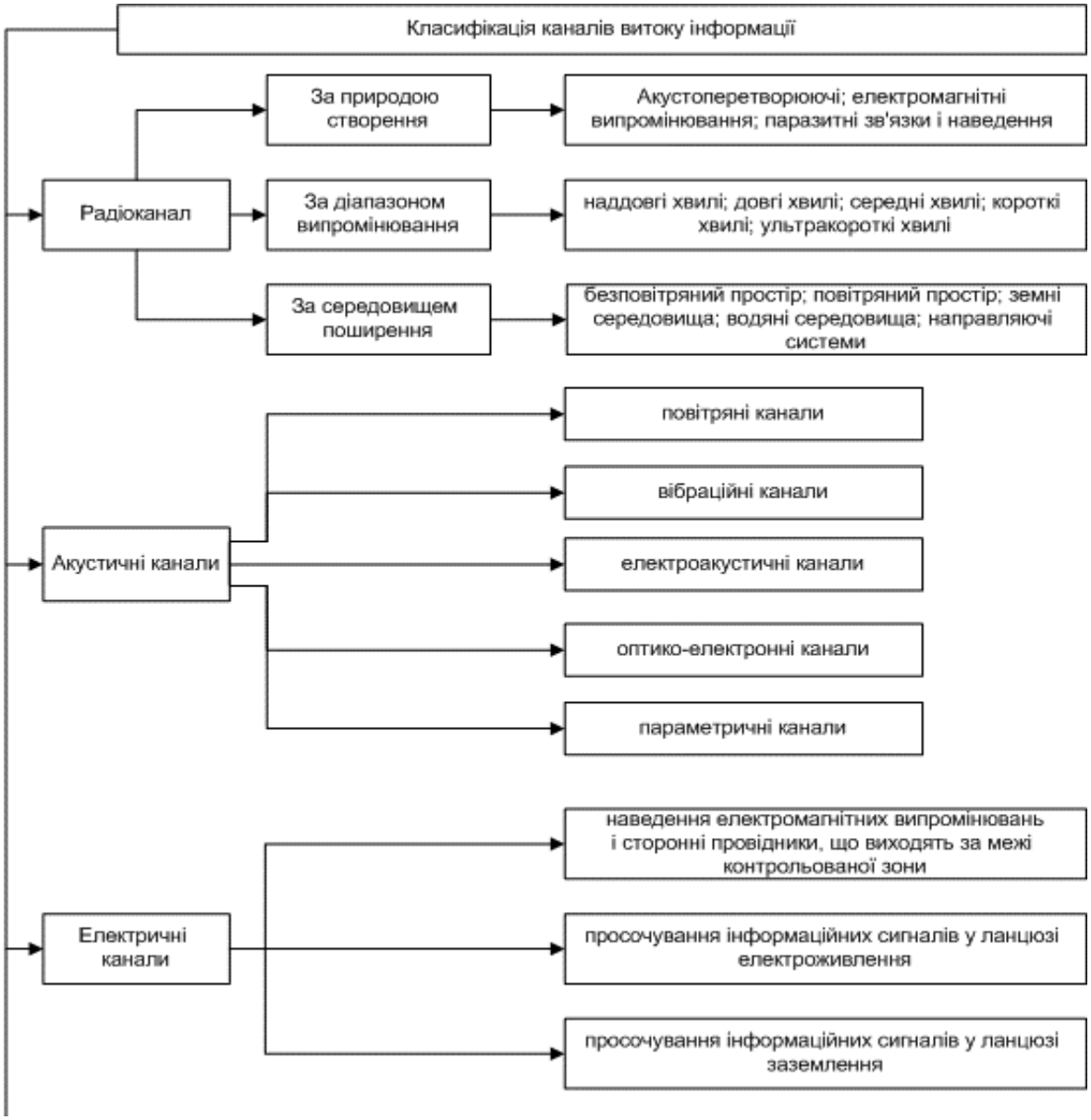

Класифікація каналів витоку інформації
Радіоканал
За природою створення
Акустоперетворюючі; електромагнітні випромінювання; паразитні зв'язки і наведення
За діапазоном випромінювання
наддовгі хвилі; довгі хвилі; середні хвилі; короткі хвилі; ультракороткі хвилі
За середовищем поширення
безповітряний простір; повітряний простір; земні середовища; водяні середовища; направляючі системи
Акустичні канали
повітряні канали
вібраційні канали
електроакустичні канали
оптико-електронні канали
параметричні канали
Електричні канали
наведення електромагнітних випромінювань і сторонні провідники, що виходять за межі контрольованої зони
просочування інформаційних сигналів у ланцюзі електроживлення
просочування інформаційних сигналів у ланцюзі заземлення

Рис. 11.1 Канали витоку інформації

Загрози з'являються тому, що існують системи або процеси, а не тому, що є якісь конкретні їхні недоліки. Так загроза пожежі існує для всіх приміщень незалежно від обсягу проведених на них протипожежних заходів. Загрози безпеки інформаційній системі можуть бути пов'язані з працівником (порушником), об'єктом (несправне обладнання або програмне забезпечення) або подією (пожежа, землетрус, зсув тощо).

На рис. 11.2 наведено варіант структурованої бази потенційних загроз для інформації, яка базується на наведених вище обґрунтуваннях.

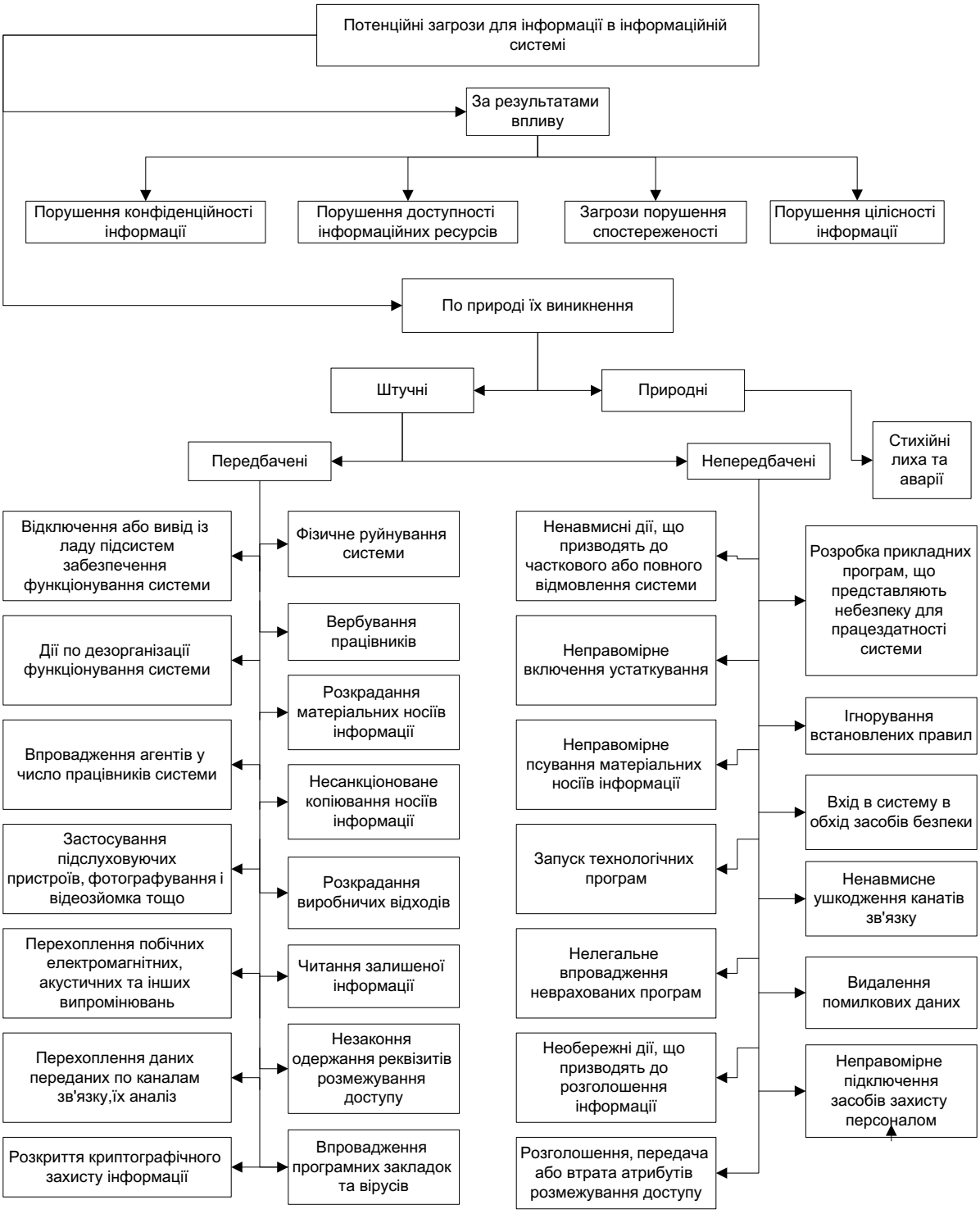


Рис. 11.2. Структурована база потенційних загроз для інформації в інформаційній системі

Для виділення типових уразливих місць в інформаційних системах можливо скористатися описом її протоколів обміну на основі еталонної моделі взаємозв'язку відкритих систем у виді ієрархії взаємодії прикладних процесів, що складаються з семи рівнів:

- фізичного - керування фізичним каналом;
- канального - керування інформаційним каналом;
- мережного - керування мережею;
- транспортного - керування передачею;
- сеансового - керування сеансом;
- представницького - керування представленням;
- прикладного - програми користувачів.

У цьому зв'язку можна виділити такі напрямки впливів:

- крадіжка цифрових носіїв;
- крадіжка результатів видачі (документів);
- зловмисні дії користувача програми;
- несанкціонований віддалений доступ;
- помилки в роботі користувачів чи програмно- технічного засобу;
- використання ліній зв'язку не за призначенням (перехоплення);
- неправильна робота ліній зв'язку (підробка).

Підходи до виявлення загроз

Різні підходи у виявлені загроз безпеці інформації в інформаційних системах наведено в табл. 11.1, з погляду еталонної моделі взаємозв'язку критих систем.

Т а б л и ц я 11.1

Різні підходи до виявлення загроз безпеці інформації в інформаційних системах з погляду еталонної моделі взаємозв'язку відкритих систем

	Рівні еталонної моделі взаємозв’язку відкритих систем						
Загрози безпеки інформації	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Землетруси	+	+	+	+	+	+	+
Пожежі	+	+	+	+	+	+	+
Урагани	+	+	+	+	+	+	+
Електромагнітні бурі	+	+	+	+	+	+	+
Радіозаглушуючі лінії зв'язку	+	+					
Віруси					+	+	+
Спеціальні програмно-технічні впливи			+		+	+	+
Вбудовані дефекти			+				
Руйнування	+	+	+	+	+	+	+
Підробка			+				+
Розсекречування						+	+
Дешифрування		+				+	+
Декодування						+	+
Перехоплення інформації		+	+	+	+	+	+
Крадіжка інформації і її носіїв						+	+
Втрата			+	+			+
Неправомірні ДІЇ					+	+	+
Помилка в роботі							+
Затримка інформації	+	+	+	+	+		
Інформаційне заглушування						+	+
Порушення доступу законних користувачів						+	+

Побічні електромагнітні випромінювання і наведення	+	+				+	

Користуючись цією таблицею, можна побудувати модель загроз для кожної конкретної організації.

Як порушник розглядається особа, яка може одержати доступ до інформації з включеними до складу інформаційної системи засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами інформаційної системи. Виділяють чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає функціональні можливості попереднього:

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

- другий рівень визначається можливістю створення і запуску цих програм з новими функціями обробки інформації;

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

- четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів інформаційної системи, аж до включення до складу інформаційної системи власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник - це фахівець вищої кваліфікації, який має повну інформацію про інформаційну систему і комплекс засобів захисту.

У кожному конкретному випадку, виходячи з конкретної технології обробки інформації, може бути визначена модель порушника, що є адекватною

реальному порушнику для визначеної інформаційної системи. При розробці моделі порушника визначається:

- припущення про категорії осіб, до яких може належати порушнику;

- припущення про кваліфікацію порушника і його технічну оснащеність (про використані для здійснення порушення методи і засоби);

- припущення про мотиви дій порушника (цілі, які переслідує рушник);

- обмеження та припущення про характер можливих дій порушників.

Стосовно інформаційної системи порушники можуть бути внутрішніми (з числа персоналу системи):

- користувачі (оператори) системи;

- персонал, що обслуговує технічні засоби;

- співробітники підрозділу розробки і супроводу програмного забезпечення (прикладні та системні програмісти);

- технічний персонал, що обслуговує приміщення (прибиральники, електрики, сантехніки та інші працівники, що мають доступ у приміщення, де розташована автоматизована система);

- керівники різних рівнів посадової ієрархії, або зовнішні (сторонні особи):

- відвідувачі (запрошені з будь-якого приводу);

- представники організацій, що взаємодіють з питань забезпечення життєдіяльності установи (енергопостачання, водопостачання, теплопостачання);

- представники конкуруючих організацій або особи, що діють за їхнім завданням;

- особи, що випадково або навмисно порушили пропускний режим (без мети порушення безпеки інформаційної системи);

- будь-які особи за межами контрольованої території.

Можна виділити три основні мотиви порушень: безвідповідальність, самоствердження, корисливий інтерес.

Усіх порушників можна класифікувати в такий спосіб.

За рівнем знань про інформаційну систему:

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

- має високий рівень знань та досвід роботи з технічними засобами системи і їхнього обслуговування;

- має високий рівень знань у галузі програмування, проектування та експлуатації інформаційних систем;

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

За рівнем можливостей (використаним методом і засобом):

- застосовуючи агентурні методи оволодіння відомостями;

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

- використовуючи тільки штатні засоби та недоліки системи захисту її подолання (несанкціоновані дії з використанням дозволених засобів), а

також компактні магнітні носії інформації, що можуть бути потай пронесені через охорону;

- застосовуючи методи та засоби активного впливу (модифікація і підохочення додаткових технічних засобів, підключення до каналів передачі даних. Упровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).

За часом дії:

- у процесі функціонування інформаційної системи (під час роботи опонентів системи);

- у період неактивних компонентів системи (у неробочий час, під час планових перерв, перерв з метою обслуговування і ремонту тощо);

- як у процесі функціонування інформаційної системи, так і в період активності компонентів системи.

За місцем дії:

- без доступу на контрольовану територію організації;

- із контрольованої території без доступу у приміщення;

- усередині приміщень, але без доступу до технічних засобів інформаційної системи;

- із робочих місць кінцевих користувачів інформаційної системи;

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

- із доступом у зону керування засобами забезпечення безпеки системи.

Класифікаційна модель порушника для інформації в інформаційній системі наведена на рис. 11.3.

Визначення конкретних значень характеристик можливих порушників у значній мірі є суб'єктивним. Модель порушника, побудована з урахуванням особливостей конкретної предметної області та технології обробки інформації може бути представлена перерахуванням декількох варіантів його виду. Кожен вид порушника має бути охарактеризований значеннями характеристик, приведених вище. Методи перевірки отриманих моделей, їхньої відповідності до реальної системи і порядок визначення потенційно вразливих місць у систем обов'язковим, при створенні моделі. Так помилки персоналу можуть становиш 55%, нечесні співробітники - 10%, скривджені особи - 9%, зовнішній напад 1..3%, віруси - 4%, проблеми фізичного захисту (стихійні лиха, порушення й електроживлення (зниження або підвищення напруги, коливання потужності опалення тощо) - 20%. Не самі інформаційні системи пишуть віруси, викрив-люють дані, викрадають важливу інформацію і обладнання.

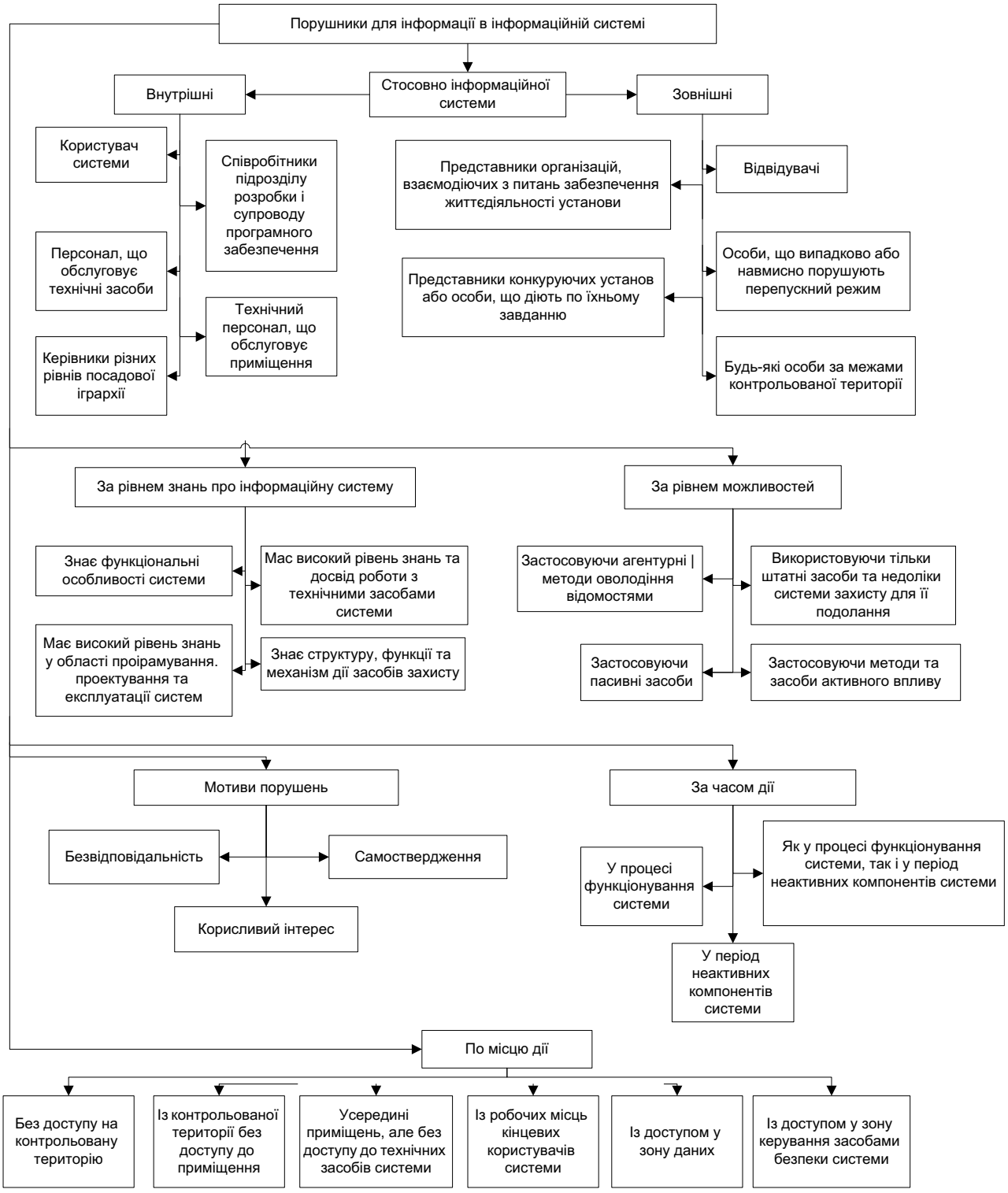


Рис. 11.3. Класифікаційна модель порушника в інформаційній системі

11.4. Аналіз функціонування інформаційної системи

При аналізі функціонування інформаційних систем потрібно розглядати всі можливі варіанти комбінацій, загроз на основі використання їхнього об'єднання та перерізу. Так, наприклад, для інформаційної системи обробки інформації з обмеженим доступом задано конкретний скінченний вектор загроз

$$X_n = (x_1, \ldots, x_n), n \in N \quad (11.1)$$

де {x} - множина потенційних загроз різного характеру, N - натуральна множина чисел.

Тоді аналіз функціонування такої інформаційної системи базується на розв'язанні таких операторних рівнянь:

$$y_k = L_k\left[\bigcup_{i=1}^{m} x_i, \bigcap_{j=1}^{q} x_j\right], k \in N \quad , \quad (11.2)$$

де

- $У_к$ - це відгук інформаційної системи при вхідній дії об'єднання $\bigcup_{i=1}^{m} x_i$ та перетину $\bigcap_{j=1}^{q} x_j$ потенційних загроз

L_k {.} - відповідний оператор дії інформаційної системи на вказану комбінацію вхідних потенційних загроз.

Сучасні інформаційні системи обробки інформації з обмеженим доступом є адоптованими до різних комбінацій потенційних загроз, тому їх функціонування можна описати певною послідовністю відповідних операторів дії у залежності від конкретної комбінації вхідних потенційних загроз.

У більшості випадків математичні моделі потенційних загроз є випадковими але бувають випадки, коли вони - детерміновані, інтегральними диференційними операторами. Тому методологія аналізу функціонування інформаційної системи є статистичною.

При створенні інформаційних систем обробки інформації з обмежуваним доступом аналіз оперативних рівнянь є певним станом, результати якого дають можливість сформулювати рекомендації забезпечення захисту інформації з подальшою їхньою реалізацією у конкретній інформаційній системі, на основі деталізації технічних характеристик розробки структури системи використання відповідної елементної бази, засобів обчислювальної техніки і т.д.

Витрати на систему захисту інформації з обмеженим доступом в інформаційній системі від несанкціонованого доступу необхідно зіставляти і приводити у відповідність з цінністю інформації, що захищається, та інших інформаційних ресурсів, що підлягають захисту, а також із збитками, що можуть бути завдані несанкціонованим доступом.

Варто відзначити, що для досягнення поставленої мети несанкціонованих дій зловмисники використовують не одну, а деяку сукупність загроз.

Зупинимось на основних етапах оцінки дій загроз в інформаційних системах обробки інформації, які мають чітку логічну послідовність у часі при вирішенні складних науково-технічних проблем, до яких належить і проблема захисту інформації в інформаційних системах.

Етап розробки фізичних і математичних моделей потенційних загроз і досліджуваних інформаційних систем.

Методологія проведення етапу теоретичних досліджень базується на:

- обґрунтуванні і постановці завдань;
- виборі методів вирішення завдань;
- аналізі результатів теоретичних досліджень.

Етап імітаційних досліджень, як правило, зводиться до комп'ютерного моделювання.

Етап моделювання по суті є основним етапом аналізу функціонування інформаційної систем обробки інформації, при цьому моделюється та оцінюється дія загроз для всіх можливих підсистем захисту інформації

Методологія і результати моделювання визначають цінність сучасник новітніх інформаційних технологій, розробкою яких на сьогодні займаються дослідники і фахівці всіх розвинених країн світу. Для сучасних інформаційних технологій, характерним є:

- методологія їхнього створення базується на використанні результатів фундаментальних теоретичних досліджень та інформації з обмеженим доступом;

- адаптація до широкого кола автоматизованих систем;

- значна фінансова вартість використання таких високоінтелектуальних технологій.

Етап створення інформаційних систем є найтривалішим за часом, комплексним за своїм змістом.

Відмітимо лише деякі характерні особливості виконання цього етапу:

- на основі отриманих теоретичних результатів і моделювання об-ґрунтовується структура конкретної системи із заданими інформаційними і технічними характеристиками;

- специфіка функціонування кожної системи визначається класом завдань, які розв'язуються такою системою в основному на базі розробки програмного математичного забезпечення;

- завдання захисту інформації при створенні системи є одним з головних і в основному визначають специфіку, цінність, адаптацію до загроз самої системи.

На етапі налагодження, випробувань і введення в експлуатацію інформаційних систем є можливість формування бази знань функціонування розробленної системи з метою визначення життєвого циклу системи на основі:

- розрахунків характеристик надійності;

- розробки методології регламентних і ремонтних робіт;

- створення відповідних баз даних вимірювань поточних характеристик і параметрів механізмів, пристроїв системи;

- методик прогнозу стану системи та інших.

Завдання аналізу дій загроз в інформаційних системах.

База знань функціонування інформаційної системи обробки включають складову компоненту бази знань захисту інформації.

Необхідно відмітити, що до завдань захисту інформації відносяться класичні завдання виявлення корисних сигналів при дії перешкод, завдання визначення їхніх характеристик, завдання розпізнавання.

Як правило, для вирішення таких завдань використовуються статистичні методи теорії випадкових процесів і математичної статистики.

Найбільш обґрунтований підхід до аналізу функціонування інформаційної системи зводиться до аналізу такої структурної схеми

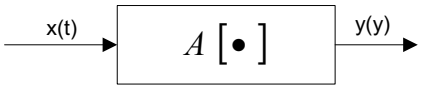


Рис. 11.4. Структурна схема еквівалентної системи

де, x(t),t є T - вхідна дія;

A[.] - оператор перетворення вхідної дії;

y(t) **-** відгук оператора.

Але на практиці у залежності від рівня деталізації практична структурна схема аналізу досліджуваної системи має такий вигляд

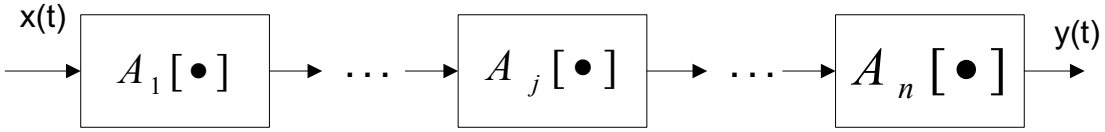


Рис. 11.5. Практична структурна схема системи

Таким чином, на практиці аналіз функціонування системи зводиться до аналізу перетворення вхідної дії x(t) складовим оператором

$$A[\cdot]=A_1[\cdot]\dots A_j[\cdot]\dots A_n[\cdot]=\prod^n A_j[\cdot] \quad (11.4)$$

У якості прикладу розглянемо лінійну систему з двох лінійних функцій, які описуються відповідними імпульсними перехідними функціями $\{\varphi_j(t), j=1,2\}$ і мають постійні у часі параметри, тобто

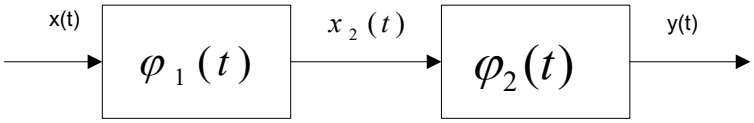


Рис. 11.6. Структурна лінійної системи

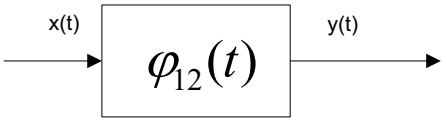


Рис. 11.7. Структурна схема еквівалентної лінійної системи

Відповідні співвідношення опису відгуку лінійної системи мають такий вид

$$x_1(t)=\int_{-\infty}^{\infty}\varphi_1(t-\tau)x(\tau)d\tau,$$

$$x_2(t)=\int_{-\infty}^{\infty}\varphi_2(t-\tau)x_1(\tau)d\tau=$$

$$=\int_{-\infty}^{\infty}\varphi_2(t-\tau)\int_{-\infty}^{\infty}\varphi(\tau-s)x(s)d\tau ds=\int_{-\infty}^{\infty}\varphi_{\Delta 2}(t-\tau)x(\tau)d\tau,$$

де $\varphi_{12}(t)=\int_{-\infty}^{\infty}\varphi_2(t-\tau)\varphi_1(\tau)d\tau$

для n-модульної лінійної системи маємо

$$\varphi_{L..n(t)=\int_{-\infty}^{\infty}\cdots} \int_{-\infty}^{t-\tau_1-\cdots-\tau_{n-2}} \int_{-\infty}^{t-\tau_1-\cdots-\tau_{n-2}} \varphi_n(t-\tau_1 - \cdots \tau_{n-1})\, \varphi_{n-1}(\tau_{n-1}) \ldots \varphi_1(\tau_1) d\tau_{n-1} \ldots d\tau_1$$

У більшості випадків оператор (11.4) складається з лінійних і нелінійних операторів відповідних модулів інформаційної системи.

Наведений приклад підтверджує факт використання класичних результатів теорії сигналів і систем для аналізу інформаційних систем обробки сигналів.

Основні завдання оцінки дій загроз в інформаційних системах обробки інформації можна умовно поділити на дві групи, які тісно взаємно пов’язані між собою, а саме:

А) завдання аналізу функціонування інформаційної системи у відповідності загроз;

Б) завдання аналізу функціонування інформаційної системи за наявності загроз.

Коло завдань групи Б) значно ширше у порівнянні із завданнями групи А), але саме результати розв'язку задач групи А) є необхідною умовою отримання оцінки дії загроз. Розглянемо принципово нові завдання групи Б).

Обґрунтувати множину потенційних загроз і визначити імовірні шляхи і методи їхньої реалізації на основі результатів аналізу функціонування конкретної інформаційної системи: класу основних задач і галузей використання результатів їхнього розв'язку; специфіки і характеру досліджуваної інформації; рівня конфіденційності інформації; оцінки умовної цінності інформації у технічному і економічному аспектах. Обґрунтувати і розробити фізичні і математичні моделі потенційних загроз, визначити їхні основні характеристики, базуючись на опублікованих результатах досліджень.

У більшості випадків моделі загроз описуються випадковими функціями. Наприклад, неоднорідний пуасонівський випадковий процес з незалежними

приростами може описувати певну послідовність появи загроз, які відбуваються випадково за часом й за інтенсивністю.

Завдання випадкових моделей загроз базується на визначенні послідовності скінченних вимірів. У більшості випадків на практиці обмежуються аналізом досліджуваних випадкових процесів у рамках кореляційної теорії. При цьому використовується одномірна і двовимірна функція розподілу досліджу вального випадкового процесу. Як правило, вибір того чи іншого закону розподілу ймовірностей формується як та чи інша статистична гіпотеза, підтвердження якої обґрунтовується результатами статистичної обробки даних вимірів досліджуваної загрози. По суті, задача ідентифікації досліджуваної загрози зводиться до обчислення статистичної оцінки її характеристик, параметрів на основі обробки даних вимірів і підтвердження статистичної гіпотези приналежності моделі загрози до відповідного класу випадкових процесів, наприклад, гаусівського, стаціонарного, періодичного, лінійного та інших. При заданих характеристиках, параметрах моделей і пристроїв інформаційної системи, моделей загроз, аналізуються дії у рамках проведення:

- теоретичних досліджень;

- моделювання;

- статистичної обробки даних вимірювань експериментальних досліджень на основі постановки відповідних задач, обґрунтування застосування методів їхнього розв'язку і отримання результатів розв'язку задач.

Аналіз отриманих результатів дає можливість оцінити технічні, економічні витрати від здійснення загроз.

Результати розв'язку послідовності задач, наведених вище, дають можливість приступити до вирішення складної науково-технічної проблеми захисту інформації у досліджуваній інформаційній системі.

Нижче наведено приклади вразливостей в різних зонах захисту, висновки з аналізу загроз в інформаційних системах, включаючи приклади загроз, що

могли б скористатися цими вразливостями. Ці приклади можна використовувати як довідкову інформацію в процесі оцінювання вразливостей. Варто також підкреслити, що в деяких випадках інші загрози також можуть використовувати ці вразливості.

Оточення та інфраструктура:

- відсутність фізичного захисту будівель, дверей і вікон (може використовувати, наприклад, загроза злодійства);

- недостатнє чи недбале використання фізичного контролю за доступом до будівель, кімнат (може використовувати, наприклад, загроза навмисного пошкодження);

- нестійкість енергосистеми (може використовувати, наприклад, загроза нестабільності енергоживлення);

- розташування в зоні ймовірного затоплення (може використовувати, наприклад, загроза затоплення).

Апаратні:

- відсутність графіка періодичної заміни (може використовувати, наприклад, загроза погіршення носіїв даних);

- чутливість до змін напруги (може використовувати, наприклад, загроза нестабільності енергоживлення);

- чутливість до коливань температури (може використовувати, наприклад, загроза екстремальних значень температури);

- чутливість до вологості, пилу, вогкості (може використовувати, наприклад, загроза запилення);

- чутливість до електромагнітного випромінювання (може використовувати, наприклад, загроза електромагнітного випромінювання);

- недостатній супровід/неправильна інсталяція даних (може використовувати, наприклад, загроза помилки обслуговуючого персоналу);

- відсутність ефективного керування змінами конфігурації (може використовувати, наприклад, загроза помилки експлуатаційного персоналу)

Програмні:

- неповні чи незрозумілі для розробників технічні вимоги (може використовувати, наприклад, загроза програмної помилки);

- відсутність чи недостатність випробовування програмного забезпечення (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженими користувачами);

- складний інтерфейс користувача (може використовувати, наприклад, загроза помилки експлуатаційного персоналу);

- відсутність ідентифікаційних і пізнавальних механізмів, таких як автентифікація користувача (може використовувати, наприклад, загроза нелегального проникнення користувача);

- відсутність контрольних точок (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженим чином);

- відомі «дірки» в програмному забезпеченні (може використовувати, наприклад загроза використання програмного забезпечення не уповноваженими користувачами);

- незахищені таблиці паролів (може використовувати, наприклад, загроза несанкціонованого доступу користувача);

- недостатнє керування паролями (паролі, які легко підібрати, збереження паролів у відкритому виді, недостатня частота зміни; може використовувати, наприклад, загроза нелегального проникнення користувача);

- неправильний розподіл прав доступу (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженим чином);

- неконтрольоване завантажування і використання програмного забезпечення (може використовувати, наприклад, загроза зловмисної програмної закладки);

- немає механізмів «виходу із системи» у разі від'єднання робочої станції від системи (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженими користувачами);

- відсутність ефективного керування змінами (може використовувати, наприклад, загроза програмної помилки);

- відсутність документації (може використовувати, наприклад, загроза помилки оперативного персоналу);

- відсутність запасних копій (може використовувати, наприклад, загроза зловмисної програмної закладки чи загроза пожежі);

- розповсюджування чи багаторазове використання носіїв даних без відповідного очищення (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженими користувачами).

Зв 'язок:

- не захищені лінії зв'язку (може використовувати, наприклад, загроза підслуховування);

- погані кабельні з'єднання (може використовувати, наприклад, загроз витоку даних з каналів зв'язку);

- відсутність ідентифікування і підтвердження відправника й одержувача (може використовувати, наприклад, загроза нелегального проникнення користувача);

- передавання паролів у відкритому виді (може використовувати, наприклад, загроза доступу до мережі не уповноваженими користувачами);

- відсутність підтвердження посилання чи одержання повідомлень (може використовувати, наприклад, загроза невизнання участі);

- вилучений доступ (може використовувати, наприклад, загроза доступу до мережі не уповноваженими користувачами);

- незахищений чутливий потік даних (може використовувати, наприклад, загроза підслуховування);

- недостатнє керування мережею (гнучкість маршрутизації; може використовувати, наприклад, загроза перевантаження трафіка).

- незахищені з'єднання загального використання (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженими користувачами).

Документи:

- збереження в незахищеному виді (може використовувати, наприклад, загроза злодійства);

- відсутність обережності у використанні (може використовувати, наприклад, загроза злодійства);

- несанкціоноване копіювання (може використовувати, наприклад загроза злодійства).

Персонал:

- відсутність персоналу (може використовувати, наприклад, загроза пов'язана з недостатньою кількістю персоналу);

- неконтрольована зовнішня робота некомпетентним персоналом (може використовувати, наприклад, загроза злодійства);

- недостатнє навчання питанням захисту (може використовувати, наприклад, загроза помилки оперативного персоналу);

- відсутність компетентності в захисті (може використовувати, наприклад, загроза помилок користувача);

- неправильне використання програмного забезпечення і устаткування (може використовувати, наприклад, загроза помилки оперативного персоналу);

- відсутність заходів контролю (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженим чином);

- відсутність методик для правильного використання засобів телекомунікації і пересилання повідомлень (може використовувати, наприклад, загроза використання мережних засобів не уповноваженим шляхом);

- неадекватні процедури прийому на роботу (може використовувати наприклад, загроза навмисного збитку).

Загальні причини вразливостей:

- окремі місця недоліків (може використовувати, наприклад, загроза недоліків послуг зв'язку);

- неадекватне реагування служб підтримки (може використовувати, наприклад, загроза відмови апаратури).

Важливо визначити, наскільки небезпечні вразливості, іншими словами, як легко ними можна скористатися. Вразливість має бути оцінена стосовно кожної загрози у відповідній ситуації. Наприклад, система може мати вразливість до загроз нелегального проникнення користувача і використання ресурсів. Вразливість нелегального проникнення користувача може бути високою через відсутність механізмів авторизації користувачів. З іншого боку, вразливість зловживання ресурсами може бути низькою, тому що навіть без механізмів авторизації користувачів ресурси, якими вони могли б зловживати, обмежені.

Результатом цього кроку повинен бути перелік вразливостей і оцінок легкості їхнього використання, наприклад, у градації високо, середньо і низько.

Модель загроз складається з таких етапів:

- збір і попередня підготовка інформації (складання запитальника);

- методи моделювання та інтерпретації інформації;

- аналіз та коригування моделі;

- оформлення результатів.

На етапі збору і попередньої підготовки інформації в першу чергу необхідно знайти відповіді на запитання:

- хто вірогідніше за все може напасти на конкретну інформацію?

- яку інформацію, скільки грошей та інших засобів можуть отримати порушники?

Щоб відповісти на ці запитання, необхідно знати:

- чи є в інформаційній системі та мережі інформація з обмеженим доступом, котра має цінність для порушника;

- чи є в системі інформація з грифом обмеження доступу;

- чи є інформація, котра може бути особливо цікавою для порушників;

- наскільки достатньо система захищена від нападів?

- які вразливі місця системи?

- які засоби захисту вже застосовувались?

При цьому необхідно чітко знати відповіді на такі питання:

- яка вірогідність того, що хто-небудь нападе на конкретну інформаційну систему?

- наскільки вірогідна кожна із виявлених конкретних загроз?

Перший етап, складання запитальника, є теоретичним. Необхідно уявити можливі напади, котрі можуть бути: вандали занесуть вірус, щоб завдати збитку, крадії можуть за замовленням украсти обладнання і програмне забезпечення, може виникнути пожежа, повінь, землетрус.

Методи моделювання та інтерпретації інформації починаються з ряду запитань:

- хто міже напасти на інформаційну систему?

- які засоби можуть використовувати нападники?

- які ресурси і компоненти системи можуть бути вкрадені або порушені?

Другий етап є конкретним. Які є вразливі місця систем з урахуванням загроз? Якщо загрози видаються мінімальними, необхідно виявити потенційно

вразливі місця. Мінімальні загрози можуть стати великими, а загрози, вірогідність котрих не врахована, - матеріалізуються. Що необхідно зробити з вразливими місцями, це - окреме питання. Мета цього етапу полягає у виявленні та перелічені загроз.

Тепер, коли відомі вразливі місця інформаційної системи з пов'язаними із ними загрозами, які методи захисту вже застосовуються системі і що ще необхідно зробити.

Іноді достатньо простих і недорогих заходів, щоб забезпечити необхідний рівень захисту системи. Іноді, щоб як слід захистити систему, необхідно, вкласти великі гроші. На цьому етапі необхідно прийняти рішення. Зрозуміло, що ступінь захисту системи, яку необхідно забезпечити, залежить як від ступеня її вразливості, так і від коштів, виділених на ці роботи. Якщо рівень загроз мінімальний, витрати і зусилля на організацію захисту будуть мінімальні. Якщо рівень загроз великий, витрати і зусилля на організацію захисту значно збільшуються.

Бажано розділити потреби в забезпеченні захисту на три категорії:

- перша категорія - це невідкладні потреби, які необхідно вирішити прямо зараз. Зламаний замок, ненавчений співробітник, дірки в огорожі тощо відносяться до цієї категорії;

- друга - це середньо термінові потреби - це зміни, які необхідно зробити в поточному фінансовому році (модернізація наявного захисного обладнання);

- третя категорія - це довготермінові потреби - витрати на них необхідно включати в бюджет наступних років, це пов'язане з модернізацією системи в цілому і прогнозовані потреби в наступному.

Незалежно від того, що вирішено на подальший час, повинен бути план дій в надзвичайних умовах. Якщо зловмисник знайшов доступ до системи, необхідно швидко знайти гроші, «закрити двері амбару і очистити стайню».

У процесі аналізу та коригування моделі загроз необхідно перерахувати усі цінності, котрі необхідно захищати в даній інформаційній системі. Приблизний перелік цінностей, котрі необхідно захищати:

для програмного забезпечення: операційна система, прикладні програми, стандартні прикладні та робочі програми, системні утиліти, комунікаційні програми;

для фізичних цінностей: системи життєзабезпечення (енергозабезпечення, водопостачання, опалення, освітлення);

споруди;

інформаційна система;

витратні матеріали (папір, магнітні носії інформації); резервне обладнання, приміщення з встановленим обладнанням тощо.

11.5.Оцінювання активів організації

Оцінювання активів організації - істотний етап всього процесу аналізу ризиків. Значення цінності, визначене для активів, мусить бути виражене в поняттях, що стосуються майна і об'єктів, залучених до ділової активності. Для оцінювання активів організація має спочатку зробити перелік усіх наявних активів, щоб забезпечити адекватне оцінювання всіх активів, доцільно згрупувати їх за типами, наприклад, інформаційні активи, програмні матеріальні носії інформації, фізичні матеріальні носії інформації і служби. Також корисно визначити власника кожного з активів, що буде відповідати за визначення значень цих активів.

Наступним кроком є вибір і погодження використовуваних шкал і критеріїв специфічних оцінок активів. Оскільки в більшості організацій зазвичай є значне різноманіття активів, швидше за все, цінності деяких активів можуть бути виражені у вартісному значенні і будуть оцінені в національній валюті, в той час як інші, виражені в якісному значенні, можуть бути оцінені діапазоном значень від «дуже низько» до «дуже високо». Рішення про використовування

шкали кількісних оцінок замість шкали якісних оцінок є компетенцією організації і має залежати від оцінюваних активів. Обидва види оцінок можна застосовувати до тих самих активів.

Типові градації, використані для якісної оцінки активів, такі: незначно, дуже низько, низько, середньо, високо, дуже високо і критично. Вибір і діапазону значень залежить від вимог організації до безпеки, розміру організації та інших чинників, визначених для організації.

Критерії, що використовуються як основа для надання значень для кожного з активів, мають бути зафіксовані в певних значеннях. Це зазвичай один з найважчих аспектів оцінювання активів, тому що значення деяких активів, імовірно, доведеться визначити суб'єктивно і, швидше за все, це будуть визначати багато різних осіб. Можливі критерії, використані для визначання значень активів, охоплюють вартість їхнього придбання, заміни чи вартість повторного створення; їхні значення можуть бути абстрактними, наприклад, значення гарного іміджу організації чи її репутації.

Ще однією основою для оцінювання активів є витрати, спричинені втратою конфіденційності, цілісності чи доступності в результаті інциденту. Ця оцінка надає три важливих доповнення значень активів як додаток вартості відшкодування, заснований на оцінюванні потенційного збитку чи несприятливо зниження ділової активності, що буде випливати з інцидентів захисту і залежною від нього множиною обставин. Треба зазначити, що цей підхід дозволяє врахувати збитки чи інші втрати коштів як необхідну складову формули оцінки ризику.

Багато активів можуть мати декілька значень наданих в процесі оцінювання. Наприклад, план ділової активності може бути оцінений на підставі зусиль, необхідних для розробки плану розвитку, що в свою чергу ґрунтується на зусиллях, пов'язаних з накопиченням даних, а також на їхньому значенні для конкурентів. Кожна з отриманих оцінок з великою ймовірністю матиме різні

значення. Присвоєне значення може бути максимальним серед всіх можливих значень чи може бути сумою деяких чи всіх можливих значень. Остаточний аналіз, що припускає визначення значення чи значень активів, має бути чітко детермінованим, тому що надане остаточне значення враховують під час визначання ресурсів, що будуть залучені для захисту активів.

Зрештою всі оцінки активів мають бути зведені до спільної основи. Це може бути виконано за допомогою критеріїв. Критерії, які можна використовувати для визначання можливих збитків, зумовлюються втратою конфіденційності, цілісності чи доступності активів:

- порушення законів і (або) розпоряджень;
- порушення ділової активності;
- зміна з позитивного на негативний вплив на репутацію;
- порушення, пов'язані з особистою інформацією;
- втрата особистої безпеки;
- несприятливий вплив на законність діяльності;
- порушення комерційної конфіденційності;
- порушення громадського порядку;
- фінансові втрати;
- збої в діловій активності;
- втрата безпеки відносно оточення.

Ці критерії - приклади положень, які потрібно враховувати під час оцінювання активів. Для визначення оцінок організація має вибрати критерії, що залежать від типу вимог безпеки і ділової активності.

Необхідно також враховувати, що деякі з критеріїв, наведених вище, можуть не відповідати потребам конкретної організації і можуть бути додані інші, відмінні від них.

Після визначення критеріїв, які необхідно брати до уваги, організація мусить погодити шкалу, що буде використовуватися для всієї організації.

Перший крок складається з визначення кількості використовуваних рівнів. Немає загальних правил, що дозволяють визначити кількість найбільш прийнятних рівнів. Більша кількість рівнів забезпечує вищий рівень деталізації оцінок, але іноді вищий рівень диференціації ускладнює в цілому сумісну оцінку для організації. Звичайно, можна використовувати будь-яке число рівнів від трьох (наприклад, низько, середньо і високо) до десяти, якщо воно не суперечить підходу, використовуваному організацією для всього процесу оцінювання ризику.

Також організація може визначити її власні межі для значень матеріальних носіїв інформації, таких як «низько», «середньо» чи «високо». Ці межі повинні бути визначені відповідно до обраних критеріїв. Наприклад, можливий фінансовий збиток: вони повинні бути виражені у вартісному значенні, однак під час розгляду втрат особистої безпеки фінансове значення не буде відповідним. Наостанок, в компетенції організації вирішити, що необхідно розглядам як «низький» чи «високий» збиток: збиток, що може бути великим для малої організації, може бути незначним для дуже великої організації.

Після досягнення мети щодо ідентифікації активів за допомогою огляду всіх активів системи інформаційних технологій треба визначити цінність активів. Ця цінність відображає важливість активів для діяльності організації, їх можна виразити в термінах захисту, таких як потенційно небажані порушення ділової активності в результаті розкриття, зміни, недоступності або знищення інформації або інших активів системи інформаційних технологій. Отже, ідентифікація активів та їхня оцінка, заснована на ділових потребах організації, є провідними чинниками при визначенні ризиків.

Вихідними даними для оцінювання активів повинні забезпечувати власники і користувачі активів. Особи, що аналізують ризик, повинні формулювати перелік активів. Вони мусять звертатися по допомогу до тих, хто займається плануванням ділової активності, фінансами, інформаційними

системами та іншою залежною діяльністю, для того щоб визначити цінність кожного з цих активів. Установлення цінності потрібно пов'язувати з вартістю придбання і отримання активів і з потенційними поразками від втрати конфіденційності, цілісності, доступності, достовірності і надійності. Кожен з ідентифікованих активів має певну цінність для організації. Проте не завжди є прямий або простий спосіб встановлення фінансової цінності для всіх параметрів. Також необхідно встановити цінність чи ступінь важливості параметру для не фінансових тобто для якісних характеристик, термінів в організації. Інакше буде важко визначити рівень захисту і кількість ресурсів, які організація має залучити, щоб захистити матеріальні носії. Наприклад, для подібних визначень цінності можна використовувати шкалу, де вона виражена у градації: низько, середньо, високо або більш детальну:

дуже низько — низько — середньо — високо — дуже високо.

Незалежно від використовуваної шкали необхідно оцінювати збитки, можливі в результаті:

- порушення законів і розпоряджень;
- втрати ефективності ділової активності;
- втрати авторитету або негативного впливу на репутацію;
- порушення конфіденційності, пов'язаної з персональною інформацією;
- втрати особистої безпеки;
- несприятливих впливів на законність діяльності;
- порушення комерційної конфіденційності;
- порушення громадського порядку;
- фінансових втрат;
- порушень бізнесової діяльності;
- впливу небезпечного оточення.

Організація також повинна визначити власні межі для оцінювання збитків як «низькі» або «високі». Наприклад, фінансовий збиток, що міг би бути

згубним для малої організації, може спричинити незначні чи часткові втрати для великої організації. Варто підкреслити на цій стадії, що метод для оцінювання повинен давати не тільки кількісну оцінку, але і якісну оцінку там, де кількісна оцінка неможлива чи недоцільна (наприклад, існує потенційна можливість втрати життєздатності чи репутації організації). Необхідно надавати чіткі обґрунтування обраних критеріїв оцінки.

Також потрібно визначити залежності одних активів від інших, тому що це може впливати на їхню цінність. Наприклад, конфіденційність даних треба зберігати протягом усього процесу обробки, тобто вимоги програми захисту обробки даних повинні залежати безпосередньо від значення, що відображає конфіденційність оброблюваних даних. Якщо бізнес-процес спирається на цілісність певних даних, вироблених програмою, вхідні дані цієї програми повинні забезпечувати відповідну надійність. Крім того, цілісність активів буде залежати від апаратних засобів і програмного забезпечення, що використовуються для її зберігання та обробки. Також апаратні засоби залежать від електроживлення тощо. Така інформація щодо залежностей буде допомагати під час ідентифікування залежних загроз і особливо вразливостей. Це також допоможе під час визначення дійсних цінностей матеріальних носіїв (прямих залежностей відносин) і, отже, гарантувати відповідний рівень захищеності.

Цінність активів, від яких залежать інші активи, можуть змінюватися таким чином:

- якщо цінність залежних активів (дані) нижча чи дорівнює цінності розглянутих активів (програмне забезпечення), цінності залишаються незмінними;

- якщо цінність залежних активів (дані) вища ніж цінність розглянутих активів (програмне забезпечення), цінність має бути збільшена згідно з:

• рівнем залежності;

• цінністю інших активів.

Організація може мати деякі активи, що мають бути доступними більше одного разу, такі як копії чи програми, подібні тим, що їх використовують у більшості організацій. Важливо враховувати цей факт під час оцінювання активів. Ці копії легкодоступні. Тому, з одного боку, треба потурбуватися про визначення всіх шляхів доступу; з іншого - потрібно шукати шляхи зменшення можливостей доступу.

Кінцевим результатом є перелік активів та їхніх цінностей щодо розкриття (забезпечення конфіденційності), зміни (забезпечення цілісності), доступності чи знищення (забезпечення доступності) і вартості відшкодування.

Величина економічної шкоди та інші наслідки, завдані або такі, що можуть бути завдані від втрати або витоку інформації, має бути меншою від витрат на забезпечення схоронності інформації, тобто має місце така умовна формалізація у виді

$$C = E + I > B$$

де С - сукупні економічні витрати, завдані або такі, що можуть бути завдані внаслідок втрати або витоку інформації, викладеної в документі;

Е - економічна шкода - матеріальні збитки, спричинені або такі, що можуть бути спричинені внаслідок втрати або витоку інформації, викладеної в документі;

І - інші наслідки - втрати, які відбулися або можуть відбутися внаслідок втрати або витоку інформації, які економічно важко обраховуються у кількісному вираженні (погіршення або розрив відносин та зв'язків з партнерами (одним або кількома), витрати на відновлення відносин та зв'язків, зрив договорів на впровадження якості нової продукції, людський фактор тощо);

В - витрати на забезпечення схоронності інформації, викладеної в документі.

Людський фактор відіграє дуже важливу роль в справі ефективного здійснення заходів щодо захисту активів від актів несанкціонованого доступу. Незважаючи на процес створення технічних засобів забезпечення безпеки

активам, ніяка технологія не в змозі замінити добре підготовлених або тих, що володіють високою мотивацією працівників служби захисту інформації з обмеженим доступом. Ефективність роботи найскладнішого сучасного обладнання залежить від рівня і навичок працівників, які мусять бути професіоналами у своїй справі.

Запитання для самоконтролю

1. *Назвіть чотири основних варіанти методики аналізування ризику.*
2. *Що може бути привабливими активами організації для потенційного порушника?*
3. *Які головні характеристики активів?*
4. *Охарактеризуйте Рис.6.1. Канали витоку інформації.*
5. *Назвіть основні підходи до виявлення загроз.*
6. *Охарактеризуйте класифікаційну модель порушника в інформаційній системі.*
7. *На чому базується методологія проведення етапу теоретичних досліджень?*

РОЗДІЛ 12. ОСНОВИ МОДЕЛЮВАННЯ ПРОЦЕСУ КІБЕРЗАХИСТУ

12.1. Методи моделювання систем кіберзахисту

Методи неформального моделювання базуються на застосуванні неформальної теорії систем. Основними частинами цієї теорії є:

структурування архітектури та процесів функціонування складних систем;

неформальні методи оцінювання;

неформальні методи оптимальних рішень.

1.1 Структурування архітектури та процесів функціонування складних систем є розвитком формального опису систем, який розповсюджується на організаційно-технічні системи.

Прикладом структурованого процесу є конвеєрне виробництво. На базі такого виробництва використовуються два принципи:

сувора регламентація технологічного процесу виробництва;

спеціалізація користувачів та обладнання.

Рахується, що конструкція продукції, яка виготовляється відповідає наступним вимогам:

виріб складається з конструктивних ієрархічних елементів (блоків, вузлів, деталей тощо);

максимальна простота, уніфікованість та стандартність конструктивних рішень та технологічних операцій.

Структурне модулювання чітко вписується в рамки структурованих процесів. На основі узагальнення принципів і методів структурного модулювання можуть бути сформульовані умови структурного опису систем і процесів, які вивчаються та порядок їх функціонування.

Такими процесами є:

повнота відображення основних елементів та їх взаємозв’язки;

адекватність;

простота внутрішньої організації елементів опису і взаємозв’язків елементів між собою;

стандартність і уніфікованість внутрішньої структури елементів і структури взаємозв’язків між ними;

модульність;

гнучкість, під якою розуміється можливість розширення та зміни структури одних компонентів моделі без будь-яких змін інших компонентів;

доступність вивчення і використання моделі будь-якому фахівцю середньої кваліфікації відповідного профілю.

В процесі проектування систем необхідно отримати їх характеристики. Деякі характеристики можуть бути отримані шляхом вимірів. Інші отримуються з використанням аналітичних співвідношень, а також в процесі обробки статистичних даних. Однак існують характеристики складних систем, які не

можуть бути отримані приведеними методами. До таких характеристик СЗІ відносяться вірогідності реалізації загроз,окремі характеристики ефективності систем захисту.

Вказані характеристики можуть бути отримані методами неформального оцінювання, тобто методами експертних оцінок.

1.2 Метод експертних оцінок представляє собою алгоритм підбору спеціалістів – експертів, надання правил отримання незалежних оцінок кожним експертом і наступною статистичною обробкою отриманих результатів.

1.3 Неформальні методи находження оптимальних рішень можуть бути розподілені по двум групам:

методи неформального зведення складної задачі до формального опису і рішення задачі формальними методами;

неформальне находження оптимального рішення.

Для моделювання систем захисту інформації необхідно використовувати наступні теорії та методи, які дозволяють звести рішення задачі до формальних алгоритмів:

теорія нечітких множин;

теорія конфліктів;

теорія графів;

формально-евристичні методи;

еволюційне моделювання.

Методи нечітких множин дозволяють отримати аналітичні вирази для кількісних оцінок нечітких умов належності елементів до однієї або іншої множини. Теорія нечітких множин добре узгоджується з умовами моделювання систем захисту,так як деякі вихідні дані моделювання (наприклад, характеристики загроз і окремі механізми захисту) не є суворо визначеними.

Теорія конфліктів є відносно новим напрямком досліджень складних людина-машинних систем. Конфлікт між зловмисником і системою захисту, на фоні випадкових загроз, є класичним для застосування теорії конфлікту. Дві протиборчі сторони мають суворо протилежні цілі. Конфлікт розвивається в умовах неоднозначності і слабкої передбаченності процесів, спроможності сторін оперативно змінювати цілі. Теорія конфліктів є розвитком теорії ігор. Теорія ігор дозволяє:

структурувати задачу, представити її в наглядному вигляді, знайти області кількісних оцінок, виявити переважаючі стратегії;

до кінця вирішити задачі, які описуються стохастичними моделями.

Теорія ігор дозволяє знайти рішення,оптимальне або раціональне в середньому. Вона мінімізує середній риск. Такій підхід неповному обсязі адекватно відображає поведінку сторін в реальному конфлікті, кожен з яких є унікальним. В теорії конфліктів реалізована спроба подолати ці недоліки теорії ігор. Теорія конфліктів дозволяє вирішувати ряд практичних задач дослідження

сложних систем. Однак вона ще не отримала широкого розповсюдження і відкрита для подальшого розвитку.

З *теорії графів* для дослідження систем захисту інформації в найбільшій ступені застосований апарат мереж Петрі. Управління умовами в вузлах мереж Петрі дозволяє моделювати процеси подолання захисту зловмисником. Апарат мереж Петрі дозволяє формалізувати процес дослідження ефективності систем захисту інформації.

До *формально-евристичних* методіввіднесені методи находження оптимальних рішень не на основі суворих математичних, логічних співвідношень, а базуючись на досвіді людини, знаннях та інтуїції які маються. Отримані рішення можуть бути далекі від оптимальних, но вони краще рішень, які отримані евристичним шляхом.

Найбільше розповсюдження з формально-еврістичних методів отримали лабіринтні і концептуальні методи.

У відповідності з лабіринтною моделлю задача надається людині у вигляді лабіринту можливих шляхів рішення. В результаті чого серед шляхів, які остались з більшою вірогідністю знаходиться шлях, який приведе до рішення задачі.

Концептуальний метод пропонує виконання дій з концептами. Під концептами розуміють узагальнені елементи і зв’язкиміж ними. Концепти отримуються людиною, можливо на інтуїтивному рівні, в процесі побудови структурованої моделі. У відповідності з концептуальним методом набор концепт універсален і йому відповідають механізми обчислення, трансформації і формування відносин, які маються у людини. Людина проводить експеримент мислення і породжує граничнуділянку лабіринту, в якій вже можливо знайти рішення.

Еволюційне моделювання представляє собою різновид імітаційного моделювання. Особливість заключається в тому, що в процесі моделювання удосконалюється алгоритм моделювання.

12.2. Аналіз моделей кіберзахисту

Моделі захисту інформації є складовими частинами загального процесу моделювання. Моделювання системи заключається в побудові образу системи, адекватного (з точністю до цілей моделювання) системи, яка проектується, і в отриманні за допомогою побудованої моделі необхідних характеристик реальної системи. Таким чином, в самому загальному випадку, весь процес моделювання можна поділити на дві складові:

- побудова моделі;

- реалізація моделі з метою отримання необхідних характеристик системи.

Основне призначення моделей - це створення умов для об’єктивної оцінки загального стану інформаційної системи з точки зору міри уразливості або рівня захищеності інформації в неї. Необхідність в таких оцінках, зазвичай, виникає під час аналізу загальної ситуації з метою відпрацювання стратегічних рішень при організації захисту інформації.

12.2.1. Класифікація моделей кіберзахисту

Системну класифікацію моделей в наступний час привести практично неможливо, так як з точки зору малого числа таких моделей для цього нема достатніх даних. Тому розглянемо спрощену класифікацію моделей захисту інформації, яка зображена на рис. 4.1.

Але, оскільки загальною рисою будь-яких моделей є їх спроможність відображати головні для цілей дослідження признаки об’єктів, які досліджуються, то найбільш відомими признаками є:

1. Способи реалізації моделей.
2. Характер процесів і явищ, які протікають в системі.
3. Характер підходу до моделювання об’єкта.
4. Призначення і специфіка об’єктів дослідження.
5. Ступінь узагальнення характеристик об’єктів дослідження, які узагальнюються.

Ці признаки знаходяться в основі класифікації, які пропонуються.

По способу реалізації моделі захисту інформації можуть бути абстрактними, матеріальними (предметними, реальними) або змішаними (матеріально-абстрактними).

Побудова ***абстрактних моделей*** в декількох випадках є єдино можливим способом моделювання захисту інформації в складних системах. Такі моделі можуть бути реалізовані в математичній, словарній, зразковій і графічній формах.

Для абстрактних (моделей мислення) моделей природа матеріального не має принципового значення.

Математичні моделі, в яких елементи, відношення та свойства систем, які моделюються, або явищ відображаються за допомогою різних математичних

засобів, можуть бути представлені в аналітичній або алгоритмічній формах. Формулі, рівняння, матриці, графи, алгоритми і програми – все це математичні моделі.

Аналітична форма застосовується в ситуації, коли залежність між змінними, які характеризують модель, описується математичними виразами або сукупністю таких виразів.

Дослідження з використанням *аналітичної моделі* можуть проводитися одним з наступних способів:

– аналітично, коли отримують в загальному вигляді, явні залежності вихідних змінних величин моделі від вхідних даних;

– численно, коли нема можливості отримати явні залежності в загальному вигляді, но можливо порахувати значення вихідних змінних даних при заданих параметрах моделі і конкретних значеннях вхідних величин;

Рис. 12.1. Класифікація моделей захисту інформації

– якісно, коли, не отримуючи рішення в явному вигляді, роблять заключення про свойства процесу, який моделюється, який описаний математичним виразом.

Рішення на основі аналітичних моделей можє бути отримано в результаті однократного прорахунку по формульним або логічним залежностям незалежно від конкретних значень характеристик (в загальному вигляді). Такий підхід зручний для виявлення закономірностей і при цьому має таку перевагу як наглядність.

Алгоритмична форма пропонує представлення моделі в вигляді алгоритму або програми. *Алгоритмичні моделі* (які слід відрізняти від алгоритмів розрахунку аналітичних моделей при іхчисленому дослідженні), як правило, не можуть бути представлені еквівалентними формулами. Характерна особливість таких моделей заклечається також в тому, що послідовність кроків їх розрахунку на комп'ютері відповідає поведінці системи, яка моделюється, тобто імітує її. Тому отримав розповсюдження термін "*Імітаційна модель*".

Словесна модель – логічний об'єкт, який відображає свойства оригінала за допомогою визначеної системи знаків або символів. Її різновидом є вербальна модель, яка надається в вигляді тексту на звичайній мові.

До *образних* відносяться моделі, які конструюються з поглядово-почуттевих елементів, які відображають визначенні свойства в поведінці об'єкта. Різновидом таких моделей є гіпотетичні моделі і макети уяви. В основі перших знаходиться гіпотеза о процесах,які протікають в системі. Під час макетування на основі вивчення причинно-слідствених зв'язків, які існують в системі, утворюється мислений образ – макет, функціонування якого тождественно відображає явища і процеси в оригіналі. Такі моделі використовуються на раньому етапі проектування систем захисту інформації.

До *графічних моделей* відносяться номограми, креслення, графіки і діаграми, які відображають співвідношення параметрів системи і дають можливість прогнозувати зміні останніх.

Матеріальні моделі захисту інформації основані на застосуванні моделей, які уявляють собою технічні конструкції. Вони можуть бути натурними або фізичними.

Натурні моделі припускають поведінку досліджень на реальному об'єкті, дозволяючи піддати його – у відповідно з замислом дослідника – визначеним впливам. Результати експериментів подібного роду мають, як правило, високу ступінь достовірності і дають можливість виявляти закономірності і особливості протікання реального процесу в системі, яка функціонує в залежності з поставленою метою. До натурних моделей можна віднести стенди, на яких

відповідні системи досліджуються в різних (в тому числі екстремальних) умовах, а також аналогічне обладнання для комплексних випробувань.

Явища та процеси, які протикають в системі, можуть також досліджуватися на спеціально підібраних або утворених для цієї мети *фізичних моделях* – технічних пристроях, які відбудовують явища той-же природи, що і явища, які моделюються. Різновидом таких моделей є *фізично подібні*, які характеризуються однаковими фізичними процесами в об'єкті і моделі.

Змішані моделі уявляють собою з'єднання знакових форм виразу процесів і явищ з матеріальними моделями. Для той частини операції, яку не можливо описати за допомогою математичногоапарату, використовують матеріальну модель, тоді як інше моделюється у знаковій формі. В цьому випадку мова іде про *матеріально-знакову модель*. До змішаних моделей відносяться також *напівнатурні моделі*, сутність яких заключається в тому, що загальну модель наряду з математичними (аналітичними або алгоритмічними) моделями будь-яких систем включається реальна апаратурна частина системи, яка моделюється.

Виходячи із **характеру процесів, які протікають в системі**, моделі можна розділити на детерміновані і стохастичні, статистичні і динамічні, а також дискретні, безперервні і дискретно-безперервні.

Детерміновані моделі відображають процеси, в яких відсутні випадкові впливи, а *стохастичні* – вірогідносні процеси.

Статистичні моделі використовують для опису поведінки об'єкту в будь-який окремий момент, тоді як *динамічні* призначені для опису його поведінки по часу.

Дискретні і *безперервні моделі* дозволяють описати процеси в системах, відповідно не маючих і маючих таке свойство, як безперервність, а *дискретно-безперевні моделі* застосовуються для дослідження систем, в яких протікають як безперервні, так і дискретні процеси.

По характеру підходу до моделювання об'єкта розрізняють структурні і функціональні моделі.

Під *структурною моделлю* розуміється опис структури об'єкта в цілому.

Функціональні моделі, які іноді мають назву *кібернетичні*, ні в якому разі не претендують на фізичну або структурну подібність оригіналу: з точки зору структури об'єкт, який досліджується, розглядається як "чорний ящик". В спрощеному вигляді методику утворення кібернетичної моделі можна описати наступним чином. Наглядаючи за реакціями системи на зовнішні впливи, підбирають математичну модель, яка подібним же чином "відкликається" на зовнішні впливи на оригінал. Встановлюючи, таким чином, аналогію поведінки об'єкта і математичної моделі ,

По призначенню і специфіці об'єкта дослідження розрізняють моделі загроз, моделі порушника, моделі політики безпеки інформації, моделі процесу

захисту інформації, моделі систем захисту інформації, моделі систем розгородження доступу до ресурсів об'єкту.

Модель загроз уявляє собою формалізований або неформалізований опис методів і засобів здійснення загроз.

Модель порушника – формалізований або неформалізований опис відповідних характеристик і поведінки порушника.

Модель політики безпеки інформації – формалізований або неформалізований опис відповідної політики під якою розуміється сукупність законів, правил, обмежень, рекомендацій, інструкцій та інших нормативних актів, які регламентують порядок обробки інформації.

Модель процесу захисту інформації відображає взаємодію між дестабілізуючими факторами, які впливають на інформацію, і протидіючими засобами захисту інформації, ітогом якого становить визначений (більш або менш високий) рівень захищеності інформації.

Модель системи захисту інформації повинна відображати основні процеси, які протікають в цієї системі з метою оптимізації процесів захисту інформації. Такі процеси в самому загальному вигляді можуть бути представлені як процеси розподілу і використання ресурсів, які виділяються на захист інформації.

Моделі систем розгородження доступу до ресурсів об'єкта, який захищається застосовуються при рішенні задач аналізу та синтезу систем (механізмів) розгородження доступу до різного виду ресурсів об'єкта, перш за все до масивів даних або полів пристроїв запам'ятання комп'ютерних систем. Виділення цих моделей до самостійного класу моделей обумовлено тим, що механізми розгородження доступу відносяться до числа найбільш важливих компонентів систем захисту інформації, от ефективності функціонування яких в значній мірі залежить загальна ефективність захисту інформації.

По ступені узагальнення характеристик об'єкта дослідження моделі поділяються на загальні, часткові і локальні. До категорії загальних відносяться моделі, які дозволяють визначити (оцінити) загальні характеристики відповідних систем і процесів на відміну від часткових і локальних моделей, які забезпечують визначення (оцінку) будь-яких часткових або локальних характеристик системи або процесів.Тут не треба путати загальні моделі зі структурними а локальні і часткові з функціональними.

12.2.2. Побудови моделей кіберзахисту інформації

Розглянемо приклади побудови основних моделей захисту інформації. Модель процесу захисту інформації, яка представлена на рис. 12.2. У відповідності з представленою раніше класифікацією визначається як загальна, графічна (яка

наглядно надає процес дослідження), математична (відображає принципи протікання процесу в математичній формі).

Аналітичний вираз, який описує цю модель, має вигляд:

$$\overline{W} = \sum_{i=1}^{n} P_i^{\text{загр}} \cdot \Delta q_i^{\text{загр}} \cdot P_i^{\text{усун}}, \qquad (12.1)$$

де $\overline{W}$ - показник якості функціонування системи захисту інформації; $P_i^{\text{загр}}$ - вірогідність появи загрози; $\Delta q_i^{\text{загр}}$ - шкода, яка вноситься в інформаційну систему; $P_i^{\text{загр}}$ - вірогідність усунення кожної *i* – ої загрози.

Недоліком такої моделі є складність визначення $P_{i\,угр}^{устр}$ системи захисту інформації, так як неможливо розглянути і точно визначити в цій моделі вірогіднісний показник надійної роботи системи захисту інформації. Також неможливо по цій моделі визначити вірогідність подолання порушником системи захисту інформації – тобто оцінювати вірогідність несанкціонованого доступу (НСД).

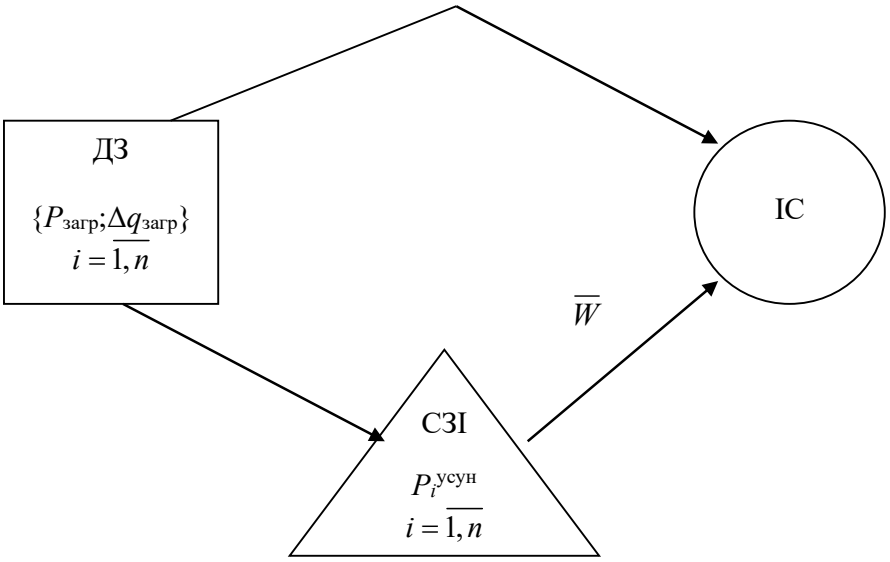


Рис. 12.2. Загальна модель процесу захисту інформації
(ДЗ – джерело загроз, ІС – інформаційна система,
СЗІ – система захисту інформації)

В якості розвитку приведеної вище моделі можна розглянути модель процесу захисту інформації, яка приведена на рис. 12.3.

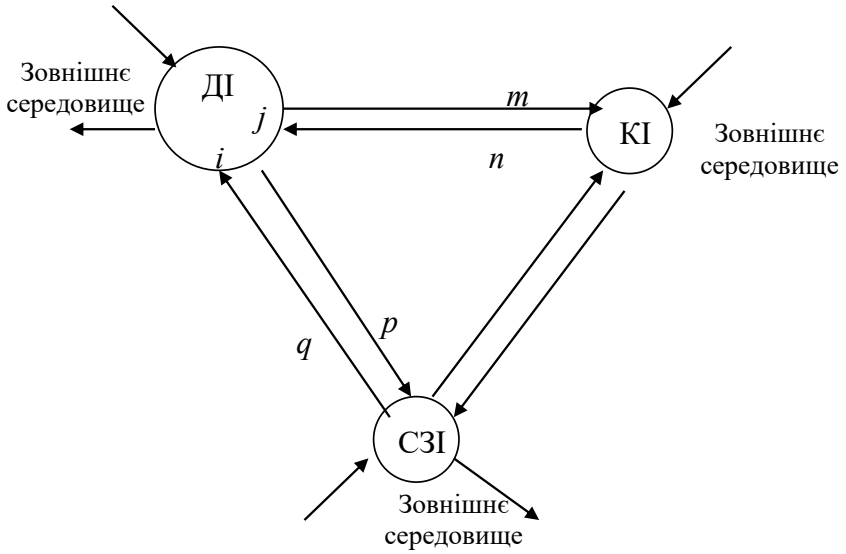


Рис. 12.3. Модель системи захисту інформації з врахуванням взаємозв'язків системи захисту інформації (СЗІ), джерела інформації (ДІ) та користувача інформації (КІ)

В цій моделі відображається взаємозв'язок самої системи захисту інформації з джерелом інформації і користувачем інформації. Причому в цій моделі враховується вплив зовнішнього середовища на усі складові (СЗІ, ДІ, КІ), які за своєю природою мають бути як природне так і штучне (дії порушника).

Аналітичним виразом цієї моделі є система рівнянь:

$$\begin{cases} A_{0j} = A_i W_{ji} W_{0i} = \left(A_n W_{in} + A_q W_{iq} + A_{i0} W_{i0} \right) W_{ji} W_{0j} \\ A_{0q} = A_p W_{qp} W_{0q} = \left(A_j W_{jp} + A_n W_{pn} + A_{p0} W_{p0} \right) W_{qp} W_{0q} \\ A_{0n} = A_m W_{nm} W_{0n} = \left(A_j W_{mj} + A_q W_{mq} + A_{m0} W_{m0} \right) W_{nm} W_{0n} \end{cases} \quad (12.2)$$

Недоліком цієї моделі є то, що вона розкриває тільки взаємозв'язки між (учасниками) процесу захисту інформації, но не показує внутрішні процеси в самій системі захисту інформації, які в основному і впливають на якісну оцінку захисту інформації.

Одним з різновидів загальної моделі процесу захисту інформації є модель захисту інформації з повним перекриттям загроз, яка надана на рис. 12.4.

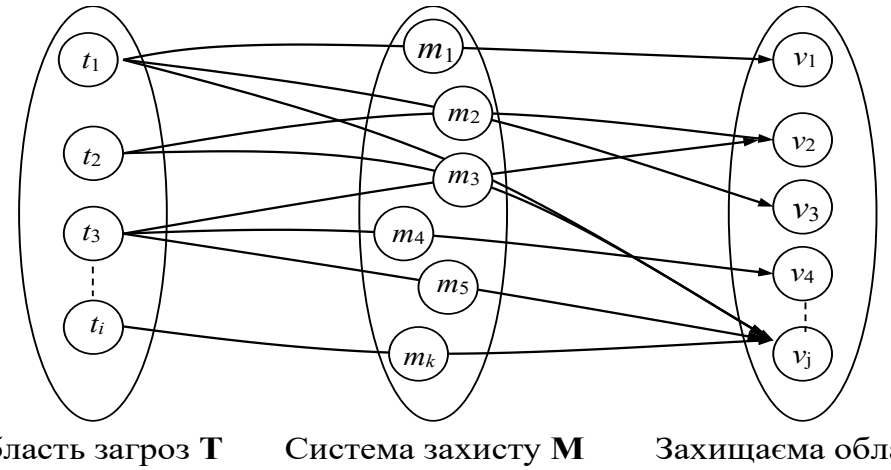


Рис. 12.4. Загальна типова модель процесу захисту інформації з повним перекриттям загроз

В цій моделі кожній загрозі, яка впливає на систему захисту, протиставиться механізм захисту зі складу системи захисту інформації.

Усі загрози повинні проходити тільки через механізм захисту, інакше нема користі від цієї моделі. Подальшим удосконаленням цієї моделі є якісний розрахунок механізмів захисту з метою оцінки ефективності роботи системи захисту інформації.

Розглянуті моделі повинні використовуватися на етапі проектування систем захисту інформації, коли ще не сформована архітектура системи, і необхідно дати попередню оцінку ефективності системи захисту інформації, яка проектується.

В якості моделей системи захисту інформації (їх часткового випадку – по класифікації, яка приведена вище – функціональної моделі) виступають моделі аналізу розгородження доступу до інформації, які виділені в окремий клас.

Розглянемо найбільш відомі:

Модель Деннінга – ієрархічна многорівнева модель захисту, в якій вводиться поняття концентрованих кілець захисту, во внутрішніх кільцях – самий жорсткий рівень безпеки і під час приближення до периферії – рівень безпеки знижується.

На рис 12.5. представлена аналітична модель багаторівневого захисту інформації від загроз НСД.

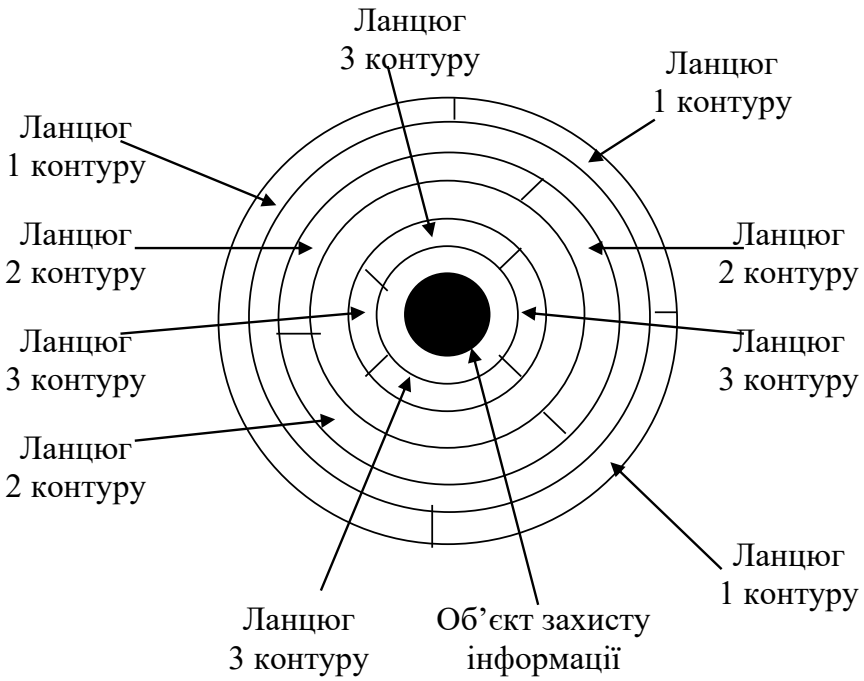


Рис. 12.5. Модель багаторівневого захисту від загроз НСД

В основу аналітичного виразу, який описує цю модель, покладена оцінка стійкості перешкод багаторівневого захисту (причому під ланцюгами контурів розуміють перешкоди, а товщина контуру відображає його стійкість):

$$P_{\text{СЗІ}} = 1 - \prod_{i=1}^{m}(1 - P_i), \qquad (12.3)$$

де i – порядковий номер перешкоди технічного захисту інформації (ТЗІ), $i = \overline{1, m}$; m – кількість перешкод, які дублюються; P_i – стійкість i-ї перешкоди,

$$P_i = P_i^{\text{блок}}\left(1 - P_{\text{відм}}\right), \qquad (12.4)$$

де $P_i^{\text{блок}}$ - вірогідність блокування i-ї перешкоди,

$$P_i^{\text{блок}} = t_{\text{н}}/T_{\text{блок}}\ T_{\text{блок}}, \qquad (12.5)$$

де $t_н$ – час подолання перешкоди порушником; $T_{блок}$ – час виявлення і блокування загрози НСД;

Вірогідність відмови системи захисту визначається наступним чином:

$$P_{відм} = e^{-\lambda t}, \quad \lambda t \tag{12.6}$$

де λ – інтенсивність відмови технічних засобів захисту; t - час функціонування системи виявлення і блокування НСД.

Недоліком моделі є відсутність обліку можливої шкоди від впливу на інформацію і ефективність функціонування системи захисту.

Модель Белла і Ла-Падула–для побудови засобів розгородження прав доступу, вводяться поняття активних суб'єктів S та пасивних суб'єктів Q, які отримують різні права доступу.

Подальшим удосконаленням моделі Белла і Ла-Падула стала модель Біба – согласно якої усі суб'єкти і об'єкти попередньо розділяються на декілько рівнів доступу, а потім на їх впливи накладаються наступні обмеження: 1) суб'єкт не може визивати на виконання об'єкти з більш низьким рівнем доступу; 2) суб'єкт не може модифікувати об'єкти з більш високим рівнем доступу. Ця модель реалізована в захищеному режимі мікропроцесорівIntel 80386+ відносно рівнів привілеїв.

В моделі Харрисонамінімальна вимога до безпеки системи заключається в тому, що користувач, якій здійснює будь-яку операцію в системі, повинен знати, приведе лі виконання цієї операції до наступного переміщення привілеї доступу до суб'єкту, який цю привілею не мав, та не повинен мати.Харрисон показав, що базуючись на матрічній моделі доступу, існує єдиний тип систем, який задовольняє вказаній вище вимозі – багатоопераційні системи (системи, які при виконані однієї високорівневої команди користувача виконують одну і тільки одну команду з базового набору команд).Недоліком такої моделі є то, що такі системи не можуть мати розповсюдження в силу своєї обмеженості і мають головним чином теоретичний інтерес.

Основою усіх розглянутих вище моделей аналізу розгородження доступу є обов'язкове використання диспетчера доступу, а сама система захисту уявляється тройкою:

$$Z = \langle S, Q, P \rangle, \tag{12.7}$$

де S – суб'єкти, до яких відносяться користувачі та їх програми, а також народжені їми програми, процеси; Q – множина об'єктів (ресурсів) системи, які можуть запрошуватися суб'єктами; до об'єктів відносяться також програми, процедури, дані, томи, файли і пристрої; P – множина прав доступу суб'єктів до об'єктів.

Загальна модель системи захисту, яка враховує формулу (12.7), представлена на рис. 12.6.

Модель Гогена-Мезігера основана на теорії автоматів. Згідно її система при кожній дії переходить з одного дозволеного стану тільки в декілька інших. Суб'єкти і об'єкти в цієї моделі захисту розбиваються на групи – домени, і перехід системи з одного стану в інший виконується тільки в відповідності з таблицею дозволів, в якій вказано які операції може виконувати суб'єкт.В цій моделі при переході системи з одного дозволеного стану в інший використовуються транзакції, що забезпечує загальну цілісність системи.

Сазерлендська (від англ. Sutherland) модель системи захисту робить акцент на взаємодії суб'єктів і потоків інформації. Також як і в попередній моделі, тут використовується машина станів з множиною дозволених комбінацій станів і набором початкових позицій. В цій моделі досліджується поведінка множини композицій функцій переходу з одного стану в інший.

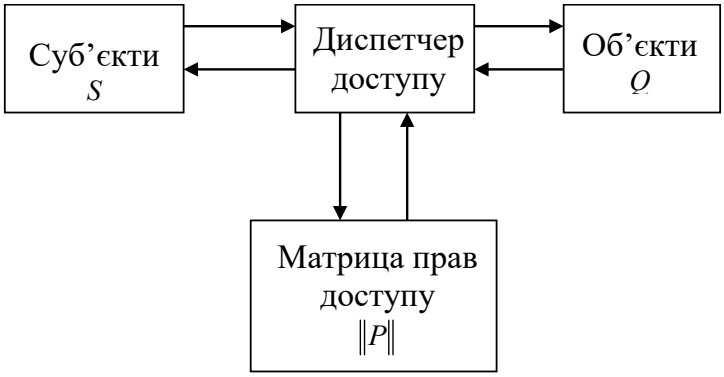


Рис. 12.6. Загальна модель системи захисту

Важливу роль в теорії захисту інформації грає модель захисту Кларка-Вільсона. Ця модель основана на постійному використанні транзакцій і старанному оформленні прав доступу суб'єктів до об'єктів. В цій моделі вперше досліджена захищеність третьої сторони в цій проблемі – сторони, яка підтримує усю систему безпеки. Цю роль в інформаційних системах грає програма – супервізор. Крім того, в моделіКларка-Вільсона транзакції вперше були побудовані по методу верифікації, тобто ідентифікація суб'єкта проводилася не тільки перед виконанням команди від нього, но і повторно після виконання. Це дозволило зняти проблему підміни автора в момент його

ідентифікації. Модель Кларка-Вільсона рахується однією з самих удосконалених у відношенні підтримання цілісності інформаційних систем.

Ще на етапі раннього проектування багато дослідників ставлять перед собою проблему абстрактного уявлення системи захисту інформації, яка проектується, в залежності від цілей, задач, місця і обстановки, в якій вона буде функціонувати. Для цього важливо розібратися в існуючих підходах побудови різних моделей захисту інформації.

Моделі захисту інформації, які були розглянуті, дозволяють систематизувати вивчення процесу моделювання, правильно підходити до оцінки моделей для подальшої побудови систем захисту інформації.

12.3. Аналіз захищеності системи кіберзахисту інформації з повним перекриттям загроз

Відомо, що до підсистеми захисту інформації інформаційної системи приділяється ряд вимог: функціональних, економічних, технічних та організаційних. Одною з головних вимог є економічна. Побудова комплексної системи захисту інформації проводиться з максимальною економічною ефективністю. В літературі оптимальні, по економічним показникам, системи розглядаються з двох різних позицій: при заданих ресурсах встановлюється максимальний рівень безпеки інформації або при заданому рівні безпеки визначаються мінімальні витрати на ресурси, які виділяються для забезпечення безпеки інформаційних технологій.

При таких підходах в процесі розробки КСЗІ виникає задача визначення оптимального об’єма ресурсів для реалізації підсистеми і вибору оптимального рівня захисту інформації.

В ряді підходів пропонується визначати вимоги до забезпечення безпеки інформації на основі експертних оцінок по сукупності таких факторів, як характер і об’єм інформаційного і програмного забезпечення, тривалості перебування інформації на об’єкті обробки інформації, структурі самого об’єкта тощо.

В інших підходах оцінка об’єма ресурсів, які необхідно виділяти для систем захисту інформації, проводиться виходячи з того, що вартість засобів забезпечення безпеки повинна бути менше розміру можливої шкоди.

В деяких підходах розглядається достатній рівень безпеки. Забезпечення такого рівня безпеки, коли вартість його подолання становить більше вартості інформації, яку необхідно отримати (ефект, який необхідно досягти), або коли за час отримання інформації вона настільки стане застарілою, що отримувати її стане неважливим. Тому в в цьому пункті тільки ставиться задача визначення оптимального рівня безпеки: важливо правильно вибрати той або інший

достатній рівень захисту, при якому витрати, риск та розмір можливої шкоди були б неруйнівними (задача аналізу ризиків).

Аналізу ризиків, під час розробки системи захисту інформації, для побудови стратегії захисту, приділяється велика увага. Аналіз ризиків використовується для вибору найбільш реальних загроз інформаційному і програмному забезпеченню КСЗІ та цілеспрямованим способам захисту інформаційного середовища.

Однак, етап аналізу ризиків має на увазі тільки оцінку реальних витрат та виграшу від застосування заходів захисту, які повинні бути обов'язково. І на основі величини виграшу пропонується приймати рішення про вибір стратегії безпеки. Величина виграшу може мати як позитивне так і негативне значення.

В першому випадку це означає, що використання КСЗІ принесе виграш, а в другому випадку це принесе додаткові витрати на забезпечення особистої безпеки.

Очевидно, такі підходи не враховують економічну ефективність КСЗІ, під якою розуміється співвідношення можливих втрат до впровадження і після впровадження систем захисту інформації з врахуванням вартості самої КСЗІ.

Прийняття оптимальних рішень в умовах ризиків і невизначеності потребує великого об'єма обчислень. Це обумовлено обмеженістю, по об'єму і номенклатурі, масивів статистичних даних, які характеризують роботу реальних систем захисту інформації у складі КСЗІ. Такий недолік інформації збільшує множину варіантів розвитку вихідних ситуацій, і кожен з них повинен бути проаналізований, що стає можливим при застосуванні теорії ігор.

При існуванні відомої функціональної залежності критерію оптимізації від вхідних управляючих параметрів, задача оптимізації зводиться до знаходження таких параметрів, при яких цільова функція доходять до екстремуму. Коли на об'єкт впливають загрози, то залежність має не функціональну а регресивну залежність, яка утворює поверхню відклику.

Для знаходження екстремуму існує два принципово різних підходів:

1. Коли мається можливість знайти *n* - факторну математичну модель в той частині простору дослідження, де розташований екстремум, то задача вирішується аналітичними або чисельними методами – формалізованим способом.

2. Коли математичний опис не отримується, то виконується експериментальний пошук області екстремуму.

12.3.1. Визначення математичної моделі конфлікту загроз з комплексною системою кіберзахисту інформації

Побудова моделі взаємовідносин загроз і систем захисту інформації може бути виконана на основі умовної гри двох або більше гравців, яка ефективно вирішується з використанням потужних технологій. В цієї моделі першим гравцем буде система захисту інформації. Стратегії КСЗІ уявляють собою набір

методів і засобів, які забезпечують захист інформації за допомогою адміністративних, технічних і програмно-апаратних складових.

Іншими (n - 1) – гравцями (n – це загальне число гравців під час моделювання) є загрози. Стратегії загроз – це реалізації впливів на КСЗІ шляхом атак, аварій систем захисту та відмов, в результаті яких буде порушені конфіденційність, цілісність, доступність та спостережність інформації.

З теорії ігор відомо, що ігри мають продовження в тому випадку, коли в грі n – гравцям дозволяється утворювати визначенні коаліції (*в цієї моделі утворювання коаліції загроз та системи захисту неможливо і не дозволяється*).

Позначимо через N множину усіх гравців, при $N = \overline{1,n}$; а через K – будь-яку підмножину цієї множини. Пускай гравці (загрози) з K домовляються між собою про узгоджені дії і, таким чином, утворюють коаліцію. Утворив коаліцію, множина K - гравців діє як один гравець проти інших гравців, і виграш цієї коаліції залежить від застосування стратегій кожним з n - гравців.

Для опису гри необхідно визначити характеристичну функцію v, яка ставить, у відповідності кожній коаліції K найбільший, вірно отриманий виграш $v(K)$. Потужність множини коаліцій, на якій визначена характеристична функція, дорівнює 2^n, причому коаліція з номером 0, є пустою коаліцією і її виграш, згідно умови, завжди дорівнює нулю.

Для рішення гри слід побудувати оптимальний розділ, який розподіляє перемоги $X = \overline{x_1, x_n}$, гравців з врахуванням наступних умов:

1. $x_i \geq v(N), i \in N$ – принцип індивідуальної раціональності.
2. $\sum_{i \in N} x_i = v(N)$ – принцип колективної раціональності.

В бескоаліційних іграх закінчення гри формується в результаті дій гравців, які в цій ситуації отримали свій виграш.

Можливість визначення кооперативної гри множиною ігор розглянута в [10, 11], де приводиться опис способів побудови біматричних ігор.

Для визначення порядку проведення, кооперативна гра задається у вигляді $n \times (n-1)$ матриць розміру $k \times g$, де n – кількість гравців, k – кількість стратегій у гравців, наприклад:

$$A_{xy} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ a_{g1} & a_{g2} & \cdots & a_{gk} \end{bmatrix}, \qquad (12.8)$$

де $a_{ij} (i = \overline{1,k},\ j = \overline{1,g})$ – виграш гравця x в грі з гравцем y. Стратегії коаліції визначаються вибором гравців – учасників коаліції (загроз або бар'єрів

механізмів захисту системи захисту інформації). Таким чином, коаліція з m гравців буде мати k^m чистих стратегій, де k – число виборів у кожного гравця.

В подальшому необхідно знайти матриці виграшей усіх коаліцій в грі з іншими гравцями (кожна загроза перекривається бар'єром у складі механізмів захисту системи захисту інформації). Кожна матриця розміру $k^m \times g^{n-m}$ (де m – кількість гравців в коаліції яка приймає участь в грі) має вигляд:

$$A_{\overline{xy}} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1k^{n-m}} \\ b_{21} & b_{22} & \cdots & b_{2k^{n-m}} \\ \cdots & \cdots & \cdots & \cdots \\ b_{g^{m_1}} & b_{g^{m_2}} & \cdots & b_{g^{m_k}{}^{n-m}} \end{bmatrix}, \qquad (12.9)$$

при $0 < m \leq n$, де b_{ij} – виграш коаліції $\bar{X}$ в грі з коаліцією $\bar{Y}$, причому i та j – комбіновані стратегії коаліції.

Кожна біматрична гра описується двома матрицями, які зводяться до задачі лінійного програмування і вирішуються за допомогою симплекс методу. В результаті отримаємо характеристичну функцію.

Для находження результатів гри використовується принцип оптимальності розподілу виграшу між гравцями, який в задачі теорії кооперативних ігор має назву вектору Шеплі.

Представимо кооперативну гру КСЗІ та загроз у вигляді сукупності біматричних ігор наступного вигляду:

$$A_{XY_{kg}} = \begin{bmatrix} -a_{11} & -a_{12} & \cdots & -a_{1k} \\ -a_{21} & -a_{22} & \cdots & -a_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{g1} & -a_{g2} & \cdots & -a_{gk} \end{bmatrix}, \qquad (12.10)$$

де X – це КСЗІ, Y_{kg} – k-та загроза (зловмисник, атака, відмова), або їх коаліція, $-a_{ij}(i = \overline{1,k},\ j = \overline{1,g})$ - включає до себе витрати на КСЗІ, яка реалізує i-ю стратегію та втрати від дій загроз, які реалізують j-ю стратегію.

$$B_{XY_{kg}} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1k^{n-m}} \\ b_{21} & b_{22} & \cdots & b_{2k^{n-m}} \\ \cdots & \cdots & \cdots & \cdots \\ b_{g^{m_1}} & b_{g^{m_2}} & \cdots & b_{g^{m_k}{}^{n-m}} \end{bmatrix}, \qquad (12.11)$$

де b_{ij} – користь від подолання КСЗІ, яка реалізує i-ю стратегію, за винятком витрат на реалізацію загрози, i – номер стратегії КСЗІ, j – номер загрози.

Таким чином матриці загроз визначаються, як:

$$A_Y = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ a_{g1} & a_{g2} & \cdots & a_{gk} \end{bmatrix}, B_Y = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1k^{n-m}} \\ b_{21} & b_{22} & \cdots & b_{2k^{n-m}} \\ \cdots & \cdots & \cdots & \cdots \\ b_{g^{m_1}} & b_{g^{m_2}} & \cdots & b_{g^{m_k n-m}} \end{bmatrix}, \quad (12.12)$$

де a_{ij} – аналіз усіх загроз, які впливають на КСЗІ, b_{ij}– користь, яку отримують загрози, від подолання КСЗІ.

Аналогічно матриці роботи КСЗІ будуть мати вигляд:

$$A_X = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ a_{g1} & a_{g2} & \cdots & a_{gk} \end{bmatrix}, B_X = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1k^{n-m}} \\ b_{21} & b_{22} & \cdots & b_{2k^{n-m}} \\ \cdots & \cdots & \cdots & \cdots \\ b_{g^{m_1}} & b_{g^{m_2}} & \cdots & b_{g^{m_k n-m}} \end{bmatrix}, \quad (12.13)$$

де a_{ij} – кількість механізмів захисту у складі КСЗІ, b_{ij}– аналіз процесу відмови або пошкодження механізмів захисту КСЗІ (або навпаки, аналіз процесу блокування механізмами захисту) загроз, які впливають на КСЗІ.

Для рішення кооперативних ігор застосовується об’єднання коаліційних ігор в стратегічні ігри і рішення кожної симплекс-методом, для подальшого находження тих або інших результатів.

Для розкриття роботи КСЗІ можна визначити матриці роботи бар’єрів у складі h – кількості механізмів захисту, які в свою чергу також розкриваються згідно (12.13).

12.3.2. Проектне моделювання конфлікту загроз з комплексною системою кіберзахисту інформації

Для формалізації процесу моделювання конфлікту загроз з КСЗІ розглянемо типову модель захисту інформації з повним перекриттям загроз (рис. 12.7).

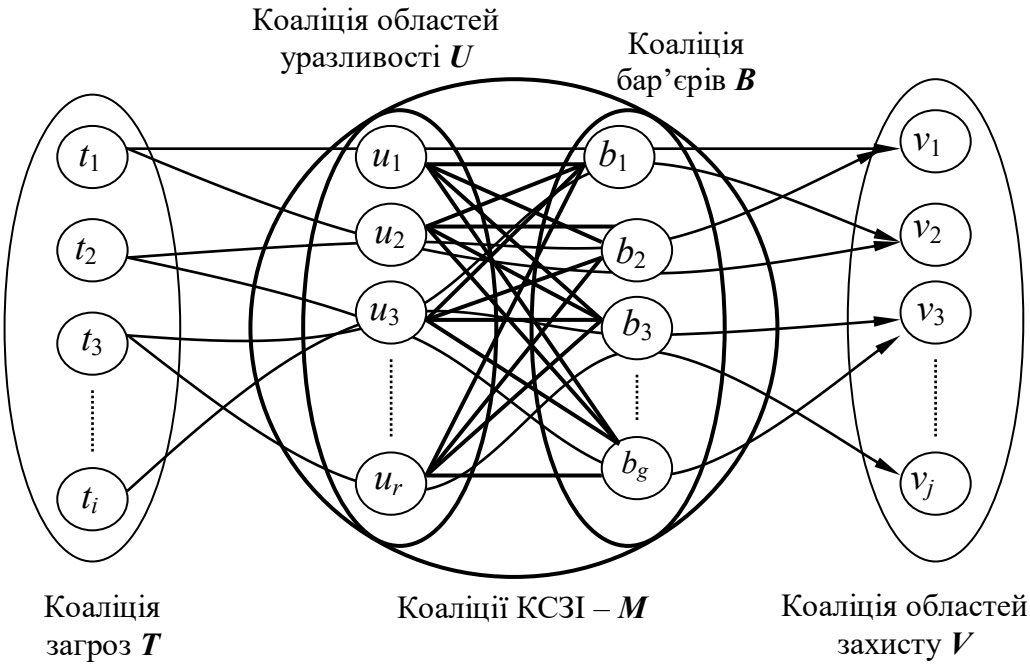


Рис. 12.7. Коаліції , які створюються в моделі захисту інформації з повним перекриттям загроз

Ця модель описує процес взаємодії загроз та ресурсів КСЗІ (бар'єрів та механізмів захисту у складі КСЗІ).

Можна виділити 3 коаліції:

$T = \{t_i\}$ – коаліція загроз, де i – кількість загроз, при $i = \overline{1, I}$;

$V = \{v_j\}$ – коаліція ресурсів інформаційної системи, які необхідно захищати, де j – кількість ресурсів, при $j = \overline{1, J}$;

$M = \{m_k\}$ – коаліція механізмів захисту КСЗІ, де k – кількість механізмів захисту у складі КСЗІ, при $k = \overline{1, K}$;

В механізмах захисту – m_k, КСЗІ – M, маються наступні коаліції:

$U = \{u_r\}$ – області уразливості КСЗІ, де r – кількість місць уразливості, при $r = \overline{1, R}$;

$B = \{b_q\}$ – бар'єри захисту, де q – кількість бар'єрів захисту КСЗІ, при $q = \overline{1, G}$.

В цьому випадку КСЗІ розглядається як сукупність коаліцій:

$$M = \{m_k\} = \{U \times B\} \qquad (12.14)$$

Згідно (12.14) механізм захисту визначається як коаліція бар'єрів, які перекривають одне з областей уразливості КСЗІ (рис. 12.8).

З урахуванням вище приведеного можна визначити умови захисту інформації:

$$\forall < t_i, v_j> \in \mathbf{M} \exists \{<u_r, b_g> \mid f(t_i, v_j)\}, \qquad (12.15)$$

де функціонал $f(t_i, v_j)$ – описує виконання умов забезпечення захисту інформації об'єкту v_j при наявності загрози t_i .

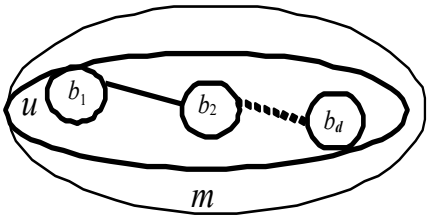


Рис. 12.8. Механізм захисту КСЗІ, який складається з коаліцій бар'єрів та областей уразливості

Таким чином, для КСЗІ з повним перекриттям загроз, існують такі бар'єри, які вступають в "гру" (в конфлікт) з загрозами для інформаційної системи (коаліцій областей захисту).

Наступальну гру коаліцій загроз можна описати аналітично у вигляді функціональних залежностей, які пов'язують характеристики загроз $t_i \in T$ та областей захисту $v_j \in V$.

Кожна з величин $v_j \in V$ залежить від r - координат областей уразливості і g - координат знаходження бар'єрів в механізмах захисту. Ступінь залежності величин v_j залежить від векторів координат областей уразливості механізмів захисту $u_r \in U$ та бар'єрів $b_g \in B$ і визначається передаточними функціями a_{kg}, c_{kg}, d_{kg}.

В загальному вигляді наступальну стратегічну гру коаліцій загроз та КСЗІ можна описати виразом у вигляді:

$$V(p) = T(p) \times \mathbf{A}_{kg} + U(p) \times \mathbf{C}_{kg} + B(p) \times \mathbf{D}_{kg}, \qquad (12.16)$$

де $V(p)$, $T(p)$, $U(p)$, $B(p)$ – матриці коаліцій, які розглядаються в грі, розмерностью $j \times 1$, де p – оператор Лапласа. $\mathbf{A}_{kg}$, $\mathbf{C}_{kg}$, $\mathbf{D}_{kg}$ – передаточні матриці взаємовідносин коаліцій, які розглядаються, розмірністю $k \times g$.

Матриці коаліцій та передаточних взаємозв'язків між ними мають вигляд:

$$V(p)=\begin{bmatrix} v_1(p) \\ v_2(p) \\ \cdots \\ v_j(p) \end{bmatrix};\ T(p)=\begin{bmatrix} t_1(p) \\ t_2(p) \\ \cdots \\ t_i(p) \end{bmatrix};\ \mathbf{A}_{kg}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ a_{g1} & a_{g2} & \cdots & a_{gk} \end{bmatrix};$$

$$U(p)=\begin{bmatrix} u_1(p) \\ u_2(p) \\ \cdots \\ u_r(p) \end{bmatrix};\ \mathbf{C}_{kg}=\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1k} \\ c_{21} & c_{22} & \cdots & c_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ c_{g1} & c_{g2} & \cdots & c_{gk} \end{bmatrix};\ B(p)=\begin{bmatrix} b_1(p) \\ b_2(p) \\ \cdots \\ b_s(p) \end{bmatrix}. \quad (12.17)$$

$$\mathbf{D}_{kg}=\begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1k} \\ d_{21} & d_{22} & \cdots & d_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ d_{g1} & d_{g2} & \cdots & d_{gk} \end{bmatrix}.$$

Підставляючи вираз (12.16) в рівняння (12.17) отримуємо кінцеву залежність результатів стратегічної гри між коаліцією загроз та сукупністю коаліцій КСЗІ.

$$\begin{bmatrix} v_1(p) \\ v_2(p) \\ \cdots \\ v_j(p) \end{bmatrix}=\begin{bmatrix} t_1(p) \\ t_2(p) \\ \cdots \\ t_i(p) \end{bmatrix}\times\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ a_{g1} & a_{g2} & \cdots & a_{gk} \end{bmatrix}+\begin{bmatrix} u_1(p) \\ u_2(p) \\ \cdots \\ u_r(p) \end{bmatrix}\times\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1k} \\ c_{21} & c_{22} & \cdots & c_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ c_{g1} & c_{g2} & \cdots & c_{gk} \end{bmatrix}+$$

$$+\begin{bmatrix} b_1(p) \\ b_2(p) \\ \cdots \\ b_s(p) \end{bmatrix}\times\begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1k} \\ d_{21} & d_{22} & \cdots & d_{2k} \\ \cdots & \cdots & \cdots & \cdots \\ d_{g1} & d_{g2} & \cdots & d_{gk} \end{bmatrix} \quad (12.18)$$

Для доказу виразу (12.18) можна розглянути рис. 12.9, на якому представлений приклад умовної гри коаліцій загроз та КСЗІ.

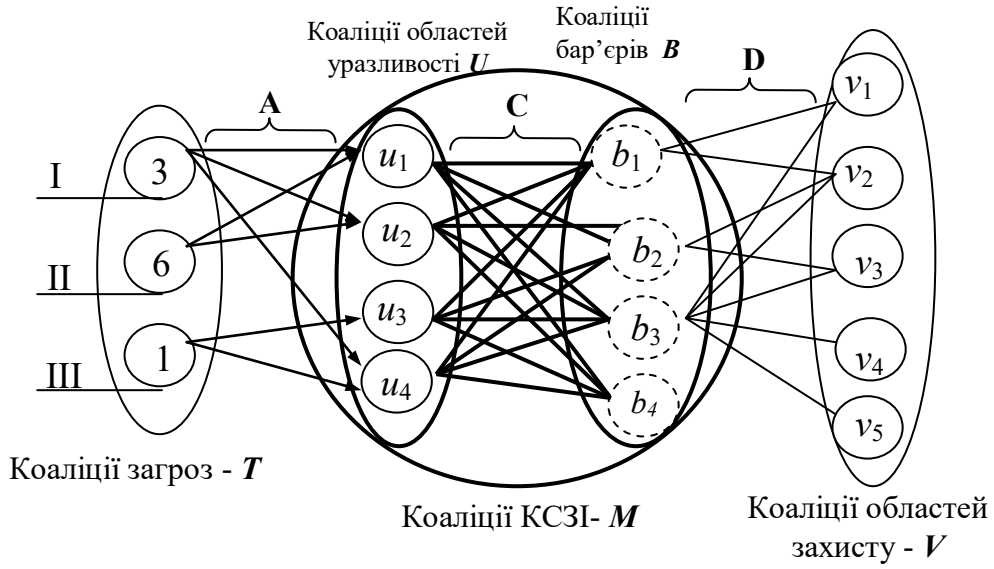


Рис. 12.9. Стратегічна гра (конфлікт) між коаліціями загроз та КСЗІ

Умовно позначимо кількість загроз (причому для розрахунку не будемо їм придавати вагові коефіцієнти. Тільки розподілимо їх на класи: атак – I, відмов – II та аварій – III). В цьому випадку не розглядаються вагові коефіцієнти можливості впливу загроз на КСЗІ, які в своєї коаліції впливають на КСЗІ.

Розглянемо крайні випадки коаліційної гри.

Приклад 1.

Умови гри: Необхідно проаналізувати роботу КСЗІ при "відсутності бар'єрів КСЗІ" (бар'єри не затримують загрози). Тобто моделюються шляхи впливу коаліції загроз на коаліцію областей захисту.

Приклад 2.

Умови гри: Необхідно проаналізувати роботу КСЗІ при наявності різних по стійкості бар'єрів захисту КСЗІ. Тобто необхідно оцінити роботу КСЗІ в умовах нестабільних по стійкості бар'єрів. При цьому бар'єр b_1 може пропустити загрозу з вірогідністю $P_{b_1} = 0,2$; бар'єр b_2 – з вірогідністю $P_{b_2} = 0,4$; а наступні бар'єри: $P_{b_3} = 0,1$; $P_{b_4} = 0,3$.

Приклад 3.

Умови гри: Необхідно проаналізувати роботу КСЗІ при наявності стійких бар'єрів захисту (бар'єри повністю блокують загрози). Тобто КСЗІ побудована правильно.

Використовуючи вираз (12.18) можна отримати графік, який зображений на рис. 12.10.

З рис. 12.10 можна зробити висновок, що ефективність роботи КСЗІ залежить від стійкості бар'єрів. Але в подальшому необхідно звернути увагу на взаємозв'язки – передаточні функції, які є зв'язуючим елементом цієї гри. Від кількості цих зв'язків в пряму залежить ефективність та стійкість роботи КСЗІ.

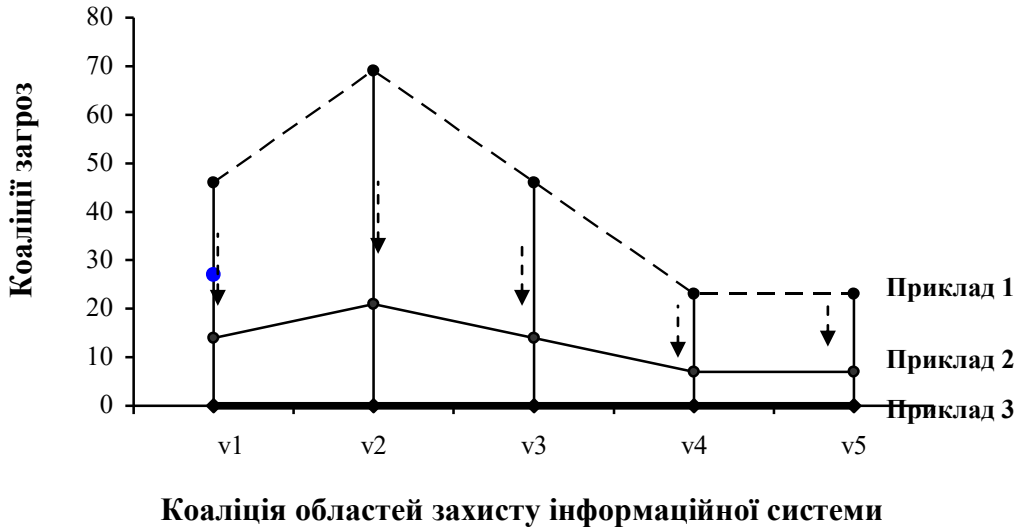


Рис. 12.10. Ефективність стратегічної гри коаліцій загроз та КСЗІ

Під час проектного моделювання необхідно розраховувати кількісні та якісні попередні показники ефективності захисту інформації системи, яка проектується. Це важливо тому, що закладені на цьому етапі критерії та показники в подальшому можуть звезти на нуль усю велику роботу, витрати та цінність інформації, які закладаються та відпрацьовуються на усіх етапах створення як інформаційної системи в цілому так і КСЗІ вчасності.

12.4. Визначення показників якості захищеності моделі кіберзахисту інформації

Показники необхідності використання КСЗІ характеризують властивість КСЗІ, яка визначає і обумовлює її корисність, специфіку, призначення і використання.

Ці показники можуть бути представлені в вигляді:

$$P_{\text{н}} = (\{N_m\}, \{G\}, \{f_m\}, \vartheta), \tag{12.19}$$

де $\{N_m\}$ – множина задач і функцій, які вирішуються в КСЗІ; $\{G\}$ – множина вимог та умов функціонування, які виконуються (у відповідності з замовленням або документацією); ϑ – кількість задач, які необхідно вирішити в КСЗІ, $m = 1, \vartheta; \{f_m\}$ – індикаторна функція впровадження задач спеціального програмного забезпечення КСЗІ, яка визначається виразом:

$$f_m = \begin{cases} 1, - & \text{задача вирішується} \\ 0, - & \text{задача не вирішується.} \end{cases} \quad (12.20)$$

Показники необхідності можуть визначатися різними відношеннями елементів множин. Найбільш представницьким (превалюючим) показником необхідності є показник впровадження функціональних задач, функцій, умов $K_{вз}$. В загальному випадку:

$$K_{вз} = \prod_{m=1}^{g} f_m, \quad (12.21)$$

де $K_{вз}$– визначає ступінь впровадженості задач в КСЗІ ($K_{вз} = 0$ або 1).

Коли хоча-б одна з задач, які необхідно вирішувати в КСЗІ, не виконується (не реалізується), КСЗІ не може в повній ступені використовуватися по призначенню. В цьому випадку $K_{вз} = 0$.

Показники продуктивності відображають основні вірогіднісно-часові характеристики процесу виконання функцій (рішення задач) КСЗІ.

В якості показників продуктивності можуть використовуватися, наприклад, потенціальна продуктивність КСЗІ при рішенні комплексу функціональних задач, математичне очікування часу реакції на вплив загроз, середній час відбиття загроз тощо. Аналіз показує, що інтегральним, головним показником цієї групи є своєчасність (оперативність), яка визначається вірогідністю $P\left(T_{обр} \le T_{д}\right)$ того, що час обробки і рішення комплексу функціональних задач виконується за час, який не перевищує директивний (визначений).

Показники надійності визначають властивості КСЗІ, які дозволяють зберігати працездатність під час відмов її елементів або груп елементів. Тобто надійність КСЗІ – це властивість системи зберігати свої функції згідно визначених розробником умов роботи її елементів.

По числу можливих станів (працездатності) елементи КСЗІ можуть знаходитися у двох станах – працездатному або непрацездатному, а по режиму застосування (функціонування) КСЗІ відноситься до систем безперервного застосування. КСЗІ відноситься до систем, які в процесі експлуатації можуть відмовитися або перейти в критичний стан.

Критеріями відмови КСЗІ є:

− припинення виконання КСЗІ заданих функцій, зниження якості функціонування до критичного рівня;

− неправильне рішення задач захисту від відмов.

Критеріями критичних станів КСЗІ є:

− відмова однієї або декількох складових частин системи, відновлення або заміна, яких, повинна проводитися в ремонтних органах;

− зниження показників якості властивостей КСЗІ до критично допустимого рівня;

− зниження напрацювання на відмову нижче заданого рівня;

− перевищення встановленого рівня існуючих (сумарних) витрат на розробку, впровадження та експлуатацію КСЗІ, яке визначає економічну невигідність системи захисту по відношенню з важливістю інформації, яку необхідно захищати.

По наслідкам відмов або досягнень критичного стану при застосуванні комп'ютерна техніка відноситься до виробів, відмови яких або перехід в критичний стан яких не приводить до катастрофічних наслідків (загрози для людини), але загрози потенційного впливу на інформацію, яка циркулює в комп'ютерних мережах, можуть привести до катастрофічних наслідків як для людини, так і для суспільства (в залежності від самої інформації і задач інформаційної системи).

По впливу відмов на результат виконання задач КСЗІ можна класифікувати як систему, у якій вихідний ефект застосування пропорціональний сумарному часу безвідмовної роботи.

По можливості відновлення працездатності після відмов, в процесі експлуатації КСЗІ відноситься до систем, які відновлюються.

Враховуючи вищесказане, в якості основного інтегрального показника надійності КСЗІ вибирається $K_г$ − коефіцієнт готовності КСЗІ до роботи. Тому коефіцієнт готовності визначається, як вірогідність того, що КСЗІ буде працездатним в випадковий момент часу:

$$K_г = {T_{рп}}/{(T_{рп} + T_{чв})}, \qquad (12.22)$$

де $T_{рп}$− час роботи КСЗІ при використанні по призначенню; $T_{чв}$− час на відновлення елементів КСЗІ.

Показники живучості КСЗІ визначають спроможність системи компенсувати (повністю або хоча-б частково) вплив небезпечних зовнішніх впливів (атак) на якість її цільового функціонування відповідним чином організованої реакцією своєї структури або алгоритму функціонування.

Тобто живучість КСЗІ це спроможність системи виконувати хоча-б мінімальний встановлений об'єм функцій при зовнішніх впливах, не передбачених умовами нормальної експлуатації.

Під час аналізу живучості КСЗІ оцінюється:

1) ціль функціонування КСЗІ (де, в якій системі і для захисту якої інформації встановлюється);

2) множина задач, рішення яких забезпечує система захисту;

$$Z = \{z_1, z_2, ..., z_k\}. \quad (12.23)$$

3) множина бар'єрів, які є складовими частинами КСЗІ.

$$B = \{b_1, b_2, ..., b_g\}. \quad (12.24)$$

В КСЗІ, яка має властивості живучості, можна визначити три типу цілей функціонування:

1. В системі захисту повинно забезпечуватися рішення всієї множини задач Z з заданою ефективністю (наприклад, з дотриманням критеріїв конфіденційності, цілісності) в вільному стані $d \in D$, тобто повинна виконуватися умова:

$$Z = \prod_{i=1}^{k} x(Z_i) = 1, \text{при } x(Z_i) = \begin{cases} 1, \text{коли задача } Z_i \text{ вирішується в КСЗІ} \\ 0, \text{в протилежному випадку.} \end{cases} \quad (12.25)$$

2. Система захисту в будь-яких можливих станах $d \in D$ повинна виконувати з заданою ефективністю деяку (пріоритетну) підмножину задач z^* з множини Z_i, які можуть виконуватися в системі у випадку звільнення необхідних ресурсів. Таким чином, множина задач, яка виконується КСЗІ, залежить від стану, в якому знаходиться система і не є постійною:

$$Z \subseteq \sum_{i=1}^{k} x(z_i^*). \quad (12.26)$$

3. Система повинна забезпечувати рішення хоча б однієї (можливо найбільш важливої) задачі $\hat{z}$ з підмножини z^* в своєму вільному стані $d \in D$, тобто:

$$Z = \subseteq \sum_{i=1}^{k} x(\hat{z_i}). \quad (12.27)$$

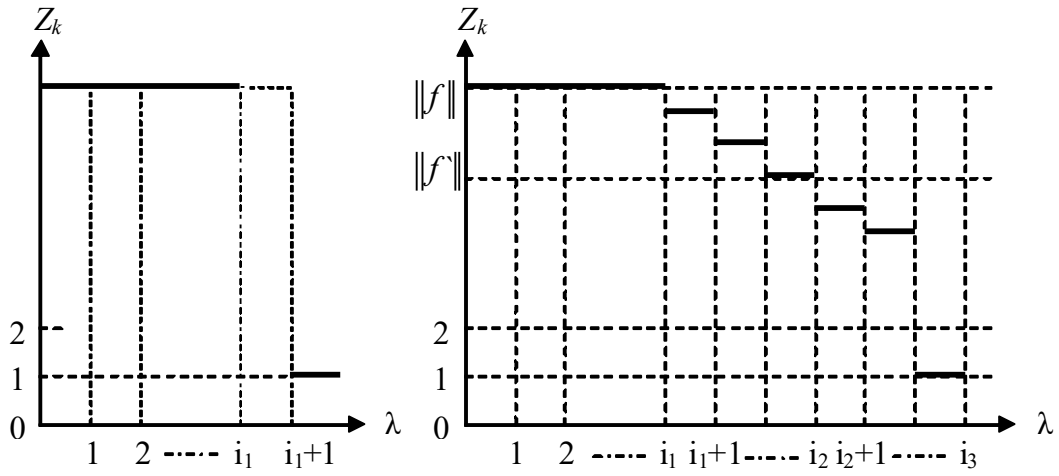
Оцінка живучості КСЗІ повинна будуватися з врахуванням цілі функціонування.

Ціль функціонування – це поняття, яке вводиться для живучих та відмовостійких систем, однак зміни цілей можливі тільки для систем, які мають властивості живучості.

Якісна залежність цілі функціонування від кількості функціональних відмов, під час впливу загроз (атак), або технічних, програмних відмов для відмовостійких та живучих систем надана на рис. 12.11.

Як зрозуміло з рисунку деградація системи, яка має властивості живучості, їде “плавно” на відміну від відмовостійких систем. Це забезпечується засобами, які дозволяють перебудовуватися на виконання “нової” цілі функціонування, для якої в системі можна добитися необхідної якості виконання

Показники ступеню захищеності інформації характеризують рівень захищеності інформації, який забезпечує КСЗІ. В цій показник, як приклад, можуть входити оцінки захищеності, які забезпечуються на окремих елементах КСЗІ (бар’єрах механізмів захисту).



а) відмовостійкі системи б) живучі системи

Рис. 12.11. Якісна залежність цілі функціонування від кількості відмов в різних системах

В загальному випадку, показник ступеню захищеності інформації в КСЗІ розглядається як:

$$P_з = \langle \{Y_i\}, \{q_i\}, n, \{P_{nj}\}, Z, \{P_{\text{дод}}\} \rangle, \qquad (12.28)$$

де $\{Y_i\}$ – множина якісних вимог до КСЗІ по захисту інформації згідно, $i = \overline{1,n;}$ – кількість класів захисту, де n – кількість бар'єрів захисту; $\{q_i\}$ – ступінь реалізації вимог i-го класу захисту; $\{P_{nj}\}$ – множина показників блокування загроз бар'єрами механізмів захисту КСЗІ, $j = \overline{1,z;}$ – кількість зон, рівнів, засобів захисту; $\{P_{\text{дод}}\}$ – множина додаткових показників, які уточнюють, при необхідності, вибір $P_{\text{з}}$.

Частіше усі вимоги захищеності інформації неможливо розглянути на етапі проектування, тому цій показник відносять до розряду обмежень і рахують у вигляді мультиплікативного критерію:

$$P_{\text{з}} = \prod_{i=1}^{n} P_{\text{зі}}, \tag{12.29}$$

де $P_{\text{зі}}$ – індикаторна функція вигляду:

$$P_{\text{зі}} = \begin{cases} 1, - & \text{вимоги виконуються} \\ 0, - & \text{вимоги не виконуються.} \end{cases} \tag{12.30}$$

Показники технічного рівня характеризують як критерії додержання відповідних концепцій на основі розробок, які існують, які мають якісні властивості по відношенню з кращими зразками (в цьому випадку засобами обчислювальної техніки, програмного забезпечення, комунікаційного обладнання тощо) та кращі показники фізичного та морального старіння.

Показник технічного рівня може бути представлений у наступному вигляді:

$$P_{\text{тр}} = \langle \{P_{\theta}\}, \{P_{\theta\text{б}}\} \rangle, \tag{12.31}$$

де $\{P_{\theta}\}$ – множина значень параметрів, які використовуються і оцінюються в КСЗІ; $\{P_{\theta\text{б}}\}$ – множина досяжних (кращих), технічно реалізованих значень параметрів окремих базових засобів в КСЗІ.

Вартісні показники характеризують матеріальні і часові витрати на КСЗІ на різних етапах життєвого циклу КСЗІ.

До складу цієї групи входять: $C_{\text{р}}$– витрати на етапі розробки, $C_{\text{ве}}$ – витрати на етапі вводу до експлуатації КСЗІ, $C_{\text{е}}$ – вартість експлуатації КСЗІ продовж визначеного строку і $C_{\text{КСЗІ}}$ – як комплексна основна вартісна складова.

Найбільш повно характеризує вартісну складову КСЗІ її загальна вартість з врахуванням витрат на основних етапах життєвого циклу. В загальному вигляді цій показник може бути представлений як:

$$C_{\text{КСЗІ}} = C_{\text{р}} + C_{\text{ве}} + C_{\text{е}}. \tag{12.32}$$

Приведена система показників якості захисту інформації в різній ступені характеризує КСЗІ. Обрані показники утворюють систему взаємопов'язаних (в загальному випадку) показників, які характеризують якісні властивості КСЗІ, з урахуванням складу, динаміки і процесів розвитку, витратних механізмів, які відрізняються повнотою і достатністю на етапі проектування.

Ще до початку розробки КСЗІ розробнику необхідно визначитися, в яких рамках повинна бути стійка КСЗІ, і як вона повинна працювати в інформаційній системі, до якої приділяються вимоги конфіденційності, цілісності, доступності та спостережності інформації. Відомо, що рівень захисту інформаційних систем визначається системою кількісних та якісних показників, які представлені, як правило, в лінгвістичній, нечітко визначеною замовником формою, які інтерпретуються через еталони параметрів. Тому формалізація проектних показників якості захисту інформації в КСЗІ є необхідною умовою для діагностики проектних рішень по створенню систем захисту інформації.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Розкрити неформальні методи моделювання комплексних систем захисту інформації.
2. Розкрити неформальні методи оптимальних рішень під час моделювання КСЗІ.
3. Розкрити порядок структурування архітектури та процесів складних систем.
4. В чому заключається процес моделювання КСЗІ та основне призначення моделей.
5. Розкрити признаки класифікації моделей захисту інформації.
6. Як класифікуються моделі захисту інформації по способу їх реалізації.
7. Як класифікуються моделі захисту інформації по характеру процесів в системі.
8. Як класифікуються моделі захисту інформації по характеру підходів до моделювання об'єктів.
9. Як класифікуються моделі захисту інформації по призначенню об'єктів дослідження.
10. Як класифікуються моделі захисту інформації по характеристикам об'єктів дослідження.
11. Розкрити загальну модель процесу захисту інформації.
12. Розкрити модель системи захисту інформації з врахуванням взаємозв'язків системи захисту інформації, джерела інформації та користувача інформації.
13. Розкрити загальну типову модель процесу захисту інформації з повним перекриттям загроз.

14. Розкрити модель багаторівневого захисту від загроз НСД.

15. Розкрити загальну модель системи захисту інформації.

16. Розкрити моделі Белла і Ла-Падула, Біба.

17. Розкрити моделі Харіссона та Гогена-Мозігера.

18. Розкрити Сазерлендську модель системи захисту та модель Кларка-Вільсона.

19. Визначити математичну модель конфлікту загроз з комплексною системою захисту інформації.

20. Розкрити показники якості захищеності КСЗІ.

21. В чому полягає відмінність відмовостійких та живучих систем захисту інформації.

РОЗДІЛ 13. МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ В СИСТЕМІ КІБЕРЗАХИСТУ

13.1. Розробка формальних моделей інформаційних відносин в системах кіберзахисту

Створення інтенсивної системи комплексного забезпечення безпеки інформаційних технологій неможливе без узагальнення накопиченого досвіду теоретичних досліджень і практичного рішення задач інформаційної безпеки, без розвиненого й адекватного наукового базису, при створенні якого необхідно враховувати виняткову складність теоретичних основ побудови систем захисту інформації. Створення наукового базису, залучення математичних інструментів для обробки даних про інформаційні системи, у свою чергу, неможливо без наявності їх математичних моделей. Оскільки кожна інформаційно-технологічна система включає підсистему захисту інформації, то математична модель необхідна також для автоматизації врахування можливості виникнення як природних, так і штучних каналів втрати інформації, аналізу результатів такої втрати з залученням сучасного математичного апарата, а також для формалізації процесу відновлення системи після атаки.

13.1.1. Модель процесів в системі кіберзахисту інформації, яка заснована на знаковій чутливості

Будь-яка атака, що діє на інформаційно-технологічну систему, на кожному з наявних у розпорядженні системи захисту інформації (СЗІ) засобів захисту відіб'ється по-різному: деякі з засобів можуть бути зруйновані повністю, деякі виведені з ладу частково, а для якихось засобів атака виявиться безпечною.

Врахування цих відмінностей у результатах впливу атаки на засоби захисту є важливим при проектуванні, моделюванні будь-якої СЗІ, а також при встановленні стійкості СЗІ до передбачуваного супротивника. Для формалізації такого врахування необхідно:

- визначити математичний параметр, що характеризує інформаційну систему при її використовуваному математичному представленні, якісні зміни якого є різними для різних збурних дій;
- вибрати спосіб формального представлення атак на СЗІ таким чином, щоб він, будучи простим в обчислювальному сенсі, дозволяв відбити безпосередню спрямованість атаки;
- вибрати простий в обчислювальному сенсі спосіб представлення результату атаки.

Рішення цих задач дасть можливість для створення моделі СЗІ, що дозволить максимально швидко визначати наслідки атаки, виділяючи «постраждалі» і «недоторкані» засоби захисту.

Поняття sign-чутливості інформаційної системи

Будь-яка інформаційна система розглядається як результат рішення задачі про її формування.

Поряд з оцінкою «класичної» чутливості для всебічного аналізу результату деяких задач з галузі інформаційної безпеки значущою також буде оцінка знакової чутливості.

Для визначення *знакової чутливості* (*sign-чутливості)* інформаційної системи у відповідність їй за певними правилами, обговорюваними нижче, ставиться об'єкт P (чи сукупність таких об'єктів):

$$P = \{p_1,..., p_k\},\ \ p_i \in R,\ \ i = \overline{1,k}. \qquad (13.1)$$

Визначення 13.1. Об'єкт P (13.1) будемо називати *sign-чутливим*, якщо навіть малі збурні дії можуть привести до зміни знаків його елементів $p_i \in R,\ \ i = \overline{1,k}$, і *sign-нечутливим* інакше.

Визначення 13.2. *Sign-чутливість інформаційної системи* визначається як sign-чутливість відповідного їй об'єкта (об'єктів) (13.1).

Очевидно, sign-чутливість (sign-нечутливість) будь-якого об'єкта P зведеться до знакової чутливості (нечутливості) його скалярних складових елементів. Природно вважати, що чим більше sign-чутливих скалярних елементів у складі P, тим більше він sign-чутливий у цілому, тим більше sign-чутливою виявиться відповідна інформаційна система. Для пояснення цього розглянемо простір R^n довільної вимірності і визначимо достатні умови знакової чутливості його елементів — точок (векторів) виду $x = (x^1, x^2,..., x^n)^T$, які розглядаються як об'єкти виду (13.1).

Будь-яке збурення для точки x можна представити як її паралельне перенесення, яке змінює в загальному випадку всі її координати, що приведе до зміни довжини й повороту вектора $x=(x^1,x^2,...,x^n)^T$ на деякий кут. Відповідно до визначення 5.1 про sign-чутливість x буде говорити наявність малих за модулем значень її координат. Нехай $x=(x^1,x^2,...,x^n)^T$ має лише одну компоненту x^j, для якої $\left|x^j\right|<<1$. Тоді перевести x в інший координатний ортант, змінивши знак x^j, можуть малі збурні дії — паралельні перенесення на малі відстані, вектори яких паралельні координатній осі, що відповідає x^j, або становлять із цією віссю малий кут чи кут, близький до розгорнутого. Якщо ж малих за модулем компонент у точки x більше однієї, то більше буде й можливостей для різних проявів збурних дій (геометрично — різних напрямків паралельних перенесень), в результаті яких x опиниться в іншому координатному ортанті. Тому природно вважати, що чим більше малих за модулем координат у складі $x=(x^1,x^2,...,x^n)^T$, тим більше sign-чутливою буде точка (вектор) x.

Твердження 13.1. Достатньою умовою sign-чутливості довільного вектора $x\in R^n$ є мализна $\|x\|_1$, де $\|\bullet\|_1$ — векторна 1-норма.

Часто під час роботи з векторами, коли вони використовуються як математичний інструмент для аналізу властивостей реальних об'єктів, застосовують нормування, що дозволяє досягти більшої визначеності в описі вектора, його геометричнім розташуванні, зменшити об'єм досліджуваної інформації, видаляючи з розгляду одну з векторних характеристик — довжину, а також дає можливість у деяких випадках відійти від неоднозначності об'єктів, що визначаються векторами (так роблять, наприклад, при визначенні сингулярних, власних векторів матриць). Тому розглянемо більш докладно поняття знакової чутливості для нормованих векторів — *нормальної знакової чутливості*, чи *nsign-чутливості*.

Нехай вектор $x\in R^n,\ \|x\|=1$. Для наочності викладу як векторна норма тут розглядається 2-норма, хоча може використовуватися й будь-яка інша. Результатом довільної збурної дії для нормованого вектора є лише його поворот на деякий кут.

Визначення 13.3. Нормований вектор x є *чутливим* до збурної дії, якщо навіть мала збурна дія може викликати значне збурення (поворот) вектора x, і *нечутливим* інакше.

Знакова ж чутливість геометрично означає, що x становить малий кут (кути) з координатною площиною (площинами) (вектор $\overrightarrow{OB}$ на рис. 13.1 ($n=3$)), про що свідчить мализна модулів його деяких координат *у порівнянні* з іншими координатами.

Твердження 13.2. Достатньою умовою nsign-нечутливості вектора $x\in R^n,\ \|x\|=1$, є порівнянність між собою значень модулів усіх його координат (малий розкид цих значень у сегменті [0,1]), що геометрично відповідає

порівнянності всіх кутів між вектором і координатними площинами. Чим менше розкид значень модулів координат вектора в сегменті [0,1], тим він менш nsign-чутливий. Найменшій nsign-чутливості відповідає рівність усіх координат вектора (рівність усіх кутів між вектором і його проекціями на координатні площини).

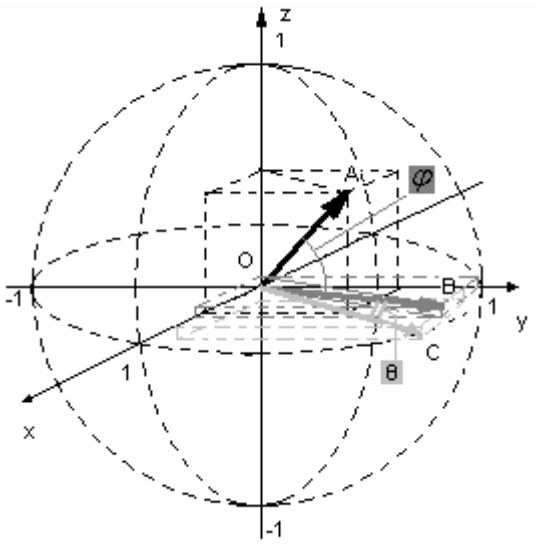


Рис. 13.1. Геометрична інтерпретація nsign-чутливості

Визначення 13.4. Нормований вектор

$$\bar{x} = \left(\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}, ..., \frac{1}{\sqrt{n}} \right)^T \in R^n,$$

що має найменшу нормальну знакову чутливість, назвемо *n-оптимальним*.

Зазначимо, що вказати вектор, який би мав найменшу знакову чутливість, очевидно неможливо.

Розглянемо більш докладно зв'язок між sign- і nsign-чутливістю вектора.

Нехай $x = (\varepsilon, \varepsilon, ..., \varepsilon)^T \in R^n$, де $|\varepsilon| << 1$, тоді $\|x\|_1 = n|\varepsilon|$ може бути як завгодно малою, тобто такий вектор x буде sign-чутливим до збурних дій, однак після його нормування одержимо n-оптимальний вектор $\bar{x}$. Очевидно, що якщо координати ненормованого вектора $x \in R^n$ малі, але порівнянні між собою за модулем, такий вектор завжди буде sign-чутливим і nsign-нечутливим одночасно.

Розглянемо інший приклад. Нехай $x = (E^{(1)}, E^{(2)}, ..., E^{(n)})^T \in R^n$, де $\left|E^{(i)}\right| >> 1,\ i = \overline{1,n}$, тобто x — sign-нечутливий, але координати вектора x не є порівнянними між собою за модулем, тобто існує хоча б пара координат, для

яких: $\left|E^{(i)}\right| << \left|E^{(j)}\right|$. Під час нормування x це приведе до значного розкиду абсолютних значень координат у сегменті [0,1] за рахунок того, що $\frac{\left|E^{(i)}\right|}{\|x\|} << \frac{\left|E^{(j)}\right|}{\|x\|}$, тобто до нормальної знакової чутливості вектора завдяки $i-$й координаті.

Зауваження 13.1. Знакова чутливість (нечутливість) і нормальна знакова чутливість (нормальна знакова нечутливість) в загальному випадку можуть не відповідати одна інший для одного вектора $x \in R^n$.

Розглянемо зв'язок між знаковою й «класичною» (відповідно до визначення 10.3) чутливістю вектора.

Нехай нормований вектор $x \in R^n$ має нормальну знакову чутливість. З цього в загальному випадку не випливає, що він є чутливим (нечутливим). Дійсно, з того, що вектор x має нормальну знакову чутливість випливає лише існування координатних площин (площини) в просторі R^n, з якими вектор x утворює малі кути (кут). Однак геометричне положення вектора в загальному випадку не пов'язане й не визначає його класичну чутливість або нечутливість: геометрія вектора не зашкодить йому відреагувати малим (великим) кутом повороту на малу збурну дію у випадку його нечутливості (чутливості). Аналогічно ніяк не визначає класичну чутливість (нечутливість) вектора його нормальна знакова нечутливість.

Нехай тепер нормований вектор $x \in R^n$ є чутливим (нечутливим) в «класичному» розумінні. У загальному випадку це визначає лише характер його реакції на малу збурну дію — величину кута відхилу від початкового положення — і ніяк не впливає на величини кутів між вектором x і координатними площинами. Таким чином, у загальному випадку чутливість (нечутливість) вектора не визначає його нормальну знакову чутливість (нормальну нечутливість).

На відміну від класичної чутливості, sign-чутливий (nsign-чутливий) вектор може не виявити свою знакову чутливість, навіть перетерпівши велике збурення ($\overrightarrow{OA}$ — результат збурення nsign-чутливого вектора $\overrightarrow{OB}$ (рис. 13.1)). Для реакції sign-чутливого вектора на збурення важливим є геометричний напрямок цього збурення під час його формального представлення, тобто прояв або невияв наслідків знакової (нормальної знакової) чутливості у вигляді зміни знака координат буде залежати від конкретики збурної дії. Однак, якщо вектор $x \in R^n$ є нечутливим, тобто кут його відхилу від початкового положення при малій збурній дії малий, то ймовірність прояву наслідків нормальної знакової чутливості при її наявності в такого вектора, тобто ймовірність того, що цей малий кут все-таки виведе вектор за межі вхідного ортанта, буде очевидно менше, ніж у чутливого у «класичному» розумінні $x \in R^n$. Таким чином, має місце наступне

Твердження 13.3. Чутливість (нечутливість) вектора і нормальна знакова чутливість (нормальна нечутливість) в загальному випадку ніяк не визначають одна іншу, але, чим менш (більш) чутливим буде вектор, тем менш (більш) імовірним буде прояв його нормальної знакової чутливості (при наявності такої) у вигляді зміни знаків (знака) координат.

Таким чином, *знакова чутливість інформаційної системи* при її формальному представленні в виді (13.1) (в виді сукупності об'єктів (13.1)) є тим математичним параметром, що характеризує систему, якісна зміна якого різна для різних збурних дій.

Побудова геометричної моделі процесів в системі захисту інформації

Поставимо у відповідність СЗІ математичний об'єкт (сукупність об'єктів) виду (13.1) наступним чином.

Нехай множина засобів захисту, що входять до СЗІ, — $X = \{x_1, x_2, ..., x_m\}$, а множина можливих атак — $V' = \{V_1', V_2', ..., V_l'\}$. Виділимо в V' атаки, для яких ніяка з них не може бути представлена як комбінація інших, і назвемо їх *незалежними*. Нехай ця множина — $V = \{V_1, V_2, ..., V_n\}$, $V \subseteq V'$. Виберемо для побудови геометричної моделі СЗІ простір R^n (його вимірність співпадає з потужністю множини V). Поставимо в співвідношення $V_i \in V$ однойменний вектор

$$V_i = ae_i, i = \overline{1,n}, \qquad (13.2)$$

де $-1 \le a < 0$ — параметр, вибір якого обговорюється нижче, e_i, $i = \overline{1,n}$ — вектори стандартного базису R^n.

Будь-яка атака $V_i \in V$, що вживана проти СЗІ, практично спрямована на деякі певні засоби захисту $\{x_{i_1}, x_{i_2}, ..., x_{i_k}\} \subseteq X$. Позначимо цю множину $\{x_{i_1}, x_{i_2}, ..., x_{i_k}\} = \overline{X}_i$. Якщо засіб $x_j \notin \overline{X}_i$, то для нього атака V_i безпечна (наприклад, атака, спрямована на виведення з ладу шумової перешкоди, буде безпечною для криптографічних засобів захисту).

Спочатку введемо в модель СЗІ сукупність m векторів простору R^n, кожний з яких відповідає конкретному засобу захисту, що входить до складу системи. Для безпосереднього визначення координат вектора використовуємо підхід, заснований на врахуванні його sign-чутливості.

Для кожного засобу захисту x_i визначимо множину «небезпечних» для нього атак, тобто всіх таких атак $V_j \in V$, що $x_i \in \overline{X}_j$. Позначимо цю множину $\overline{V}_i = \{V_{i_1}, V_{i_2}, ..., V_{i_t}\}$, а $\overline{\overline{V}}_i = V / \overline{V}_i$. Тоді координати однойменного вектора $x_i = \left(x_i^1, x_i^2, ..., x_i^n\right)$, який відповідає засобу $x_i \in X$, визначаться наступним чином:

$$x_i^j = \begin{cases} \varepsilon, \text{ если } V_j \in \overline{V}_i, \\ \qquad\qquad , \quad j = \overline{1,n}, \\ 1, \text{ если } V_j \in \overline{\overline{V}}_i \end{cases} \tag{13.3}$$

де $0 < \varepsilon << 1$.

Для кожного засобу захисту x_i значення координат відповідного вектора явно вказують на атаки, спрямовані проти x_i.

Спочатку кожний вектор x_i знаходиться в першому координатному ортанті, різні координати вектора мають різну знакову чутливість. Для більшої наочності й зручності подальшого викладу побудуємо в R^n опуклий многогранник (у виродженому випадку — опуклий многокутник) S так, щоб кожна з його вершин співпадала з кінцем одного з векторів $x_1, x_2, ..., x_m$, а кінці векторів, що не є вершинами, належали внутрішності S. Многогранник S разом з векторами $x_1, x_2, ..., x_m$ розглядається як геометрична модель СЗІ і позначається $GM1$.

Результат будь-якої атаки V_i природно формалізувати за допомогою паралельного перенесення S вздовж вектора $V_i = ae_i$. Такий спосіб моделювання не тільки надзвичайно простий, він за змістом відповідає тому, що насправді атака завжди спрямована проти інформаційно-технологічної системи в цілому, а її безпосередній вплив на конкретні засоби захисту — це лише спосіб прояву. Крім того, при врахуванні знакової чутливості координат векторів $x_1, x_2, ..., x_m$ результат дії певної атаки буде принципово відрізнятися для різних засобів захисту: можуть «постраждати», змінивши знак своїх координат і початковий координатний ортант, вектори, що відповідають тим засобам, для яких атака була «небезпечною». У той же час, вектори, що відповідають засобам, для яких дана атака була безпечною, хоч і збуряться, але залишаться в межах початкового ортанта. У загальному випадку кути відхилу різних векторів $x_1, x_2, ..., x_m$, які входять до складу моделі $GM1$, від свого початкового положення завдяки атаці будуть різні.

Як було відзначено вище, атака V_j, $V_j \in \overline{V}_i$, проти конкретного засобу захисту x_i може або повністю знищити його, або вивести з ладу частково, лише послабивши його захисні властивості. Моделювання знищення x_i, що відбувається за рахунок переходу вектора, який відповідає атакованому засобу, у відмінний від початкового координатний ортант, досягається шляхом паралельного перенесення S на вектор $V_j = ae_j$, довжина якого $|a|$ більша за ε. При частковім виведенні з ладу x_i довжина відповідного атаці вектора паралельного перенесення повинна бути меншою за ε, що в підсумку збільшить

міру sign-чутливості вектора x_i, залишаючи його в межах вхідного ортанта. Можливо, ступінь часткового руйнування має кілька градацій, що спричинить відмінність у довжині вектора $V_j = ae_j$ паралельного перенесення для S при моделюванні різних проявів цієї атаки.

У результаті атаки V_j при запропонованому способі її формалізації зміниться лише одна j-а координата векторів $x_1, x_2, ..., x_m$, які входять до $GM1$, ставши рівної

$$\bar{x}_i^{(j)} = x_i^{(j)} + a, \qquad (13.4)$$

усі інші координати залишаться без змін. Таким чином, відповідно до (10.4) має місце наступне твердження, що дає оцінку для обчислювальної складності процесу моделювання атаки.

Твердження 13.4. Обчислювальні витрати для моделювання результату атаки на СЗІ при використанні $GM1$ становлять m арифметичних операцій, тобто визначаються лише кількістю наявних засобів захисту, не залежать від виду атаки.

Запропонований спосіб побудови $GM1$ надзвичайно зручний для відображення у вже існуючій моделі змін у СЗІ й множині V. Розглянемо докладно такі модифікації.

1. Додавання в СЗІ нових засобів захисту приведе лише до механічного додавання нових векторів у вже існуючу геометричну модель, яке ніяк не торкнеться побудованих раніше $x_1, x_2, ..., x_m$.

2. Нехай СЗІ зазнає атаки, відсутньої в множині $V = \{V_1, V_2, ..., V_n\}$, але такої, що є комбінацією деяких атак з V. Її моделювання здійснюється на основі елементарних векторних операцій. Нехай, наприклад, атака є деякою комбінацією V_1, V_3. Вона формалізується у вигляді лінійної комбінації відповідних векторів V_1, V_3:

$$W = \alpha e_1 + \beta e_3,$$

де α, β містять інформацію про конкретний прояв кожної з атак V_1, V_3, тобто відіграють роль параметра a в (13.2). Вектор W визначить паралельне перенесення для S. Насправді атака W у цьому випадку може розглядатися як послідовне застосування V_1, V_3, і хоча в реальності розподіл за часом між V_1, V_3 може бути відсутнім, геометрично результат буде абсолютно аналогічний завдяки обраному способу моделювання атаки.

3. Нехай на СЗІ спрямована атака U, яка не належить множині V і не може бути представлена як комбінація елементів цієї множини. «Поповнення» множини V атакою U відіб'ється на моделі СЗІ. По-перше, таке поповнення повинне перевести модель із простору R^n в простір R^{n+1}, по-друге, змінити

координати векторів $x_1, x_2, ..., x_m$ моделі $GM1$. Розглянемо докладно процес модифікації моделі СЗІ в цьому випадку.

Позначимо $U = V_{n+1}$. Нехай атака U спрямована на засоби захисту $x_{u_1}, x_{u_2}, ..., x_{u_k}$, які складають множину $\overline{X}_{n+1}$, а для інших засобів вона безпечна. Для врахування можливості виникнення такої атаки спочатку модель $GM1$ будується не в просторі R^n, а відразу в просторі R^{n+1}, в площині x^{n+1}=1. Це забезпечить рівність 1 останньої координати всіх векторів $x_1, x_2, ..., x_m$: спочатку, поки атака U не належить множині V' як потенційно можлива для СЗІ, вона безпечна для всіх засобів захисту. Введення атаки U у множину V спричинить зміну останньої координати тільки для точок, які відповідають засобам захисту із множини $\overline{X}_{n+1}$, що потребує точно $k \le m$ арифметичних операцій. Ця координата буде дорівнювати ε, що завершить процес модифікації початкової геометричної моделі.

Врахування можливості появи декількох нових атак $U_1, U_2, ..., U_t$ проводиться аналогічно, тільки модель СЗІ спочатку будується не в просторі R^n, а відразу в просторі R^{n+t}, при цьому t останніх координат усіх векторів $x_1, x_2, ..., x_m \in R^{n+t}$ спочатку покладаються рівними 1.

Для випадку $n = 3$, $m = 3$ наочна ілюстрація геометричної моделі СЗІ $GM1$ без врахування можливості виникнення нових атак наведена на рис. 13.2. Внаслідок заподіяної атаки V_2 зруйнувався лише засіб x_2, про що свідчить вектор, який відповідає цьому засобу, що змінив координатний ортант.

Якщо в основу побудови геометричної моделі СЗІ покласти нормальну знакову чутливість, тобто спочатку нормувати вектори $x_1, x_2, ..., x_m$, які відповідають засобам захисту (в результаті отримаємо вектори $x_1', x_2', ..., x_m'$), то модель, що відповідає представленій на рис. 13.2, буде мати вигляд, зображений на рис. 10.3. Далі геометрична модель, заснована на нормальній знаковій чутливості векторів, позначається $GM2$. Многогранник (многокутник) S перейде в деяку зв'язну n-вимірну поверхню, яка є частиною n-вимірної сфери, що є кращим з погляду зручності обробки й аналізу геометричного об'єкта. Моделювання атаки V_i завдяки нормованості $x_1', x_2', ..., x_m'$ зручніше проводити за допомогою повороту сукупної моделі $GM2$ на кут, площина якого паралельна координатній осі, що відповідає i-й координаті вектора. Таким чином, результатом атаки є поворот усіх векторів $x_1', x_2', ..., x_m'$, що входять до $GM2$, на один кут. Перехід вектора в інший координатний ортант завдяки його нормальній знаковій чутливості буде сигналізувати про руйнування відповідного засобу захисту подібно тому, як це відбувалося в $GM1$.

Для $GM2$ з врахуванням твердження 13.4 має місце

Твердження 13.5. Обчислювальні витрати для моделювання результату атаки на СЗІ при використанні моделі $GM2$ становлять $\underline{O}(mn)$ арифметичних операцій.

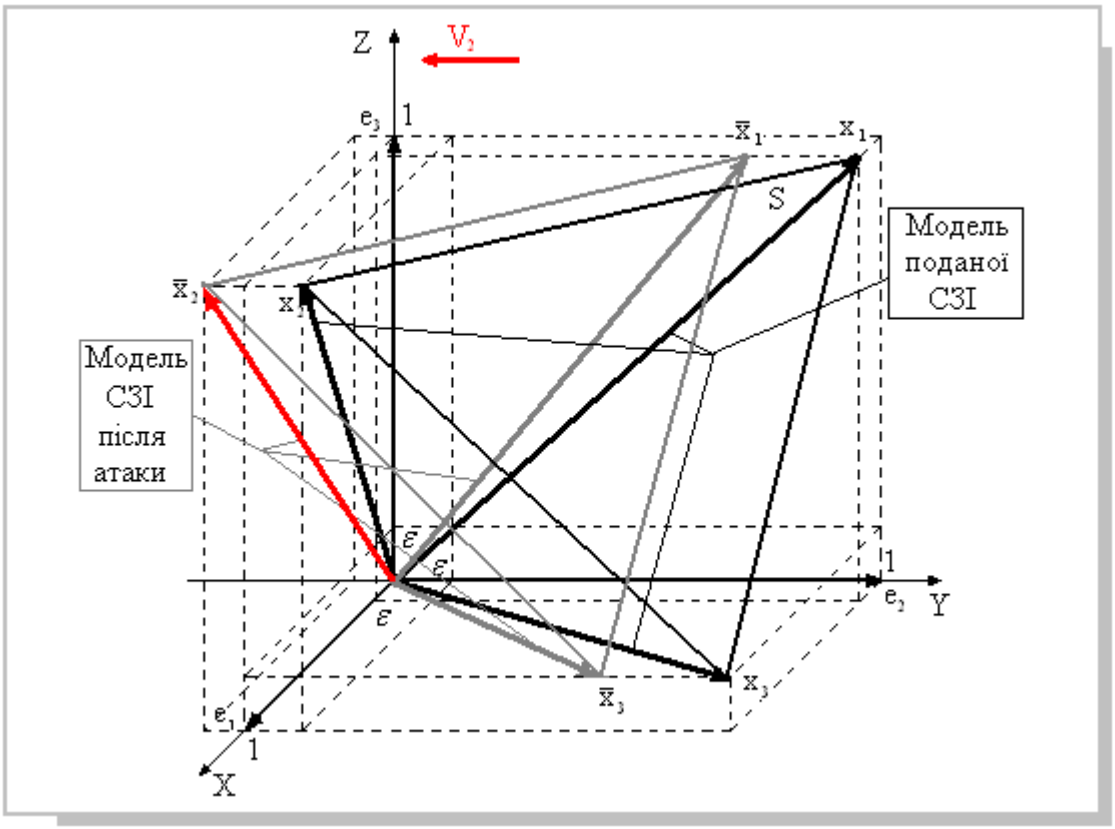


Рис. 13.2. Геометрична модель поданої СЗІ і результат атаки

Оскільки $GM1$ і $GM2$ є формальними представленнями одної СЗІ, отримані одна з іншої, важливим є збереження «статусу» кожного засобу захисту в $GM2$ відносно $GM1$: множини $\overline{V}_i$ «небезпечних» атак для кожного засобу захисту x_i повинні залишитися без змін. Інакше кажучи, знакова чутливість (нечутливість) векторів $x_1, x_2, ..., x_m$ повинна точно відповідати нормальній знаковій чутливості (нормальній нечутливості) $x_1', x_2', ..., x_m'$. Порушення відповідності може відбутися, якщо для деякого вектора x_k значення всіх координат великі, і при цьому існує хоча б одна пара таких, які значно відрізняються між собою, що неможливо за побудовою векторів $x_1, x_2, ..., x_m$ (співвідношення (13.3)), або у випадку, коли серед векторів $x_1, x_2, ..., x_m$ є sign-чутливий по всім координатам $x_i = (\varepsilon, \varepsilon, ..., \varepsilon)^T$. Завдяки цьому природно припустити, що серед усіх засобів захисту, що належать СЗІ, немає таких, для яких усі атаки з множини V є «небезпечними». Оскільки зроблене припущення відповідає реальним СЗІ,

воно не обмежує область застосування запропонованого способу побудови геометричної моделі.

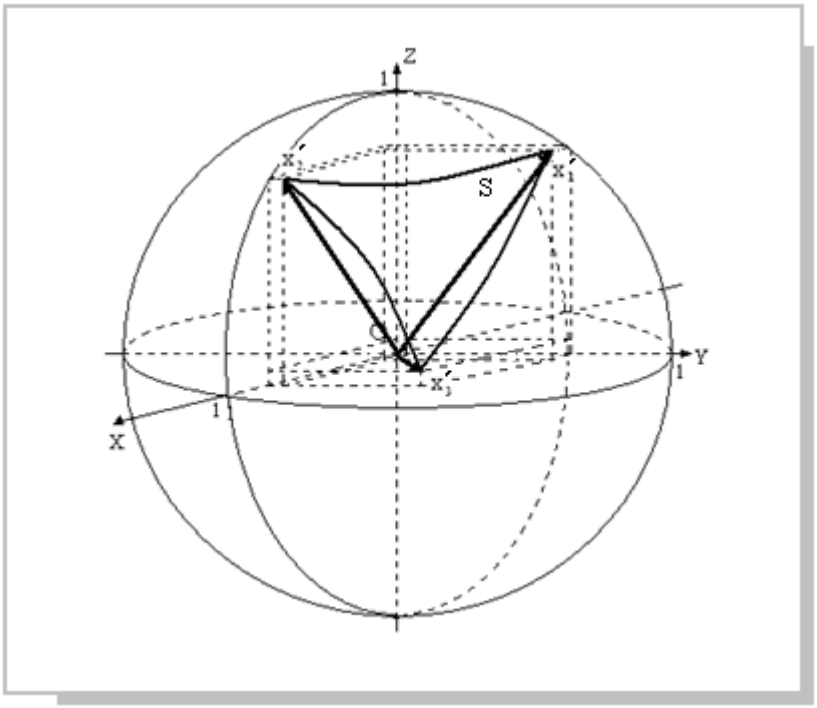


Рис. 13.3. Геометрична модель процесів в СЗІ,
яка заснована на векторній nsign-чутливості

Для обґрунтування наступного зауваження розглянемо приклад. Нехай вектори $x_1,\ x_2 \in R^4$ — нормовані, знаходяться в першому координатному ортанті:

$$x_1 = (0.450,\ 0.210,\ 0.520,\ 0.695)^T,\ x_2 = (0.210,\ 0.695,\ 0.513,\ 0.513)^T.$$

Розкид значень координат у сегменті [0,1] в них однаковий і дорівнює 0.485, а тому твердження 13.2 принципово не може дати відповідь на запитання про вибір з них менш nsign-чутливого вектора.

Зауваження 13.2. Як міру нормальної знакової чутливості ($n-$*міру*) довільного нормованого вектора $x = (x^1, x^2, ..., x^n)^T$, що знаходиться в першому координатному ортанті, природно взяти ступінь його відмінності від $n-$оптимального, чисельним відображенням якого є кут між векторами x і $n-$оптимальним.

Повертаючись до розглянутого вище прикладу, обчислюючи кути між $x_1,\ x_2$ і $n-$оптимальним вектором простору R^4 — $\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)^T$ — отримаємо,

що кути між ним і x_1, x_2 відповідно дорівнюють $20.4^\circ, 15^\circ$, що говоре на користь меншої нормальної знакової чутливості x_2.

Оскільки визначити найменш sign-чутливий вектор неможливо, то неможливим буде і встановлення аналога n – міри для sign-чутливості векторів.

Зауваження 13.3. Уведення n – міри дозволяє порівнювати nsign-чутливості до збурних дій різних нормованих векторів і здійснювати вибір найменш і найбільш nsign-чутливих векторів, тобто таких, які мають найменший і найбільший кут з n – оптимальним відповідно, що дає можливість у геометричній моделі СЗІ $GM2$ здійснювати вибір найбільш «слабкого» і найбільш «сильного» до передбачуваних атак, розглянутих у сукупності, засобу захисту.

Таким чином, запропоновано два способи побудови геометричної моделі СЗІ, в основу яких покладені sign-, nsign-чутливість системи, що виступає в ролі математичного параметра, якісна зміна якого є різною для різних збурних дій. Обидві моделі є наочними, ілюстративними, простими в обчислювальному сенсі при своїй реалізації.

При запропонованому способі моделювання наслідки sign-чутливості (nsign-чутливості) наочно вказують на «слабкі» і «сильні» ланки в СЗІ завдяки різній реакції на одну збурну дію векторів, що відповідають різним засобам захисту: вектор або залишається в початковому координатному ортанті, або змінює його. Кожна з моделей $GM1$, $GM2$ має деякі переваги в порівнянні з іншою. Так перша модель більш проста при реалізації, тому що не потребує нормування векторів, що входять до її складу, обчислювальні витрати для здійснення якого становлять $\underline{O}(mn)$ арифметичних операцій, друга модель дає більше інформації про властивості засобів захисту, що належать СЗІ. Вибір конкретної реалізації геометричної моделі буде визначатися безпосередньо задачею, для рішення якої модель використовується.

Будучи простими, наочними, $GM1$, $GM2$, які побудовані з метою простого в обчислювальному сенсі врахування відмінностей у результатах впливу атаки для різних засобів захисту, вони не відображають процеси, що відбуваються безпосередньо з інформацією, що циркулює в розглянутій СЗІ, а тому не вирішують одну з основний задач при моделюванні системи — задачу контролю над станом інформації.

13.1.2. Модель захищеної інформаційно-технологічної системи, яка заснована на принципах функціонування нервової системи людини

«Некласичний» підхід у теорії керування, який розвивається з кінця минулого століття, що ґрунтується на аналогіях архітектури й цілей функціонування складних технічних і біологічних систем — природних систем

керування, є найбільш перспективним на сьогоднішній день при формалізації інформаційних систем. У зв'язку із цим як базис для створення принципово нової моделі інформаційно-технологічної системи використовуються основні принципи функціонування нервової системи людини.

Аналогії архітектури й цілей функціонування нервової системи людини і системи захисту інформації

Логіка використання нервової системи людини (НСЛ) для моделювання інформаційно-технологічної системи випливає з очевидної аналогії між обраною біологічною системою й системою інформаційної безпеки (рис. 13.4). Слід враховувати, що процес моделювання тут носить комплексний характер і використовує НСЛ, починаючи з форми представлення інформації, програмування інформаційних полів і закінчуючи архітектурою інформаційно-технологічних систем з вбудованими механізмами забезпечення інформаційної безпеки й еволюційним протіканням процесів.

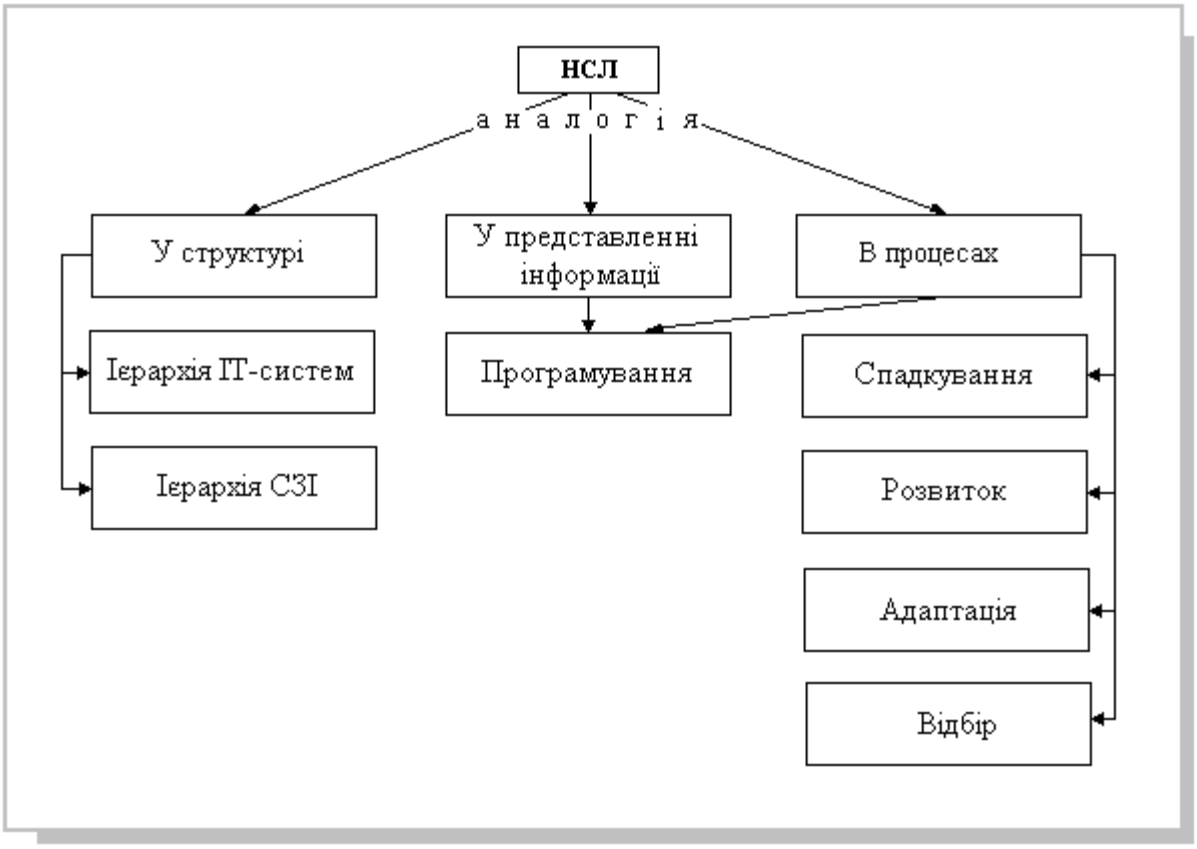


Рис. 13.4. Аналогія між нервовою системою людини й системою інформаційної безпеки

Моделювання захищених інформаційних процесів засноване на єдності представлення інформації в ієрархії НСЛ, у якій повідомлення передаються універсальним контейнером, що визначається структурованим інформаційним

полем ДНК. Структурований характер мають розподілені інформаційні поля нейронних комплексів нервової системи, завдяки яким у НСЛ існують адаптивні механізми пам'яті, що накопичують життєвий досвід. Можливість реалізації адаптивних механізмів пам'яті в штучних інформаційних полях — основна передумова еволюції інформаційно-технологічної системи. Програмування в НСЛ носить надлишковий розподілений характер, що забезпечує високу функціональну стійкість інформаційних процесів.

Окремі спотворення інформації, з одного боку, компенсуються надмірністю інформаційних полів, а з іншого — дозволяють реалізувати механізм мутацій і еволюційні процеси розвитку й відбору. Зокрема, адаптивні процеси в інформаційних полях дозволяють інформаційно-технологічній системі розвиватися й накопичувати досвід в умовах розширення поля загроз, а спадкування досвіду в наступних реалізаціях системи зводиться до передачі відповідних інформаційних полів. Ієрархія адаптивної системи інформаційної безпеки відображає розподіл функцій захисту на керуючу (перевірка форм представлення інформації і т.д.) і керовану, що реалізує взаємодію системи із середовищем (рис. 13.5). Архітектурною особливістю НСЛ є внутрішній характер механізмів захисту, що реалізується в ієрархії інформаційно-технологічної системи.

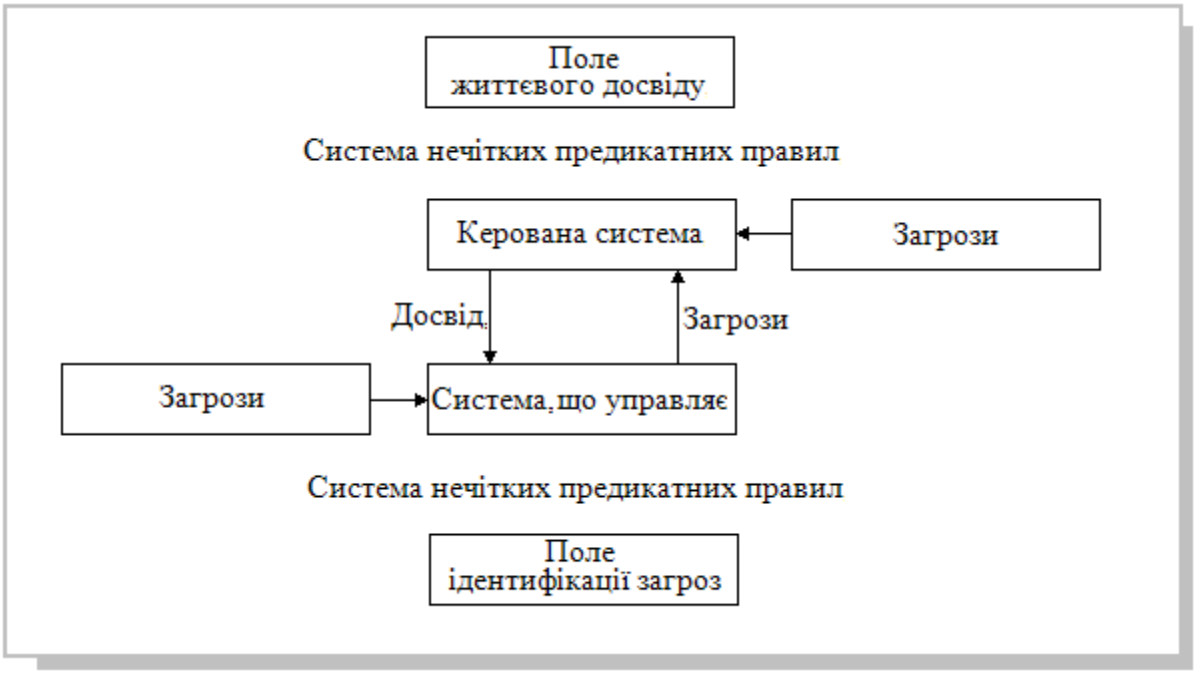


Рис.13.5. Ієрархія адаптивної системи інформаційної безпеки

При моделюванні штучних систем слід враховувати, що при реалізації адаптивних механізмів НСЛ й інформаційних полів функції захисту інформації повинні бути внутрішніми функціями проектованої системи.

Виділення основних принципів і цілей функціонування нервової системи людини

Оскільки відображення в математичному описі всієї сукупності фізіологічних закономірностей і властивостей при обов'язковому обмеженні детальності, специфіки й об'єму характеристик і підсистем, що включаються в модель, не можливе, у першу чергу, необхідно виділити основні принципи роботи НСЛ, відповідно до яких буде будуватися її математична модель й модель інформаційно-технологічної системи.

Загальносистемними (основними) характеристиками НСЛ назвемо такі властивості й відносини, вага яких у формуванні цієї системи досить виражена. їхній відбір повинен подолати природне протиріччя між докладністю (адекватністю) моделі і її ефективністю (конструктивністю) як інструмента дослідження.

Великий вплив на розвиток математичних моделей не тільки НСЛ, але і, наприклад, системи кровообігу та т.п. зробила концепція розподілу системи на *керуючу* й *керовану* частини, яка застосовується і нижче. При цьому як *керуюча система* виступає СЗІ, що моделюється з використанням основних принципів функціонування НСЛ, яка є складовою частиною сукупної інформаційно-технологічної системи — *об'єкта керування*.

Основні принципи організації й функціонування нервової системи, на базі яких формується модель інформаційної системи:

- *Автономність* — керуюча система є підмножиною об'єкта керування й керує їм на основі знань, отриманих самостійно під час взаємодії з навколишнім середовищем за допомогою блоку датчиків і виконуючого органа;
- *Дискретність* — відомо, що мозок містить скінченне число нейронів, зв'язків і т.д., нервові імпульси людини також дискретні; завдяки цьому й модель повинна відповідати цим властивостям, тобто керуюча система повинна зберегти дискретність як структури, так і принципів функціонування;
- *Максимальна початкова пристосованість* — у реальних умовах процес становлення НСЛ (керуючої системи) з метою пристосування до життя в певному середовищі для виживання відбувається під впливом природного добору. При моделюванні нервової системи природний добір повинен бути замінений максимальним використанням апріорної інформації. Це використання інформації повинне відображати наявність пристосованості об'єкта керування й керуючої системи до умов функціонування;
- *Мінімум вхідних даних* — для людини при його народженні властива наявність таких інформаційних просторів, заповнення яких відбувається в ході життя. Аналогічно: керуюча система в момент початку її функціонування містить деякі невизначені властивості, становлення яких відбувається за допомогою накопичення знань при функціонуванні системи в реальних умовах.

Основними цільовими функціями керуючої системи є:

- виживання об'єкта керування;
- накопичення знань.

З біології відомо, що ці дві цільові функції взаємозалежні між собою в тому розумінні, що досягнення однієї сприяє підвищенню ймовірності досягнення іншої. Завдяки цьому зосередимо увагу на першій цільовій функції (доцільність вибору саме цієї функції пояснюється також специфікою об'єкта, що є кінцевою метою моделювання: основним для СЗІ є збереження інформації — виживання об'єкта керування).

Етапи побудови графово-матричної моделі захищеної інформаційно-технологічної системи

Будемо використовувати як модель об'єкта керування зважений граф зі структурним відношенням «складатися з». Використання такого принципу побудови графа образа об'єкта, яким є інформаційно-технологічна система, має ряд важливих властивостей:

1. Таке структурне відношення дає можливість відбити ієрархію об'єкта керування, автоматично здійснює ієрархічну декомпозицію, необхідну для аналізу системи захисту інформації. Ієрархія — найбільш загальний метод класифікації, використовуваний людиною. Така класифікація відтворює первинну форму координації чи організації

- коркових процесів,
- їхніх психічних співвідносних понять,
- їх вираз в символах і мовах.

Основна задача в ієрархії, що полягає в оцінці вищих рівнів, виходячи із взаємодії її різних рівнів, а не з безпосередньої залежності від елементів на цих рівнях, збігається з основною задачею при аналізі системи. Шляхом ієрархічної композиції, по суті, ухиляються від безпосереднього зіставлення великого й малого. Крім того, ієрархічні моделі мають значимі переваги перед моделями інших видів:

- дають можливість дослідження «ступеня впливу» пріоритетів на верхніх рівнях на пріоритети елементів нижніх рівнів;
- надають докладну інформацію про структуру системи;
- є, як правило, стійкими (малі збурення викликають малий ефект);
- гнучкими (додавання до добре структурованої ієрархії не руйнують її характеристики).

2. При такому моделюванні керуючої системи легко задовольняються основні принципи НСЛ 1, 2:

- автономність виконується автоматично при побудові графа; блок датчиків представляє із себе останній рівень деталізації (сукупність листків графа), через

який відбувається зв'язок з зовнішнім середовищем і всі можливі збурні дії на систему;

- дискретність забезпечується властивостями графа як математичного об'єкта: граф — це сукупність двох дискретних скінченних множин вершин і пар вершин (ребер), будь-яке перетворення графа — дискретне;

3. Для запропонованої моделі будь-який рівень деталізації є легко досяжним, а також не викликає труднощів модифікація існуючих рівнів деталізації, що є важливою вимогою при створенні моделі будь-якої фізіологічної системи, тому що апріорі, до одержання моделі, найчастіше неможливо визначитися з тим, наскільки «докладної» повинна бути модель:

- більша деталізація буде досягатися введенням нового рівня листків у наявному графі;
- при зайвій наявній деталізації її зменшення еквівалентне побудові гомоморфної згортки підграфа, що містить листки, які відповідають «нецікавим» у даний момент деталям, і вершини попереднього рівня кореневої структури графа, суміжної зі згаданими листками;

4. Будь-яка модифікація керуючої системи зведеться до зміни структури суміжності відповідного підграфа. У даний момент розроблені різні схеми зберігання графа, застосування яких дозволяє проводити обробку графів, зокрема, модифікацію структури суміжності, використовуючи для цього досить мале число арифметичних операцій. Наприклад, у схемі, заснованої на використанні списків суміжності, що вимагає для зберігання масиви із загальною довжиною $|X|+2|E|+1$, де X, E — множини вершин і ребер графа відповідно, а $|X|,|E|$ — їх потужності, або в схемі, заснованої на введенні поля зв'язків, де загальна довжина масивів для зберігання дорівнює $|X|+4|E|$. Завдяки способу побудови графа-моделі, як буде видно нижче, потужність множини ребер порівнянна з потужністю множини вершин.

Перейдемо безпосередньо до побудови зваженого графа-моделі інформаційно-технологічної системи, що представляє дерево.

Етап 1. Початковий вид графа-моделі.

Система в цілому розглядається як ізольована вершина (рис.13.6),

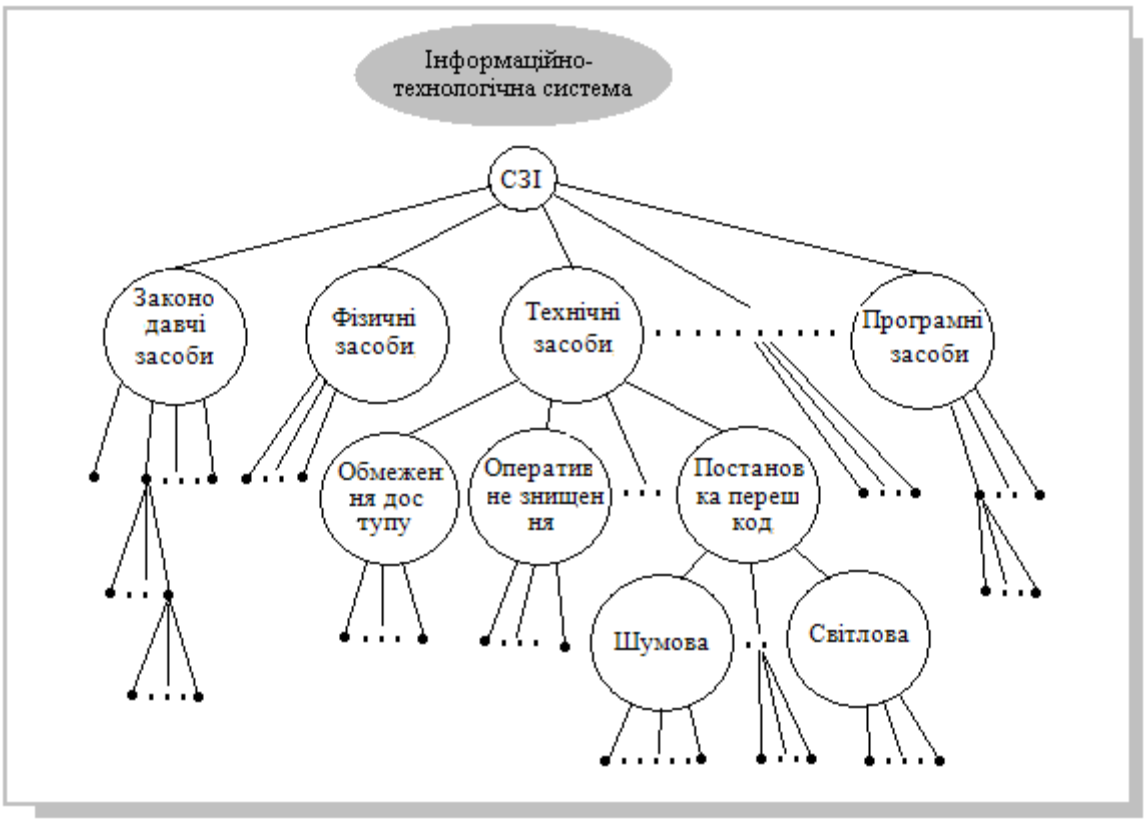


Рис.13.6. Початковий вид графа інформаційної системи

що не має зв'язків з вершинами підграфа, який відповідає СЗІ: доступ СЗІ до інформації, що циркулює в системі, відсутній.

СЗІ представляється у вигляді сукупності засобів, що входять у неї як складові частини, кожній з яких відповідає вершина графа, яка знаходиться у другому рівні його кореневої структури (КСР) (рис.13.7 — всі вершини позначені натуральними числами від 1 до *n*). Кожний наступний рівень кореневої структури є наступним рівнем деталізації. Раціональний ступінь детальності визначається припустимими класами збурень і керуючих впливів.

Значення вагових коефіцієнтів графа, повинні відображати реальну цінність того або іншого засобу захисту для функціонування всієї системи. Конкретні значення коефіцієнтів ґрунтуються на практичному досвіді при максимальнім використанні апріорної інформації для забезпечення умови максимальної початкової пристосованості, забезпечують додатну напіввизначеність (додатну визначеність) матриці суміжності графа.

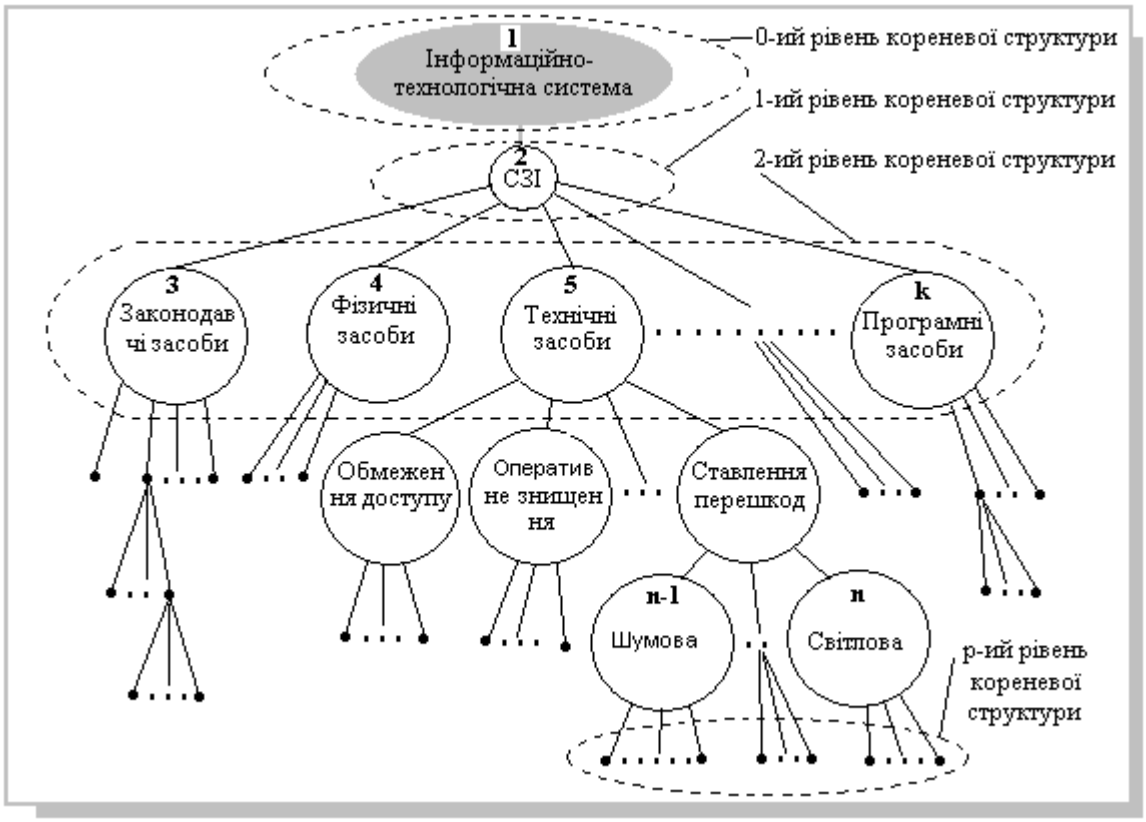


Рис.13.7. Коренева структура рівнів графа інформаційно-технологічної системи

Етап 2. Побудова матриці суміжності графа-моделі.

Матриця суміжності G зваженого графа-моделі інформаційно-технологічної системи завдяки його неорієнтованості є симетричною.

За допомогою нормального спектрального розкладання однозначно визначаються спектр і ВВ G.

Етап 3. Формалізація інформації, що циркулює в системі.

Введення зв'язку <1,2> (рис. 13.7) приводить до того, що інформація, що підлягає захисту, стає доступною СЗІ***. В результаті матриця суміжності*** G одержує збурення, що приводить до збурення ВЗ і ВВ, що однозначно її визначають. *Отримані збурення повного набору параметрів* G *є формальним представленням циркулюючої в інформаційно-технологічній системі інформації*, що підлягає захисту.

Спілкування СЗІ з навколишнім середовищем здійснюється через блок датчиків-листків (аналог периферичної НСЛ): всі атаки на систему виражаються у впливі на листки, вагові коефіцієнти яких малі в порівнянні з коефіцієнтами, що відповідають вершинам, які знаходяться на попередніх рівнях КСР. Вага вершини на кожному рівні визначається як додатне число, більше або рівне сумі ваг суміжних з нею вершин, що знаходяться на наступному рівні кореневої структури. Приклад зваженого графа-моделі системи, що ілюструє можливе

співвідношення між ваговими коефіцієнтами вершин різних рівнів, представлений на рис. 13.8 (поруч із вузлом — його номер, усередині вузла — його можлива вага).

Математичним виразом атаки буде зменшення вагових коефіцієнтів, що відповідають атакованим засобам захисту.

Говорячи про довільну інформаційно-технологічну систему, необхідно відзначити, що розмір відповідного їй графа може бути в загальному випадку досить великий, що приводить до певних труднощів при його обробці й аналізі. У зв'язку із цим значимими стають використовувані схеми зберігання графів, їх вимоги до пам'яті. Очевидно, що при аналізі інформаційно-технологічної системи з використанням відповідного графа основною операцією буде виявлення відносин суміжності між вузлами, адже саме ці відносини явно

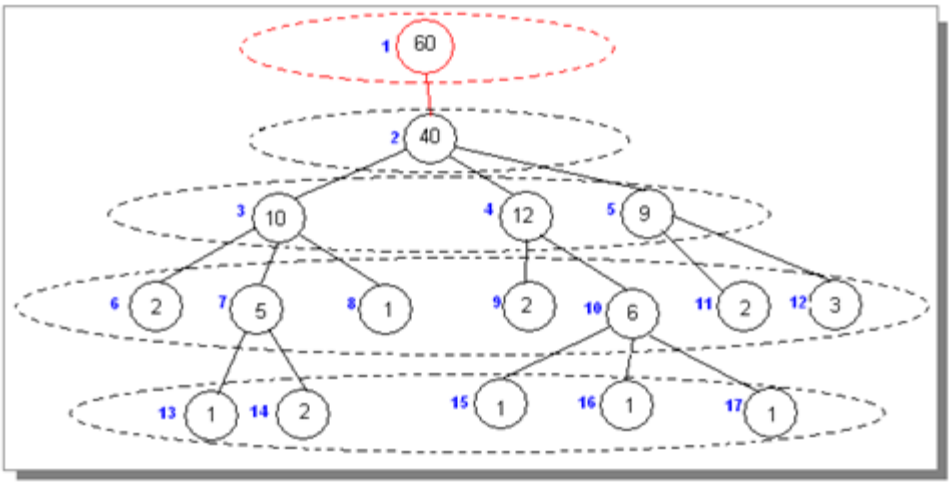


Рис. 13.8. Приклад зваженого графа системи

вказують на ієрархію системи. Тому необхідним є такий спосіб представлення графа інформаційно-технологічної системи, який би дозволяв легко (в обчислювальному сенсі) встановлювати суміжності й при цьому був економічним у сенсі пам'яті.

Математичні параметри, що характеризують інформаційно-технологічну систему

Формальне введення інформації в систему збурює всі або деякі однозначно визначені нормальним спектральним розкладанням ВЗ і ВВ матриці суміжності графа-моделі G, приводячи її до виду $\overline{G}$. Сукупність цих збурень є формальним представленням для циркулюючої в СЗІ інформації, але не тільки для неї: встановлення зв'язку між сукупною інформаційно-технологічною системою й СЗІ відкриває доступ в останню не тільки для інформації, але й для всіх складових інформаційно-технологічної системи, відсутніх безпосередньо в СЗІ. В загальному випадку інформація формально представляється деякою

підмножиною множини збурень ВЗ і ВВ матриці G при переході до виду $\overline{G}$. Оскільки виділення цієї підмножини є важким, для контролю над станом інформації будемо аналізувати всю сукупність збурень ВЗ і ВВ G.

Твердження 13.6. Зміни в стані інформації, яка зберігається системою, представляються у вигляді збурень тих ВЗ і ВВ матриці $\overline{G}$, які були збурені при введенні інформації в СЗІ, тобто при переході матриці суміжності графа-моделі від виду G до виду $\overline{G}$. Аналіз стану інформації зводиться до аналізу збурень згаданих ВЗ і ВВ.

Оскільки матриця $\overline{G}$ симетрична, її спектр містить лише добре обумовлені ВЗ відповідно до співвідношення. Добра обумовленість ВЗ приводить до нечутливості спектра матриці $\overline{G}$ до збурних дій, або, інакше кажучи, до того, що збурення ВЗ $\overline{G}$ за модулем порівнянні з величиною самої збурної дії, що не можна в загальному випадку сказати про ВВ. Розглянемо ці питання докладно.

Теорема 13.1. Нехай збуренням $\delta_{k_1},...,\delta_{k_p}$ піддалися ВЗ $\lambda_{k_1},...,\lambda_{k_p}$ матриці $\overline{G}$, що привело до її збурення $\Delta\overline{G}$. Тоді величина $\left\|\Delta\overline{G}\right\|$ не залежить від того, які саме ВЗ були збурені, а залежить лише від модулів цих збурень.

Доведення.

$$\overline{G}+\Delta\overline{G}=U\,diag(\lambda_1,...,\lambda_{k_1-1},\lambda_{k_1}+\delta_{k_1},\lambda_{k_1+1},...,\lambda_{k_p-1},\lambda_{k_p}+\delta_{k_p},\lambda_{k_p+1},...,\lambda_n)U^T$$

Тоді,

$$\Delta\overline{G}=\sum_{j=1}^{p}\delta_{k_j}u_{k_j}u_{k_j}^T,$$

$$\left\|\Delta\overline{G}\right\|_2=\max_{1\le j\le p}\left|\delta_{k_j}\right|.$$

Зв'язок між $\left\|\Delta\overline{G}\right\|$ і збуреннями ВЗ $\delta_{k_1},...,\delta_{k_p}$ залежить від вибору конкретної матричної норми. Наприклад, якщо розглянути норму Фробеніуса, то для $\Delta\overline{G}$, з врахуванням зв'язку між розглянутою матричної й векторною 2-нормою, буде мати місце співвідношення:

$$\left\|\Delta\overline{G}\right\|_F=\left\|\sum_{j=1`}^{p}\delta_{k_j}u_{k_j}u_{k_j}^T\right\|_F\le\sum_{j=1}^{p}\left|\delta_{k_j}\right|\left\|u_{k_j}\right\|_2\left\|u_{k_j}^T\right\|_2=\sum_{j=1}^{p}\left|\delta_{k_j}\right|\le p\max_{1\le j\le p}\left|\delta_{k_j}\right|,$$

висновок теореми залишається вірним.

Таким чином, величина збурної дії на матрицю не дає інформації про те, які саме ВЗ піддалися збуренню. При побудові графово-матричної моделі інформаційної системи питання про локалізацію збурень ВЗ матриці

суміжності, викликаних введенням інформації в СЗІ, є визначальним і вимагає подальших досліджень, результати яких приводяться далі.

Теорема 13.2. Нехай збурна дія $\Delta\overline{G}$ привела до збурень $\Delta_{k_1},...,\Delta_{k_p}$ ВВ $u_{k_1},...,u_{k_p}$ матриці $\overline{G}$. Величина цієї збурної дії визначається значеннями $\Delta_{k_1},...,\Delta_{k_p}$, а також ВЗ $\lambda_{k_1},...,\lambda_{k_p}$ матриці $\overline{G}$, які відповідають $u_{k_1},...,u_{k_p}$ (навіть якщо ці ВЗ не збурилися).

Доведення. Для матриці $\overline{G}+\Delta\overline{G}$, враховуючи, має місце співвідношення:

$$\overline{G}+\Delta\overline{G}=\sum_{\substack{i=1\\ i\neq k_1,...,k_p}}^{n}\lambda_i u_i u_i^T+\sum_{j=1}^{p}\lambda_{k_j}(u_{k_j}+\Delta_{k_j})(u_{k_j}+\Delta_{k_j})^T=$$

$$=\sum_{i=1}^{n}\lambda_i u_i u_i^T+\sum_{j=1}^{p}\lambda_{k_j}(u_{k_j}\Delta_{k_j}{}^T+\Delta_{k_j}u_{k_j}^T+\Delta_{k_j}\Delta_{k_j}{}^T)= \qquad (13.5)$$

$$=\overline{G}+\sum_{j=1}^{p}\lambda_{k_j}(u_{k_j}\Delta_{k_j}{}^T+\Delta_{k_j}u_{k_j}^T+\Delta_{k_j}\Delta_{k_j}{}^T).$$

З (13.5), враховуючи погодженість спектральної матричної норми й векторної 2-норми, отримаємо:

$$\left\|\Delta\overline{G}\right\|_2=\left\|\sum_{j=1}^{p}\lambda_{k_j}(u_{k_j}\Delta_{k_j}{}^T+\Delta_{k_j}u_{k_j}^T+\Delta_{k_j}\Delta_{k_j}{}^T)\right\|_2\le$$

$$\le\sum_{j=1}^{p}\left|\lambda_{k_j}\right|(\left\|u_{k_j}\right\|_2\left\|\Delta_{k_j}\right\|_2+\left\|\Delta_{k_j}\right\|_2\left\|u_{k_j}\right\|_2+\left\|\Delta_{k_j}\right\|_2^2)=$$

$$=\sum_{j=1}^{p}\left|\lambda_{k_j}\right|(2\left\|\Delta_{k_j}\right\|_2+\left\|\Delta_{k_j}\right\|_2^2),$$

звідки випливає висновок теореми.

Чутливість ВВ u_i, який відповідає ВЗ λ_i, в межах матриці G визначається відповідно до співвідношень:

$$\sin\theta_i\le\frac{2\left\|\Delta G\right\|_2}{gap_{abs}(i,G)}, \qquad (13.6)$$

$$\sin\theta_i\le\frac{2\left\|\Delta G\right\|_2}{gap_{abs}(i,\overline{G})}, \qquad (13.7)$$

де ΔG — збурення матриці G, $\overline{G} = G + \Delta G$, $\overline{u_i}$ — нормований збурений ВВ, θ_i — гострий кут між u_i і $\overline{u_i}$,

$$gap_{abs}(i, G) = \min_{i \neq j} \left\| \lambda_j \right| - \left| \lambda_i \right\| \tag{13.8}$$

— абсолютна відокремленість ВЗ λ_i матриці G.

Доведемо (13.6), оскільки (13.7) є наслідком. Нехай $G = U \Lambda U^T$ — СР матриці G, тоді

$$\overline{G} = G + \Delta G = \overline{U}\,\overline{\Lambda}\,\overline{U}^T \tag{13.9}$$

визначає СР збуреної матриці $\overline{G}$.

Нехай вектор d є ортогональним вектору u_i і такий, що $u_i + d$ за напрямком співпадає з вектором $\overline{u_i}$, тобто $u_i + d$ — ненормований ВВ матриці $G + \Delta G$, який відповідає i-му ВЗ. З (13.9) безпосередньо випливає, що

$$(G + \Delta G)\overline{U} = \overline{U}\,\overline{\Lambda}\,. \tag{13.10}$$

Якщо розглянути i-і стовпці в матричній рівності (10.10), то отримаємо:

$$(G + \Delta G)\overline{u}_i = \overline{\lambda}_i \overline{u}_i\,, \tag{13.11}$$

де $\overline{\lambda}_i$ — i-е ВЗ $G + \Delta G$. Помножимо обидві частини рівності (5.11) на $\|u_i + d\|_2$:

$$(G + \Delta G)(u_i + d) = \overline{\lambda}_i (u_i + d)\,. \tag{13.12}$$

Віднімаючи з рівності (13.12) рівність $Gu_i = \lambda_i u_i$, позначаючи $\Delta\lambda = \overline{\lambda}_i - \lambda_i$, і перегруповуючи члени, отримаємо:

$$(G - \lambda_i I)d = (\Delta\lambda I - \Delta G)(u_i + d), \tag{13.13}$$

де I — одинична матриця.

Оскільки $u_i^T (G - \lambda_i I) = 0$, то вектори, в обох частинах рівності (13.13), ортогональні вектору u_i, крім того, вектор d ортогональний u_i за побудовою. Це означає, що якщо вектори $z = (\Delta\lambda I - \Delta G)(u_i + d)$, d розкласти по власному ортонормованому базису $u_1, ..., u_i, ..., u_n$, то ці розкладання будуть мати вид:

$$z = \sum_{\substack{j=1 \\ j \neq i}}^{n} z_j u_j \,,\; d = \sum_{\substack{j=1 \\ j \neq i}}^{n} d_j u_j \,, \tag{13.14}$$

де z_j, d_j — коефіцієнти відповідних розкладань.

Оскільки $(G - \lambda_i I)u_j = (\lambda_j - \lambda_i)u_j$,то

$$(G - \lambda_i I)d = (G - \lambda_i I)\sum_{\substack{j=1 \\ j \neq i}}^{n} d_j u_j = \sum_{\substack{j=1 \\ j \neq i}}^{n} (\lambda_j - \lambda_i) d_j u_j = z = \sum_{\substack{j=1 \\ j \neq i}}^{n} z_j u_j \,.$$

Рівність розкладань по власному базису

$$\sum_{\substack{j=1 \\ j \neq i}}^{n} (\lambda_j - \lambda_i) d_j u_j = \sum_{\substack{j=1 \\ j \neq i}}^{n} z_j u_j$$

означає рівність відповідних коефіцієнтів цих розкладань:

$$(\lambda_j - \lambda_i) d_j = z_j \,,\;\; j = \overline{1,n},\; j \neq i \,. \tag{13.15}$$

Визначаючи d_j з (13.15) і підставляючи в рівність (13.14) для d, отримаємо:

$$d = \sum_{\substack{j=1 \\ j \neq i}}^{n} \frac{z_j}{(\lambda_j - \lambda_i)} u_j \,.$$

Враховуючи ортонормованість векторів u_j і елементарні властивості модуля,

$$tg\theta_i = \|d\|_2 = \sqrt{\sum_{\substack{j=1 \\ j \neq i}}^{n} \left(\frac{z_j}{\lambda_j - \lambda_i} \right)^2} \le \sqrt{\sum_{\substack{j=1 \\ j \neq i}}^{n} \left(\frac{z_j}{|\lambda_j| - |\lambda_i|} \right)^2} \le \frac{1}{gap_{abs}(i,G)} \sqrt{\sum_{\substack{j=1 \\ j \neq i}}^{n} z_j^2} = \frac{\|z\|_2}{gap_{abs}(i,G)} \,. \tag{13.16}$$

Оскільки

$z = (\Delta\lambda I - \Delta G)(u_i + d) = \Delta\lambda(u_i + d) - \Delta G(u_i + d)$,

то, використовуючи властивості норми й погодженість спектральної матричної норми й векторної 2-норми, отримаємо:

$$\|z\|_2 \le \left(|\Delta\lambda| + \|\Delta G\|_2 \right) \|u_i + d\|_2 \,. \tag{13.17}$$

З (5.16) $|\Delta\lambda| \le \|\Delta G\|_2$, що приводить нерівність (5.17) до виду:

$$\|z\|_2 \le 2\|\Delta G\|_2 \|u_i + d\|_2 = 2\|\Delta G\|_2 \cos\theta_i . \qquad (13.18)$$

Тоді з (10.16), враховуючи (10.18), отримаємо (10.6).

Зі співвідношень (10.6), (10.7) випливає істинність наступного твердження.

Твердження 13.7. Абсолютна відокремленість ВЗ матриці є мірою чутливості відповідного ВВ до збурних дій.

Теорема 13.3. Мализна збурень ВВ матриці $\overline{G}$ не гарантує мализну норми збурної дії $\Delta\overline{G}$ на інформаційно-технологічну систему.

Доведення. Оскільки нерівність (13.6) має місце для кожного ВЗ матриці $\overline{G}$, то з нього отримуємо:

$$\max_{1\le i\le n}\left(\frac{1}{2}\sin\theta_i \; gap_{abs}(i,\overline{G})\right) \le \left\|\Delta\overline{G}\right\|_2 , \qquad (13.19)$$

звідки безпосередньо випливає висновок теореми, а також те, що якщо при збуренні $\overline{G}$ її ВЗ не змінюються чи змінюються незначно, то навіть порівняно великі збурення ВВ, що відповідають погано абсолютно відокремленим ВЗ ($gap_{abs}(i,\overline{G})$ мала), приведуть до малого значення $\left\|\Delta\overline{G}\right\|_2$.

Чутливі ВВ можуть відхилитися на великий кут при малій збурній дії (навіть через округлення, що відбуваються при обчисленнях), і тим самим їхнє збурення не дає дійсної інформації про величину збурної дії (про серйозність атаки), про яку можна судити лише по збуреннях ВВ, що відповідають ВЗ із найбільшими абсолютними відокремленостями.

Локалізація інформації в моделі системи

При запропонованому способі побудови графа-моделі інформаційно-технологічної системи існує можливість точної формальної локалізації місцезнаходження збереженої у системі інформації, тобто визначення тих ВЗ і ВВ матриці суміжності G, збурення яких є формальним представленням інформації системи.

Лема 13.1. Формальним представленням інформації, що циркулює в інформаційно-технологічній системі при описаному способі побудови графа-моделі, будуть збурення максимальних ВЗ його матриці суміжності G.

Доведення. Позначимо g_{ij} , $i, j = \overline{1,n}$, елементи матриці G. Нехай

$$R_i = \sum_{j=1,\, j\ne i}^{n} \left|g_{ij}\right|, i = \overline{1,n} . \qquad (13.20)$$

Відповідно до леми Гершгоріна [39], всі ВЗ матриці G будуть знаходитися в об'єднанні замкнених кругів $\overline{B}(g_{ii}, R_i)$ з центрами в точках g_{ii} і радіусами (13.20) (кругів Гершгоріна), тобто для кожного ВЗ λ матриці G знайдеться хоча б один круг $\overline{B}(g_{ii}, R_i)$ такий, що: $|g_{ii} - \lambda| \le R_i$.

Тоді, враховуючи структуру матриці G, її максимальне ВЗ $\lambda_{\max} = g_{11}$, оскільки радіус відповідного круга Гершгоріна дорівнює 0.

При введенні ребра $<1,2>$ постраждають лише круги $\overline{B}(g_{11},0)$ і $\overline{B}(g_{22}, R_2)$: їхні радіуси збільшаться на величину вагового коефіцієнта ребра $<1,2>$, що не виключає навіть їх можливого перетинання. Всі інші круги Гершгоріна залишаться незбуреними. Це приведе до збурення максимальних ВЗ (у загальному випадку їх кількість більше або дорівнює 2), залишаючи мінімальні без змін.

Лема 13.2. Формальне введення інформації в СЗІ не зменшить найбільше ВЗ G.

Доведення. Матриця $\overline{G}$ — невироджена й симетрична з елементами $\overline{g}_{ij}$, $i, j = \overline{1,n}$, до того ж тільки $\overline{g}_{12} \ne g_{12} = 0$. Для всіх інших елементів матриць $\overline{G}$ і G $\overline{g}_{ij} = g_{ij}$. Представимо $\overline{G}$ в виді:

$$\overline{G} = \begin{pmatrix} H & B^T \\ B & U \end{pmatrix},$$

де $H = H^T - m \times m$-матриця з власними значеннями $\theta_1 \le ... \le \theta_m$ (у нашому випадку $H = (\overline{g}_{11})$, має одне ВЗ $\theta_1 = \overline{g}_{11}$, $B = (\overline{g}_{21}, 0, ..., 0)^T$), а власні значення $\overline{G}$ — $\overline{\lambda}_1 \le ... \le \overline{\lambda}_n$. Тоді за теоремою Коші про розподіл має місце співвідношення:

$$\overline{\lambda}_j \le \theta_j \le \overline{\lambda}_{j+n-m}, \ \forall j = \overline{1,m}. \qquad (13.21)$$

Розглянувши праву частину (13.21) при $m = 1, j = 1$, отримаємо висновок теореми: $\theta_1 \le \overline{\lambda}_n$.

Зауваження 13.7. Представимо $\overline{G}$ в виді:

$$\overline{G} = \left(\begin{array}{c|cc} \theta & \gamma & 0^T \\ \hline \gamma & & \\ 0 & & U \end{array}\right)$$

де $\theta = \overline{g}_{11}, \gamma = \overline{g}_{21}$. Виходячи з леми Гершгоріна, $\overline{\lambda}_n \in [\theta - \gamma, \theta + \gamma]$. Припустимо, що є додаткова інформація: $\overline{\lambda}_n$ — єдине ВЗ $\overline{G}$ в більшому сегменті $[\theta - \beta, \theta + \beta]$, $\gamma < \beta$. Тоді можна стверджувати, що

$$\overline{\lambda}_n \in [\theta - \gamma^2/\tau, \theta + \gamma^2/\tau], \qquad (13.22)$$

де $\tau = \left(\beta + \sqrt{\beta^2 + 4\gamma^2}\right)/2$.

Оцінка (13.22) значно поліпшує оцінку для $\overline{\lambda}_n$, яка витікає з леми Гершгоріна. Для описаного способу побудови графа інформаційно-технологічної системи $\overline{g}_{11} > \overline{g}_{22}$, а радіуси кругів Гершгоріна $\overline{B}(\overline{g}_{11}, \overline{g}_{12})$ і $\overline{B}(\overline{g}_{22}, R_2)$ невеликі. Тому, з великою часткою ймовірності, $\overline{g}_{11} - \overline{g}_{12} > \overline{g}_{22} + R_2$, а $\beta = \overline{g}_{11} - \overline{g}_{22} - R_2$ (рис. 13.9).

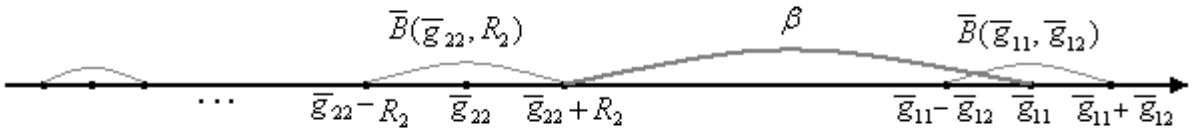


Рис. 13.9. Визначення β для уточнення області локалізації $\overline{\lambda}_n$

Така формальна локалізація інформації, що підлягає захисту, у самій «вершині спектра» матриці суміжності графа-моделі інформаційно-технологічної системи, як буде показано, дуже зручна.

Лема 13.3. При описаному способі побудови графа-моделі формальний процес введення інформації в СЗІ обов'язково збурить ВВ матриці G, що відповідають максимальним ВЗ.

Доведення. Матриця G за побудовою є блочно-діагональної, тобто розкладною:

$$G = \left(\begin{array}{c|ccc} g_{11} & 0^T & & \\ \hline 0 & g_{22} & g_{23} \cdots & g_{2n} \\ & g_{32} & g_{33} \cdots & g_{3n} \\ & \cdots & \cdots & \cdots \\ & g_{n2} & g_{n3} \cdots & g_{nn} \end{array}\right).$$

ВЗ розкладної матриці визначаються об’єднанням ВЗ її блоків. Таким чином, серед ВЗ G є присутнім g_{11}, а відповідний ортонормований лексикографічно додатний ВВ буде визначатися як $(1,0,...,0)^T$. При введенні інформації в СЗІ з появою ребра $<1,2>$ блочно-діагональна структура матриці G буде зруйнована. Як було показано, максимальні ВЗ збуряться, а структура ВВ, що відповідає найбільшому ВЗ, очевидно зміниться відносно $(1,0,...,0)^T$. Таким чином, введення інформації в систему обов'язково збурить ВВ, що

відповідають максимальним ВЗ, незважаючи на те, що ці вектори найменш чутливі до будь-яких збурних дій.

Необхідний рівень захищеності системи

Оскільки «спілкування» СЗІ з навколишнім середовищем формально здійснюється через блок датчиків-листків, то будь-яка атака на систему виражається у впливі на листки, які відповідають атакованим засобам захисту, і моделюється за допомогою зменшення значень діагональних елементів матриці суміжності графа-моделі, що відповідають «постраждалим» вузлам-листкам.

У загальному випадку атака може або повністю знищити атакований засіб, або вивести його з ладу частково, або ніяк не відіб'ється на його роботі. У першому випадку діагональний елемент матриці суміжності, який відповідає знищеному засобу захисту, стане нульовим, що рівнозначно виключенню його з СЗІ. На матричному рівні це еквівалентно відніманню від матриці суміжності $\overline{G}$ додатно напіввизначеної діагональної матриці того ж розміру, єдиний ненульовий елемент якої відповідає вузлу, що пов'язаний з «постраждалим» засобом захисту. Величина цього ненульового елемента дорівнює ваговому коефіцієнту даного засобу захисту.

Матриця $\overline{G}$ за побудовою є *невід'ємною* (всі її елементи невід'ємні), симетричною і нерозкладною, тобто симетричними переставленнями її рядків і однойменних стовпців вона не може бути приведена до виду:

$$\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}, \qquad (13.23)$$

де B, C — квадратні матриці.

Дійсно, якби таке було можливо, то відповідний граф мав би, принаймні, дві компоненти зв'язності, кожна з яких відповідала б діагональному блоку матриці (13.23), що є хибним. З теореми Фробеніуса випливає, що матриця з такими властивостями завжди має додатне ВЗ $\lambda_{\max}$, яке є коренем кратності один характеристичного рівняння, а модулі всіх інших ВЗ не перевищують $\lambda_{\max}$. Якщо зіставити це з лемою 13.2, то звідси безпосередньо буде випливати, що навіть при можливім перетинанні кругів Гершгоріна $\overline{B}(g_{11},0)$ і $\overline{B}(g_{22},R_2)$ після збільшення їх радіусів за рахунок введення ребра $<1,2>$, ми не отримаємо кратності максимального ВЗ.

Власному значенню $\lambda_{\max}$ відповідає ВВ, всі координати якого ненульові й одного знака. Крім того, з початкового результату Вейля про монотонність, витікає, що якщо $\overline{G} = \overline{\overline{G}} + Y$, де Y і $\overline{\overline{G}}$ — симетричні матриці, до того Y — додатно напіввизначена, то ВЗ матриці $\overline{\overline{G}}$ не перевищують відповідних ВЗ $\overline{G}$.

Таким чином, результатом будь-якої атаки, що виводить з ладу деякий засіб захисту (або частково руйнує його, що формалізується зменшенням його вагового коефіцієнта), буде певне збурення ВЗ матриці $\overline{G}$: вони не збільшаться.

В реальних умовах можливі атаки на СЗІ, які не тягнуть за собою ніяких негативних наслідків для інформації, що захищається. Адекватна математична модель інформаційно-технологічної системи повинна враховувати таку можливість: якщо зменшення ВЗ матриці $\overline{G}$ в результаті атаки не торкнулося тих ВЗ, у збуреннях яких зберігається інформація системи, то такою атакою можна знехтувати.

Покажемо, що побудована графово-матрична модель допускає можливість повного збереження інформації при деяких атаках, тобто допускає можливість незмінності ВЗ, що зберігають у своїх початкових збуреннях інформацію системи, при збурній дії.

Оскільки вагові коефіцієнти листків малі в порівнянні з ваговими коефіцієнтами вузлів попередніх рівнів КСР графа-моделі інформаційно-технологічної системи, то круги Гершгоріна, що відповідають листкам, будуть на числовій осі розташовані зліва від всіх інших, у досить малому околі нуля. Крім того, кожний листок є суміжним лише з одним вузлом (цей вузол знаходиться на попередньому рівні КСР), тому в рядку матриці суміжності, що відповідає листку, буде лише один ненульовий позадіагональний елемент, значення якого також невелике (найчастіше — це 1), тобто радіус відповідного круга Гершгоріна малий. Обнуління діагонального елемента, що відповідає розглянутому листку, приведе до зсуву відповідного круга Гершгоріна вліво (центр перейде в 0) зі збереженням радіуса, що гарантовано збурить лише найменші ВЗ. Таким чином, завдяки запропонованому способу побудови графа й формальній локалізації інформації в максимальних ВЗ, модель не виключає можливості «безпечної» для СЗІ атаки.

Оскільки математичним результатом атаки на систему є незбільшення ВЗ матриці $\overline{G}$, то відповіддю на атаку (при необхідності такої) повинне стати незменшення ВЗ збуреної матриці $\overline{G}$. Цього можна добитися, наприклад, відповідно до теореми Вейля, за рахунок додавання до «постраждалої» матриці $\overline{G}$ діагональної матриці з невід'ємними діагональними елементами (додатно напіввизначеної), що відповідає збільшенню вагових коефіцієнтів для деяких вузлів, тобто збільшенню реальної цінності для роботи сукупної інформаційно-технологічної системи деяких з засобів захисту, що залишилися недоторканими. Визначимо, якою повинна бути формальна необхідна, хоча, можливо, і недостатня, відповідь СЗІ на атаку.

Оскільки матриця $\overline{G}$ симетрична, невироджена, додатно визначена (додатно напіввизначена), всі її ВЗ додатні (невід'ємні). Покажемо, що обнуління діагонального елемента, яке відбувається при моделюванні атаки, що

знищує відповідний засіб захисту, приведе до того, що найменше ВЗ збуреної матриці $\overline{G}$ стане від'ємним.

Теорема 13.4. Якщо хоча б один діагональний елемент невиродженої симетричної матриці A дорівнює нулю, то $\lambda_1 < 0$.

Доведення. Припустимо, що $a_{11} = 0$. Представимо A в виді:

$$A = \begin{pmatrix} H & B^T \\ B & U \end{pmatrix},$$

де $H = H^T - m \times m$-матриця, ВЗ якої $\theta_1 \le ... \le \theta_m$, а ВЗ A — $\lambda_1 \le ... \le \lambda_n$. Тоді за теоремою Коші про розподіл має місце співвідношення (13.21), ліва частина якого при $m = 1, j = 1$ має вид: $\lambda_1 \le \theta_1$. Оскільки $\theta_1 = a_{11} = 0$, то в припущенні, що матриця A невироджена, отримаємо: $\lambda_1 < 0$.

Нехай тепер $a_{kk} = 0,\ k \ne 1$. Якщо $P_{1,k}$ — стандартна матриця переставлень ($P_{1,k}$ отримана з одиничної $n \times n$-матриці шляхом переставлення першого і k-го рядків), то для неї мають місце співвідношення:

$$P_{1,k} = P_{1,k}{}^T;\ \ P_{1,k}\, P_{1,k}{}^T = P_{1,k}{}^2 = I$$

I — одинична $n \times n$-матриця, тобто $P_{1,k}$ — ортогональна матриця. Нехай

$$B = P_{1,k} A\, P_{1,k},$$

тобто матриця B отримана з A шляхом подібного перетворення, яке не змінює спектр матриці:

$$\det(B - \lambda I) = \det\left(P_{1,k} A P_{1,k} - \lambda I\right) = \det\left(P_{1,k}(A - \lambda I) P_{1,k}\right) = \det(A - \lambda I).$$

Однак переставлення першого і k-го рядків і однойменних стовпців A, яке є результатом множення зліва і справа на $P_{1,k}$, вивели нульовий елемент $a_{kk} = 0$ на місце (1,1) в матриці B, а це означає, що мінімальне ВЗ B, а тому і A, від'ємне.

Лема 13.4. Нехай матриця $\overline{\overline{G}} = \overline{G} + \Delta G$ з елементами $\overline{\overline{g}}_{ij}$ отримана з симетричної і додатно визначеної матриці $\overline{G}$ з елементами $\overline{g}_{ij}$ шляхом обнуління елемента, який знаходиться на місці (n,n), тобто $\overline{\overline{g}}_{nn} = 0$. Тоді інерція [36] матриці $\overline{\overline{G}}$ визначається як $(n-1, 1, 0)$, тобто $\overline{\overline{G}}$ буде мати одне від'ємне ВЗ.

Доведення. Оскільки матриця $\overline{G}$ є додатно визначеною, то вона автоматично задовольняє умовам теореми 13.2 про *LU*-розкладання. Якщо

$\overline{\overline{G}}^{(k)}$, $\overline{G}^{(k)}$, $k=\overline{1,n}$, — головні підматриці матриць $\overline{\overline{G}}$ і $\overline{G}$ відповідно, то діагональні елементи u_{kk} для $k=\overline{1,n-1}$ верхньої трикутної матриці U для $\overline{\overline{G}}$ задовольняють співвідношенню

$$u_{kk}=\frac{\det\overline{\overline{G}}^{(k)}}{\det\overline{\overline{G}}^{(k-1)}}=\frac{\det\overline{G}^{(k)}}{\det\overline{G}^{(k-1)}}>0,\quad k=\overline{1,n-1}. \tag{13.24}$$

Кількість від'ємних діагональних елементів у матриці U, отриманої під час трикутного LU-розкладання матриці $\overline{\overline{G}}-\sigma I$, де I — одинична матриця, відповідає кількості ВЗ матриці $\overline{\overline{G}}$, менших σ. Тоді кількість від'ємних діагональних елементів у матриці U, яка отримана LU-розкладанням матриці $\overline{\overline{G}}$, визначає кількість від'ємних ВЗ в матриці $\overline{\overline{G}}$. Зі співвідношення (13.24) випливає, що число додатних ВЗ в $\overline{\overline{G}}$ — $\pi\geq n-1$, а з теореми 13.4 — мінімальне ВЗ $\overline{\overline{G}}$ є від'ємним. Завдяки припущенню про невиродженість матриці $\overline{\overline{G}}$ від'ємне ВЗ одне.

Теорема 13.5. Нехай матриця $\overline{\overline{G}}$ отримана із симетричної і додатно визначеної матриці $\overline{G}$ шляхом обнуління довільного єдиного діагонального елемента. Тоді інерція матриці $\overline{\overline{G}}$ визначається як $(n-1,1,0)$.

Доведення. Аналогічно доведенню теореми 13.4.

Наслідок. Якщо під час атаки на інформаційно-технологічну систему руйнуванню піддався єдиний засіб захисту, то це приведе до появи єдиного від'ємного ВЗ (мінімального ВЗ) у матриці суміжності графа-моделі.

Таким чином, необхідна відповідь системи на будь-яку атаку повинна привести до повернення найменшого ВЗ матриці суміжності графа-моделі до невід'ємного виду. Забезпечити додатність мінімального ВЗ, залишаючи нуль, що говорить про руйнування атакованого засобу захисту, на головній діагоналі матриці, неможливо за доведеним вище. Тому метою повинно бути зменшення модуля мінімального ВЗ, щоб його знаком можна було знехтувати, вважаючи $\lambda_1\approx 0$.

Кількісні оцінки складових інформаційно-технологічної системи

При прийнятому підході до рішення задачі про моделювання інформаційно-технологічної системи важливу роль відіграють вагові коефіцієнти вершин (вузлів) графа-моделі, що відповідають елементам системи. Значення вагових коефіцієнтів повинні бути такими, щоб чисельно відображати реальну значущість будь-якого засобу захисту (або групи засобів) для функціонування інформаційно-технологічної системи в цілому, незважаючи на їхню відмінність (технічні, законодавчі, програмні і інші засоби). Для

забезпечення одного з основних принципів функціонування НСЛ, максимальної початкової пристосованості, вагові коефіцієнти повинні бути отримані, виходячи з практичного досвіду при максимальнім використанні апріорної інформації.

Запропонована графова модель інформаційно-технологічної системи представляє із себе ієрархічну структуру.

Нехай "≤" — бінарне відношення нестрогого порядку на деякій множині S. Для будь-якого відношення $x \le y,\ x, y \in S$, можна визначити відношення $x < y$, що означає $x \le y, x \ne y$.

Кажуть, що y *покриває* x, якщо $x < y$ і не існує такого $t \in S$, що $x < t < y$.

Визначення 13.5. Нехай X — скінченна частково впорядкована множина з найбільшим елементом $\bar{x}$. Множина X є *ієрархією*, якщо існує така розбивка X на підмножини $L_k,\ k = \overline{1,h}$, де $L_1 = \{\bar{x}\}$, що виконуються наступні умови:

$$(x \in L_k) \Rightarrow \left(x^- \subset L_{k+1},\ k = \overline{1,h-1}\right), \text{ де } x^- = \{y \mid x \text{ покриває } y\};$$

$$(x \in L_k) \Rightarrow \left(x^+ \subset L_{k-1},\ k = \overline{2,h}\right), \text{ де } x^+ = \{y \mid y \text{ покриває } x\}.$$

Для кожного $x \in X$ існує вагова функція, сутність якої залежить від явища, для якого будується ієрархія:

$$w_x : x^- \to [0,1], \quad \sum_{y \in x^-} w_x(y) = 1.$$

Множини L_k називаються *рівнями ієрархії*, w_x — *функція пріоритету* щодо елемента x.

Інакше кажучи, ієрархія є певний тип системи, заснований на припущенні, що елементи системи можуть групуватися в незв'язані множини. Елементи кожної групи перебувають під впливом елементів деякої певної групи й, у свою чергу, впливають на елементи іншої групи. У математичній теорії ієрархій розробляються методи оцінки впливу рівня на сусідній верхній рівень за допомогою композиції відповідних внесків (пріоритетів) елементів нижнього рівня стосовно елемента верхнього рівня. Ця композиція може поширюватися вверх по ієрархії.

Будемо вважати, що елементи в кожній групі (рівні) ієрархії незалежні.

Запропонована модель інформаційно-технологічної системи представляє ієрархію, для якої $L_1 = \{s\}$, де s відповідає сукупній системі, а кожний рівень ієрархії L_k є одночасно й рівнем КСР графа-моделі (рис.13.10 порівн. з рис.13.7).

Для досягнення поставленої мети визначимо пріоритети елементів кожного рівня ієрархії L_k стосовно s, тобто чисельно виразимо значущість будь-якого засобу захисту (або сукупності засобів) для функціонування системи в цілому,

використовуючи для цього *модифікований* метод аналізу ієрархій (МАІ) з урахуванням особливостей побудованої ієрархічної моделі.

МАІ виник у результаті розробки методології для моделювання неструктурованих, погано формалізуємих задач в економіці, теорії керування і т.д., параметри яких не піддаються ефективним кількісним оцінкам. Він широко використовується й добре зарекомендував себе при рішенні різних задач не тільки економіки, але й теорії дослідження операцій, при аналізі ризику, при побудові експертних систем і в багатьох інших галузях. Математична правочинність МАІ базується на *методі власного значення* й принципі *ієрархічної композиції*, що мають чітке математичне обґрунтування, і в загальному виді може бути описаний у такий спосіб.

Припускається, що задані елементи деякого m-го рівня ієрархії і один елемент e наступного більш високого рівня. Необхідно визначити «ступінь впливу», або пріоритети, елементів m-го рівня щодо їхньої важливості для елемента e. Для цього елементи m-го рівня порівнюються парами по силі їх впливу на e. Числа, що відображають досягнуту при порівнянні згоду в міркуваннях, заносяться в матрицю, для якої обчислюється ВВ, що відповідає найбільшому ВЗ. ВВ забезпечує впорядкування пріоритетів, а ВЗ є мірою погодженості міркувань.

Однак вхідна інформація в розглянутому методі надходить як інформація від експертів. І хоча в МАІ є можливість перевірки експертної інформації на несуперечність за допомогою індексу погодженості, це не вирішує всіх проблем, пов'язаних з використанням експертних оцінок.

Дійсно, при «незадовільнім» значенні індексу погодженості потрібне коректування вхідних даних з наступним перерахуванням результатів отриманих пріоритетів, що спричиняє чималі додаткові обчислювальні витрати. Крім того, можливості експертів подавати несуперечливу інформацію при збільшенні кількості параметрів задачі обмежені. Тому при використанні МАІ з метою побудови моделі інформаційно-технологічної системи, а саме, для визначення вагових коефіцієнтів вузлів графа системи, пропонується метод, що зменшує вплив суб'єктивізму на вхідну інформацію шляхом використання не експертних оцінок, а статистичних даних.

Перший етап. Накопичення статистичних даних про роботу інформаційно-технологічної системи.

Нехай аналіз системи проводиться протягом часу T_e. Припускається, що набір елементів, що входять у систему, за час T_e не змінюється. Нехай x_j відповідає конкретному засобу захисту, якому в графовій моделі ставиться в співвідношення вершина-листок (найвищий рівень деталізації). Серед наявних у СЗІ засобів захисту є як постійно діючі, так і ті, що вмикаються при виявленні спроби напади. Назвемо *позитивним результатом роботи* x_j ситуацію, коли активація даного засобу (в випадку, коли x_j належить до другої групи) чи його

неперервна робота (коли x_j належить до першої групи) приводить до запобігання несанкціонованого доступу.

Кількість всіх позитивних результатів роботи x_j протягом T_e позначимо $k(x_j)$. Назвемо *коефіцієнтом ефективної роботи* $f(x_j)$ засобу x_j відношення

$$f(x_j) = \frac{k(x_j)}{K},$$

де K — загальна кількість спроб несанкціонованого доступу до системи, що вживають протягом T_e.

Зміна набору елементів, що входять у СЗІ, приведе до зміни коефіцієнтів ефективної роботи й необхідності їх перерахування.

Статистичні дані накопичуються не тільки для окремих засобів захисту, але й для їхніх сукупностей, в які ці засоби логічно об'єднані при побудові графа (вершини графа, що не є листками). Наприклад, припустимо, що несанкціонований доступ був відвернений завдяки шумовій перешкоді. При зборі статистичних даних такий випадок приведе до збільшення на одиницю кількості позитивних результатів роботи безпосередньо засобу «шумова перешкода», сукупностей «постановка перешкод», «технічні засоби захисту» і т.д. (див. рис. 13.10).

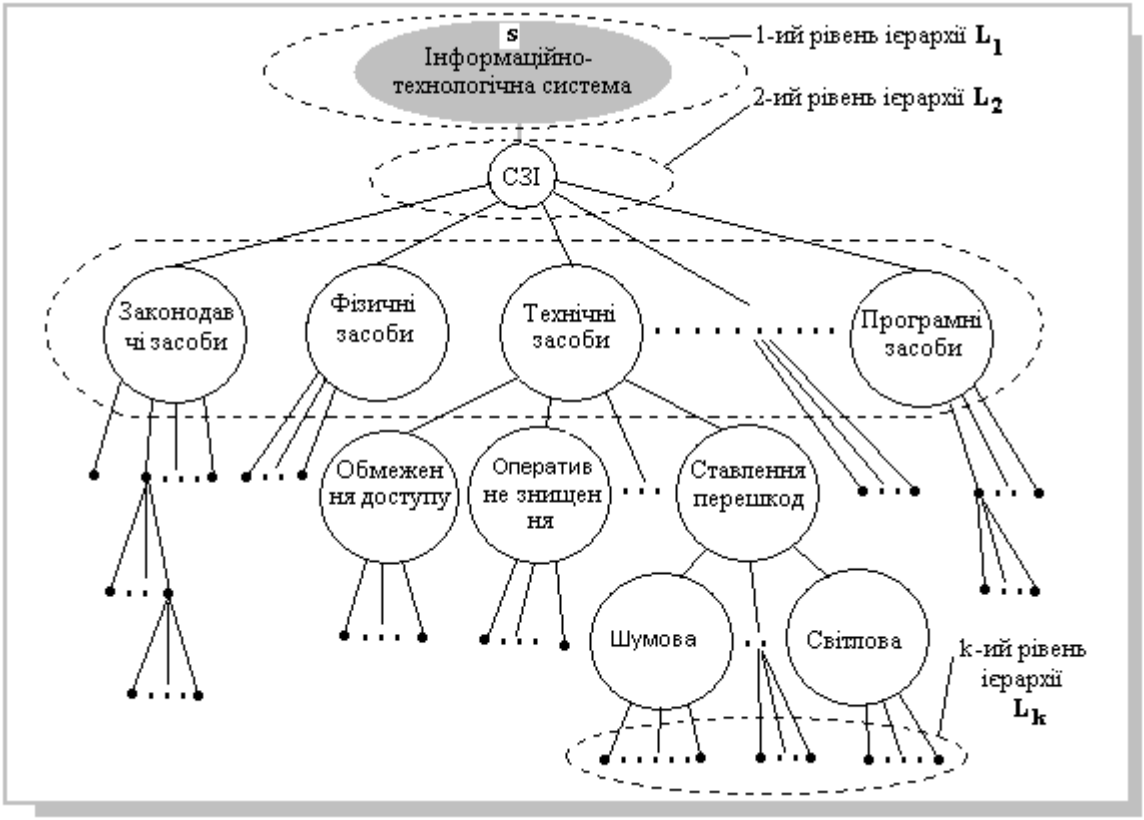


Рис. 13.10. Структура рівнів ієрархії моделі інформаційно-технологічної системи

Коефіцієнти ефективної роботи для сукупностей засобів захисту будуть визначатися аналогічно тому, як це було запропоновано вище для x_j. Якщо $y_j \in L_k$ відображає деяку сукупність засобів, які знаходяться на наступному рівні ієрархії (КСР) L_{k+1} і позначаються як $x_1, x_2, ..., x_n$, то в загальному випадку

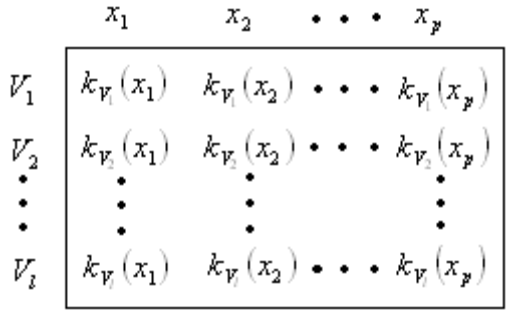
$$k(y_j) \geq \sum_{i=1}^{n} k(x_i), \quad f(y_j) \geq \sum_{i=1}^{n} f(x_i), \tag{13.25}$$

де $k(y_j)$ і $f(y_j)$ — відповідно кількість позитивних результатів роботи й коефіцієнт ефективної роботи для сукупності y_j.

Знаки нерівностей у співвідношеннях (13.25) пояснюються тим, що при побудові математичної моделі неможливо врахувати абсолютно всі фактори, що впливають на функціонування сукупної інформаційно-технологічної системи. Можливо, що в реальній системі до складу y_j входить крім засобів $x_1, x_2, ..., x_n$ ще, наприклад, x_0, значущість якого настільки незначна, що при побудові моделі він не був врахований окремо.

Зауваження 13.8. Збір статистичних даних необов'язково проводити за допомогою аналізу реальних атак на інформаційно-технологічну систему. При моделюванні будь-якої СЗІ необхідно, щоб вона виявилася стійкою стосовно порушника (передбачуваного противника). Тому будемо вважати відомим набір $\{V_1, V_2, ..., V_l\}$ можливих атак. Моделюючи фізично ці атаки, частково або повністю штучно «виводячи з ладу» той засіб захисту, на який спрямована атака, проведемо збір необхідних даних, описаних вище.

Такий спосіб збору статистичних даних дає можливість розширити набір наявних характеристик роботи системи. Нехай атака V_j спрямована безпосередньо на засіб x_i. Приведемо штучно систему до стану, який відповідає результату атаки V_j. Цю модифіковану систему замість вхідної використовуємо для накопичення кількості позитивних результатів роботи її елементів, як було запропоновано вище. Зробимо це для кожної можливої атаки V_j. Нехай $x_1, x_2, ..., x_p$ — вся множина засобів захисту розглянутої СЗІ (множина листків у графі-моделі). Складемо матрицю S:



де $k_{V_j}(x_m)$ — кількість позитивних результатів роботи засобу x_m в системі, яка зазнала попередньо атаку V_j «без відповіді».

Якщо атака V_j повністю зруйнувала засіб x_i, на який була спрямована, то $k_{V_j}(x_i) = 0$. По матриці S визначається матриця коефіцієнтів ефективної роботи для описаних випадків модифікації системи.

Зауваження 13.9. Завдяки припущенню про потенційну відомість супротивника й скінченності набору можливих атак немає необхідності навчання системи в тому розумінні, як це робиться для штучних нейронних мереж. Задача розпізнавання системою невідомої атаки й «правильної» відповіді на цю атаку не ставиться.

Зауваження 13.10. Використання коефіцієнтів ефективної роботи як вагових для відповідних вершин графа-моделі, яке, на перший погляд, здається можливим, небажане. Специфіка графово-матричної моделі інформаційно-технологічної системи, що ґрунтується на принципах роботи НСЛ, така, що числові значення вагових коефіцієнтів повинні якнайточніше відповідати реальній значущості кожного засобу або сукупності засобів для функціонування системи, а статистичні оцінки є досить точними лише на дуже великих вибірках. Якщо проміжок часу T_e виявиться недостатньо тривалим, то значення $f(x_j)$ можуть сильно відрізнятися від реальних. Однак *загальна тенденція порівняльної значущості різних засобів захисту між собою* для запобігання несанкціонованого доступу, тобто для функціонування сукупної системи, яка є основною для одержання вагових коефіцієнтів при обраному способі побудови моделі, виявиться навіть тоді, коли значення T_e є невеликим. У зв'язку з цим робиться наступний крок у процесі отримання вагових коефіцієнтів.

Другий етап. Початкове визначення вагових коефіцієнтів вершин, що відповідають компонентам СЗІ.

Для оцінки впливу різних компонентів на всю інформаційно-технологічну систему й знаходження пріоритетів цих компонентів скористаємося МАІ. Ієрархія графової моделі системи не є повною (ієрархія називається *повною*, якщо для $\forall x \in L_k$ множина $x^+ = L_{k-1}$ для будь-якого k). Більш того, будь-яка $x \in L_k$ суміжна лише з одною вершиною, яка знаходиться в попередньому рівні

L_{k-1}. Як буде показано нижче, ця особливість значно зменшить загальний об'єм арифметичних операцій, необхідних для одержання шуканих значень пріоритетів, у порівнянні з кількістю операцій для загального випадку повної ієрархії.

Зауваження 13.11. Незалежно від того, чи буде ієрархія повною, або для деякого рівня L_k буде виконуватися $x^- \neq L_{k+1}$, функцію w_x, що фігурує у визначенні ієрархії, можна одноманітно визначити для всіх L_k, дорівнюючи її нулю для тих елементів в L_{k+1}, які не належать x^-.

Очевидно, кількість рівнів ієрархії графа-моделі більша двох. Нехай $x_1, x_2, ..., x_n$ — елементи одного рівня ієрархії (вершини одного рівня КСР графа інформаційно-технологічної системи). Визначимо початкові ваги вершин $w_1, w_2, ..., w_n$ вагою впливу (пріоритетом) $x_1, x_2, ..., x_n$ на суміжний з ними елемент y_j попереднього рівня. Для цього формується $n \times n$-матриця A парних порівнянь сили впливу $x_1, x_2, ..., x_n$ на y_j, для чого використовуються отримані на першому етапі коефіцієнти ефективної роботи. Елементи a_{ij} матриці A будемо визначати за наступним правилом з використанням шкали з цілими значеннями $\{1,2,...,9\}$, пріоритетність якої в порівнянні з іншими шкалами обґрунтована.

Не обов'язково визначати верхню межу шкали як 9. Однак необхідно відзначити, що використання більш високої верхньої межі шкали парних порівнянь, зокрема, використання діапазону від 0 до ∞ може виявитися недоцільним або навіть некорисним, тому що припускає, що людське судження якимось чином здатне оцінити відносну перевагу будь-яких двох об'єктів, що не відповідає дійсності. Добре відомо з практичного досвіду, що здатність людини розрізняти перебуває в досить обмеженому діапазоні, і коли є значна нерозмірність між порівнюваними об'єктами або діями, висновки тяжіють до того, щоб бути довільними, і часто виявляються далекими від дійсності. Таким чином, шкала повинна мати скінченний діапазон. Межі повинні бути досить близькими в діапазоні, який відображає дійсну можливість робити відносні порівняння.

$$a_{ij} = \begin{cases} 1, \text{якщо } f_i \text{ і } f_j \text{ мають однакові значення} \\ 3, \text{якщо } f_i \text{ незначно більше } f_j \\ \frac{1}{3}, \text{якщо } f_j \text{ незначно більше } f_i \\ 5, \text{якщо } f_i \text{ значно більше } f_j \\ \frac{1}{5}, \text{якщо } f_j \text{ значно більше } f_i \\ 7, \text{якщо } f_i \text{ явно більше } f_j \\ \frac{1}{7}, \text{якщо } f_j \text{ явно більше } f_i \\ 9, \text{ якщо } f_i \text{ абсолютно перевершує } f_j \\ \frac{1}{9}, \text{якщо } f_j \text{ абсолютно перевершує } f_i \end{cases}, \quad i, j = \overline{1,n}. \tag{13.26}$$

Здатність людини визначати якісні розмежування добре представлена п'ятьма категоріями: рівний, слабкий, сильний, дуже сильний і абсолютний. Можна прийняти компромісні категорії між сусідніми, визначеними вище, коли потрібна більша точність, що приводить до дев'ятьох значень, які можуть бути добре погодженими. Зручності такої шкали підтверджуються практикою. Крім того, часто використовуваний для оцінки окремих предметів практичний метод полягає в класифікації стимулів у трихотомію зон: неприйняття, байдужності, прийняття. Для більш тонкої класифікації в кожну із цих зон також закладений принцип трихотомії: ділення на низький, помірний і високий ступені. Таким чином, знову є дев'ять відтінків значущих особливостей.

З (13.26) випливає, що $a_{ii} = 1, i = \overline{1,n}$, а для позадіагональних елементів:

$$a_{ij} = \frac{1}{a_{ji}}, \ i, j = \overline{1,n}.$$

Така матриця A називається *обернено-симетричною* (reciprocal matrix). Числа 2,4,6,8 і їх обернені значення використовуються при складанні матриці парних порівнянь для полегшення компромісів між судженнями, що небагато відрізняються від основних. Отримана матриця повинна бути якнайбільш погодженою. У загальному випадку під погодженістю суджень розуміється, що при наявності основного масиву неопрацьованих даних усі інші дані логічно можуть бути отримані з них, використовуючи відношення транзитивності. Матрицю A назвемо *погодженою*, якщо

$$a_{ik} = a_{ij} a_{jk}, \quad i, j, k = \overline{1,n}.$$

Мірою погодженості виступає максимальне ВЗ матриці A, а відповідний ВВ забезпечує *впорядкування пріоритетів*. Дійсно, очевидним для погодженості матриці є випадок, коли порівняння засновані на точних вимірах, тобто шукані ваги $w_1, w_2, ..., w_n$ відомі. Тоді

$$a_{ij} = \frac{w_i}{w_j}, \ i, j = \overline{1,n}, \tag{13.27}$$

$$a_{ij} a_{jk} = \frac{w_i}{w_j} \frac{w_j}{w_k} = \frac{w_i}{w_k} = a_{ik}, \quad i, j, k = \overline{1,n}.$$

З (13.27) витікає, що $a_{ij} \frac{w_j}{w_i} = 1, \ i, j = \overline{1,n}$. Тоді $\sum_{j=1}^{n} a_{ij} \frac{w_j}{w_i} = n, \ i = \overline{1,n}$, чи $\sum_{j=1}^{n} a_{ij} w_j = n w_i, \ i = \overline{1,n}$, а в матричному виді :

$$Aw = nw, \tag{13.28}$$

тобто w — ВВ A, який відповідає ВЗ n.

Розглянемо співвідношення (10.28) докладніше:

$$\begin{pmatrix} \frac{w_1}{w_1} & \frac{w_1}{w_2} & \cdots & \frac{w_1}{w_n} \\ \frac{w_2}{w_1} & \frac{w_2}{w_2} & \cdots & \frac{w_2}{w_n} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{w_n}{w_1} & \frac{w_n}{w_2} & \cdots & \frac{w_n}{w_n} \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = n \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}. \tag{13.29}$$

З (13.29) очевидно, що всі вектор-стовпці (вектор-рядки) матриці A колінеарні (їх відповідні координати пропорційні), ранг A дорівнює одиниці, а її спектр містить єдине ненульове ВЗ. Сума ВЗ матриці і її слід $tr(A)$, де

$$tr(A) = \sum_{i=1}^{n} a_{ii}, \tag{13.30}$$

пов'язані співвідношенням:

$$\sum_{i=1}^{n} \lambda_i = tr(A). \tag{13.31}$$

Завдяки властивостям A з (13.31), враховуючи (13.30), отримуємо, що

$$\sum_{i=1}^{n} \lambda_i = n, \tag{13.32}$$

тоді єдине ненульове ВЗ A, виходячи з (13.32), визначається як

$$\lambda_{\max} = n.$$

Відповідно до теореми Перрона, власному значенню $\lambda_{\max}$ відповідає ВВ $w_{\max}$ матриці A з додатними координатами. Для забезпечення одиничності $w_{\max}$ будемо розглядати нормовані ВВ, а норму вектора w визначимо як:

$$\|w\| = \sum_{i=1}^{n} |w_i|. \tag{13.33}$$

Тоді для $w_{\max}$ відповідно до (13.33) отримаємо:

$$\|w_{\max}\| = \sum_{i=1}^{n} w_{\max i} = 1,$$

де $w_{\max i}$, $i = \overline{1,n}$, — компоненти вектора $w_{\max}$.

Таким чином, при погодженості матриці A (ідеальний випадок) її найбільше ВЗ дорівнює n, більш того, можна показати, що додатна обернено-симетрична матриця *погоджена тоді й тільки тоді*, коли $\lambda_{\max} = n$.

Однак виконання вимоги (13.27) на практиці нереальне: a_{ij} будуть відхилятися від «ідеальних» відношень $\frac{w_i}{w_j}$, а тому співвідношення (13.28) не буде мати місця. Завдяки цьому надзвичайно важливою є чутливість ВЗ, зокрема $\lambda_{\max}$, до збурних дій, для встановлення якої значення мають наступні 2 теореми.

Нехай T – довільна матриця.

Теорема 13.6. ВЗ матриці T є неперервними функціями її елементів.

Доведення. Оскільки ВЗ матриці T — це корені її характеристичного рівняння

$$\det(T - \lambda I) = 0, \tag{13.34}$$

коефіцієнти якого є поліноміальними, а тому, неперервними функціями від елементів матриці, то достатньо показати, що корені многочлена $P = \det(T - \lambda I)$ — неперервні функції його коефіцієнтів.

Число коренів многочлена P, що знаходяться всередині контуру γ, дорівнює:

$$\frac{1}{2\pi i}\oint_{\gamma}\frac{P'(z)}{P(z)}dz\,. \tag{13.35}$$

При малому збуренні P значення $\dfrac{P'(z)}{P(z)}$ також збуриться мало (оскільки P — многочлен, то P' — також многочлен), що приведе до малої ж зміни значення виразу (13.35), а завдяки тому, що величина (13.35) є цілочисловою, то в дійсності вона не змінить свого значення взагалі. Таким чином, кількість коренів всередині γ залишиться такою ж. Але тоді корені в результаті збурної дії не зможуть опинитися поза контуром γ, яким би малим цей контур не був, якщо збурення P є достатньо малим. Завдяки цьому корені є неперервними функціями коефіцієнтів многочлена, а тому і елементів матриці.

Теорема 13.7. Нехай T — невід'ємна незвідна матриця загального виду, тобто всі елементи t_{ij} матриці T невід'ємні, і за допомогою переставлень вона не може бути представлена у вигляді

$$\begin{pmatrix} T_1 & 0 \\ T_2 & T_3 \end{pmatrix},$$

де T_1, T_2 — квадратні матриці, 0 — нульова матриця відповідного розміру. Тоді:

$$\min_i \sum_{j=1}^{n} t_{ij} \le \lambda_{\max} \le \max_i \sum_{j=1}^{n} t_{ij}\,, \tag{13.36}$$

$$\min_j \sum_{i=1}^{n} t_{ij} \le \lambda_{\max} \le \max_j \sum_{i=1}^{n} t_{ij}\,. \tag{13.37}$$

Доведення. За теоремою Фробеніуса ВВ матриці T, який відповідає $\lambda_{\max}$, має додатні компоненти і, з точністю до постійного множника, єдиний. Позначимо $l = (1,1,\ldots,1)^T$. Компоненти вектора Tl являють собою суми рядків матриці T. Нехай

$$m = \min_i \sum_{j=1}^{n} t_{ij} = \min_i (Tl)_i\,,\ M = \max_i \sum_{j=1}^{n} t_{ij} = \max_i (Tl)_i\,,$$

тоді

$$ml \le Tl \le Ml. \qquad (13.38)$$

Нерівність (13.38) розуміється покомпонентно. Рівність в (13.38) буде спостерігатися тільки тоді, коли $m = M$.

Нехай w — лівий ВВ матриці T, що відповідає $\lambda_{\max}$:

$$w^T T = \lambda_{\max} w^T. \qquad (13.39)$$

Множачи обидві частини нерівності (10.38) на w^T зліва, а (10.39) на l справа, відповідно отримаємо

$$w^T ml \le w^T Tl \le w^T Ml, \qquad (13.40)$$

$$w^T Tl = \lambda_{\max} w^T l. \qquad (13.41)$$

Підставляючи праву частину (13.41) в (13.40), маємо:

$$w^T ml \le \lambda_{\max} w^T l \le w^T Ml. \qquad (13.42)$$

Ділення (13.42) на додатне число $w^T l$ приведе до нерівності (13.36). Аналогічно доводиться і (13.37).

Виходячи з теорем 13.6, 13.7 і враховуючи дослідження, для додатних обернено-симетричних матриць, можна зробити висновок, що малі збурення елементів a_{ij} додатної обернено-симетричної матриці приведуть до малих же збурень її ВЗ, а це означає, що $\lambda_{\max}$, яке є максимальним ВЗ в задачі

$$Aw = \lambda_{\max} w \qquad (13.43)$$

з реально сформованою матрицею парних порівнянь (елементи a_{ij} відхиляються від відношень $\frac{w_i}{w_j}$), залишиться близьким до n, а інші ВЗ до нуля. Відхилення $\lambda_{\max}$ від n є мірою погодженості матриці A. Завдяки цьому відношення

$$(\lambda_{\max} - n)/(n-1) \qquad (13.44)$$

називається *індексом погодженості*. Задовільним вважається випадок, коли значення (13.44) менше або дорівнює 0.1. Якщо індекс погодженості перевищує 0.1, то можливим є «перегляд міркувань», тобто коректування матриці A. Одним з найбільше часто використовуваних для цього способів є ітераційний метод послідовного коректування на кожній ітерації тих елементів A, для яких

абсолютна різниця між a_{ij} і $\frac{w_i}{w_j}$ є найбільшою, за допомогою заміни a_{ij} на $\frac{w_i}{w_j}$ і перерахування вектора пріоритетів.

Встановимо тепер пріоритет кожного елемента побудованої ієрархічної моделі інформаційно-технологічної системи щодо головної мети — системи в цілому. Інакше кажучи, визначимо пріоритети (вагові коефіцієнти) для вершин будь-якого рівня КСР графа-моделі щодо вершини $s = L_1$, що є максимальним елементом ієрархії (коренем дерева).

Третій етап. Остаточне визначення вагових коефіцієнтів вершин графа-моделі — кількісних оцінок складових інформаційно-технологічної системи.

Нехай $Y = \{y_1,...,y_{m_k}\} \subseteq L_k$, а $X = \{x_1,...,x_{m_{k+1}}\} \subseteq L_{k+1}$. Відповідно до зауваження 13.11, можна припустити, що $Y = L_k$, $X = L_{k+1}$. Нехай елемент $z \in L_{k-1}$ такий, що будь-який елемент множини Y належить множині z^-. Для кожного елемента $x_i, i = \overline{1, m_{k+1}}$, визначений пріоритет цього елемента $w_{y_j}(x_i)$ стосовно кожного елемента $y_j, j = \overline{1, m_k}$, попереднього рівня. Для кожного елемента y_j з рівня ієрархії L_k визначений його пріоритет $w_z(y_j)$ стосовно $z \in L_{k-1}$ (рис. 13.11). Якщо через w позначити функцію пріоритету елементів з X стосовно z, то

$$w(x_i) = \sum_{j=1}^{m_k} w_{y_j}(x_i) w_z(y_j), i = \overline{1, m_{k+1}}. \qquad (13.45)$$

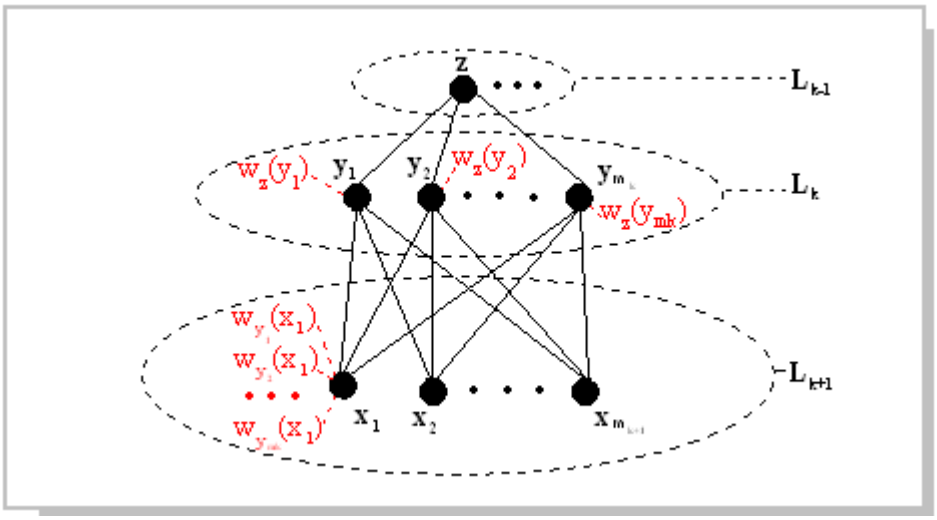


Рис. 13.11. Послідовне визначення пріоритетів елементів ієрархії

Співвідношення (13.45) представляє із себе процес зважування пріоритетів x_i щодо елементів y_j за допомогою пріоритетів y_j щодо z і в матричному виді може бути записане як:

$$W = B\overline{W}, \qquad (13.46)$$

де елементи матриці B

$$b_{ij} = w_{y_j}(x_i), \quad i = \overline{1, m_{k+1}}, \quad j = \overline{1, m_k},$$

елементи векторів $W, \overline{W}$ — це $w(x_i)$, $i = \overline{1, m_{k+1}}$, і $w_z(y_j)$, $j = \overline{1, m_k}$, відповідно. Таким чином, кожний процес перерахування пріоритетів елементів $\{x_1, ..., x_{m_{k+1}}\}$ відповідно до (13.46) потребує

$$\underline{O}(m_{k+1} m_k) \qquad (13.47)$$

арифметичних операцій.

Очевидно, процес послідовного обчислення пріоритетів $\{x_1, ..., x_{m_{k+1}}\} = L_{k+1}$ можна продовжити по індукції щодо елементів рівнів $L_{k-2}, ..., L_1$, тим самим визначаючи пріоритети будь-якого елемента ієрархії щодо головної мети L_1.

Для неповної ієрархії розглянутої графової моделі інформаційно-технологічної системи перерахування пріоритетів за формулою (13.45) потребує набагато менше обчислювальних витрат, ніж визначається співвідношенням (13.47). Кожний елемент $\{x_1, ..., x_{m_{k+1}}\} = L_{k+1}$ буде мати ненульове значення пріоритету тільки стосовно одного елемента y_j попереднього рівня L_k (рис. 13.12). Тоді формула (13.45) для перерахування пріоритетів буде виглядати

$$w(x_i) = w_{y_j}(x_i) w_z(y_j), \; i = \overline{1, m_{k+1}},$$

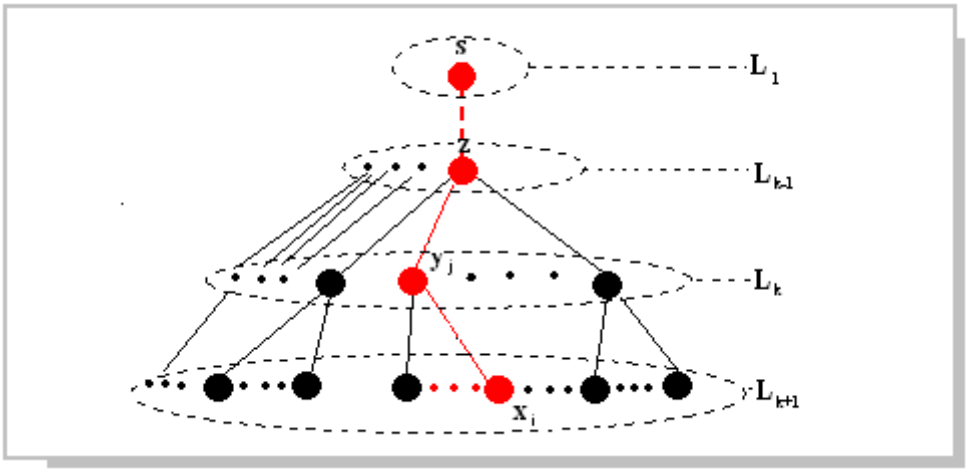


Рис. 13.12. Ланцюг впливу елемента x_i на максимальний елемент ієрархії інформаційно-технологічної системи

де y_j — це єдиний елемент попереднього рівня ієрархії, для якого $w_{y_j}(x_i) \neq 0$. Таким чином, для одного перерахування пріоритетів елементів $\{x_1,...,x_{m_{k+1}}\}$ знадобиться m_{k+1} арифметичних операцій. Для того, щоб обчислити пріоритет деякого елемента x_i побудованої ієрархічної графової моделі інформаційно-технологічної системи стосовно його впливу на систему в цілому, необхідно перемножити пріоритети вузлів простого ланцюга, що з'єднує x_i з s, що потребує арифметичних операцій на одиницю менше, ніж номер рівня ієрархії, який містить x_i.

Моделювання атаки на захищену інформаційну систему

Нехай атака на інформаційно-технологічну систему спрямована безпосередньо на конкретний засіб захисту x_i (в графі-моделі йому відповідає листок). У загальному випадку математичним виразом для атаки буде зменшення вагового коефіцієнта $w(x_i)$ атакованого засобу.

Зменшення $w(x_i)$ приведе до збурення матриці суміжності $\overline{G}$ графа інформаційно-технологічної системи, що, у свою чергу, збурить її ВЗ. Спочатку матриця $\overline{G}$ є додатно напіввизначеною (додатно визначеною). Після збурення дана властивість може бути порушена. Зокрема, якщо $w(x_i)$ стане нульовим (засіб x_i зруйновано), це, відповідно до теореми 13.4, обов'язково приведе до появи від'ємного ВЗ в збуреній матриці суміжності графа. Як було показано вище, необхідна відповідь системи на атаку повинна привести мінімальне ВЗ матриці суміжності до виду: $\lambda_{\min} \approx 0$, щоб його знаком можна було знехтувати. Такий результат може бути досягнений за рахунок збільшення ваг неатакованих засобів захисту. Модифікація ваг повинна бути проведена відповідно до встановлених вище відносних пріоритетів елементів інформаційно-технологічної системи. За допомогою запропонованого методу кількісної оцінки складових елементів системи перерахуємо вагові коефіцієнти всіх вузлів графа-моделі, попередньо змінивши кількість позитивних результатів роботи елементів відповідно до матриці S, побудованої в пункті 7. Очевидно, що з виведенням з ладу деякого засобу захисту, ваги засобів, що залишилися, відповідні вузли яких не лежать у графі-моделі на простому ланцюгу, що з'єднує x_i з s (рис. 13.12), не зменшаться. Серед наявних у розпорядженні СЗІ засобів захисту є як постійно діючі, так і ті, що активуються при виявленні спроби нападу. Зростання вагового коефіцієнта для засобів другого типу буде означати їхню активацію.

Таким чином, *відповідь* системи на атаку моделюється шляхом перерахування вагових коефіцієнтів елементів СЗІ, що приводить до активації деяких засобів захисту. Якщо така відповідь не приведе матрицю суміжності графа-моделі інформаційно-технологічної системи до виду, для якого $\lambda_{\min} \approx 0$, то

відповідь СЗІ є недостатньою, необхідне підключення додаткових засобів, що не входили у неї до атаки.

Зауваження 13.12. Обнуління або зменшення $w(x_i)$ приведе до збурення ВЗ матриці суміжності $\overline{G}$ графа-моделі, що в математичному сенсі й викличе необхідність відповіді системи на здійсненну атаку. Якщо збурення, що відбулися, не торкнулися максимальних ВЗ, у початкових збуреннях яких зберігається інформація, що циркулює в системі, або лише незначно збурили їх (результат збурної дії порівнянний з шумом округлень), то інформація при атаці не постраждала. Інакше несанкціонований доступ до інформації відбувся.

Зауваження 13.13. Оскільки формальна відповідь інформаційно-технологічної системи на атаку полягає в перерахуванні вагових коефіцієнтів вершин графа-моделі, то у випадку, коли граф системи має досить великий розмір, виникає проблема його чисельної обробки (велика кількість арифметичних операцій для перерахування ваг). Корисним способом дослідження великої кількості елементів, що знаходяться на одному рівні ієрархії, є групування їх у *кластери* відповідно до їхньої відносної важливості. У такий спосіб можна отримати кластери найважливіших елементів, елементів помірної важливості, а також малої важливості, для яких проводиться попарне порівняння їх відносного впливу на відповідний критерій (елемент) з розташованого вище рівня. Після аналізу кластерів елементи в кожному з них порівнюються парами по їхній відносній важливості. Якщо елементів занадто багато, то вони знову можуть бути згруповані. Групування в кластери в підсумку дає ті ж самі значення пріоритетів складових сукупної системи, що й при базовому підході.

Динамічна модель захищеної інформаційно-технологічної системи

Необхідність перерахування ваг вершин графа-моделі інформаційно-технологічної системи при моделюванні атаки неявно приводить до *динамічної моделі системи*. Основне розрахункове співвідношення (13.43) приймає вид:

$$A(t)w(t) = \lambda_{\max}(t)w(t), \qquad (13.48)$$

визначаючи всі складові його частини як функції часу t.

При роботі з динамічними дискретними функціями $a_{ij}(t)$ — коефіцієнтами матриці $A(t)$ — їх зазвичай апроксимують лінійними, степеневими, показниковими, логарифмічними функціями. Виходячи зі специфіки побудови графової моделі, коефіцієнти $A(t)$ є кусково-сталими функціями на всьому часовому проміжку функціонування інформаційно-технологічної системи, маючи розриви першого роду в точках $t = t_i$, що відповідають часу атаки на систему або часу відповіді системи на атаку.

Отримання рішення задачі (13.48) в явному виді через $a_{ij}(t)$ у загальному випадку надзвичайно важке. Дійсно, для обчислення точного значення $\lambda_{\max}(t)$ необхідно знайти корені характеристичного многочлена (13.34) для $A(t)$, степінь якого дорівнює вимірності матриці $A(t)$. Отримати корені многочлена прямими методами в довільному випадку можливо, коли його степінь не перевищує чотирьох. Нехай, наприклад, вимірність $A(t)$ дорівнює 2. Матричне рівняння (13.48) буде мати вид:

$$\begin{pmatrix} 1 & a(t) \\ \dfrac{1}{a(t)} & 1 \end{pmatrix} \begin{pmatrix} w_1(t) \\ w_2(t) \end{pmatrix} = \lambda_{\max}(t) \begin{pmatrix} w_1(t) \\ w_2(t) \end{pmatrix}. \qquad (13.49)$$

При цьому характеристичне рівняння для матриці $A(t)$ визначається в такий спосіб:

$$(1-\lambda)^2 - 1 = 0,$$

а тому $\lambda_{\max}(t) = 2$ незалежно від значення t, звідки відразу випливає, що будь-яка кососиметрична додатна матриця є погодженою. Оскільки $rank(A(t)) = 1$, то з системи (13.49) достатньо розглянути одне рівняння, наприклад, перше, з якого отримаємо, що $w_1(t) = a(t)w_2(t)$. Зафіксувавши довільно одну з координат вектора $w(t) = (w_1(t), w_2(t))^T$, наприклад, $w_2(t) = 1$, отримаємо $w(t) = (a(t), 1)^T$, а нормалізований вид для вектора пріоритетів

$$\left(\frac{a(t)}{a(t)+1}, \frac{1}{a(t)+1} \right)^T.$$

Для кусково-сталої функції $a(t)$ значення пріоритетів будуть змінюватися тільки в точках $t = t_i$, де $a(t)$ має стрибки.

Аналогічні результати, що виражають компоненти вектора пріоритетів через функції, які є елементами матриці порівнянь, можуть бути отримані, коли вимірність $A(t)$ буде дорівнювати 3 або 4.

Якщо розглянути обернено-симетричну матрицю $A(t)$ розміром 4×4 з елементами, які є функціями часу, то можна показати, що вектор пріоритетів визначається залежно від елементів матриці наступним чином:

$$w_1 = \frac{w_1^0}{Q}, \quad w_2 = \frac{w_2^0}{Q}, \quad w_3 = \frac{w_3^0}{Q}, \quad w_4 = \frac{w_4^0}{Q},$$

де

$$Q=(\lambda_{\max}-1)^3+(a_{14}+a_{24}+a_{34})(\lambda_{\max}-1)^2+\left[(a_{12}a_{24}-3)+(a_{13}+a_{23})a_{34}+\left(\frac{1}{a_{12}}+\frac{1}{a_{13}}\right)a_{14}+\frac{a_{24}}{a_{23}}\right]\times$$

$$\times(\lambda_{\max}-1)+\left[(a_{12}a_{23}a_{34}-a_{12}-a_{24}-a_{34})+\left(\frac{a_{13}a_{24}}{a_{23}}+\frac{a_{13}a_{34}}{a_{23}a_{12}}\right)+\frac{a_{14}a_{23}+a_{12}a_{24}}{a_{13}}\frac{a_{14}-a_{13}}{a_{12}a_{23}}\right],$$

$$w_1^0=a_{14}(\lambda_{\max}-1)^2+(a_{12}a_{24}+a_{13}a_{34})(\lambda_{\max}-1)+\left(a_{12}a_{23}a_{34}+\frac{a_{13}a_{24}}{a_{23}}-a_{14}\right),$$

$$w_2^0=a_{24}(\lambda_{\max}-1)^2+\left(a_{23}a_{34}+\frac{a_{14}}{a_{12}}\right)(\lambda_{\max}-1)+\left(\frac{a_{13}a_{34}}{a_{12}}+\frac{a_{14}a_{23}}{a_{13}}-a_{24}\right), \qquad (13.50)$$

$$w_3^0=a_{34}(\lambda_{\max}-1)^2+\left(\frac{a_{24}}{a_{23}}+\frac{a_{14}}{a_{13}}\right)(\lambda_{\max}-1)+\left(\frac{a_{14}}{a_{12}a_{23}}+\frac{a_{12}a_{24}}{a_{13}}-a_{34}\right),$$

$$w_4^0=(\lambda_{\max}-1)^2-3(\lambda_{\max}-1)+\left(\frac{a_{12}a_{23}}{a_{13}}+\frac{a_{13}}{a_{12}a_{23}}-a_{34}\right).$$

Зауваження 13.14. При аналізі виразів для компонентів вектора пріоритетів ((13.50), а також див. задачу 13.70) стає очевидним, що якщо будь-який коефіцієнт у даному рядку матриці парних порівнянь збільшується (зменшується), то величина координати ВВ, відповідної цьому рядку, збільшується (зменшується) щодо інших координат. Ця властивість притаманна й загальному випадку обернено-симетричної матриці.

Зауваження 13.15. Зменшення коефіцієнта в рядку матриці парних порівнянь моделі інформаційно-технологічної системи означає, що засіб захисту, що відповідає цьому рядку, піддався атаці, яка привела до часткового або повного виведення його з ладу. Відповідно до зауваження 13.14, його пріоритет (координата ВВ) зменшиться щодо інших компонентів, що відбувається в повній відповідності до реального функціонування системи.

Нехай вимірність $A(t)$ більша чотирьох. Використовуємо підхід розкладання ієрархії на кластери. Для цього для кожного вузла $y_j \in L_{k-1}$ множина всіх суміжних з ним вузлів з рівня L_k розбивається не більш, ніж на 4 кластери (рис. 13.13). Тоді $\lambda_{\max}(t)$ для матриці $A(t)$ парних порівнянь впливу кластерів на відповідний критерій ($y_j \in L_{k-1}$) можливо буде точно виразити через коефіцієнти $A(t)$. Подальші дії аналогічні описаним у зауваженні 13.13.

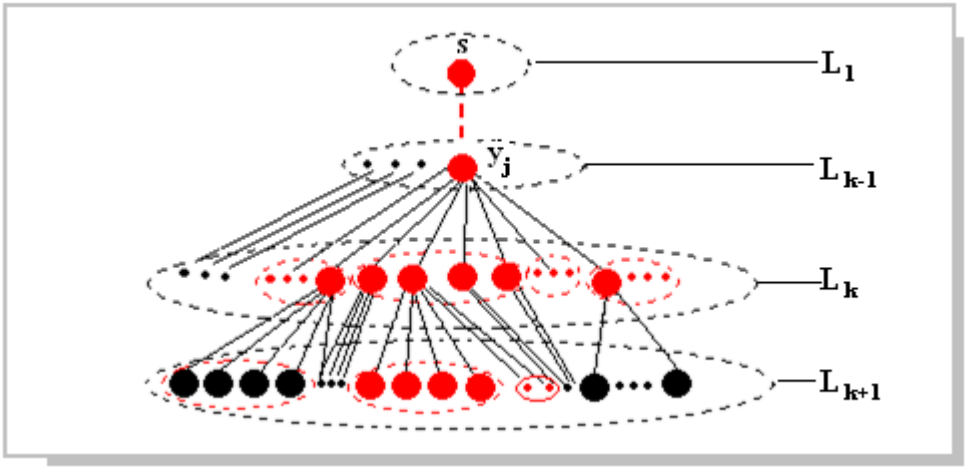


Рис. 13.13. Розкладання ієрархії на кластери у випадку динамічної моделі інформаційно-технологічної системи

Очевидно, що для можливості послідовного виразу ваг вершин через коефіцієнти матриць парних порівнянь кількість кластерів, вплив яких досліджується на конкретний елемент ієрархії, при розбивці необхідно не повинна перевищувати чотирьох.

Енергетична цінність інформаційно-технологічної системи

Вагові коефіцієнти вершин побудованого графа-моделі інформаційно-технологічної системи відображають реальну значущість об'єктів, яким вони відповідають, для функціонування всієї системи, а матриця суміжності $\overline{G}$ несе в собі інформацію про сукупну «цінність» системи й відносних цінностях її складових частин.

Подивимось на матрицю $\overline{G}$ як на цифрове представлення деякого двовимірного сигналу. Цей сигнал однозначно визначає інформаційно-технологічну систему.

Одною з основних характеристик сигналу з $n \times n$-матрицею $\overline{G}$ з елементами $\overline{g}_{ij}$ є його енергія E:

$$E = \sum_{i=1}^{n} \sum_{j=1}^{n} \overline{g}_{ij}^{2} = \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} P(u,v), \qquad (13.51)$$

де $P(u,v),\ u,v = \overline{0,n-1}$, — енергетичний спектр сигналу.

Таким чином, як одна з числових характеристик інформаційно-технологічної системи може розглядатися енергія сигналу $\overline{G}$.

Нехай F — матриця довільного двовимірного цифрового сигналу.

Теорема 13.8. Енергія сигналу дорівнює сумі квадратів СНЧ його матриці F.

Доведення. Сингулярне розкладання (13.9) матриці F може бути представленим у вигляді суми зовнішніх добутків, подібно (13.11):

$$F = U\Sigma V^T = \sum_{i=1}^{n} \sigma_i u_i v_i^T .$$

Таке представлення розбиває F на n сигналів $\sigma_i u_i v_i^T$, сумарна енергія яких дає E (13.51). Енергія сигналу $\sigma_i u_i v_i^T = \sigma_i \left(u_{1i},\ldots,u_{mi}\right)^T \left(v_{1i},\ldots,v_{ni}\right)$ в просторовій області буде дорівнювати:

$$\sigma_i{}^2 \left(u_{1i}{}^2 v_{1i}^2 + \ldots + u_{1i}^2 v_{ni}^2 + u_{2i}^2 v_{1i}^2 + \ldots + u_{2i}^2 v_{ni}^2 + \ldots + u_{mi}^2 v_{1i}^2 + \ldots + u_{mi}^2 v_{ni}^2\right) =$$

$$= \sigma_i^2 (u_{1i}^2 (v_{1i}^2 + \ldots + v_{ni}^2) + \ldots + u_{mi}^2 (v_{1i}^2 + \ldots + v_{ni}^2)) =$$

$$= \sigma_i^2 \left(u_{1i}^2 + \ldots + u_{mi}^2\right)\left(v_{1i}^2 + \ldots + v_{ni}^2\right) = \sigma_i^2 .$$

Таким чином, повна енергія сигналу F визначається як $E = \sigma_1{}^2 + \ldots + \sigma_n{}^2$.

Наслідок. Енергія двовимірного цифрового сигналу, матриця якого F є симетричною, дорівнює сумі квадратів ВЗ F

$$E = \lambda_1{}^2 + \ldots + \lambda_n{}^2 . \qquad (13.52)$$

Визначення 13.7. Назвемо *енергетичною цінністю інформаційно-технологічної системи* енергію матриці суміжності $\overline{G}$ її графа-моделі, яка розглядається як двовимірний сигнал.

Відповідно до визначення 13.7 і співвідношення (13.52) *енергетична цінність інформаційно-технологічної системи повністю визначається спектром матриці* $\overline{G}$.

Якщо сигнали мало відрізняються між собою, то мала відмінність і між значеннями їх енергій. Протилежне, загалом кажучи, не вірне. Але якщо числові значення енергій сильно відрізняються, то необхідним буде й значна відмінність між сигналами.

Якщо всі ВЗ $\overline{G}$ невід'ємні, то відповідно до (13.52) збільшення або зменшення ВЗ приводить до аналогічної зміни енергії двовимірного сигналу. Інакше, якщо є ВЗ різних знаків, а саме це відбувається при моделюванні повного виведення з ладу деякого засобу захисту системи, цього стверджувати не можна. Якщо відповідь СЗІ на атаку приведе найменше ВЗ до значення, знаком якого можна знехтувати, то значна відмінність енергетичних цінностей системи до впливу й після відповіді на атаку при їх порівнянні буде необхідно

вимагати додаткових дій по коректуванню СЗІ з залученням нових засобів захисту. Такі міркування накреслюють ще один шлях аналізу стану інформації, збереженої в системі, заснований на аналізі збурення енергетичної цінності інформаційно-технологічної системи, що відбулося в результаті атаки.

13.2 Формалізація взаємовідносин порушника і системи кіберзахисту інформації

13.2.1. Формалізація дій порушника під час впливу на систему кіберзахисту

Розробка математичної моделі інформаційно-технологічної системи неможлива без врахування передбачуваного для системи противника, без створення його моделі. Питання розробки адекватних математичних моделей порушника (і не тільки інформаційного — різних терористичних організацій і інших типів кримінальних груп) з метою залучення строгого математичного апарата й обчислювальної техніки для автоматизації розробки можливих шляхів боротьби з терористичними угрупованнями, а також для формалізації аналізу результатів контртерористичних дій стало дуже гостро.

Будемо розглядати противника інформаційно-телекомунікаційної системи як окремий випадок терористичної групи.

Аналіз традиційних шляхів при моделюванні групи противника

Традиційним шляхом для відображення групи людей з зазначенням взаємних відносин між ними є використання теорії графів. Це обумовлене сукупністю факторів, серед яких наочність отриманої моделі, можливість адекватного відображення за допомогою стандартних операцій на графах реальних дій над групами й подій у групах, існування розробленого математичного апарата для роботи з графами, включаючи велику кількість евристичних методів, що добре зарекомендували себе на практиці.

У даний момент у науковому світі надзвичайно активізувалася робота з математичного моделювання терористичних організацій і інших типів кримінальних груп. Але більшість з існуючих моделей, інформація про які доступна з відкритих джерел, далекі від досконалості: вони мають обмежений і недостатньо інформативний характер, оскільки слабо враховують або не враховують взагалі ієрархію організації.

Розробимо загальну графову модель довільної групи противника зі строго обґрунтованим врахуванням ієрархії за допомогою використання зваженого неорієнтованого графа. Введення значень ваги для вершин і ребер буде

відбуватися при максимальнім використанні апріорної інформації про кримінальну групу (противника).

Запропонована математична модель дасть можливість для використання нових методів обробки графів, що не застосовувалися раніше, для рішення задачі про руйнування угруповання, а також чисельної оцінки збитку, заподіяного противникові за допомогою контртерористичних дій.

Підвищення інформативності моделі противника (порушника) за рахунок використання зваженого графа

Розглянемо задачі, пов'язані з організацією контртерористичних дій, рішення яких здійснюється з використанням графових математичних моделей противника. Окремі індивідуми представляються в такій моделі у вигляді вузлів (вершин), пари яких з'єднуються ребром, якщо існує певний взаємозв'язок між відповідними членами розглянутої групи.

Нехай організація противника у своїй ієрархії має 3 основних рівня:

- лідера (керівника) або декількох лідерів,
- представників сполучної ланки,
- безпосередніх виконавців.

Найпростіший варіант графової моделі (неорієнтований незважений граф), де ребра з'єднують вершини в тому випадку, якщо між відповідними членами існує безпосередній зв'язок, представлений на рис. 13.14 (вузли, відповідні лідерам організації, середній ланці і виконавцям, для наочності мають чорний, темний і світлий сірий кольори). Граф очевидно є зв'язним. Зазвичай безпосереднього зв'язку між лідерами і виконавцями не існує, хоча така можливість і не виключається.

Традиційно графові моделі противника (порушника) використовуються для рішення наступних задач.

Задача 1. Визначення членів противника, блокування (знищення) яких реально можливо здійснити, і це блокування приведе до розпаду організації противника на декілька незв'язаних між собою підгруп. Результатом такого розпаду може стати як повне знищення групи (припинення її функціонування), так і зниження ефективності її діяльності.

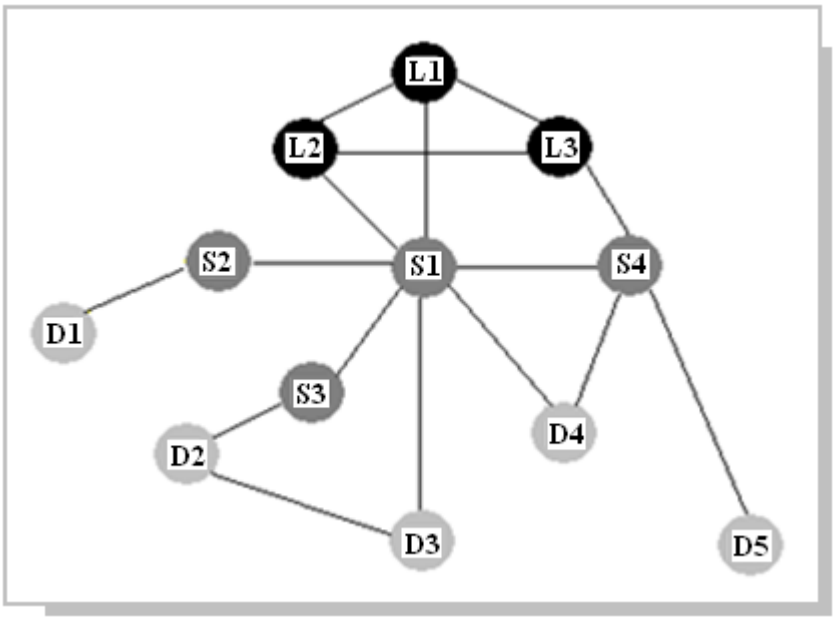


Рис. 13.14. Приклад графової моделі противника (порушника)

Мовою графів дана задача буде формулюватися наступним чином: необхідно визначити множину вузлів (множину, що містить мінімальну кількість вузлів), видалення яких приведе до розпаду зв'язного графа на декілька компонент зв'язності. Якщо така множина містить один вузол, то він називається *точкою зчленування.* В прикладі, наведеному на рис. 13.14, точкою з членування є S1. Блокування цього єдиного члена групи противника (порушника) приводить до її розпаду на чотири підгрупи, причому три з них стають «обезглавленими», а тому часто недієздатними (рис. 13.15). Але таке можливе не завжди.

Задача 2. Виділення в організації противника (порушника) таких зв'язків між членами, розрив яких приводить до розпаду групи на окремі частини, незв'язані між собою, що очевидно значно обмежить можливості діяльності розглянутої кримінальної структури.

Мовою графів задача формулюється наступним чином: визначити множину ребер (мінімальну за кількістю множину ребер) у графі, видалення яких спричинить його розпад на декілька компонент зв'язності.

Для отримання задовільного результату при рішенні поставлених задач графова модель противника (порушника) повинна мати максимальну інформативність, враховувати ієрархію розглянутого кримінального угруповання.

Для цього будемо розглядати як модель противника (порушника) неорієнтований зважений граф (для додаткового врахування ієрархії може використовуватися нумерація вершин: спочатку нумеруються лідери, потім середня ланка, останніми — безпосередні виконавці, хоча це необов'язково). Введення значень ваги для вершин і ребер відбувається при максимальнім

використанні апріорної інформації про супротивнику й має визначальне значення в запропонованій моделі.

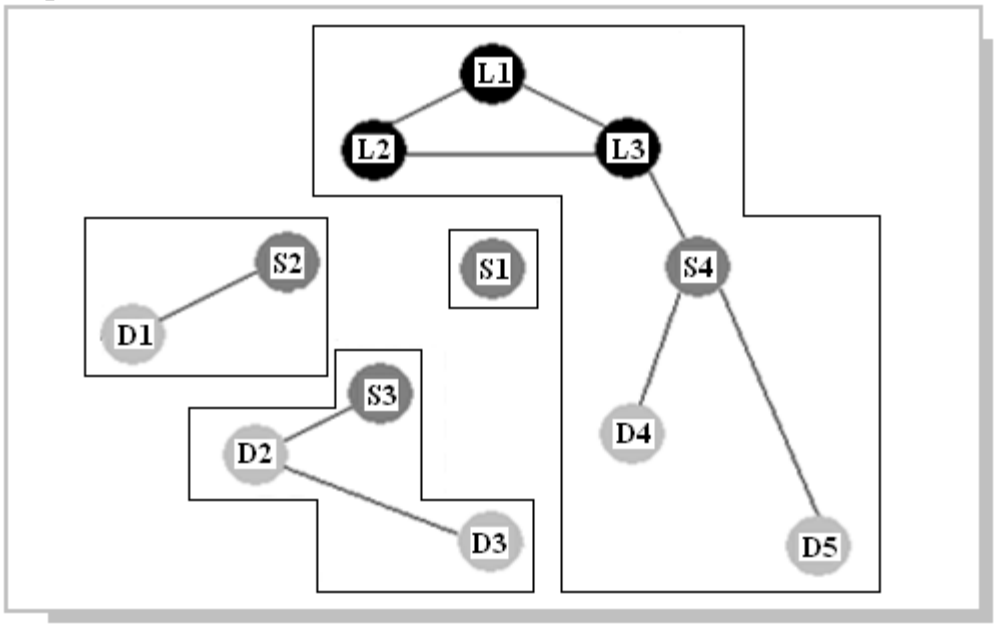


Рис. 13.15. Вид графової моделі противника (порушника) після видалення точки зчленування графа

Серед основних факторів, врахування яких впливає на формування ваги вершини в графовій моделі противника (порушника) інформаційно-технологічної системи, у першу чергу, виділимо:

- Поінформованість (П) конкретного члена групи про можливості засобів захисту інформації, що використовуються у системі й представляють зацікавленість для даного індивідуума;
- Матеріальні й часові можливості (МЧМ) противника (порушника) (обмеженість проміжку часу й матеріальних ресурсів для проведення конкретної атаки);
- Роль (Р) розглянутого члена в групі противника (порушника) (тим самим забезпечується врахування ієрархії).

Крім того, при формуванні вагового коефіцієнта вершини необхідно також врахувати класифікацію потенційних порушників за рівнем їх знань і навичок (РЗН) поводження з системою наступним чином:

1. Знає функціональні особливості системи, основні закономірності її функціонування;
2. Має високий рівень знань і досвід роботи з технічними засобами системи;
3. Має високий рівень знань в галузі програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

4. Знає структуру, функції й механізм дії засобів захисту, їх сильні й слабкі сторони.

Залежно від того, до якої категорії відноситься конкретний член організації противника (порушника), визначається значення складової частини вагового коефіцієнта вузла графа, що відповідає безпосередньо цьому члену (чим більше порядковий номер категорії в запропонованому вище переліку, тим більша повинна бути відповідна частина вагового коефіцієнта).

Зауваження 13.16. Обчислення вагових коефіцієнтів вершин графа-моделі передбачуваного противника (порушника) інформаційно-технологічної системи (пріоритетів членів групи) може бути проведене, наприклад, з використанням МАІ, де як критерії для визначення пріоритетів розглядаються П, МЧМ, Р, РЗН.

Вага ребра, яка визначається як пріоритетність відповідної лінії зв’язку, також може обчислюватися за допомогою МАІ з наступними критеріями:

- Реальна цінність інформації, яка передається за допомогою даної лінії зв'язку (наприклад, у більшості випадків можна припустити, що інформація, яка надходить від керівників групи, є більш важливою, ніж інформація, якою обмінюються між собою безпосередні виконавці);
- Надійність розглянутої лінії зв'язку (наприклад, зв'язок при безпосередньому контакті є більш надійним, ніж при використанні телефонної лінії).

Приклад зваженого графа-моделі можливого противника (порушника) наведений на рис. 13.16 (порядок нумерації відповідає ієрархії членів організації, у середині вузла — його номер, поруч із вузлом — його вага, поруч із ребром у дужках — вага ребра).

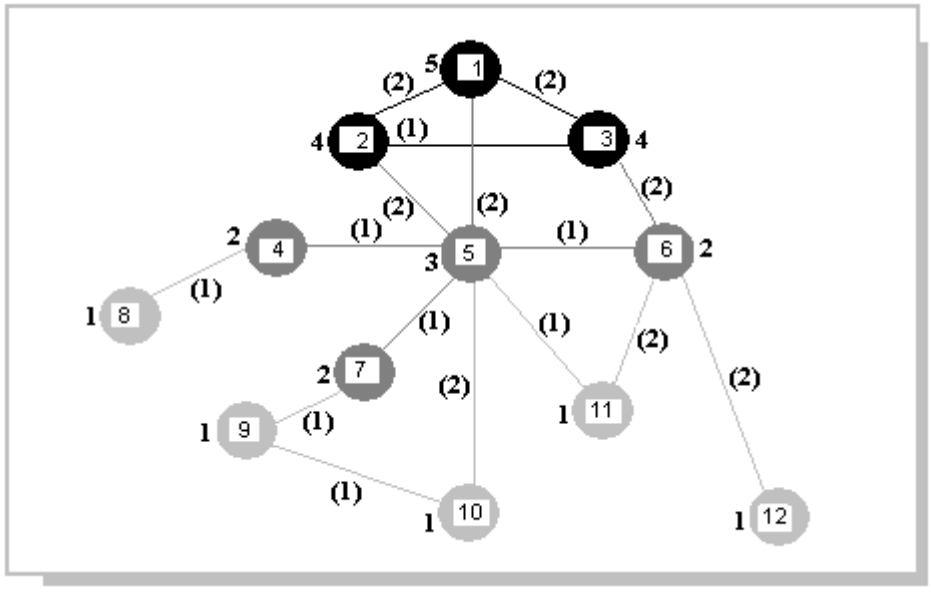


Рис. 13.16. Модель групи противника (порушника)
у вигляді зваженого графа

Зауваження 13.17. Використання зваженого графа при моделюванні організації противника (порушника) дає можливість врахувати її ієрархію, не переходячи до орієнтованого графа. Такий перехід, зазвичай, ускладнює процес обробки графа. Крім того, матриця суміжності неорієнтованого графа є симетричною, що дає можливість у деяких алгоритмах обробки значно зменшити кількість необхідних арифметичних операцій.

Аналіз структури й діяльності групи противника (порушника) на основі графової моделі

Задачі 1,2, які розв'язуються контртерористичними організаціями в процесі боротьби з кримінальними групами, були сформульовані в попередньому пункті в загальному виді. Результат блокування (видалення) деяких членів або якихось зв'язків групи, що приводить до її розпаду на окремі підгрупи, у реальності може виявитися зовсім незначним з погляду зниження дієздатності противника (порушника). Наприклад, якщо знищити зв'язок між членами S4 і D5 (міст у графовій моделі противника (порушника) (рис. 13.14)), це навряд чи нанесе відчутний удар по всій групі, тому що частина, яка залишилася без D5, збереже як абсолютну більшість своїх членів, так і наявність усіх ієрархічних ланок.

Одним з основних питань при моделюванні кримінальних мереж і активних дій над ними є питання про те, коли розглянуту структуру можна вважати зруйнованою або знищеною. Варіант знищення всіх членів групи розглядатися не буде, тому що, незважаючи на те, що такий варіант часто є прийнятним і навіть бажаним, він з великою часткою ймовірності може виявитися принципово нездійсненним (або нездійсненним за певний обмежений проміжок часу при наявності певного обмеженого матеріального ресурсу).

Розглянемо можливе рішення задачі 1. По графовій моделі групи визначається множина всіх простих, або «командних», ланцюгів, початок і кінець яких відповідає лідерові й безпосередньому виконавцеві відповідно. По отриманій множині визначається така сукупність вузлів графа, кожний з яких є присутнім хоча б в одному ланцюзі, а кожний ланцюг вносить у цю сукупність єдиний вузол. Видалення із графа такої сукупності, зруйнує всі існуючі «командні» ланцюги. У цьому випадку робиться висновок про знищення терористичного угруповання.

Побудуємо алгоритм для здійснення знищення групи противника (порушника), використовуючи в якості моделі запропонований вище зважений неорієнтований граф. Для цього скористаємося КСР графа-моделі з коренем у вузлі, що має найбільшу вагу, тобто, що відповідає лідерові (варіант, коли максимальну вагу мають декілька вершин, розглядається нижче). Для графа, зображеного на рис. 13.16, така КСР буде мати вигляд, представлений на рис. 13.17.

Всі «командні» ланцюги — це прості ланцюги графа, що виходять з нульового рівня КСР і закінчуються або вершиною, степінь якої дорівнює 1, або вершиною, що знаходиться в останньому рівні КСР; якщо v_k, v_m — дві послідовні вершини такого ланцюга, то номер рівня в КСР, який містить v_k, не більший за номер рівня, в якому опинилася вершина v_m. Вузли, що потрапили в один рівень структури, визначать сукупність, видалення якої приведе до розпаду графа на окремі компоненти завдяки розриву всіх ланцюгів зв'язків, тобто до знищення терористичної групи в зазначеному вище розумінні. Зазначимо, що при цьому не треба було явне визначення множини «командних» ланцюгів — вони виникають автоматично завдяки побудові КСР.

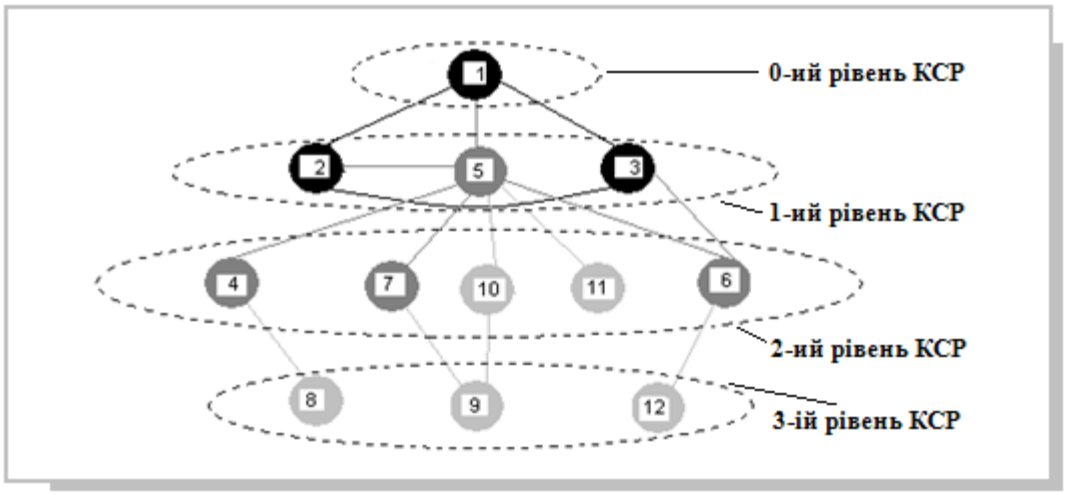


Рис. 13.17. Коренева структура рівнів зваженого графа противника (порушника)

Нехай є кілька вершин з максимальною вагою. Тоді при побудові КСР роль «кореня» буде відігравати не один вузол: усі вершини графа з максимальними ваговими значеннями, що відповідають лідерам противника (порушника), розташовуються на нульовому рівні структури або поєднуються в один *макровузол*. Інші кроки для виділення відокремлюючої множини графа залишаються без зміни.

Розглянемо варіант нанесення удару по кримінальній структурі, коли метою є знищення (блокування) мінімальної (або просто малої) кількості її членів. Переходячи до графової інтерпретації, задача полягає в пошуку мінімальної відокремлюючої множини графа (або відокремлюючої множини, що містить малу кількість вершин). Для цього буде потрібна довга й вузька КСР, у якій доцільно виключати вузли з того рівня, де їх кількість буде найменшою. Найдовша КСР відповідає кореню, що є периферійним вузлом графа. Однак пошук периферійних вузлів є дорогою процедурою, яка потребує

для свого здійснення, як правило, більш, ніж $\underline{O}(|X||E|)$ арифметичних операцій, де $|X|$ — кількість вершин, а $|E|$ — кількість ребер графа, і для графа великого розміру може виявитися досить громіздкою в обчислювальному сенсі. Враховуючи це, будемо використовувати КСР з коренем у *псевдоперифері́йному вузлі*, алгоритм пошуку якого представлений на рис. 13.18.

Рис. 13.18. Алгоритм пошуку псевдоперифері́йного вузла

Скористаємося КСР, наведеною на рис. 13.17, як початковою для пошуку псевдоперифері́йного вузла графа-моделі, представленої на рис. 13.16. В останньому рівні виберемо вузол з мінімальним степенем: $x = 12$. Провівши дії, передбачені алгоритмом, отримаємо як псевдоперифері́йний вузол $x = 8$. КСР з коренем у цьому вузлі зображена на рис. 13.19. Рівні, що містять мінімальну кількість вузлів — це перший і другий. Який з них обрати, щоб нанести більшу шкоду сукупному угрупованню противника (порушника)?

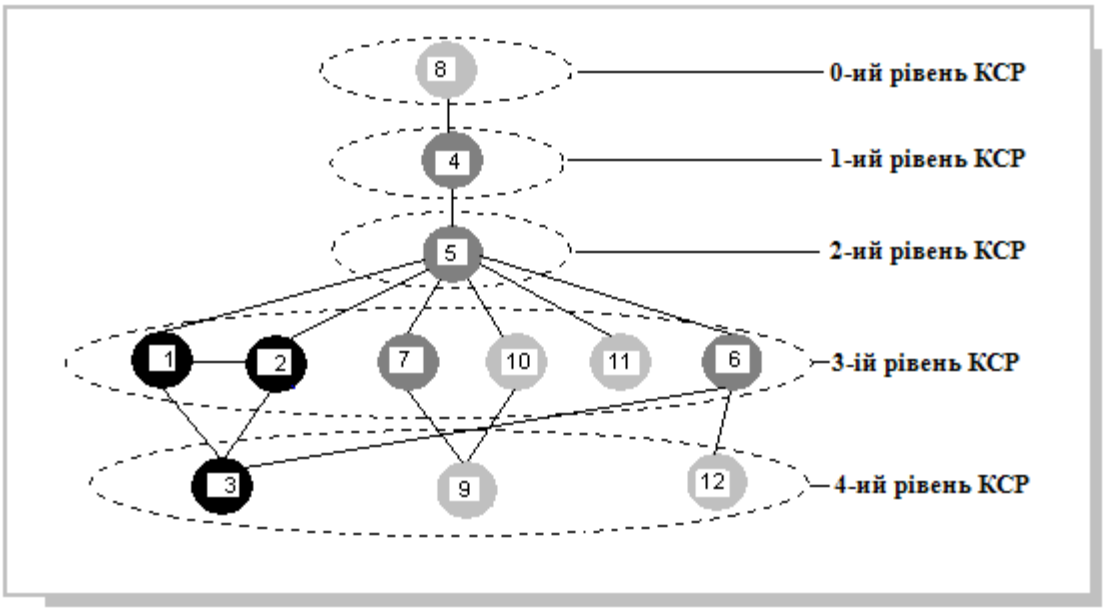


Рис. 13.19. Структура рівнів з коренем у псевдоперифері́йному вузлі

Перевагу має другий рівень: степінь вузла 5 більше, ніж вузла 4, тому очікується, що при виключенні п'ятого вузла кількість зв'язних компонентів, на які розпадеться граф, може виявитися більше, ніж при виключенні вузла 4 (зазначимо, що доцільність виключення вузла 5 (S1) (рис. 13.14, 13.16) з метою розбивки групи на підгрупи була встановлена раніше, виходячи лише з візуального зображення графа, що при його великому розмірі може виявитися нездійсненним).

Однак при плануванні контртерористичних дій має значення не тільки кількість отриманих у результаті розрізнених частин групи (компонент зв'язності графа). Важливим є сукупний збиток, заподіяний угрупованню при видаленні тих або інших його членів, зв'язків. Можлива ситуація, коли руйнування численних зв'язків деякого індивідуума (відповідний вузол графа має великий степінь) може виявитися малозначним для групи в цілому, і лише один розірваний зв'язок приведе до фактичного знищення противника (порушника).

Для чисельної оцінки збитку, заподіяного кримінальному угрупованню виключенням з його складу деяких членів, скористаємося матрицею суміжності його графа-моделі, яку надалі будемо позначати $PROT$. Для графа, зображеного на рис. 13.16, ця матриця має вид:

$$PROT=\begin{pmatrix} 5 & 2 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 4 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 1 & 3 & 1 & 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(на головній діагоналі — вагові коефіцієнти вершин, позадіагональні елементи — вагові коефіцієнти ребер). Завдяки неорієнтованості графа матриця є симетричною. Вона повністю визначає зважений граф, а тому характеризує всю сукупну групу противника (порушника). Кожна з характеристик такої матриці є характеристикою й реальної людської групи.

Назвемо *ваговою енергією терористичної групи* (E_{tr}) енергію сигналу, цифровим відображенням якого є матриця суміжності $PROT$ графової моделі противника (порушника):

$$E_{tr} = \|PROT\|^2,$$

де $\|\bullet\|$ — матрична норма Фробеніуса.

Виключення певного члена групи — певної вершини графа разом з інцидентними ребрами — для матриці суміжності буде виражатися у видаленні з неї рядка й стовпця, номери яких відповідають номеру виключеної вершини. Енергію групи противника (порушника) після виключення з неї членів $x_{k_1}, x_{k_2}, ..., x_{k_p}$ будемо позначати $E_{tr}(x_{k_1}, x_{k_2}, ..., x_{k_p})$. Чим менше значення

$E_{tr}(x_{k_1}, x_{k_2}, ..., x_{k_p})$, тобто чим більше воно відрізняється від E_{tr}, тим більш «значущих» для функціонування сукупного угруповання членів вдалося блокувати. Показник $E_{tr}(x_{k_1}, x_{k_2}, ..., x_{k_p})$ використовується для порівняння результатів передбачуваного знищення тих або інших членів противника (порушника). Залежно від підсумків порівняння робиться висновок про доцільність знищення конкретної сукупності членів групи. Алгоритм для визначення відокремлюючої множини графа противника (порушника), що пропонується, представлений на рис. 13.20.

Крок 1. Знайти псевдопериферійний вузол x у графі супротивника

Крок 2. У кореневій структурі рівнів

$$\Im(x) = \{L_0(x), L_1(x), ..., L_{l(x)}(x)\}$$

знайти рівень $L_i(x)$, що містить найменше число вузлів графа.

а) Якщо $L_i(x)$ визначається однозначно, то покласти $I = i$, перейти на крок 3.

б) Нехай $L_i(x)$ визначається неоднозначно, тобто $i \in IND$, $|IND| > 1$, де IND - деяка множина індексів рівнів КСР $\Im(x)$.

Обчислити

$$E_{tr}(L_i(x)) \text{ для } \forall i \in IND,$$

Визначити

$$E_{\min} = \min_{i \in IND} E_{tr}(L_i(x)),$$

$$I = \arg\min_{i \in IND} E_{tr}(L_i(x)).$$

Крок 3. $L_I(x)$ - шуканий рівень КСР, що виключається з неї

Рис. 13.20. Алгоритм для визначення відокремлюючої множини графа противника (порушника)

Зауваження 13.18. В запропонованому алгоритмі використовується порівняння вагових енергій терористичних груп після видалення їх деяких членів. Скориставшись симетричністю матриці суміжності неорієнтованого графа, для оцінки $E_{tr}(L_i(x))$ можна обчислювати норму не всієї матриці суміжності, а лише її верхньої (або нижньої) трикутної частини, що дозволить скоротити обчислювальну роботу в порівнянні з початковим варіантом практично у два рази.

Зауваження 13.19. Кількість арифметичних операцій для реалізації запропонованого алгоритму визначення відокремлюючої множини з метою її виключення для графа з множиною вершин X визначається як $\underline{O}(|X|^2)$.

Звичайно, такий алгоритм не гарантує відділення лідерів від безпосередніх виконавців, але розбивка на зв'язні компоненти в кожному разі приведе до ослаблення групи противника (порушника) й зажадає певного часу на її відновлення.

Таким чином, використання при побудові моделей різних кримінальних груп зважених графів є перспективним напрямком, що дає можливість врахувати ієрархію противника (порушника) без переходу до орієнтованого графа й введення в графову модель різних додаткових математичних об'єктів. Симетричність матриці суміжності графової моделі дає потенційну можливість виграшу в кількості арифметичних операцій при обробці отриманого графа в порівнянні з тим варіантом, коли граф виявляється орієнтованим. Введення поняття вагової енергії терористичної групи дає основу для розробки нового підходу до проблеми чисельної оцінки збитку, заподіяного кримінальній групі, на підставі якого будується алгоритм для визначення відокремлюючої множини графа противника (порушника).

Звичайно, багато задач на графах для одержання точного рішення вимагають повного перебору, однак наявність великої кількості евристичних алгоритмів, що добре зарекомендували себе на практиці при обробці графів, дають можливість розраховувати на успішне використання деяких з цих алгоритмів і на графових моделях противника (порушника).

Розглянемо задачу, пов'язану з аналізом структури групи противника (порушника), що полягає безпосередньо в визначенні такого її члена, «положення» якого в групі мінімізує витрати, які конкретизуються нижче, на встановлення зв'язків з іншими членами. Така людина є «максимально зручною» сполучною ланкою в групі: поширення будь-якої інформації в організації найбільш ефективно, з погляду оптимізації витрат, проводити за його допомогою, а блокування такого члена групи сповільнить і значно послабить діяльність організації в цілому. Крім того, впровадження агента замість такого знищеного члена кримінальної групи, дозволить агентові встановити контакти з усіма членами групи, використовуючи для цього мінімальні сукупні витрати, що підвищить імовірність виконання дорученої йому задачі у виділений обмежений проміжок часу при обмежених ресурсах.

На основі запропонованої графово-матричної моделі противника (порушника) проведемо розробку ефективних методів рішення поставленої задачі, розглянутої як узагальнення *задачі про розміщення пункту обслуговування в мережах* (графах), де сума найкоротших відстаней від шуканого пункту до заданих вершин графа повинна бути мінімальною

(оптимальне в зазначеному сенсі місце розміщення пункту обслуговування називається *медіаною* графа).

Нехай $G(X,E)$ — зважений граф, який є моделлю групи противника (порушника), де X — множина вершин з ваговими коефіцієнтами $q(x) \geq 0, \forall x \in X$, кожна з яких відповідає конкретному члену групи ($|X| = n$), а E — множина неупорядкованих пар вершин (ребер) $< x, y >, \quad x, y \in X$, з ваговими коефіцієнтами $l(x,y)$, які визначають часові (або матеріальні, або сумарні матеріально-часові) витрати на встановлення безпосереднього зв'язку між індивідуумами, відповідними до вершин x, y ($|E| = m$). Зазначимо, що сукупні витрати на встановлення зв'язку між певними членами організації будуть залежати не тільки від часу, але й від того, на якому щаблі ієрархічних сходів розташовані розглянуті індивідууми (мовою графів — від вагових коефіцієнтів вершин). Нижче $l(x,y)$ будемо називати *довжиною ребра* $< x, y >$.

Нехай $C(x,z), x,z \in X$, — простий ланцюг графа $G(X,E)$, який з'єднує вершини x,z, відстань між якими — $d(x,z)$. Задача про медіану в графі-моделі $G(X,E)$ полягає в знаходженні такої вершини $x^* \in X$, для якої

$$F(x^*) = \min_{x \in X} \sum_{y \in X} q(y) d(x,y). \qquad (13.53)$$

Обчислювальна складність рішення такої задачі буде залежати від кількості арифметичних операцій, затрачуваних на знаходження відстаней $d(x,y)$. Одним з найбільш популярних алгоритмів знаходження $d(x,y)$ є алгоритм Дейкстри, який потребує для знаходження довжин найкоротших шляхів від даної вершини x до всіх вершин графа $\underline{O}(n^2)$ операцій. Тоді обчислювальна складність рішення задачі (13.53) буде визначатися як $\underline{O}(n^3)$, і є досить значною для графа великого розміру.

Нижче пропонуються алгоритми рішення задачі (13.53), що дозволяють суттєво зменшити кількість арифметичних операцій для отримання остаточного результату.

Використання кореневої структури рівнів для рішення задачі про медіану графа-моделі

Оскільки граф-модель є зв'язним, то кількість ребер-зв'язків m в ньому задовольняє співвідношенню:

$$n - 1 \leq m \leq \frac{(n-1)n}{2}. \qquad (13.54)$$

Ліва частина нерівності (13.54) відповідає кількості ребер у дереві, права — в повному графі. Припустимо, що кількість існуючих у групі противника (порушника) безпосередніх зв'язків для кожного з її членів, а тому і сукупна кількість зв'язків, невелика й представляється, як $m = \underline{O}(n)$ (це припущення відповідає, наприклад, вимозі забезпечення максимальної скритності групи). Крім того, припустимо, що більшість ребер мають рівні вагові коефіцієнти (більшість зв'язків між безпосередніми виконавцями, а також між представниками середньої ланки ієрархії реально оцінювати з однаковими витратами), які, не обмежуючи спільності міркувань, ми покладемо для зручності рівними одиниці. Інші вагові коефіцієнти $l(x, y) \in N$. Приклад такої графової моделі представлений на рис. 13.21(а) (поруч з кожним ребром (вершиною) — значення вагового коефіцієнта, усередині вершини — її номер).

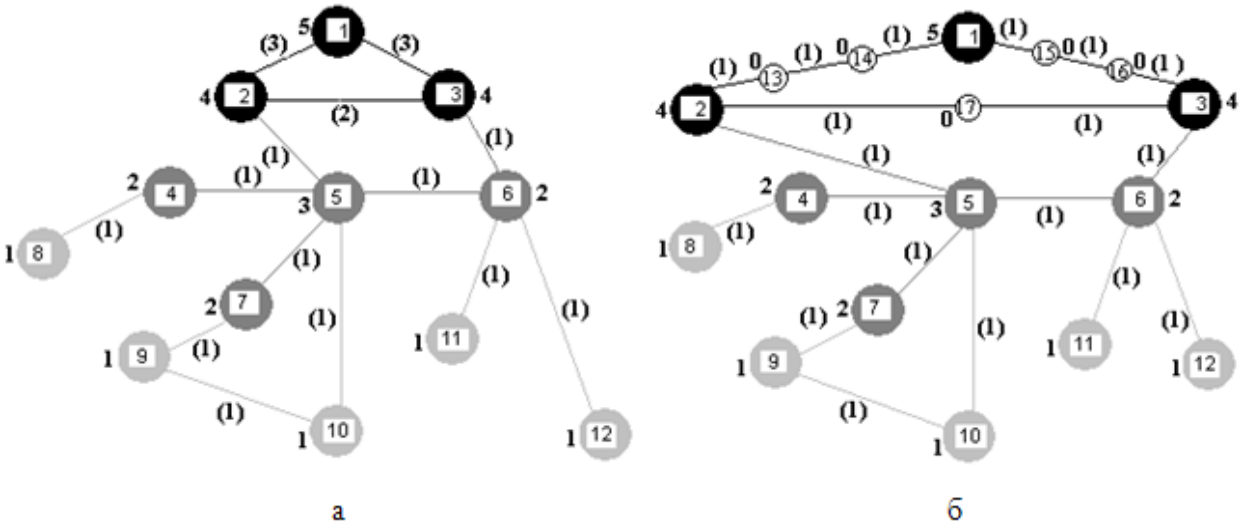


Рис. 13.21. Графова модель противника (порушника): початковий вид (а); вид після перетворення (б)

Перетворимо вхідну графову модель $G(X, E)$ в граф $\overline{G}(\overline{X}, \overline{E})$ наступним чином:

1. Позначимо

$E_d = \{< x, y > \in E \mid l(x, y) \neq 1\}$.

На кожному ребрі $< x, y > \in E_d$ введемо $l(x, y) - 1$ додаткових вершин, що приведе до зникнення ребра $< x, y >$ і появи нових додаткових $l(x, y)$ ребер. Всі введені нові вершини $x_{d_1}, ..., x_{d_p}$ визначать множину X_d, а нові ребра — $\overline{E_d}$. Тоді:

$$X_d \cup X = \overline{X}; \qquad E \setminus E_d \cup \overline{E_d} = \overline{E};$$

2. Для $x_{d_i} \in X_d$, $i = \overline{1,p}$, покладемо $q(x_{d_i}) = 0$. Такий ваговий коефіцієнт приведе до того, що кожна введена вершина ніяк не вплине на рішення задачі (4.53);

3. Для $< x, y > \in \overline{E_d}$ покладемо $l(x, y) = 1$.

Таким чином, усі вагові коефіцієнти ребер у перетвореному графі $\overline{G}(\overline{X}, \overline{E})$ дорівнюють одиниці, кількість ребер зросла незначно. Для прикладу графа-моделі, зображеного на рис. 13.21(а), результат його перетворення $\overline{G}(\overline{X}, \overline{E})$ представлений на рис. 13.21(б).

Для визначення відстаней від довільної обраної вершини $\bar{x} \in \overline{X}$ до будь-якої іншої вершини графа $\overline{G}(\overline{X}, \overline{E})$ побудуємо КСР з коренем у вершині $\bar{x}$ (для $\bar{x} = 1$ структура зображена на рис. 13.22). Очевидно, $d(\bar{x}, \bar{y}), \bar{y} \in \overline{X}$, визначається номером рівня КСР, який містить $\bar{y}$, і у випадку, коли $\bar{x}, \bar{y} \in X$,

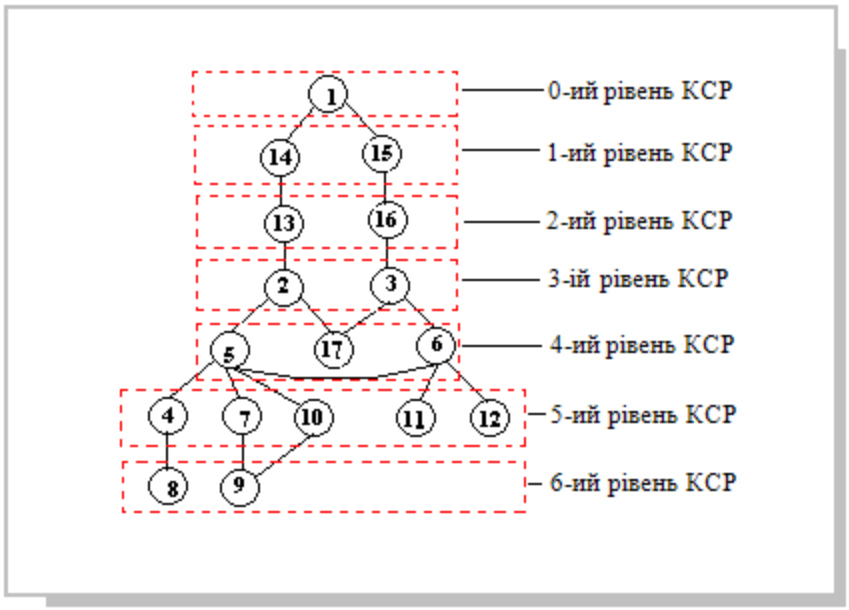


Рис. 13.22. Коренева структура рівнів $\overline{G}(\overline{X}, \overline{E})$ з коренем в вузлі $\bar{x} = 1$

отримаємо, що $d(\bar{x}, \bar{y})$ в графі $\overline{G}(\overline{X}, \overline{E})$ дорівнює відстані між відповідними вершинами в графі $G(X, E)$. Таким чином, обчислювальні витрати для визначення всіх відстаней від заданої вершини $\bar{x}$ до інших вершин графа визначаються кількістю арифметичних операцій для побудови КСР, яка оцінюється як $2\left|\overline{E}\right|$. Тоді сукупні обчислювальні витрати для рішення задачі (13.53) визначаться як $2\left|\overline{E}\right\|\overline{X}\left|\right.$, а завдяки припущенням, які були зроблені вище, складуть $\underline{O}(n^2)$ арифметичних операцій.

Задача про знаходження медіани в просторі R_1^{n-1}

Нехай R_1^{n-1} — нормований простір вимірності $n-1$ над полем дійсних чисел R з нормою

$$\|x\| = \sum_{i=1}^{n-1} \left| x^i \right| \text{ для } \forall x = (x^1, x^2, ..., x^{n-1}) \in R_1^{n-1},$$

а графова модель групи противника (порушника) $G(X,E)$ представляє *дерево* ($|E| = n-1$), до того всі $l(x,y) = 1$. Якщо це не так, вводяться додаткові вершини з нульовими ваговими коефіцієнтами, як запропоновано вище.

Граф $G(X,E)$ відображається в лінійний простір R_1^{n-1} наступним чином. Нехай I^{n-1} — одиничний куб в R_1^{n-1}:

$$I^{n-1} = \{z = (z^1, z^2, ..., z^k, ..., z^{n-1}) \mid 0 \le z^k \le 1,\ k = \overline{1, n-1}\}.$$

Фіксуємо довільну вершину x_1 графа $G(X,E)$. Кожній вершині $x_i \in X$, $i = \overline{1,n}$, ставиться в співвідношення точка $z_i \in R_1^{n-1}$ з координатами

$$z_i = (z_i^1, z_i^2, ..., z_i^k, ..., z_i^{n-1}), i = 1,2,...,n, \qquad (13.55)$$

де z_i^k дорівнює нулю або одиниці залежно від того, входить чи не входить у простий ланцюг $C(x_1, x_i)$ ребро $v_k \in E, k = \overline{1, n-1}$. Якщо x_i і x_j — суміжні вершини графа G, то точки z_i і z_j з'єднуються ребром. У підсумку виходить дерево G' в просторі R_1^{n-1}. З (13.55) витікає, що різним вершинам графа G відповідають різні вершини куба I^{n-1}, до того ж суміжним вершинам графа G відповідають суміжні вершини куба I^{n-1}, кожному ребру $v_k \in E, k = \overline{1, n-1}$ поставлене у відповідність те ребро w_k куба I^{n-1}, кінці якого — образи вершин ребра v_k.

Таким чином, графи G і G' на кубі I^{n-1} — ізоморфні. Кожній вершині z_i графа G' надається та ж вага, що і вершині x_i графа G.

Задача знаходження медіани графа G звелася до задачі про знаходження медіани в просторі R_1^{n-1} множини точок.

Нехай $S = \{z_1, z_2, ..., z_n\}$ — система точок з R_1^m, а

$$q : S \to R^+.$$

Розглянемо функціонал

$$f(z) = \sum_{j=1}^{n} q(z_j) \left\| z - z_j \right\|. \qquad (13.56)$$

Знайдемо множину елементів z_0, які мінімізують (13.56), тобто таких елементів, для яких

$$f(z_0) = \min_z f(z).$$

Нехай $z = (z^1, z^2, ..., z^m)$ — деяка точка простору R_1^m. Розглянемо послідовність різниць $z^i - z_1^i$, $z^i - z_2^i$, …, $z^i - z_n^i$, $i = \overline{1,m}$.

Покладемо для кожного $i = \overline{1,m}$:

$$I_i^+ = \{j \mid z^i - z_j^i > 0\}; \quad I_i^0 = \{j \mid z^i - z_j^i = 0\}; \quad I_i^- = \{j \mid z^i - z_j^i < 0\}.$$

Теорема 13.9. Елемент $z = (z^1, z^2, ..., z^m)$ простору R_1^m буде мінімізувати функціонал (13.56) тоді й тільки тоді, коли для кожного $i = \overline{1,m}$ виконуються умови:

$$\sum_{j \in I_i^+ U I_i^0} q(z_j) \geq \sum_{j \in I_i^-} q(z_j); \qquad \sum_{j \in I_i^+} q(z_j) \leq \sum_{j \in I_i^0 U I_i^-} q(z_j). \tag{13.57}$$

Доведення. Функціонал (13.56) представимо в вигляді

$$f(z) = \sum_{j=1}^{n} q(z_j) \left\| z - z_j \right\| = \sum_{i=1}^{m} \sum_{j=1}^{n} q(z_j) \left| z^i - z_j^i \right| = \sum_{i=1}^{m} f_i(z^i), \tag{13.58}$$

де

$$f_i(z^i) = \sum_{j=1}^{n} q(z_j) \left| z^i - z_j^i \right|. \tag{13.59}$$

Виходячи зі співвідношення (13.58), функціонал (13.56) представляється у вигляді суми невід'ємних функцій $f_i(z^i)$, $i = \overline{1,m}$, однієї змінної z^i, і всі змінні z^i, $i = \overline{1,m}$, є незалежними, а тому мінімум функціонала $f(z)$ буде досягатися при мінімальних значеннях $f_i(z^i)$, $i = \overline{1,m}$, тобто для мінімізації $f(z)$ достатньо мінімізувати кожну з функцій (13.59). Сукупність аргументів, які мінімізують (13.59), визначить координати точки (точок), що мінімізують (13.56): задача оптимізації функції m змінних $z^1, z^2, ..., z^m$ звелась до m задач мінімізації функцій однієї змінної.

Покажемо, що кожна кусково-лінійна функція (13.59) опукла вниз, користуючись для цього визначенням, тобто перевіримо, що для $\forall z^i, \overline{z^i}$, $\forall \lambda: \ 0 < \lambda < 1$ має місце співвідношення:

$$f_i\left(\lambda z^i + (1-\lambda)\overline{z^i}\right) \le \lambda f_i\left(z^i\right) + (1-\lambda) f_i\left(\overline{z^i}\right). \qquad (13.60)$$

Дійсно,

$$f_i\left(\lambda z^i + (1-\lambda)\overline{z^i}\right) = \sum_{j=1}^{n} q(z_j)\left|\lambda z^i + (1-\lambda)\overline{z^i} - z_j^i\right| = \sum_{j=1}^{n} q(z_j)\left|\lambda z^i + (1-\lambda)\overline{z^i} - \lambda z_j^i - (1-\lambda) z_j^i\right| \le$$

$$\le \sum_{j=1}^{n} q(z_j)\left(\left|\lambda z^i - \lambda z_j^i\right| + \left|(1-\lambda)\overline{z^i} - (1-\lambda) z_j^i\right|\right) = \lambda \sum_{j=1}^{n} q(z_j)\left|z^i - z_j^i\right| + (1-\lambda)\sum_{j=1}^{n} q(z_j)\left|\overline{z^i} - z_j^i\right| =$$

$$= \lambda f_i\left(z^i\right) + (1-\lambda) f_i\left(\overline{z^i}\right),$$

що доводить співвідношення (13.60).

З кускової лінійності й опуклості вниз функцій (13.59) випливає, що найменше значення кожна з цих функцій може досягати або в одній точці ${z_0}^i$, яка співпадає з деякою z_j^i, або в нескінченній множині точок, що складають відрізок $\left[z_j^i, z_{j+1}^i\right]$.

Без втрати спільності міркувань будемо вважати, що для даного $i = \overline{1,m}$ має місце $z_1^i \le z_2^i \le \ldots \le z_n^i$ (якщо це не так, то впорядкуємо цю сукупність за зростанням й отримаємо нову нумерацію). Тоді для будь-якого $z_k^i < z^i < z_{k+1}^i$ (при цьому вважаємо $z_0^i = -\infty, z_{n+i}^i = \infty$) маємо:

$$\frac{df_i(z^i)}{dz^i} = \sum_{j=1}^{n} q(z_j)\, sign(z^i - z_j^i) = \sum_{j=1}^{k} q(z_j) - \sum_{j=k+1}^{n} q(z_j). \qquad (13.61)$$

Очевидно, що похідна функції $f_i(z^i),\ i = \overline{1,m},$ не існує в точках $z^i = z_j^i,\ j = \overline{1,n}$, але сама функція $f_i(z^i),\ i = \overline{1,m}$, в цих точках є неперервною. Це означає, що точки $z^i = z_j^i,\ j = \overline{1,n}$, є для $f_i(z^i),\ i = \overline{1,m}$, підозрілими на екстремум. Припустимо, що в деякій ${z_0}^i$, яка співпадає з якоюсь із точок $z_j^i,\ j = \overline{1,n}$, виконуються умови (13.57), тоді при переході через цю точку похідна (13.61) змінить свій знак з мінуса на плюс, а це означає відповідно до першої достатньої умови локального екстремуму функції однієї змінної, що в ${z_0}^i$ функція $f_i(z^i),\ i = \overline{1,m}$, приймає найменше значення.

Вірно і навпаки. Припустимо, що функція $f_i(z^i),\ i = \overline{1,m},$ має мінімальне значення в єдиній точці ${z_0}^i$. Оскільки похідна (13.61) змінить свій знак з мінуса на плюс під час переходу через точку мінімуму, то з рівності (13.61) безпосередньо випливає співвідношення (13.57).

Наслідок 1. Множина точок $z_0{}^i$, які визначають мінімум функції (13.59), складається або з одного елемента сукупності z_j^i, $j=\overline{1,n}$, або з точок відрізка $\left[z_j^i, z_{j+1}^i\right]$.

Наслідок 2. Умови (13.57) еквівалентні наступним умовам:

$$\sum_{j\in I^+\cup I_0} q(z_j) \geq \frac{1}{2}Q; \qquad \sum_{j\in I^+} q(z_j) \leq \frac{1}{2}Q; \tag{13.62}$$

для кожного $i=\overline{1,m}$, де $Q=\sum_{j=1}^{n} q(z_j)$.

Наслідок 3. Якщо для деякої точки z_j виконується

$$q(z_j) > \frac{1}{2}Q,$$

то z_j є єдиною точкою простору R_1^m , в якій функціонал (13.56) досягає найменшого значення.

Наслідок 4. Множина рішень z_0 задачі мінімізації функціонала (13.56) являє собою деякий паралелепіпед P^t простору R_1^m, вимірність якого задовольняє нерівності $0 \leq t \leq m$.

Зауваження 13.20. Розглянута вище задача належить до задач кусково-лінійного програмування, і висновки теореми можуть також бути отримані з критерію оптимальності задач кусково-лінійного програмування.

Зауваження 13.21. З умови (13.57) видно, що положення оптимальної точки $z_0 \in R_1^m$ залежить тільки від чисел $q(z_j)$ і порядку елементів послідовності $z_1^i, z_2^i, ..., z_n^i$ для кожного $i=\overline{1,m}$. Це означає, що мінімум функціонала (13.56) не залежить від метричних співвідношень між елементами $z_1, z_2, ..., z_n$ простору R_1^m.

Деякі з запропонованих авторами даної роботи алгоритмів для рішення задачі про знаходження медіани в просторі R_1^{n-1} множини точок $S=\{z_1, z_2, ..., z_n\}$ представлені на рис. 13.23 - 13.25. Їхній загальний нульовий крок виглядає наступним чином:

Крок 0. Впорядкувати систему чисел $z_1^i, z_2^i, ..., z_n^i$ для кожного $i=\overline{1,m}$, розглянути для даного i сукупність $z_1^i \leq z_2^i \leq ... \leq z_n^i$.

Крок 1. *Якщо*

$n+1 \neq F_k$, де F_k - одне з чисел Фібоначчі,

то

до початкової множини точок $z_1^i, z_2^i, \ldots, z_n^i$ додати необхідне число фіктивних точок з вагами $q(z_j^i) = 0$, щоб у результаті отримати число Фібоначчі

Крок 2. Скоротити інтервал пошуку оптимальної точки z_0^i, користуючись методом Фібоначчі.

Точки $z_{F_{k-1}}^i, z_{n-F_{k-1}}^i$ - нульове й перше наближення відповідно, що співпадають з вхідними дискретними заданими точками.

Крок 3. Перевірити в точках $z_{F_{k-1}}^i, z_{n-F_{k-1}}^i$ умови (4.62), визначити інтервал подальшого пошуку, який також є числом Фібоначчі. Процес пошуку продовжувати доти, поки не будуть виконані умови (4.62).

Рис. 13.23. Алгоритм, заснований на числах Фібоначчі

Зауваження 13.22. Самий трудомісткий для всіх розглянутих алгоритмів знаходження медіани в просторі R_1^m — нульовий загальний крок, що полягає в сортуванні елементів $z_1^i, z_2^i, \ldots, z_n^i$, який і визначає загальну кількість арифметичних операцій, що потребують запропоновані алгоритми. Алгоритми сортування n чисел, засновані на порівнянні елементів, мають обчислювальну складність $\underline{O}(n^2)$ операцій, а кращі з них обмежуються кількістю порівнянь $\underline{O}(n \log_2 n)$. Тоді в сукупності нульовий крок потребує в найкращому разі $\underline{O}(mn \log_2 n)$.

Повернемося до задачі знаходження медіани дерева G, яка вище була зведена до задачі про знаходження медіани в просторі R_1^{n-1} множини точок. За побудовою всі значення $z_1^i, z_2^i, \ldots, z_n^i$ для кожного $i = \overline{1, n-1}$ дорівнюють або нулю, або одиниці. А це означає, що їх упорядкування зведеться до послідовного розміщення всіх нулів, починаючи з першої позиції, а всіх одиниць — починаючи з останньої позиції, що потребує лише $\underline{O}(n)$ операцій порівняння значень $z_l^i, l = \overline{1, n}$, з нулем. Тоді *сукупні обчислювальні витрати нульового кроку, а тому і кожного з запропонованих алгоритмів складуть* $\underline{O}(n^2)$ операцій.

Крок 1. Взяти як початкове наближення $\bar{z} = z^i_{[n/2]}$, $ind = n/2$, $p = 1$.

Крок 2. Перевірити для чергового наближення умови (4.62)

Якщо

обидві умови (4.62) виконані,

то

$z_0^{\,i} = \bar{z}$,

перехід на крок 3;

інакше

якщо

виконана тільки перша умова (4.62)

то

як чергове наближення використовується точка $\bar{z} = z^i_{[ind]}$, де $ind = ind - n/2^{p+1}$. Оптімум знаходиться на сегменті $\left[z^i_{[ind-n/2^{p+1}]}, z^i_{[ind+n/2^{p+1}]}\right]$.

$p = p + 1$. Перехід на крок 2;

інакше

як чергове наближення використовується точка $\bar{z} = z^i_{[ind]}$, де $ind = ind + n/2^{p+1}$. Оптімум знаходиться на сегменті $\left[z^i_{[ind-n/2^{p+1}]}, z^i_{[ind+n/2^{p+1}]}\right]$.

$p = p + 1$. Перехід на крок 2;

Крок 3. Для обчислення всіх рішень перевірити виконання умов (4.62) для сусідніх з $z_0^{\,i}$ точок. Якщо для сусідніх з $z_0^{\,i}$ точок не виконуються умови (4.62), то рішення $z_0^{\,i}$ єдине.

Рис. 13.24. Алгоритм послідовного пошуку

Довільний граф-модель.

Нехай граф-модель противника (порушника) $G(X,E)$ не є деревом, містить довільне число ребер, яке задовольняє співвідношенню (13.54). У цьому випадку обчислювальна складність рішення задачі (13.53) на порядок більша, ніж для графа, що є деревом. При великому розмірі графа ця відмінність стає значною.

Для зменшення кількості арифметичних операцій для рішення задачі (13.53) з довільним зваженим графом $G(X,E)$ пропонується спочатку замінити вхідний граф його мінімальним остовним деревом $G_{0_{\min}}(X,E_{0_{\min}})$. Звичайно, зроблена заміна графової моделі приведе до того, що рішення задачі (13.53) для $G_{0_{\min}}(X,E_{0_{\min}})$ може відрізнятися від рішення тієї ж задачі для $G(X,E)$. Дійсно, розглянемо для прикладу граф і його мінімальне остовне дерево, які зображені на рис. 13.26.

Очевидно відстань $d(2,3)$, яка визначена за допомогою остовного дерева, буде відрізнятися від дійсного значення $d(2,3)$ в поданому графі. Однак, як показує обчислювальний експеримент, значення $\min\limits_{x\in X}\sum\limits_{y\in X} q(y)d(x,y)$ для

$G_{0_{\min}}(X, E_{0_{\min}})$ в більшості випадків незначно відрізняється від $\min\limits_{x \in X} \sum\limits_{y \in X} q(y) d(x, y)$ для графа $G(X, E)$. Тому запропоновані вище методи рішення задачі (13.53) можуть бути використані як евристичні для довільних графових моделей великого розміру після попередньої заміни графа на його мінімальне остовне дерево.

Крок 1. Взяти як початкове наближення $z^i_{[n/2]}$, де $[\bullet]$ - ціла частина аргумента

Крок 2. Перевірити для початкового наближення умови (4.62)

Якщо

обидві умови (4.62) виконані,

то

$z_0{}^i = z^i_{[n/2]}$,

перехід на крок 3;

інакше

якщо

виконана тільки перша умова (4.62)

то

як перше наближення береться точка $z^i_{[n/2-1]}$.

Рішення шукається шляхом послідовного просування вліво від одної точки до іншої, поки друга умова (4.62) не буде виконана. Нехай для цього необхідно k кроків, тоді $z_0{}^i = z^i_{[n/2-k]}$.

Перехід на крок 3;

інакше

як перше наближення береться точка $z^i_{[n/2+1]}$.

Рішення шукається шляхом послідовного просування вправо від одної точки до іншої, поки перша умова (4.62) не буде виконана. Нехай для цього необхідно t кроків, тоді $z_0{}^i = z^i_{[n/2+t]}$.

Перехід на крок 3;

Крок 3. Для обчислення всіх рішень перевірити виконання умов (4.62) для сусідніх з $z_0{}^i$ точок. Можливі випадки нескінченної множини рішень:

$$z^i_{[n/2+t]} \le z^i_0 \le z^i_{[n/2+t+1]} \quad \text{чи} \quad z^i_{[n/2-(k+1)]} \le z^i_0 \le z^i_{[n/2-k]}$$

Рис. 13.25. Алгоритм дихотомії

Обчислювальна складність кожного з таких евристичних методів буде визначатися як

$$T + \underline{O}(n^2),$$

де T — кількість арифметичних операцій для побудови мінімального остовного дерева.

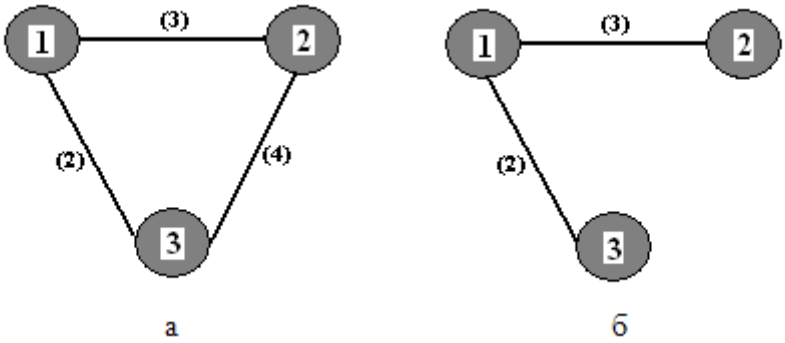


Рис. 13.26. Початковий граф (а); мінімальне остовне дерево (б)

Очевидно, що для мінімізації загальних обчислювальних витрат порядок T не повинен перевищувати двох. Цю вимогу можна забезпечити, використовуючи для побудови мінімального остовного дерева, наприклад, алгоритм найближчого сусіда, обчислювальна складність якого $\underline{O}(n^2)$.

Використання графової математичної моделі групи противника (порушника) дозволяє отримати ефективні з погляду обчислювальних витрат методи для рішення різних задач, пов'язаних з аналізом структури розглянутої групи, а також планування контртерористичних дій, які зводяться до рішення відомих задач на графах.

Розвинутий математичний апарат теорії графів, ефективні чисельні методи їх обробки дозволяють говорити про значні перспективи використання зваженого графа як математичної моделі при подальшому аналізі діяльності й структури різних кримінальних груп.

13.2.2. Метод оцінки стійкості системи кіберзахисту інформації при впливі порушника

Скористаємося графово-матричними моделями противника (порушника) й інформаційно-технологічної системи для розробки методу перевірки стійкості СЗІ до передбачуваної загрози.

Крок 1. Побудова сукупної графово-матричної моделі інформаційно-технологічної системи й противника (порушника).

Спочатку сукупна графова модель представляє із себе об'єднання зважених графів, що відповідають інформаційно-технологічній системі й супротивникові. Матриця суміжності C такої моделі є блочно-діагональною:

$$C = \begin{pmatrix} \overline{G} & 0 \\ 0 & PROT \end{pmatrix}.$$

Наявність нульових блоків природна: поки супротивник ніяк не впливає на СЗІ, зв'язки між $\overline{G}$ і $PROT$ відсутні.

Проведене об'єднання ніяк не відіб'ється на ВЗ матриці $\overline{G}$: спектр блочно-діагональної матриці є об'єднанням власних значень блоків.

Припустимо, що зважений граф, який відповідає гіпотетичній інформаційно-технологічній системі, має вигляд, представлений на рис. 13.27,

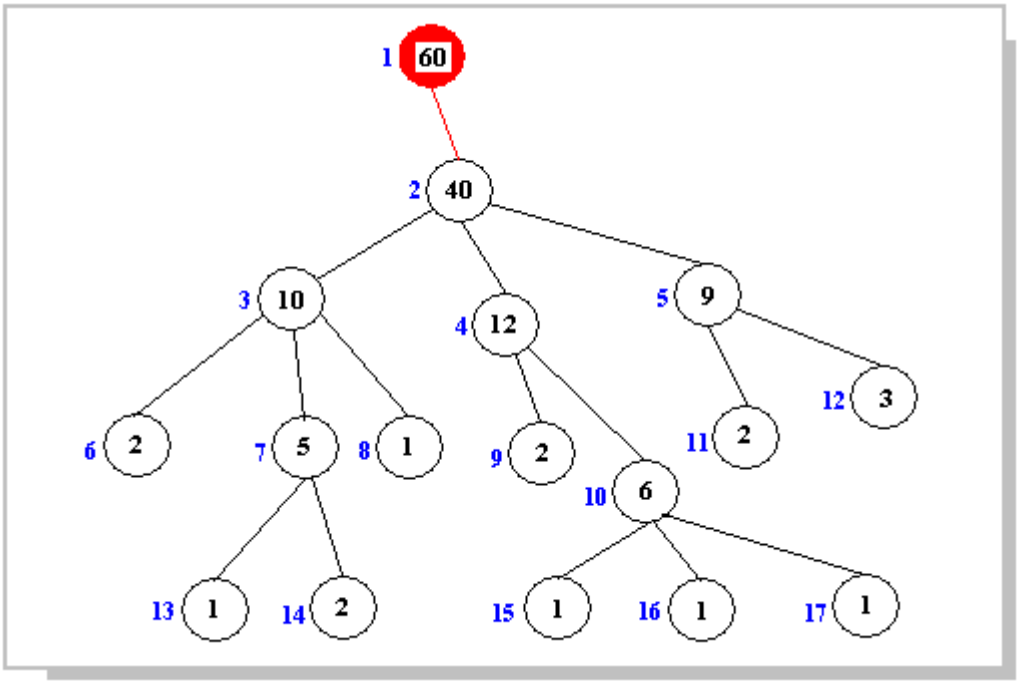


Рис. 13.27. Зважений граф системи

тоді його матриця суміжності $\overline{G}$:

$$\overline{G} = \begin{pmatrix}
60 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 40 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 10 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 12 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 9 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

а граф, що відповідає супротивникові, представлений на рис. 13.16. Спектр матриці C для прикладу, що розглядається, складається з наступних значень (підкресленням виділені ВЗ блоку $PROT$, жирним шрифтом — елементи спектра $\overline{G}$, в збуреннях яких зберігається інформація системи):

-1.8409	-1.3242	-0.0165	0.4503	0.6777	0.7003	0.8809	1.0000	1.0000
1.1226	1.5708	1.7694	1.8405	1.8935	1.8994	2.1513	2.3738	2.8624
3.0678	4.7565	5.1317	5.3367	6.3851	**9.2632**	9.3294	**10.3859**	**12.2301**
39.3298	**60.7725**							

Крок 2. Моделювання атаки противника (порушника).

Раніше моделювання атаки на засіб x_i проводилося за допомогою зменшення (аж до обнуління) вагового коефіцієнта $w(x_i)$ цього засобу (пункти 9.1 – 6, 8). Назвемо цей спосіб *способом А*. Математичним виразом моделювання атаки за допомогою способу А був зсув круга Гершгоріна $\overline{B}(w(x_i),R_i)$, відповідного засобу захисту x_i, на $w(x_i)-w_a(x_i)$ одиниць вліво, де $w_a(x_i)$ — ваговий коефіцієнт вже атакованого засобу x_i. Такий зсув розширював область, що містить спектр матриці суміжності, вліво, приводячи до збурення деяких або всіх елементів спектра в межах нової утримуючої їх області, яка є об'єднанням всіх кругів Гершгоріна. У граничному випадку центр кола Гершгоріна $\overline{B}(w(x_i),R_i)$ неатакованої системи після атаки опинявся в початку координат (рис. 13.28(а)).

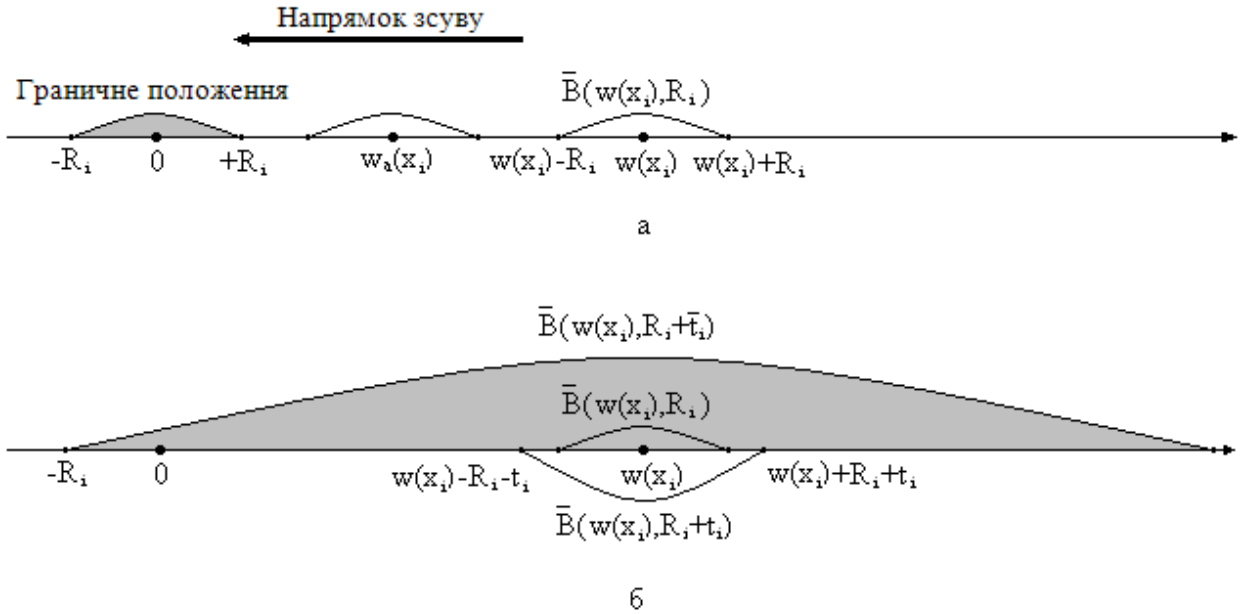


Рис. 13.28. Формальне відображення атаки на інформаційну систему: спосіб А (а); спосіб Б (б)

Розглянемо можливий спосіб моделювання атаки з використанням сукупної моделі інформаційно-технологічної системи й противника (порушника), який назвемо *способом Б*. Припускається, що здійснення впливу противника (порушника) буде спрямовано безпосередньо на засоби захисту (листки в графі системи), і вплив здійснюється членами-виконавцями організації противника (порушника). Спосіб Б моделює атаку, вводячи новий зв'язок між вершиною, відповідною до активного члена-противника (порушника), і тим листком у графі інформаційно-технологічної системи, який відповідає атакованому засобу захисту x_i, що відобразиться у збуренні матриці суміжності сукупного графа. Результатом атаки буде руйнування блочно-діагональної структури C, підсумком якого є матриця $\overline{C}$ (рис. 13.29), і збурення ВЗ, що відповідають блоку $\overline{G}$.

Нехай ваговий коефіцієнт ребра, що з'явилося, — t_i. Математичним виразом моделювання атаки за допомогою способу Б є збільшення радіуса круга Гершгоріна $\overline{B}(w(x_i), R_i)$ на t_i одиниць, що приведе (як і в способі А) до зміни області локалізації ВЗ матриці суміжності графа-моделі системи, а тому до збурення всіх або деяких її ВЗ. Питання: яким повинен бути ваговий коефіцієнт t_i, щоб спосіб Б забезпечив такі ж можливості для збурень ВЗ матриці суміжності графа системи, що й спосіб А, тобто щоб область локалізації ВЗ у способі Б була не меншою, ніж у способі А? Очевидно (рис. 13.28(б)) це гарантовано лише в тому граничному випадку, коли

$$t_i = \bar{t}_i = w(x_i),$$

тобто як ваговий коефіцієнт ребра, що виникає внаслідок атаки, використовується ваговий коефіцієнт атакованого засобу захисту.

Крок 3. Аналіз спектра матриці суміжності атакованої інформаційно-технологічної системи.

Побудуємо нормальне СР матриці суміжності $\overline{C}$, отриманої на кроці 2, і проаналізуємо її спектр. Якщо збурення, які відбулися в ході моделювання атаки, не торкнулися тих ВЗ, у початкових збуреннях яких зберігається інформація системи, то СЗІ є стійкою стосовно передбачуваного противника (порушника). Інакше СЗІ потребує доробки.

Зауваження 13.23. Зміна круга Гершгоріна атакованого засобу відповідно до способу Б моделювання атаки, залишаючи потенційно ті ж можливості для збурень ВЗ матриці суміжності графа інформаційно-технологічної системи за рахунок забезпечення небільшої нижньої межі області локалізації ВЗ, ніж в способі А, реально може допустити більші збурення ВЗ (рис. 13.28), хибно сигналізуючи про нестійкість СЗІ до противника (порушника). Але у випадку

встановлення стійкості способом Б, аналогічний висновок буде отриманий й при використанні способу А, при цьому обчислювальна складність (спосіб Б) буде значно менше, тому що ніяких змін вагового коефіцієнта атакованого засобу тут не потрібно.

Повернемося до розглянутого вище прикладу. ВЗ матриці $\overline{C}$ після передбачуваного впливу противника (порушника) (рис. 13.29) виглядають наступним чином (жирним шрифтом виділені елементи спектра, у яких зберігається інформація системи):

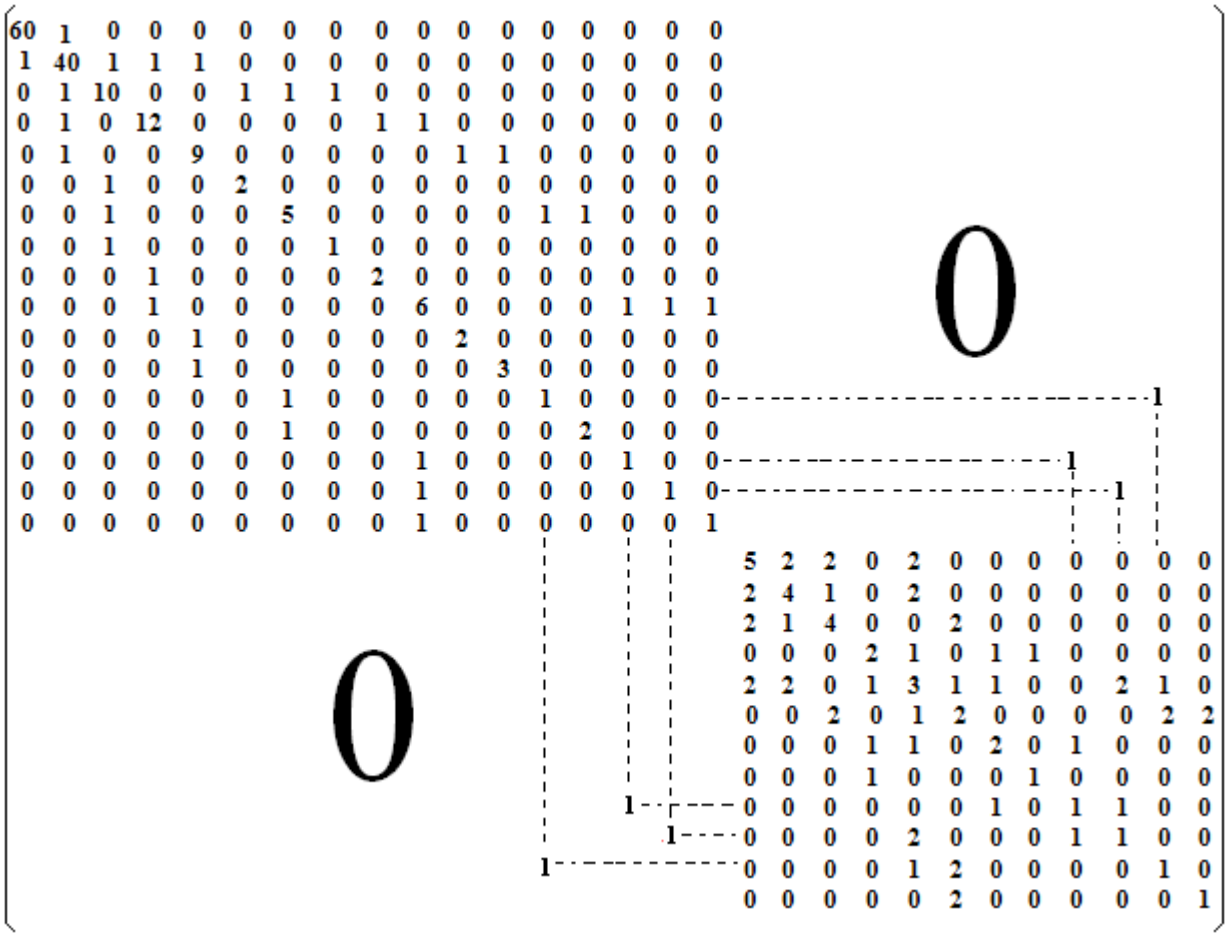


Рис. 13.29. Матрична модель атакованої системи

-1.9718	-1.5802	-0.4296	-0.2436	0.0904	0.7111	0.8657	0.9859
1.0000	1.5870	1.8405	1.8879	1.8977	1.9363	2.2576	2.4310
2.6821	2.8624	3.1409	4.7794	5.1130	5.4336	6.4083	**9.2632**
9.3327	**10.3860**	**12.2302**	**39.3298**	**60.7725**			

ВЗ, початкові збурення яких містять інформацію, не змінилися під впливом атаки. Таким чином, наявна в розпорядженні СЗІ є стійкою стосовно заподіяної атаки.

Зауваження 13.24. Кількість арифметичних операцій, необхідних для отримання відповіді на запитання про стійкість СЗІ до передбачуваного противника (порушника) з використанням запропонованого вище методу, порівнянна з кількістю операцій, затрачуваним на побудову нормального спектрального розкладання матриці суміжності сукупної графової моделі інформаційно-технологічної системи й противника (порушника), тобто виражається як $\underline{O}(N^3)$ (N — загальна кількість вершин у графах системи й противника (порушника)) для щільних матриць при використанні прямих алгоритмів для рішення симетричної проблеми власних значень.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Як атака, що діє на інформаційно-технологічну систему, може вплинути на різні засоби захисту інформації? Чому врахування відмінностей у результатах впливу атаки є важливим під час проектуванні системи захисту інформації?

2. Що необхідно для формалізації врахування відмінностей у результатах впливу атаки на різні засоби захисту інформаційно-технологічної системи?

3. Коли об’єкт $P=\{p_1,...,p_k\},\ p_i\in R,\ i=\overline{1,k}$ називається sign-чутливим (sign-нечутливим)? Навести приклади sign-чутливих (sign-нечутливих) об’єктів.

4. Чим визначається sign-чутливість (sign-нечутливість) об’єкта $P=\{p_1,...,p_k\},\ p_i\in R,\ i=\overline{1,k}$?

5. Як визначається sign-чутливість інформаційної системи?

6. Як пов'язані між собою sign-чутливість інформаційної системи з sign-чутливістю скалярних елементів у складі відповідного їй математичного об'єкта?

7. Достатні умови знакової чутливості векторів $x=(x^1,x^2,...,x^n)^T$, які належать простору R^n.

8. Достатня умова nsign-нечутливості вектора.

9. Який вектор називається n-оптимальним? Яку властивість має такий вектор?

10. Як пов'язані між собою sign- і nsign-чутливість, знакова і «класична» чутливість вектора?

11. Якісна зміна якого математичного параметра, що характеризує інформаційну систему, різна залежно від характеру збурної дії? Відповідь обґрунтувати.

12. Принципи побудови математичного об'єкта виду $P = \{p_1,...,p_k\},\ p_i \in R,\ i = \overline{1,k}$, що відповідає системі захисту інформації.

13. Обґрунтування вибору вимірності простору для побудови геометричної моделі системи захисту інформації.

14. Способи моделювання атак і засобів захисту при побудові геометричної моделі системи захисту інформації.

15. Основні етапи побудови геометричної моделі системи захисту інформації $GM1$, заснованої на знаковій чутливості інформаційної системи.

16. Чим визначаються обчислювальні витрати для моделювання результату атаки на систему захисту інформації при використанні геометричної моделі $GM1$?

17. Як відображаються в наявній геометричній моделі $GM1$, що заснована на знаковій чутливості, зміни в реальній системі захисту інформації?

18. Основні етапи побудови геометричної моделі системи захисту інформації $GM2$, заснованої на нормальній знаковій чутливості.

19. Що є формальним сигналом про руйнування засобу захисту при використанні геометричних моделей $GM2$ і $GM1$ системи захисту інформації?

20. Обчислювальні витрати для моделювання результату атаки на систему захисту інформації при використанні моделі $GM2$.

РОЗДІЛ 14. КЕРУВАННЯ ДОСТУПОМ ДО ІНФОРМАЦІЇ

14.1. Ідентифікація та аутентифікація

Ідентифікацію та аутентифікацію можна вважати основою програмно-технічних засобів кібербезпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб’єктів. Ідентифікація й аутентифікація – це перша лінія оборони, «прохідна» інформаційного простору організації.

Ідентифікація дозволяє суб’єктові (користувачеві, процесу, що діє від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім’я). За допомогою аутентифікації друга сторона переконується, що суб’єкт дійсно той, за кого він себе видає. Як синонім слова «аутентифікація» іноді використовують словосполучення «перевірка дійсності».

Аутентифікація буває однобічною (звичайно клієнт доводить свою дійсність серверу) і двосторонньою (взаємною). Приклад однобічної аутентифікації – процедура входу користувача в систему.

У мережевому середовищі, коли сторони ідентифікації/аутентифікації територіально рознесені, у розглянутого сервісу є два основних аспекти [10,11,12]:

• що слугує аутентифікатором (тобто використовується для підтвердження дійсності суб'єкта);

• як організований (і захищений) обмін даними ідентифікації/аутентифікації.

Суб'єкт може підтвердити свою дійсність, пред'явити принаймні одну з сутностей:

• щось, що він знає (пароль, особистий ідентифікаційний номер, криптографічний ключ і т. п.);

• щось, чим він володіє (особисту картку або інший пристрій аналогічного призначення);

• щось, що є частиною його самого (голос, відбитки пальців і т. п., тобто свої біометричні характеристики).

У відкритому мережевому середовищі між сторонами ідентифікації/аутентифікації не існує перевіреного маршруту; це значить, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманими й використаними для перевірки дійсності. Необхідно забезпечити КЗ від пасивного й активного прослуховування мережі, тобто від перехоплення, зміни й/або відтворення даних. Передача паролів у відкритому вигляді, мабуть, незадовільна; не рятує становище й шифрування паролів, тому що воно не захищає від відтворення. Потрібні більш складні протоколи аутентифікації.

Надійна ідентифікація й аутентифікація ускладнені не тільки через мережеві загрози, але й з цілого ряду причин. По-перше, майже всі аутентифікаційні сутності можна довідатися, украсти або підробити. По-друге, є протиріччя між надійністю аутентифікації, з одного боку, і зручностями користувача й системного адміністратора, з іншого. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити аутентифікаційну інформацію (адже його посаду могла зайняти інша людина), а це не тільки клопітно, але й підвищує ймовірність того, що хтось може підглянути за введенням даних. По-третє, чим надійніший засіб КЗ, тим він дорожчий.

Сучасні засоби ідентифікації/аутентифікації повинні підтримувати концепцію єдиного входу в мережу. Єдиний вхід у мережу – це, у першу чергу, вимога зручності для користувачів. Якщо в корпоративній мережі багато інформаційних сервісів, що допускають незалежний обіг, то багаторазова ідентифікація/аутентифікація стає занадто обтяжливою. На жаль, поки не можна сказати, що єдиний вхід у мережу став нормою.

Таким чином, необхідно шукати компроміс між надійністю, доступністю за ціною й зручністю використання й адміністрування засобів ідентифікації й аутентифікації.

Цікаво відзначити, що сервіс ідентифікації/аутентифікації може стати об'єктом атак на доступність. Якщо система сконфігурована так, що після певної кількості невдалих спроб пристрій введення ідентифікаційної інформації (такий, наприклад, як термінал) блокується, то зловмисник може припинити роботу легального користувача буквально декількома натисканнями клавіш.

14.2. Парольна аутентифікація

Голова перевага парольної аутентифікації – простота й звичність. Паролі давно вбудовані в операційні системи й інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте за сукупністю характеристик їх варто визнати найслабшим засобом перевірки дійсності.

Щоб пароль краще запам'ятався, його найчастіше роблять простим (ім'я подруги, назва спортивної команди й т. п.). Однак простий пароль неважко вгадати, особливо якщо знати пристрасті даного користувача.

Іноді паролі з самого початку не зберігаються в таємниці, тому що мають стандартні значення, зазначені в документації, і далеко не завжди після встановлення системи відбувається їхня зміна.

Уведення пароля можна підглянути. Іноді для підглядання використовуються навіть оптичні прилади.

Паролі нерідко повідомляють колегам, щоб ті могли, наприклад, підмінити на якийсь час власника пароля. Теоретично, в подібних випадках більш правильно залучити засоби керувань доступом, але на практиці так ніхто не робить: а таємниця, яку знають двоє, вже не таємниця.

Пароль можна вгадати «методом грубої сили», використовуючи, скажімо, словник. Якщо файл паролів зашифрований, але доступний для читання, його можна скачати до себе на комп'ютер і спробувати підібрати пароль, запрограмувавши повний перебір (передбачається, що алгоритм шифрування відомий).

Проте важливі заходи дозволяють значно підвищити надійність парольного захисту [13,14]:

- накладення технічних обмежень (пароль повинен бути не занадто коротким, він повинен містити букви, цифри, знаки пунктуації й т. п.);
- керування терміном дії паролів: їхня періодична зміна;
- обмеження доступу до файлу паролів;

• обмеження числа невдалих спроб входу в систему, це утруднить застосування «методу грубої сили»:

• навчання користувачів;

• використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може породжувати тільки благозвучні й, отже, паролі, які добре запам'ятовуються).

Перераховані заходи доцільно застосовувати завжди, навіть якщо поряд з паролями використовуються інші методи аутентифікації.

14.3. Одноразові паролі

Розглянуті вище паролі можна назвати багаторазовими: їхнє розкриття дозволяє зловмисникові діяти від імені легального користувача. Набагато сильнішим засобом, стійким до пасивного втручання до мережі, є одноразові паролі.

Найбільш відомим програмним генератором одноразових паролів є система S/KEY компанії Bellcore. Ідея цієї системи полягає в нижчевикладеному. Нехай є однобічна функція *f* (тобто функція, обчислити обернену до якої за прийнятний час неможливо). Ця функція відома й користувачеві, і серверу аутентифікації. Нехай, далі, є секретний ключ *K*, відомий тільки користувачеві.

На етапі початкового адміністрування користувача функція *f* застосовується до ключа *K n* разів, після чого результат зберігається на сервері. Після цього процедура перевірки дійсності користувача виглядає так [13,14]:

• сервер надсилає на систему користувача число *(n-1)*;

• користувач застосовує функцію до секретного ключа *K (n-1)* разів і відправляє результат по мережі на сервер аутентифікації;

• сервер застосовує функцію *f* до отриманого від користувача значення й порівнює результат з раніше збереженою величиною. У випадку збігу дійсність користувача вважається встановленою, сервер запам'ятовує нове значення (прислане користувачем) і зменшує на одиницю лічильник *(n)*.

Насправді реалізація влаштована дещо складніше (крім лічильника сервер посилає значення, використовуване функцією *f*), але для нас зараз це неважливо. Оскільки функція *f* не обернена, перехоплення пароля, так само як і одержання доступу до сервера аутентифікації, не дозволяють взнати секретний ключ *K* і передбачити наступний одноразовий пароль.

Система S/KEY має статус Internet-стандарту (RFC 1938).

Інший підхід до надійної аутентифікації складається в генерації нового пароля через невеликий проміжок часу (наприклад, кожних 60 секунд), для чого можуть використовуватися програми або спеціальні інтелектуальні карти (з практичної точки зору такі паролі можна вважати одноразовими). Серверу аутентифікації повинен бути відомий алгоритм генерації паролів й асоційовані з ним параметри; крім того, годинники клієнта й сервера повинні бути синхронізовані.

Сервер аутентифікації Kerberos

Kerberos – це програмний продукт, розроблений у середині 1980-х років у Массачусетському технологічному інституті, зазнав з тих часів принципових змін. Клієнтські компоненти Kerberos присутні в більшості сучасних операційних систем.

Kerberos призначений для вирішення такого завдання. Є відкрита (незахищена) мережа, у вузлах якої зосереджені суб'єкти – користувачі, а також клієнтські й серверні програмні системи. Кожен суб'єкт має секретний ключ. Щоб суб'єкт *C* міг довести свою дійсність суб'єктові *S* (без цього *S* не стане обслуговувати *C*), він повинен не тільки назвати себе, але й продемонструвати знання секретного ключа. *C* не може просто надіслати *S* свій секретний ключ, по-перше, тому, що мережа відкрита (доступна для пасивного й активного прослуховування), а, по-друге, тому, що *S* не знає (і не повинен знати) секретний ключ *C*. Потрібен менш прямолінійний спосіб демонстрації знання секретного ключа.

Система Kerberos являє собою довірену третю сторону (тобто сторону, якій довіряють усе), що володіє секретними ключами суб'єктів, яких обслуговують, і допомагає їм у попарній перевірці дійсності.

Щоб за допомогою Kerberos одержати доступ до *S* (звичайно це сервер), *C* (як правило, клієнт) посилає Kerberos запит, що містить відомості про нього (клієнта) і про запитувану послугу. У відповідь Kerberos повертає так званий квиток, зашифрований секретним ключем сервера, і копію частини інформації з квитка, зашифровану секретним ключем клієнта. Клієнт повинен розшифрувати другу порцію даних і переслати її разом з квитком серверу. Сервер, розшифрувавши квиток, може порівняти його вміст із додатковою інформацією, присланою клієнтом. Збіг свідчить про те, що клієнт зміг розшифрувати призначені йому дані (адже вміст квитка нікому, крім сервера й Kerberos, недоступний), тобто продемонстрував знання секретного ключа. Виходить, клієнт – саме той, за кого себе видає. Підкреслимо, що секретні ключі в процесі перевірки дійсності не передавалися по мережі (навіть у зашифрованому вигляді) – вони тільки використовувалися для шифрування. Як організований первинний обмін ключами між Kerberos і суб'єктами і як суб'єкти зберігають свої секретні ключі – питання окреме.

Проілюструємо описану процедуру (рис. 11.1).

Рисунок 11.1. Перевірка сервером *S* дійсності клієнта *C*

- **Клієнт *C* → Kerberos**: c, s,… (клієнт надає Kerberos інформацію про себе і про запитуваний сервіс)
- **Kerberos → клієнт *C*:** (d1) Kc, (Tc.s) Ks (Kerberos повертає квиток, закодований ключем сервера, і додаткову інформацію, закодовану ключем клієнта)
- **Клієнт *C* → сервер *S*:** d2, (Tc.s) Ks (клієнт посилає на сервер квиток і додаткову інформацію). Тут c та s – відомості (наприклад, ім'я), відповідно, про клієнта й сервер, dl та d2 – додаткова (стосовно квитка) інформація, Tc.s – квиток для клієнта *C* на обслуговування в сервера *S*, Кс й Ks – секретні ключі клієнта й сервера, {info}K – інформація info, зашифрована ключем К.

Наведена схема – вкрай спрощена версія реальної процедури перевірки дійсності. Нам же важливо відзначити, що Kerberos не тільки стійкий до мережевих загроз, але й підтримує концепцію єдиного входу в мережу.

14.4. Ідентифікація/аутентифікація за допомогою біометричних даних

Біометрія являє собою сукупність автоматизованих методів ідентифікації й/або аутентифікації людей на основі їх фізіологічних і поведінкових характеристик. До числа фізіологічних характеристик належать особливості відбитків пальців, сітківки й роговиці очей, геометрія руки й особи й т. п. До поведінкових характеристик відносять динаміку підпису (ручний), стиль роботи з клавіатурою. На стику фізіології й поведінки знаходяться аналіз особливостей голосу й розпізнавання мови.

Біометрією в усьому світі займаються дуже давно, однак довгий час усе, що було пов'язане з нею, відрізнялося складністю й дорожнечею. Останнім часом попит на біометричні продукти, в першу чергу у зв'язку з розвитком електронної комерції, постійно й досить інтенсивно зростає. Це зрозуміло, оскільки, з точки зору користувача, набагато зручніше «пред'явити» себе самого, ніж щось запам'ятовувати. Попит породжує пропозицію, тому на ринку з'явилися відносно недорогі апаратно- програмні продукти, орієнтовані, в основному, на розпізнавання відбитків пальців [21,22].

У загальному вигляді робота з біометричними даними організована в такий спосіб. Спочатку створюється й підтримується база даних характеристик потенційних користувачів. Для цього біометричні

характеристики користувача знімаються, обробляються, і результат обробки (названий біометричним шаблоном) заноситься в базу даних (такі вихідні дані, як результат сканування пальця або роговиці, звичайно не зберігаються).

Надалі для ідентифікації (і одночасно аутентифікації) користувача процес зняття й обробки повторюється, після чого виробляється пошук у базі даних шаблонів. У випадку успішного пошуку особистість користувача та її дійсність вважаються встановленими.

Для аутентифікації досить зробити порівняння з одним біометричним шаблоном, обраним на основі попередньо введених даних.

Звичайно біометрію застосовують разом з іншими аутентифікаторами, такими, наприклад, як інтелектуальні карти. Іноді біометрична аутентифікація є лише першим рубежем захисту й слугує для активації інтелектуальних карт, що зберігають криптографічні секрети; у такому випадку біометричний шаблон зберігається на тій же карті.

Активність у сфері біометрії дуже велика. Організовано відповідний консорціум (http://www.biometrics.org). Активно ведуться роботи зі стандартизації різних аспектів технології (формату обміну даними, прикладного програмного інтерфейсу й т. п.), публікується маса рекламних статей, у яких біометрія подається як засіб забезпечення надбезпеки, що став доступним широким масам.

На наш погляд, до біометрії варто ставитися досить обережно. Необхідно враховувати, що вона піддана тим же загрозам, що й інші методи аутентифікації. По-перше, біометричний шаблон порівнюється не з результатом первинної обробки характеристик користувача, а з тим, що прийшов до місця порівняння. А, як відомо, під час маршрутизації багато чого може відбутися. По-друге, біометричні методи не надійніші, ніж база даних шаблонів. По-третє, варто враховувати різницю між застосуванням біометрії на контрольованій території, під пильним оком охорони, і в «польових» умовах, коли, наприклад, до пристрою сканування роговиці можуть піднести муляж і т.п. По-четверте, біометричні дані людини змінюються, так що база шаблонів має потребу в супроводі, що створює певні проблеми і для користувачів, і для адміністраторів.

Але головна небезпека полягає в тому, що будь-яка «пробоїна» для біометрії виявляється фатальною. Паролі, при всій їхній ненадійності, у крайньому випадку, можна змінити. Загублену аутентифікаційну карту можна анулювати й завести нову. Палець же, око або голос змінити не можна. Якщо біометричні дані виявляться скомпрометовані, доведеться, як мінімум, робити істотну модернізацію всієї системи.

14.5. Логічне Керування доступом

Із традиційної точки зору засоби керування доступом дозволяють специфікувати і контролювати дії, які суб'єкти (користувачі й процеси) можуть виконувати над об'єктами (інформацією й іншими комп'ютерними ресурсами). У даному підрозділі мова йде про логічне керування доступом, що, на відміну від фізичного, реалізується програмними засобами. Логічне керування доступом – це основний механізм багатокористувацьких систем, покликаний забезпечити конфіденційність і цілісність об'єктів й, певною мірою, їхню доступність (шляхом заборони обслуговування неавторизованих користувачів) [24,27].

Розглянемо формальну постановку завдання в традиційному трактуванні. Є сукупність суб'єктів і набір об'єктів. Завдання логічного керування доступом полягає в тому, щоб для кожної пари «об'єкт-об'єкт-суб'єкт-об'єкт» визначити безліч припустимих операцій (залежних від деяких додаткових умов) і контролювати виконання встановленого порядку.

Відношення «об'єкт-об'єкт-суб'єкт-об'єкт» можна подати у вигляді матриці доступу, у рядках якої перераховані суб'єкти, у стовпцях – об'єкти, а в клітинках, розташованих на перетині рядків і стовпців, записані додаткові умови (наприклад, час і місце дії) і дозволені види доступу. Фрагмент матриці може виглядати, наприклад, так (табл. 11.1).

Таблиця 11.1. Фрагмент матриці доступу

	Файл	Програма	Лінія зв'язку	Реляційна таблиця
Користувач – 1	orw системної консолі	e	rw з 8:00 до 18:00	
Користувач – 2				a
«o» – означає дозвіл на передачу прав доступу іншим користувачам «r» – читання, «w» – запис, «e» – виконання, «a» – додавання інформації				

Тема логічного керування доступом – одна з найскладніших у сфері інформаційної безпеки. Справа в тому, що саме поняття об'єкта (а тим більше видів доступу) змінюється від сервісу до сервісу. Для операційної системи до об'єктів належать файли, пристрої та процеси. Стосовно файлів і пристроїв звичайно розглядаються права на читання, запис, виконання (для програмних файлів), іноді на видалення й додавання. Окремим правом може бути можливість передачі повноважень доступу іншим суб'єктам (так зване право володіння). Процеси можна створювати й знищувати. Сучасні операційні системи можуть підтримувати й інші об'єкти.

Для систем керування реляційними базами даних об’єкт – це база даних, таблиця, подання, збережена процедура. До таблиць застосовуються операції пошуку, додавання, модифікації й видалення даних, у інших об’єктів інші види доступу.

Розмаїтість об’єктів і застосовуваних до них операцій веде до принципової децентралізації логічного керування доступом. Кожен сервіс повинен сам вирішувати, чи дозволити конкретному суб’єктові ту або іншу операцію. Теоретично це узгоджується з сучасним об’єктно-орієнтованим підходом, на практиці ж призводить до значних труднощів. Головна проблема в тім, що багатьом об’єктам можна одержати доступ за допомогою різних сервісів (можливо, при цьому доведеться перебороти деякі технічні труднощі). Так, до реляційних таблиць можна дістатися не тільки засобами СУКБД, але й шляхом безпосереднього читання файлів або дискових розділів, підтримуваних операційною системою (розібравшись попередньо в структурі зберігання об’єктів бази даних). У результаті при заданні матриці доступу потрібно брати до уваги не тільки принцип розподілу привілеїв для кожного сервісу, але й існуючі зв’язки між сервісами (доводиться піклуватися про узгодженість різних частин матриці). Аналогічні труднощі виникають при експорті/імпорті даних, коли інформація про права доступу, як правило, губиться (оскільки на новому сервісі вона не має сенсу). Отже, обмін даними між різними сервісами становить особливу небезпеку з точки зору керування доступом, а при проектуванні й реалізації різнорідної конфігурації необхідно подбати про погоджений розподіл прав доступу суб’єктів до об’єктів і про мінімізацію числа способів експорту/імпорту даних.

Контроль прав доступу виробляється різними компонентами програмного середовища – ядром операційної системи, сервісами безпеки, системою керування базами даних, програмним забезпеченням проміжного шару (таким, як монітор транзакцій) і т. д. Проте можна виділити загальні критерії, на підставі яких вирішується питання про надання доступу й загальні методи зберігання матриці доступу.

При ухваленні рішення про надання доступу звичайно аналізується така інформація [2,5]:

- ідентифікатор суб’єкта (ідентифікатор користувача, мережева адреса комп’ютера й т. п.). Подібні ідентифікатори є основою довільного (або дискреційного) керування доступом;
- атрибути суб’єкта (мітка безпеки, група користувача й т. п.). Мітки безпеки – основа примусового (мандатного) керування доступом.

Матрицю доступу, через її розрідженість (більшість клітинок – порожні), нерозумно зберігати у вигляді двовимірного масиву. Звичайно її зберігають по стовпцях, тобто для кожного об'єкта підтримується список

«допущених» суб'єктів разом з їхніми правами. Елементами списків можуть бути імена груп і шаблони суб'єктів, що є значною допомогою адміністраторові. Деякі проблеми виникають тільки при видаленні суб'єкта, коли доводиться видаляти його ім'я з усіх списків доступу; втім, ця операція відбувається нечасто.

Списки доступу – винятково гнучкий засіб. З їхньою допомогою легко виконати вимогу про гранулярність прав з точністю до користувача. За допомогою списків нескладно додати права або явно заборонити доступ (наприклад, щоб покарати декількох членів групи користувачів). Безумовно, списки є кращим засобом довільного керування доступом.

Переважна більшість операційних систем і систем керування базами даних реалізує саме довільне керування доступом. Основа перевага довільного керування – гнучкість. Загалом кажучи, для кожної пари «об'єкт-об'єкт-суб'єкт-об'єкт» можна незалежно задавати права доступу (особливо легко це робити, якщо використовуються списки керування доступом). На жаль, у «довільного» підходу є ряд недоліків. Розосередженість керування доступом призводить до того, що довіреними повинні бути багато користувачів, а не тільки системні оператори або адміністратори. Через неуважність або некомпетентність співробітника, що знає секретну інформацію, цю інформацію можуть довідатися і всі інші користувачі. Отже, довільність керування повинна бути доповнена твердим контролем за реалізацією обраної політики безпеки.

Другий недолік, що здається основним, полягає в тому, що права доступу існують окремо від даних. Ніщо не заважає користувачеві, що має доступ до секретної інформації, записати її в доступний всім файл або замінити корисну утиліту її «троянським» аналогом. Подібне «розділення» прав і даних істотно ускладнює проведення декількома системами погодженої політики безпеки й, головне, робить практично неможливим ефективний контроль узгодженості.

Повертаючись до питання подання матриці доступу, вкажемо, що для цього можна використовувати також функціональний спосіб, коли матрицю не зберігають у явному вигляді, а щораз обчислюють вміст відповідних клітинок. Наприклад, при примусовому керуванні доступом застосовується порівняння міток безпеки суб'єкта та об'єкта.

Зручною надбудовою над засобами логічного керування доступом є обмежувальний інтерфейс, коли користувача позбавляють самої можливості спробувати зробити несанкціоновані дії, внести в число видимих йому об'єктів тільки ті, до яких він має доступ. Подібний підхід звичайно реалізують у межах системи меню (користувачеві показують лише

припустимі варіанти вибору) або за допомогою таких обмежувальних оболонок, як restricted shell в ОС Unix.

На закінчення підкреслимо важливість керування доступом не тільки на рівні операційної системи, але й у межах інших сервісів, що входять до складу сучасних додатків, а також, наскільки це можливо, на «стиках» між сервісами. Тут на перший план виходить існування єдиної політики безпеки організації, а також кваліфіковане й погоджене системне адміністрування.

14.6. Рольове керування доступом

При великій кількості користувачів традиційні підсистеми керування доступом стають украй складними для адміністрування. Число зв'язків у них пропорційно добутку кількості користувачів на кількість об'єктів. Необхідні рішення в об'єктно-орієнтованому стилі, здатні ці складнощі понизити.
Таким рішенням є рольове керування доступом (РКД). Суть його в тому, що між користувачами та їхніми привілеями з'являються проміжні сутності – ролі. Для кожного користувача одночасно можуть бути активними кілька ролей, кожна з яких дає йому певні права (рис. 11.2).

Рисунок 11.2. Користувачі, об'єкти й ролі

Рольовий доступ нейтральний стосовно конкретних видів прав і способів їхньої перевірки; його можна розглядати як об'єктно- орієнтований каркас, що полегшує адміністрування, оскільки він дозволяє зробити підсистему розмежування доступу керованою при якій завгодно великій кількості користувачів насамперед за рахунок встановлення між ролями зв'язків, аналогічних успадкуванню в об'єктно-орієнтованих системах. Крім того, ролей повинно бути значно менше, ніж користувачів. У результаті число адміністрованих зв'язків стає пропорційним сумі (а не добутку) кількості користувачів й об'єктів [2,5].

Рольовий доступ розвивається більше 10 років (сама ідея ролей, зрозуміло, є значно старшою) як на рівні операційних систем, так і у рамках СУКБД й інших інформаційних сервісів. Зокрема, існують реалізації рольового доступу для Web-серверів.

У 2001 році Національний інститут стандартів і технологій США запропонував проект стандарту рольового керування доступом, основні положення якого розглянемо.

Рольове керування доступом оперує такими основними поняттями:

- користувач (людина, інтелектуальний автономний агент і т. п.);

- сеанс роботи користувача;
- роль (звичайно визначається відповідно до організаційної структури);
- об’єкт (сутність, доступ до якої розмежовується; наприклад, файл ОС або таблиця СУКБД);
- операція (залежить від об’єкта; для файлів ОС – читання, запис, виконання й т. п.; для таблиць СУКБД – вставляння, видалення й т. п., для прикладних об’єктів операції можуть бути більш складними);
- право доступу (дозвіл виконувати певні операції над певними об’єктами).

Ролям приписуються користувачі й права доступу; можна вважати, що вони (ролі) іменують відносини «багато хто до багатьох» між користувачами й правами. Ролі можуть бути приписані багатьом користувачам; один користувач може бути приписаний декільком ролям. Під час сеансу роботи користувача активізується підмножина ролей, яким він приписаний, у результаті чого він стає власником об’єднання прав, приписаних активним ролям. Одночасно користувач може відкрити кілька сеансів.

Між ролями може бути визначене відношення часткового порядку, так зване успадкуванням. Якщо роль r_2 є спадкоємицею r_1, то всі права r_1 приписуються r_2, а всі користувачі r_2 приписуються r_1. Очевидно, що успадкування ролей відповідає успадкуванню класів в об’єктно-орієнтованому програмуванні, тільки правам доступу відповідають методи класів, а користувачам – об’єкти (екземпляри) класів.

Відношення успадкування є ієрархічним, причому права доступу й користувачі поширюються по рівнях ієрархії назустріч один одному. У загальному випадку успадкування є множинним, тобто в однієї ролі може бути кілька попередниць (і, природно, декілька спадкоємиць, яких ми будемо називати також спадкоємицями).

Можна уявити собі формування ієрархії ролей, починаючи з мінімуму прав (і максимуму користувачів), приписуваних ролі «співробітник», з поступовим уточненням складу користувачів і додаванням прав (ролі «системний адміністратор», «бухгалтер» і т.п.), аж до ролі «керівник» (що, втім, не означає, що керівникові надаються необмежені права; як й іншим ролям, відповідно до принципу мінімізації привілеїв, цій ролі доцільно дозволити тільки те, що необхідно для виконання службових обов’язків). Фрагмент подібної ієрархії ролей показаний на рис. 11.3.

Рисунок 11.3. Фрагмент ієрархії ролей

Для реалізації ще одного згадуваного раніше важливого принципу інформаційної безпеки вводиться поняття поділу обов'язків, причому у двох виглядах: статичному й динамічному.

Статичний поділ обов'язків накладає обмеження на приписування користувачів ролям. У найпростішому випадку членство в деякій ролі забороняє приписування користувача певній сукупності інших ролей. У загальному випадку дане обмеження задається як пара «безліч ролей – число» (де безліч складається, принаймні, з двох ролей, а число повинно бути більшим 1), так що ніякий користувач не може бути приписаний зазначеному (або більшому) числу ролей з заданої кількості.

При наявності успадкування ролей обмеження набуває більш складного вигляду, але суть залишається простою: при перевірці членства в ролях потрібно враховувати приписування користувачів ролям-спадкоємицям.

Динамічний поділ обов'язків відрізняється від статичного тільки тим, що розглядаються ролі, одночасно активні (у різних сеансах) для даного користувача (а не ті, котрим користувач статично приписаний). Наприклад, один користувач може відігравати роль і касира, і контролера, але не одночасно; щоб стати контролером, він повинен спочатку закрити касу. Тим самим реалізується так зване тимчасове обмеження довіри, що є аспектом мінімізації привілеїв.

Розглянутий проект стандарту містить специфікації трьох категорій функцій, необхідних для адміністрування РКД.

- **Адміністративні функції** (створення й супровід ролей та інших атрибутів рольового доступу): створити/видалити роль/користувача, приписати користувача/право ролі або ліквідувати існуючу асоціацію, створити/видалити відношення успадкування між існуючими ролями, створити нову роль і зробити її спадкоємицею/попередницею існуючої ролі, створити/видалити обмеження для статичного/динамічного поділу обов'язків.
- **Допоміжні функції** (обслуговування сеансів роботи користувачів): відкрити сеанс роботи користувача з активацією якого мається на увазі набір ролей; активувати нову роль, деактивувати роль; перевірити правомірність доступу.
- **Інформаційні функції** (одержання відомостей про поточну конфігурацію з урахуванням відносин успадкування). Тут проводиться поділ на обов'язкові й необов'язкові функції. До числа перших належить одержання списку користувачів, приписаних ролі, і списку ролей, яким приписаний користувач.

Усі інші функції віднесені до розряду необов'язкових. Це одержання інформації про права, які приписані ролі, про права заданого користувача (які він має як член певної сукупності), про активні на даний момент сеансу ролі і

права, про операції, які роль/користувач правочинен зробити з заданим об'єктом, про статичний/динамічний розподіл обов'язків.
Можна сподіватися, що запропонований стандарт допоможе сформувати єдину термінологію й, що більш важливо, дозволить оцінювати РУД-продукти з єдиних позицій, за єдиною шкалою.

14.7. Керування доступом в Java-середовищі

Java – це об'єктно-орієнтована система програмування, тому й керування доступом у ній спроектовано й реалізовано в об'єктному стилі. Із цієї причини розглянути Java-середовище для нас дуже важливо.

Насамперед, зупинимося на еволюції моделі безпеки Java. В JDK 1.0 була запропонована концепція «пісочниці» (sandbox) – замкненого середовища, – у якій виконуються потенційно ненадійні програми (апплети, що надійшли по мережі). Програми, що розташовуються на локальному комп'ютері, вважалися абсолютно надійними, і їм було доступно все, що доступно віртуальній Java-машині [6,8].

У число обмежень, що накладаються «пісочницею», входить заборона на доступ до локальної файлової системи, на мережеву взаємодію з усіма хостами, крім джерела апплета, і т. п. Незалежно від рівня безпеки, що досягається при цьому, (а проблеми виникали й з розподілом свій/чужий, і з визначенням джерела апплета), накладені обмеження варто визнати занадто обтяжливими: можливості для змістовних дій в апплетів майже не залишається.

Щоб упоратися з цією проблемою, в JDK 1.1 увели розподіл джерел (точніше, розповсюджувачів) апплетів на надійні та ненадійні (джерело визначалося за електронним підписом). Надійні апплети прирівнювалися в правах до «рідного» коду. Зроблене послаблення вирішило проблеми тих, кому прав не вистачало, але захист залишився неешелонованим й, отже, неповним.

В JDK 1.2 сформувалася модель безпеки, використовувана й в Java 2.

Від моделі «пісочниці» відмовилися. Сформувалися три основні поняття:

- джерело програми;
- право й сукупність;
- політика безпеки.

Джерело програми визначається парою (URL, розповсюджувачі програми). Останні задаються набором цифрових сертифікатів.

Право – це абстрактне поняття, згідно з яким, як і прийнято в об'єктному середовищі, стоять класи й об'єкти. У більшості випадків право визначається двома ланцюжками символів – ім'ям ресурсу й дією.

Наприклад, ресурсом може виступати файл, а дією – читання. Найважливішим методом «правових» об'єктів є implies. Він перевіряє, чи витікає одне право (запитуване) з іншого (наявного).

Політика безпеки задає відповідність між джерелом і правами програм, що надійшли з нього (формально можна вважати, що кожному джерелу відповідає своя «пісочниця»). В JDK 1.2 «рідні» програми не мають яких-небудь привілеїв у плані безпеки, і політика стосовно них може бути будь-якою. У результаті вийшов традиційний для сучасних ОС і СУКБД механізм прав доступу з такими особливостями [10,20]:

- Java-програми виступають не від імені користувача, що їх запустив, а від імені джерела програми. (Це досить глибоке й прогресивне трактування, якщо його правильно розвинути);
- немає поняття власника ресурсів, що міг би змінювати права; останні задаються винятково політикою безпеки (формально можна вважати, що власником усього є той, хто формує політику);
- механізми безпеки забезпечені об'єктною обгорткою.

Досить важливим поняттям у моделі безпеки JDK. 1.2 є контекст виконання. Коли віртуальна Java-машина перевіряє права доступу об'єкта до системного ресурсу, вона розглядає не тільки поточний об'єкт, але й попередні елементи стека викликів. Доступ надається тільки тоді, коли потрібне право мають усі об'єкти в стекові. Розробники Java називають це реалізацією принципу мінімізації привілеїв.

На перший погляд, врахування контексту вважається логічним. Не можна допускати, щоб виклик якого-небудь методу розширював права доступу хоча б з тієї причини, що доступ до системних ресурсів здійснюється не прямо, а за допомогою системних об'єктів, що мають усі права.

На жаль, подібні твердження суперечать одному з основних принципів об'єктного підходу – принципу інкапсуляції. Якщо об'єкт *A* звертається до об'єкта *B*, він не може й не повинен знати, як реалізований *У* і якими ресурсами він користується для своїх цілей. Якщо *A* має право викликати який-небудь метод *У* з певним значенням аргументів, *У* зобов'язаний обслужити виклик. В іншому випадку при формуванні політики безпеки доведеться враховувати можливий перелік викликів об'єктів, що, звичайно ж, нереально.

Розробники Java усвідомлювали цю проблему. Щоб упоратися з нею, вони ввели поняття привілейованого інтервалу програми. При виконанні такого інтервалу контекст ігнорується. Привілейована програма відповідає за себе, не цікавлячись передісторією. Аналогом привілейованих програм є файли з бітами перевстановлення ідентифікатора користувача/групи в ОС Unix, що зайвий раз підтверджує традиційність підходу, реалізованого в

JDK 1.2. Відомі загрози безпеки, які привносять подібні файли. Тепер цей не найкращий засіб ОС Unix перейшов до Java.

Можливий підхід до керування доступом у розподіленому об'єктному середовищі

Вважається, що на сьогодні проблема керування доступом існує в трьох майже не пов'язаних між собою проявах:

- традиційні моделі (дискреційна й мандатна);
- модель «пісочниця» (запланована для Java-середовища й близької їй системі Safe-Tel);
- модель фільтрації (використана в міжмережевих екранах).

На наш погляд, необхідно об'єднати існуючі підходи на основі їхнього розвитку й узагальнення.

Формальна постановка завдання розмежування доступу може виглядати в такий спосіб.

Розглядається сукупність об'єктів (у сенсі об'єктно-орієнтованого програмування). Частина об'єктів може бути контейнерами, що групують об'єкти-компоненти, які задають для них загальний контекст та виконують загальні функції й реалізують перебір компонентів. Контейнери або вкладені один у одного, або не мають загальних компонентів.З кожним об'єктом асоційований набір інтерфейсів, забезпечених дескрипторами (ДЕ). До об'єкта можна звернутися тільки за допомогою ДЕ. Різні інтерфейси можуть надавати різні методи й бути доступними для різних об'єктів.

Кожен контейнер дозволяє опитати набір ДЕ об'єктів-компонентів, що задовольняють деяку умову. Результат, що повертається, у загальному випадку залежить від зухвалого об'єкта.

Об'єкти ізольовані один від одного. Єдиним видом міжоб'єктної взаємодії є виклик методу.

Передбачається, що використовуються надійні засоби аутентифікації й захисту комунікацій. У плані розмежування доступу локальні й вилучені виклики не розрізняються.

Передбачається також, що дозвіл або заборона на доступ не залежать від можливого паралельного виконання методів (синхронізація є окремою проблемою, що тут не розглядається).

Розмежовується доступ до інтерфейсів об'єктів, а також до методів об'єктів (з урахуванням значень фактичних параметрів виклику). Правила розмежування доступу (ПРД) задаються у вигляді предикатів над об'єктами.

Розглядається завдання розмежування доступу для виділеного контейнера СС, компонентами якого повинні бути зухвалий й/або викликуваний об'єкти. ДЕ цього контейнера є загальновідомим. Уважається

також, що між зовнішніми, стосовно виділеного контейнера, об’єктами можливі будь-які виклики.

Виконання ПРД контролюється монітором обігів.

При виклику методу ми будемо розділяти дії, вироблені зухвалим об’єктом (ініціація виклику) і викликуваним методом (прийом і завершення виклику).

При ініціації виклику може вироблятися перетворення ДЕ фактичних параметрів до вигляду, доступного викликуваному методу («трансляція інтерфейсу»). Трансляція може мати місце, якщо викликуваний об’єкт не входить у той же контейнер, що й зухвалий.

Параметри методів можуть бути вхідними й/або вихідними. При прийомі виклику виникає інформаційний потік із вхідних параметрів у викликуваний об’єкт. В момент завершення виклику виникає інформаційний потік з викликуваного об’єкта у вихідні параметри. Ці потоки можуть фігурувати в правилах розмежування доступу.

Структуруємо сукупність всіх ПРД, виділивши чотири групи правил [21,22]:

- політика безпеки контейнера;
- обмеження на викликуваний метод;
- обмеження на зухвалий метод;
- обмеження, що їх накладають добровільно.

Правила, загальні для всіх об’єктів, що входять у контейнер З, назвемо політикою безпеки даного контейнера.

Нехай метод M_1 об’єкта O_1 у точці P_1 свого виконання повинен викликати метод M об’єкта O. Правила, які повинен задовольняти M, можна розділити на чотири підгрупи:

- правила, що описують вимоги до формальних параметрів виклику;
- правила, що описують вимоги до семантики M;
- реалізаційні правила, що накладають обмеження на можливі реалізації M;
- правила, що накладають обмеження на викликуваний об’єкт O.

Метод M об’єкта O, потенційно доступний для виклику, може висувати до зухвалого об’єкта такі групи вимог:

- правила, що описують вимоги до фактичних параметрів виклику;
- правила, що накладають обмеження на зухвалий об’єкт.

Можна виділити три різновиди предикатів, що відповідають семантиці й/або особливостям реалізації методів:

- твердження про фактичні параметри виклику методу M у точці P_1;

- предикат, що описує семантику методу *M*;
- предикат, що описує особливості реалізації методу *M*.

Перераховані обмеження можна назвати добровільними, оскільки вони відповідають реальній поведінці об’єктів і не пов’язані з якими-небудь зовнішніми вимогами.

Запропонована постановка завдання розмежування доступу відповідає сучасному етапу розвитку програмування, вона дозволяє відобразити найскладнішу політику безпеки, знайти баланс між багатством виразних можливостей й ефективністю роботи монітора обігів.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Ідентифікація й аутентифікація. Керування доступом.
2. Що використовується як аутентифікатор в мережевому середовищі?
3. Парольна аутентифікація.
4. Заходи, які дозволяють підвищити надійність парольного захисту.
5. Одноразові паролі.
6. Основні поняття рольового керування доступом.
7. Що собою являє Internet-стандарт (RFC 1938)?
8. Основні поняття керування доступом.
9. Ідентифікація/аутентифікація за допомогою біометричних даних.
10. Керування доступом. Основні поняття.
11. Рольове керування доступом.
12. Які засоби об’єктно-орієнтованого підходу використовує рольове керування доступом?
13. Основні поняття рольового керування доступом.
14. Назвіть категорії функцій, необхідних для адміністрування РКД.
15. Керування доступом в Java-середовищі.
16. Особливості механізму прав доступу.

РОЗДІЛ 15. КЕРУВАННЯ РИЗИКАМИ

15.1. Реалізація підходів до аналізування ризиків

Аналізування ризиків високого рівня

Спочатку необхідно провести початкове аналізування ризику високого рівня, щоб вибрати підхід (основне чи докладне аналізування ризику), що відповідає кожній системі інформаційних технологій. Це аналізування ризику високого рівня розглядає практичну цінність системи інформаційних технологій, оброблену інформацію і ризики з погляду ділової активності організації. Вихідні дані для вирішення щодо вибору відповідного для системи інформаційних технологій підходу можна використовувати такі підстави:

– ділові цілі, що їх досягають за допомогою системи інформаційних технологій;

– рівень залежності ділової активності організації від системи інформаційних технологій, тобто, чи впливає функція, яку розглядає організація, на її виживання або ефективність ділової активності, залежної від цієї системи, чи на конфіденційність, цілісність, доступність, обліковість, достовірність і надійність інформації, оброблюваної цією системою;

– рівень інвестування в цю систему інформаційної технології в умовах розробки, підтримування чи заміни системи;

– активи системи інформаційних технологій, для яких організація безпосередньо надала значення.

Коли ці положення оцінені, рішення прийняти легко. Якщо цілі системи важливі для ділової активності організації, якщо витрати на заміну системи високі чи якщо значення активів мають високі рівні ризику, то необхідне детальне аналізування ризику для системи. Кожна з цих умов може бути достатньою для необхідності детального аналізування ризику.

Загальне правило застосування: якщо відсутність захисту системи інформаційних технологій може спричинити істотну шкоду чи ушкодження в організації, її діловим процесам чи її активам, то необхідне докладне

аналізування ризику для визначання потенційних ризиків. У всіх інших випадках для досягнення відповідного рівня захисту досить застосування основного підходу.

Основний підхід

Мета основного захисту полягає в тому, щоб установити мінімальну кількість засобів захисту і захистити всі чи деякі системи інформаційних технологій організації. Використовуючи цей підхід, можна застосувати основний захист у всій організації, і, як відзначено вище, додатково використовувати докладний аналіз ризику для захисту систем інформаційних технологій з високими рівнями ризику чи систем, вирішальних для справи. Використання основного підходу зменшує капіталовкладення, які організація повинна робити у здійснення аналізу ризику.

Відповідний основний захист можна забезпечити, використовуючи каталоги засобів захисту, які містять перелік засобів захисту для системи інформаційних технологій від найзагальніших загроз. Рівень основного захисту може бути відкоригований відповідно до потреб організації. Докладне оцінювання загроз, вразливостей і ризиків не потрібне. Усе, що треба зробити для здійснення основного захисту, – це вибрати ті частини каталогу засобів захисту, що стосуються розглянутої системи інформаційних технологій. Після визначення засобів захисту уже реалізованих на місці порівнюють із засобами захисту, перерахованими в основному каталозі. Ті, яких немає на місці, повинні бути реалізовані.

Основні каталоги можуть визначити засоби захисту, які потрібно конкретно використовувати, або вони можуть пропонувати перелік необхідних вимог захисту, врахованих в будь-яких засобах захисту, відповідних розглянутій системі. Обидва підходи мають переваги. Одна з цілей основного

підходу – узгодженість засобів захисту по всій організації, якої можна досягти обома підходами.

Кілька уже наявних документів надають перелік основних засобів захисту. Також іноді схожі оточення можна спостерігати серед компаній того самого промислового сектора. Після експертизи основних вимог їх можна використовувати для основних каталогів захисту, які можуть використовувати багато різних організацій. Наприклад, каталоги основних засобів захисту могли б бути отримані від:

– міжнародних і державних організацій зі стандартизації;

– стандартів чи рекомендацій промислового сектора;

– іншої організації, бажано з подібними діловими цілями і відповідного розміру.

Організація може, звичайно, також створити власну основу, установлюючи відповідність із типовим оточенням і **з** діловими цілями.

Докладне аналізування ризику

Докладне аналізування ризику для системи інформаційних технологій містить визначення структури ризиків і оцінку їхніх величин. Необхідність у докладному аналізуванні ризику може бути визначена без зайвих витрат часу і коштів, коли огляди високого рівня проводять для всіх систем, які супроводжуються докладним аналізом ризику тільки високого рівня чи вирішальних систем.

Аналізують ризик визначанням потенційних несприятливих уражень, небажаних подій і ймовірності їхньої появи. Небажані події можуть впливати на ділову активність службовців чи на будь-який цінний об’єкт організації. Несприятливе ураження в результаті небажаного випадку – складова частина

можливих збитків, пов’язаних із значенням активів і їхніх ризиків. Імовірність появи уражень залежить від того, наскільки привабливі активи для потенційного нападника, від імовірності появи загроз і легкості, з якою уразливість можна використати. Результати аналізу ризику приведуть до ідентифікації і вибору засобів захисту, що їх можна використовувати для зменшення визначених ризиків до припустимого рівня.

Докладний аналіз ризику містить глибоку перевірку на кожному із кроків, показаних на рис. 15.1. Цим керуються при виборі перевірених засобів захисту як частини процесу керування ризиком. Необхідні вимоги для цих засобів захисту подані в методиці безпеки системи інформаційних технологій і пов’язані з планом безпеки інформаційної технології. Множина інцидентів і зовнішніх чинників, що можуть впливати на необхідні вимоги захисту системи, може спричинити перегляд усього аналізу ризику чи його частини. Це такі впливи: недавні інциденти, істотні зміни системи, заплановані зміни чи наслідки інцидентів, які потрібно розглядати.

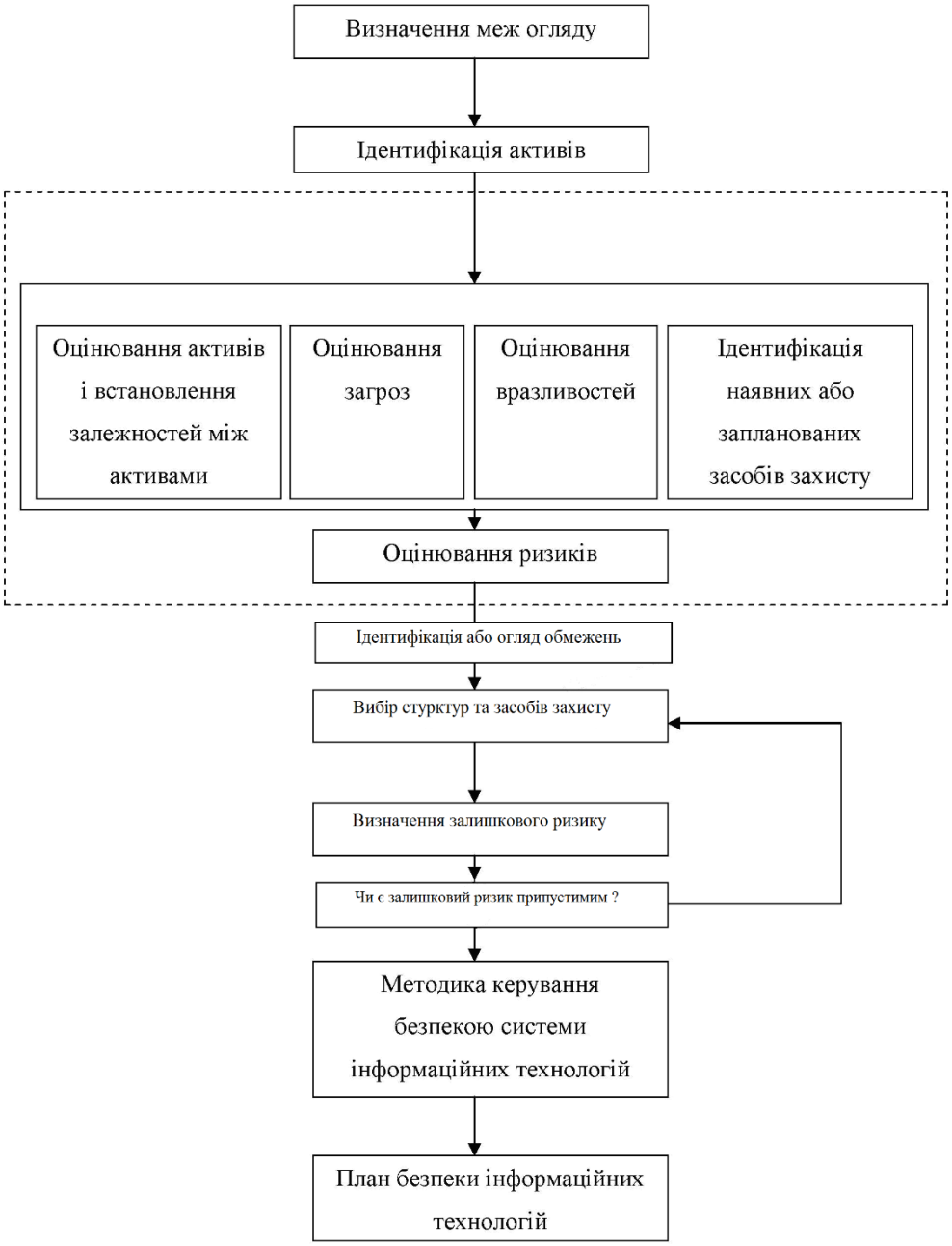


Рис. 15.1. Керування ризиком, з використанням детального аналізу ризику

Існує ряд методів для ефективного аналізування ризику, починаючи від контрольного переліку основних підходів і закінчуючи основними методами структурованого аналізу. Можна використовувати автоматизовані (за допомогою інформаційної системи) чи звичайні базові інструкції. Незалежно

від того, який метод чи інструкцію використовує організація, вони повинні принаймні стосуватися положень, визначених у наступних пропозиціях. Також важливо, щоб методи гармонізували з мікро-політикою організації.

Після завершення детального огляду аналізу ризиків системи результати огляду: активи і їхня значимість, загрози, вразливості і рівні ризиків, а також визначені засоби захисту – повинні бути збережені, наприклад, у базі даних. Очевидно, методи, що використовують засоби програмного забезпечення, здійснюють це набагато простіше. Таке представлення, згадуване іноді як модель, можна використовувати, щоб досягти істотного ефекту, оскільки через якийсь час відбуваються зміни в конфігурації, в оброблюваних типах інформації, у сценаріях загроз тощо. У цьому разі вихідними даними стають тільки самі зміни для визначання впливу на необхідні засоби захисту. Надалі такі моделі можна швидко використовувати для досліджування різних параметрів, обговорювати у процесі розробки нової системи, використовувати для інших подібних систем.

Визначання меж огляду

Як показано на рис. 15.1, перед збором подібної інформації для ідентифікації активів і їхньої оцінки, потрібно визначити межі огляду. Точне визначання меж у цій стадії дає змогу уникнути непотрібної роботи і поліпшити якість аналізування ризику. Кінцевий опис чітко визначить, що з наведеного нижче треба розглядати під час огляду аналізу ризиків для розглянутої системи інформаційних технологій:

– активи інформаційних технологій (наприклад апаратні засоби, програмне забезпечення, інформація);

– люди (наприклад персонал, субпідрядники, інший зовнішній персонал);

– оточення (наприклад будівлі, обладнання);

– діяльність (виконувані роботи).

15.2. Ідентифікація та оцінювання активів

Актив – це компонент або частина всієї системи, для якої організація безпосередньо визначає цінність, і отже, яка потребує захисту. Для ідентифікації активів треба брати до уваги те, що система інформаційних технологій складається не тільки з апаратних засобів і програмного забезпечення. Наприклад, типи активів можуть бути такими:

– інформація (дані) (наприклад файли, що містять фінансові подробиці, інформація про продукцію);

– апаратні засоби (наприклад інформаційна система, друкувальний пристрій);

– програмне забезпечення, в тому числі прикладне (наприклад програми обробки тексту, програми, розроблені для спеціальних цілей);

– апаратура зв’язку (наприклад телефони, мідний кабель, скловолокно);

– програмно-апаратне забезпечення (наприклад гнучкі диски, постійна пам’ять на компакт-диску (CD ROM), програмовані ROM);

– документи (наприклад контракти);

– грошові засоби (кошти) (наприклад у банкоматах);

– вироблені товари;

– служби (наприклад інформаційні служби, обчислювальні ресурси);

– конфіденційність і служби довіри (наприклад служби оплати);

– устаткування оточення;

– персонал;

– імідж організації.

Всі активи у встановлених межах огляду повинні бути визначені і навпаки, будь-які активи, що їх вилучають з меж огляду з будь-якої причини, повинні бути вміщені в інший огляд, для впевненості, що їх не забудуть і не пропустять.

Оцінювання активів і встановлювання залежностей між активами

Після досягнення мети щодо ідентифікації активів, за допомогою огляду всіх активів системи інформаційних технологій, треба визначити цінність активів. Ця цінність відображає важливість активів для діяльності організації. Їх можна виразити в термінах захисту, таких як потенційно небажані порушення ділової активності в результаті розкриття, зміни, недоступності і (або) знищення інформації або інших активів системи інформаційних технологій. Отже, ідентифікація активів і їхня оцінка, заснована на ділових потребах організації, є провідними чинниками при визначанні ризиків.

Вихідними даними для оцінювання активів повинні забезпечувати власники і користувачі активів. Особи(-а), що аналізують ризик, повинні формувати перелік активів. Вони повинні звертатися по допомогу до тих, хто займається плануванням ділової активності, фінансами, інформаційними системами та іншою залежною діяльністю, для того щоб визначити цінність кожного з цих активів. Установлення цінності потрібно пов’язувати з вартістю придбання і підтримування активів і з потенційними ураженнями від втрати конфіденційності, цілісності, доступності, обліковості, достовірності і надійності. Кожен з ідентифікованих активів повинен мати цінність для організації. Проте не завжди є прямий або простий спосіб встановлювання фінансової цінності для всіх параметрів. Також необхідно встановити цінність чи ступінь важливості для не фінансових параметрів, тобто для якісних характеристик, строків у організації. Інакше буде важко визначити рівень захисту і кількість

ресурсів, які організація повинна залучити, щоб захистити активи. Наприклад, для подібних визначень цінності можна використовувати шкалу, де виражають її у градації низько, середньо, високо, чи більш детальну: дуже низько – низько – середньо – високо – дуже високо.

Далі детальніше подані можливі шкали для визначення цінності активів з урахуванням можливих збитків.

Оцінювання активів організації – істотний етап всього процесу аналізування ризику. Значення цінності, визначене активам, повинне бути виражене в поняттях, що стосуються майна і об'єктів, залучених у діловій активності. Для оцінювання активів організація повинна спочатку зробити перелік усіх наявних активів. Щоб забезпечити адекватне оцінювання всіх активів, доцільно згрупувати їх за типами, наприклад, інформаційні активи, програмні активи, фізичні активи і служби. Також корисно визначити власника кожного з активів, що буде відповідати за визначення значень цих активів.

Наступним кроком є вибір і погодження використовуваних шкал і критеріїв специфічних оцінок активів. Оскільки в більшості організацій зазвичай є значне різноманіття активів, швидше за все, цінності деяких активів можуть бути виражені у вартісному значенні і будуть оцінені в національній валюті, в той час як інші, виражені в якісному значенні, можуть бути оцінені діапазоном значень від “дуже низько” до “дуже високо”. Рішення про використовування шкали кількісних оцінок замість шкали якісних оцінок є компетенцією організації і має залежати від оцінюваних активів. Обидва види оцінок можна використовувати до тих самих активів.

Типові градації, використовувані для якісної оцінки активів, такі: незначно, дуже низько, низько, середньо, високо, дуже високо і критично. Вибір і діапазон значень залежить від вимог організації до безпеки, розміру організації й інших чинників, визначених для організації.

Критерії, що використовуються як основа для надання значень для кожного з активів, повинні бути зафіксовані в однозначних термінах. Це зазвичай один з найважчих аспектів оцінювання активів, тому що значення деяких активів, імовірно, доведеться визначити суб'єктивно і швидше за все це буде визначати багато різних осіб. Можливі критерії, використовувані для визначання значень активів, охоплюють вартість їх придбання, заміни чи вартість повторного створення; їхні значення можуть бути абстрактними, наприклад, значення гарного іміджу організації чи її репутації.

Ще однією основою для оцінювання активів є витрати, спричинені втратою конфіденційності, цілісності чи доступності в результаті інциденту. Ця оцінка надає три важливих доповнення значень активів як додаток вартості відшкодування, що оснований на оцінюванні потенційного збитку чи несприятливого зниження ділової активності, що буде випливати з інцидентів захисту з залежною від нього множиною обставин. Треба зазначити, що цей підхід дозволяє врахувати збитки чи інші втрати коштів як необхідну складову формули оцінки ризику.

Багато активів можуть мати декілька наданих значень в процесі оцінювання. Наприклад, план ділової активності може бути оцінений на підставі зусиль, необхідних для розробки плану розвитку, що в свою чергу ґрунтується на зусиллях, пов'язаних з накопичуванням даних, а також на їхньому значенні для конкурентів. Кожна з отриманих оцінок з великою ймовірністю матиме різні значення. Надане значення може бути максимальним серед всіх можливих значень чи може бути сумою деяких чи всіх можливих значень. Остаточний аналіз, що припускає визначання значення чи значень активів, повинний бути чітко детермінованим, тому що надане остаточне значення активів враховують під час визначання ресурсів, що будуть залучені для захисту активів.

Зрештою всі оцінки активів мають бути зведені до спільної основи. Це може бути виконано за допомогою критеріїв. Критерії, що їх можна використовувати для визначання можливих збитків, зумовлюються втратою конфіденційності, цілісності чи доступності активів:

– порушення законів і (або) розпоряджень;

– порушення ділової активності;

– зміна з позитивного на негативний вплив на репутацію;

– порушення, пов’язані з особистою інформацією;

– втрата особистої безпеки;

– несприятливий вплив на законність діяльності;

– порушення комерційної конфіденційності;

– порушення суспільного порядку;

– фінансові втрати;

– збої в діловій активності;

– втрата безпеки стосовно оточення.

Ці критерії – приклади положень, які потрібно враховувати під час оцінювання активів. Для визначення оцінок організація повинна вибрати критерії, що залежать від типу вимог безпеки і ділової активності. Необхідно також враховувати, що деякі з критеріїв, перерахованих вище, можуть не відповідати потребам конкретної організації і можуть бути додані інші, відмінні від них.

Після визначення критеріїв, які необхідно прийняти до уваги, організація повинна погодити шкалу, що буде використовуватися для всієї організації. Перший крок складається з визначення кількості використовуваних рівнів. Немає правил, що дозволяють визначити кількість найбільш прийнятних рівнів. Більша кількість рівнів забезпечує вищий рівень деталізації оцінок, але іноді вищий рівень диференціації ускладнює в цілому сумісну оцінку для організації.

Звичайно, можна використовувати будь-яке число рівнів від трьох (наприклад, “низько”, “середньо” і “високо”), до десяти, якщо воно не суперечить підходу, використовуваному організацією для всього процесу оцінювання ризику.

Також, організація може визначити її власні межі для значень активів, таких як “низько”, “середньо” чи “високо”. Ці межі повинні бути вибрані відповідно до обраних критеріїв, наприклад, можливий фінансовий збиток; вони повинні бути виражені у вартісному значенні, однак під час розгляду втрат особистої безпеки, фінансове значення не буде відповідним. Наостанок, в компетенції організації вирішити, що необхідно розглядати як “низький” чи “високий” збиток: збиток, що може бути великим для малої організації, може бути незначним для дуже великої організації.

Незалежно від використовуваної шкали необхідно оцінювати збитки, можливі в результаті:

– порушення законів і (або) розпоряджень;

– втрати ефективності ділової активності;

– втрати авторитету або негативного впливу на репутацію;

– порушення конфіденційності, пов’язаної з персональною інформацією;

– втрати особистої безпеки;

– несприятливих впливів на законність діяльності;

– порушення комерційної конфіденційності;

– порушення суспільного порядку;

– фінансових втрат;

– порушень бізнесової діяльності;

– впливу небезпечного оточення.

Організація повинна турбуватися про інші критерії, важливі для її ділової активності, що повинні бути додані до вже обраних критеріїв. Організація також повинна визначити власні межі для оцінювання збитків як “низькі” або

“високі”. Наприклад, фінансовий збиток, що міг би бути згубним для малої організації, може спричинити незначні чи часткові втрати для великої організації.

Варто підкреслити на цій стадії, що метод для оцінювання повинен давати не тільки кількісну оцінку, але і якісну оцінку там, де кількісна оцінка неможлива чи недоцільна (наприклад, існує потенційна можливість втрати життєздатності чи репутації організації). Необхідно надавати чіткі обґрунтування обраних критеріїв оцінки.

Також потрібно визначити залежності одних активів від інших, тому що це може впливати на їхню цінність. Наприклад, конфіденційність даних треба зберігати протягом усього процесу обробки, тобто вимоги програми захисту обробки даних повинні залежати безпосередньо від значення, що відображає конфіденційність оброблюваних даних. Якщо бізнес-процес спирається на цілісність певних даних, вироблених програмою, вхідні дані цієї програми повинні забезпечувати відповідну надійність. Крім того, цілісність інформації буде залежати від апаратних засобів і програмного забезпечення, що використовуються для її зберігання та обробки. Також апаратні засоби залежать від електроживлення і, можливо, від кондиціонування повітря. Така інформація щодо залежностей буде допомагати під час ідентифікації залежних загроз і особливо вразливостей. Це також допоможе під час визначення дійсних цінностей активів (прямих залежностей відносин) і, отже, гарантувати відповідний рівень захищеності.

Цінність активів, від яких залежать інші активи, може змінюватися так:

– якщо цінність залежних активів (наприклад дані) нижчі чи дорівнюють цінності розглянутих активів (наприклад програмне забезпечення), цінності залишаються незмінними;

– якщо цінність залежних активів (наприклад дані) вища ніж цінність розглянутих активів (наприклад програмне забезпечення), цінність повинно бути збільшена згідно з:

• рівнем залежності;

• цінністю інших активів.

Організація може мати деякі активи, що повинні бути доступними більше одного разу, такі як копії чи програми інформаційних систем, подібні тим, що їх використовують у більшості організацій. Важливо враховувати цей факт під час оцінювання активів. Ці копії легко доступні, тому, з одного боку, треба потурбуватися про визначення всіх шляхів доступу; з іншого – потрібно шукати шляхи зменшення можливостей доступу.

Кінцевим результатом цього є перелік активів і їхніх цінностей щодо розкриття (забезпечення конфіденційності), зміни (забезпечення цілісності), доступності чи знищення (забезпечення доступності) і вартості відшкодування.

15.3. Оцінювання загроз

Загроза потенційно може нашкодити системі інформаційних технологій і її активам за умов прояву. Якщо загроза трапиться, то це може вплинути на систему інформаційних технологій і викликати небажані інциденти і, відповідно, порушення. Загрози можуть мати природне чи людське походження і можуть бути випадковими чи навмисними. Випадкові і навмисні джерела загроз повинні бути визначені, а імовірність їхньої появи необхідно оцінити. Важливо, щоб ніяка залежна загроза не була пропущена, тому що це може спричинити пошкодження чи ослаблення в системі захисту інформаційної технології.

Вихідні дані для оцінювання загрози треба отримувати від власників активів чи користувачів, від персоналу відділу кадрів, від фахівців із

планування і фахівців інформаційних технологій, і від людей, відповідальних за захист організації.

В розділі 11.3 першого тому наведено детальний перелік типових загроз. Перелік можна використовувати в процесі оцінювання загроз. Загрози можуть бути викликані одним чи кількома навмисними, чи випадковими (природними) подіями. Перелік наводить для кожної такої загрози її тип, де Д (навмисна), А (випадкова), Е (навколишня). Д – використовують для всіх навмисних дій, націлених на активи інформаційної технології, А – використовують для визначання всіх людських дій, що можуть призводити до ушкодження активів ІТ, Е – використовують для всіх інцидентів, що не ґрунтуються на людських діях.

Також доцільно ознайомитись з іншими каталогами загроз (можливо, специфічними для вашої організації чи ділової активності), тому що не можна скласти єдиний вичерпний перелік. Деякі з найзагальніших проявів загроз такі:

– помилки і виправлення;

– обман і злодійство;

– саботаж службовців;

– втрата фізичного та інфраструктурного супроводу:

– навмисний злом, наприклад, несанкціоноване проникнення;

– модифікація коду;

– промислове шпигунство.

У разі використовування каталогів загроз чи більш ранніх оцінювань загроз потрібно знати, що загрози постійно модифікуються, особливо якщо ділове ото-чення чи інформаційні технології змінюються. Наприклад, віруси 90-их значно складніші ніж 80-их. Цікаво, що реалізація засобів захисту, таких як

перевіряння на наявність вірусу, майже завжди веде до розробки нових вірусів, що мають імунітет до поточних засобів захисту. Після визначення джерела загрози (хто і що викликали загрозу) і її спрямованості (тобто на які елементи системи може вплинути загроза), необхідно визначити імовірність виникнення загрози. У цьому випадку потрібно брати до уваги:

– частоту загроз (визначити, як часто вони можуть виникати, спираючись на досвід, статистичні дослідження та інше), якщо статистичні дослідження існують;

– мотивацію, усвідомлені можливості і здатності, ресурси, доступні потенційним нападникам, і привабливі моменти та вразливості активів системи інфор-маційних технологій для потенційного нападника і навмисних джерел загроз;

– географічні чинники, такі як близькість до хімічних чи нафтових заводів, можливість появи критичних метеорологічних умов, і чинники, що можуть впливати на людські помилки і несправність устаткування, випадкові джерела загроз.

Залежно від ступеня точності може виникнути необхідність розбивати активи на складові і установлювати зв’язки загроз із складовими. Наприклад, у фізичних активах можуть спочатку розглядати “центральні сервери даних”, а коли визначено, що ці сервери перебувають у географічно різних місцях, то розглядають окремо “центральний сервер даних 1” і “центральний сервер даних 2”, тому що можуть бути деякі різні загрози і з різними впливами. Так само програмні активи можна спочатку розцінювати як “прикладне програмне забезпечення”, а пізніше розбити на кілька видів “прикладного програмного забезпечення”. Прикладом стосовно активів даних може слугувати початкове визначення як “кримінальне досьє”, а пізніше поділ на “текст кримінального досьє” і “зображення до кримінального досьє”.

У разі завершення оцінювання загроз буде отримано перелік ідентифікованих загроз, активів чи груп активів, на які загрози можуть впливати, і оцінок ймовірностей появи загроз у градації “високо”, “середньо” чи “низько”.

15.4. Оцінювання вразливостей

Ця оцінка містить визначення недоліків у фізичному оточенні, організації, процедурах, персоналі, керуванні, адмініструванні, апаратних засобах, програмному забезпеченні чи апаратурі зв’язку, які можуть використовуватись загрозами для заподіяння шкоди активам і діяльності, яку вони супроводжують. Сама присутність вразливостей не заподіює шкоди, для чого повинна ще існувати загроза, яка використовує цю вразливість. Вразливість, для якої не існує відомих загроз, не вимагає застосування засобів захисту, але вона все-таки повинна бути ідентифікована і контролюватися щодо змін. Треба зазначити, що неправильно реалізовані чи працюючі зі збоями засоби захисту або засоби захисту, що їх використовують неправильно, можуть приховувати в собі вразливості.

Вразливості можуть бути пов’язані з властивостями чи атрибутами активів, які можливо використати у спосіб або з метою, іншими від визначених у момент купівлі чи виготовлення активів. Наприклад, одна з властивостей постійного запам’ятовувача з перезаписуванням – та, що інформація, яка зберігається в ньому, може бути стерта і змінена. Це – один з конструктивних критеріїв постійного запам’ятовування з перезаписом. Проте ця властивість також надає можливість недозволеного знищення інформації на постійному запам’ятовувачі з перезаписуванням. Це може бути вразливістю.

Оцінювання ідентифікує вразливості, що можуть використовуватись загрозами, та оцінює імовірний рівень їхньої недостатності, тобто легкості

використання. Наприклад, деякими активами легко розпоряджатися, їх легко сховати чи транспортувати – ці властивості можуть спричинити вразливості. Вихідні дані для оцінювання вразливості повинні бути отримані від власників активів чи користувачів, від фахівців і експертів з устаткування систем інформаційних технологій по апаратному і програмному забезпеченню. Приклади вразливостей:

– незахищені зв'язки (наприклад Internet);

– непідготовлені користувачі;

– невірний вибір і використовування паролів;

– відсутність відповідного контролю за доступом (логічним і (або) фізичним);

– відсутність резервного копіювання інформації чи програмного забезпечення;

– розташування на ділянках, де можливі повені.

Далі наведено приклади вразливостей в різних зонах захисту, включаючи приклади загроз, що могли б скористатися цими вразливостями. Ці приклади можна використовувати як довідкову інформацію в процесі оцінювання вразливостей. Варто також підкреслити, що в деяких випадках інші загрози також можуть використовувати ці вразливості.

Оточення та інфраструктура:

– відсутність фізичного захисту будівель, дверей і вікон (може використовувати, наприклад, загроза злодійства);

– недостатнє чи недбале використання фізичного контролювання за доступом до будівель, кімнат (може використовувати, наприклад, загроза навмисного пошкодження);

– нестійкість енергосистеми (може використовувати, наприклад, загроза нестабільності енергоживлення);

– розташування в зоні ймовірного затоплення (може використовувати, наприклад, загроза затоплення).

***Апаратні засоби**:*

– відсутність графіка періодичної заміни (може використовувати, наприклад, загроза погіршення носіїв даних);

– чутливість до змін напруги (може використовувати, наприклад, загроза нестабільності енергоживлення);

– чутливість до коливань температури (може використовувати, наприклад, загроза екстремальних значень температури);

– чутливість до вологості, пилу, вогкості (може використовувати, наприклад, загроза запилення);

– чутливість до електромагнітного випромінювання (може використовувати, наприклад, загроза електромагнітного випромінювання);

– недостатній супровід/неправильна інсталяція даних (може використовувати, наприклад, загроза помилки обслуговуючого персоналу);

– відсутність ефективного керування змінами конфігурації (може використовувати, наприклад, загроза помилки експлуатаційного персоналу).

***Програмні засоби**:*

– неповні чи незрозумілі для розробників технічні вимоги (може використовувати, наприклад, загроза програмної помилки);

– відсутність чи недостатність випробовування програмного забезпечення (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженими користувачами);

– складний інтерфейс користувача (може використовувати, наприклад, загроза помилки експлуатаційного персоналу);

– відсутність ідентифікаційних і пізнавальних механізмів, таких як автентифікація користувача (може використовувати, наприклад, загроза нелегального проникнення користувача);

– відсутність контрольних точок (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженим способом);

– відомі “дірки” в програмному забезпеченні (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженими користувачами);

– незахищені таблиці паролів (може використовувати, наприклад, загроза несанкціонованого доступу користувача);

– недостатнє керування паролями (паролі, які легко підібрати, збереження паролів у відкритому вигляді, недостатня частота зміни; може використовувати, наприклад, загроза нелегального проникнення користувача);

– невірний розподіл прав доступу (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженим способом);

– неконтрольоване завантаження і використання програмного забезпечення (може використовувати, наприклад, загроза зловмисної програмної закладки);

– немає механізмів “виходу із системи” у разі від’єднання робочої станції від системи (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженими користувачами);

– відсутність ефективного керування змінами (може використовувати, наприклад, загроза програмної помилки);

– відсутність документації (може використовувати, наприклад, загроза помилки оперативного персоналу);

– відсутність запасних копій (може використовувати, наприклад, загроза зловмисної програмної закладки чи загроза пожежі);

– розповсюджування чи багаторазове використовування носіїв даних без відповідного очищення (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженими користувачами).

Зв'язок:

– незахищені лінії зв'язку (може використовувати, наприклад, загроза підслуховування);

– погані кабельні з'єднання (може використовувати, наприклад, загроза витоку даних із каналів зв'язку);

– відсутність ідентифікації і підтвердження відправника й одержувача (може використовувати, наприклад, загроза нелегального проникнення користувача);

– передавання паролів у відкритому вигляді (може використовувати, наприклад, загроза доступу до мережі не уповноваженими користувачами);

– відсутність підтвердження посилання чи одержання повідомлення (може використовувати, наприклад, загроза невизнання участі);

– вилучений доступ (може використовувати, наприклад, загроза доступу до мережі не уповноваженими користувачами);

– незахищений чутливий потік даних (може використовувати, наприклад, загроза підслуховування);

– недостатнє керування мережею (гнучкість маршрутизації; може використовувати, наприклад, загроза перевантаження трафіка).

– незахищені з’єднання загального використання (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженими користувачами).

Документи:

– збереження в незахищеному вигляді (може використовувати, наприклад, загроза злодійства);

– відсутність обережності у використанні (може використовувати, наприклад, загроза злодійства);

– несанкціоноване копіювання (може використовувати, наприклад, загроза злодійства).

Персонал:

– відсутність персоналу (може використовувати, наприклад, загроза, пов’язана з недостатньою кількістю персоналу);

– неконтрольована зовнішня робота некомпетентним персоналом (може використовувати, наприклад, загроза злодійства);

– недостатнє навчання питанням захисту (може використовувати, наприклад, загроза помилки оперативного персоналу);

– відсутність компетентності в захисті (може використовувати, наприклад, загроза помилок користувача);

– неправильне використання програмного забезпечення і устаткування (може використовувати, наприклад, загроза помилки оперативного персоналу);

– відсутність заходів контролю (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженим способом);

– відсутність методик для правильного використання засобів телекомунікації і пересилання повідомлень (може використовувати, наприклад, загроза використання мережних засобів не уповноваженим шляхом);

– неадекватні процедури прийому на роботу (може використовувати, наприклад, загроза навмисного збитку).

Загальні причини вразливостей:

– окремі місця недоліків (може використовувати, наприклад, загроза недоліків послуг зв'язку);

– неадекватне реагування служб підтримки (може використовувати, наприклад, загроза відмови апаратури).

Можна визначити, наскільки небезпечні вразливості, іншими словами, як легко ними можна скористатися. Вразливість повинна бути оцінена щодо кожної загрози, яка може використовувати вразливість у відповідній ситуації. Наприклад, система може мати вразливість до загроз нелегального проникнення користувача і використовування ресурсів. Вразливість нелегального проникнення користувача може бути високою через відсутність механізмів авторизації користувачів. З іншого боку, вразливість зловживання ресурсами може бути низькою, тому що навіть без механізмів авторизації користувачів, ресурси, якими вони могли б зловживати, обмежені.

Результатом цього кроку повинен бути перелік вразливостей і оцінок легкості їх використовування, наприклад, у градації високо, середньо і низько.

Ідентифікація наявних і (або) запланованих засобів захисту

Засоби захисту, ідентифіковані після огляду аналізування ризику, повинні бути доповненням до вже наявних і запланованих засобів захисту. Важливо, щоб наявні і заплановані засоби захисту були визначені як частина цього

процесу, щоб уникнути непотрібної роботи чи витрат, наприклад, під час дублювання засобів захисту. Може виявитися, що для наявних чи запланованих засобів захисту немає обґрунтувань. У цьому випадку потрібно перевірити, чи засіб захисту потрібно вилучити і замінити іншим, більш підхожим, чи треба лишити його для подальшого виконання своїх функцій (наприклад через вартість).

Крім того, треба виконати перевірку, щоб установити після огляду аналізу ризику, чи сумісні обрані засоби захисту з наявними і запланованими засобами захисту, тобто, що обрані та наявні засоби захисту не суперечать один одному.

Під час визначення наявних засобів захисту треба перевірити, чи правильно вони функціонують. Якщо захисний засіб, на який покладено певну функцію захисту, не функціонує в процесі ділової активності, він є джерелом можливої вразливості.

Результат цього кроку – перелік всіх наявних і запланованих засобів захисту і стан їх впровадження і використовування.

15.5.Оцінювання ризиків

Ризики – функція цінності активів стосовно небезпеки, імовірності загроз, що трапляються і можуть викликати потенційні порушення в діловій активності, легкості використовування вразливості ідентифікованими загрозами, і будь-яких наявних чи запланованих засобів захисту, що можуть зменшувати ризик.

Є різні напрямки встановлення зв’язків цих чинників; наприклад, значення, надані активам, вразливостям і загрозам поєднуються, щоб одержати значення вимірювань ризику.

Аналізування ризиків складається з багатьох стадій, що були обговорені в цій та інших частинах цього підручника. Стадії:

– визначання і оцінювання активів (оцінювання потенційних порушень ділової активності);

– оцінювання загроз;

– оцінювання вразливостей;

– оцінювання наявних або запланованих заходів захисту;

– оцінювання ризиків.

Заключний етап повинен визначити повноту ризиків. Як відзначено раніше, активи, що мають цінність і певний рівень вразливості, перебувають у небезпеці щоразу, коли з'являється загроза. Оцінка ризиків – комбінація потенційних порушень ділової активності, небажаних інцидентів, рівнів оцінених загроз і вразливості. Ризики – вимір впливів, яким можуть бути піддані система і пов'язана з нею організація.

Мета аналізування ризику полягає в тому, щоб визначити і оцінити ризики, яким піддано системи інформаційних технологій та її активи, щоб визначити і вибрати відповідні і вмотивовані заходи захисту. Під час оцінювання ризиків необхідно враховувати деякі положення, включаючи порушення та імовірність.

Порушення може бути оцінено кількома способами, з використанням кіль-кісних, наприклад вартісних, і оцінок якості (може бути засноване на викори-стовуванні ознак таких, як помірковано чи несприятливо), чи комбінації обох. Щоб визначити імовірність прояву загрози, потрібно встановити часовий інтервал, у якому активи будуть мати цінність чи повинні бути захищені. На імовірність прояву загрози впливають такі фактори:

– привабливість активів, особливо коли розглядають навмисну людську загрозу;

– простота перетворення активів на матеріальну винагороду, особливо якщо розглядають навмисну людську загрозу;

– технічні можливості носія загрози, що використовується для навмисної людської загрози;

– імовірність загрози;

– чутливість до вразливостей експлуатації щодо технічних і нетехнічних вразливостей.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. В чому заключається змішаний підхід?
2. Назвіть основні переваги змішаного підходу.
3. Як залежать засоби захисту один від одного?
4. Охарактеризуйте Рис. 15.1. Керування ризиком, з використан-ням детального аналізу ризику.
5. Дайте визначення поняттю активів *системи*
6. Як здійснюється оцінювання загроз?

РОЗДІЛ 16. КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ. ЗАГАЛЬНІ ПОЛОЖЕННЯ

16.1. Політика інформаційної безпеки

Політика інформаційної безпеки – це пакет документів, який описує і регламентує систему управління інформаційною безпекою підприємства.

Метою політики являється впровадження та ефективне управління системою забезпечення інформаційної безпеки, спрямованої на захист інформаційних активів підприємства, забезпечення безперервної діяльності підприємства, мінімізації ризиків інформаційної безпеки.

Основним завданням інформаційної безпеки є захист інформаційних активів підприємства від зовнішніх та внутрішніх навмисних та ненавмисних загроз.

Політика розповсюджується на всі аспекти життєдіяльності підприємства та застосовується до всіх активів підприємства, які можуть впливати на кінцеву продукцію.

Як основні об’єкти області діяльності інформаційної безпеки, розглядаються наступні види активів: інформаційні активи, програмне забезпечення, фізичні активи, сервісні активи. Для кожного активу визначаються можливі ризики та шляхи їх мінімізації.

Політика регламентує управління доступом та паролями, чітке розподілення ролей та обов’язків, визначення вимог безпеки для кожного активу, впровадження політики в інформаційні системи, підтримку рівня безпеки на належному рівні, навчання співробітників інформаційній безпеці, проведення контролю безпеки інформаційних систем, управління інцидентами, класифікацію та забезпечення конфіденційності інформації, антивірусний захист, резервне копіювання, ліцензійну чистоту, вхідний/вихідний контроль комп’ютерної техніки, забезпечення фізичної безпеки, контроль виконання вимог політики та інших аспектів інформаційної безпеки.

Види моделей політики інформаційної безпеки

Формальний вираз політики безпеки називають моделлю політики безпеки. Формальні моделі потрібні, тому що тільки за їх допомогою можна довести існування певного рівня безпеки системи, спираючись на об'єктивні й незаперечні постулати математичної теорії.

Серед моделей ПБ найвідомішими є дискреційна, мандатна та рольова. **Дискреційна політика безпеки.**

Основою дискреційної політики безпеки є дискреційне управління доступом (Discretionary Access Control – DAC), яке визначається двома умовами:

- усі суб'єкти й об'єкти мають бути однозначно ідентифіковані;

- права доступу суб'єкта до об'єкта системи визначаються на основі певних правил зовнішніх відносно системи.

Ця політика одна з найпоширеніших в світі, вона реалізується за допомогою матриці доступу, яка фіксує множину об'єктів та суб'єктів, доступних кожному суб'єкту.

До переваг дискреційної політики безпеки можна віднести достатньо просту реалізацію відповідних механізмів захисту. Однак багатьох проблем захисту ця політика розв'язати не може.

Наведемо найбільш суттєві **недоліки** дискреційної політики безпеки:

1. Вона не витримує атак за допомогою "Троянського коня", це означає, що система захисту, яка реалізує дискреційну політику безпеки, погано захищає від проникнення вірусів у систему та інших способів прихованої руйнівної дії.

2. Вона не має автоматичного визначення прав. Оскільки множина об'єктів безперервно змінюється, то задати заздалегідь вручну перелік прав кожного суб'єкта на доступ до об'єктів неможливо. Тому матриця доступу різними способами агрегується, наприклад, суб'єктами залишаються тільки користувачі, а у відповідну клітину матриці вставляються формули функцій, обчислення яких визначає права доступу суб'єкта, породженого користувачем, до об'єкта.

3. Дискреційна політика безпеки не має контролю поширення прав доступу. Якщо власник файлу передає вміст файлу іншому користувачеві, то той відповідно набуває права власника на цю інформацію. Отже, права можуть поширюватись, і після кількох кроків передача прав може відбутися незалежно від волі першого власника файлу. Побудувати алгоритм перевірки, чи призведуть його дії до порушень безпеки чи ні – неможливо.

Мандатна політика

Основу мандатної (повноважної) політики безпеки (МПБ) становить мандатне управління доступом (Mandatory Access Control – MAC), яке передбачає, що:

- всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;
- у системі визначено лінійно упорядкований набір міток секретності;
- кожному об'єкту системи надано мітку секретності, яка визначає цінність інформації, що міститься в ньому, ─ рівень секретності об'єкта в АС;
- кожному суб'єкту системи надано мітку секретності, яка визначає рівень довіри до нього в АС і називається його рівнем доступу.

Основна мета мандатної політики безпеки ─ запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу. Вона оперує поняттями інформаційного потоку і цінності інформаційних об'єктів. Цінність інформаційних об'єктів (або їх мітки рівня секретності) часто дуже важко визначити, але попарним порівнянням можна встановити впорядкований за цінністю список інформаційних об'єктів. Мандатна політика безпеки у сучасних системах захисту на практиці реалізується мандатним контролем на найнижчому апаратно-програмному рівні.

Пристрій мандатного контролю називають монітором звернень, який порівнює мітки рівня секретності кожного об'єкта з мітками рівня доступу суб'єкта. За результатом порівняння міток приймається рішення про допуск.

Переваги мандатної політики безпеки порівняно з дискреційною політикою безпеки:

1. Мандатна політика безпеки має вищий ступінь надійності, оскільки завдяки їй відстежуються не тільки правила доступу суб'єктів системи до об'єктів, а й стан самої ІС. Таким чином, канали витоку в системах такого типу не закладені первісно (що є в положеннях дискреційної політики безпеки), а можуть виникнути тільки при практичній реалізації систем внаслідок помилок розробника;

2. Правила мандатної політики безпеки ясніші і простіші для розуміння розробниками і користувачами АС;

3. Мандатна політика безпеки стійка до атак типу "Троянський кінь";

4. Мандатна політика безпеки дає можливість точного математичного доведення, що система в заданих умовах підтримує політику безпеки.

Недоліки мандатної політики безпеки:

1. Вона дуже складна для практичної реалізації;

2. Вимагає значних ресурсів КС;

3. Не завжди можна ідентифікувати величезну кількість інформаційних потоків у системі.

Мандатна політика безпеки прийнята всіма розвинутими державами світу. Вона розроблялася, головним чином, для збереження секретності (тобто конфіденційності) інформації у військових організаціях. Питання ж цілісності за її допомогою розв'язуються частково, як побічний результат захисту секретності.

Рольова політика безпеки

Рольова політика безпеки (Role Base Access Control – RBAC) здійснює керування доступом на основі матриці прав доступу для ролей, і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів. Рольова модель є політикою, яка поєднує гнучкість керування доступом (як у дискреційній політиці безпеки) із жорсткістю правил контролю доступу (як у мандатній політиці безпеки).

У дискреційній політиці безпеки поняття "суб'єкт" замінено поняттями "користувач" і "роль".

Користувач ─ це людина, яка працює з системою і виконує певні службові обов'язки.

Роль ─ це діюча в системі абстрактна сутність, з якою пов'язаний набір повноважень необхідний і достатній для здійснення певної діяльності.

Рольова політика безпеки застосовується досить широко, тому що вона є найбільш близькою до реального життя.

Користувачі, що працюють у системі, завжди виконують певні службові обов'язки, тобто виконують деякі ролі, ніяким чином не пов'язані з їх особистістю. Тому цілком логічно призначати повноваження не реальним користувачам, а абстрактним ролям, які представляють учасників певного процесу обробки інформації з певними службовими обов'язками.

При використанні рольової політики безпеки керування доступом здійснюється в дві стадії: по-перше, для кожної ролі вказується набір повноважень, що представляють набір прав доступу до об'єктів, і, по-друге, кожному користувачеві призначається список доступних йому ролей. У моделі рольової політики безпеки визначаються множини:

- множина користувачів;
- множина ролей;
- множина повноважень на доступ до об'єктів;
- множина сеансів роботи користувачів з системою.

Для перелічених множин визначаються відношення, які встановлюють для кожної ролі набір наданих їй повноважень, а також для кожного користувача – набір доступних йому ролей.

З практичної точки зору політику безпеки доцільно розділити на три рівні.

До верхнього рівня відносять рішення, що стосуються підприємства в цілому та приймаються керівництвом підприємства:

- формулювання цілей в області інформаційної безпеки;
- визначення загальних напрямків досягнення цих цілей;
- рішення сформувати чи переглянути комплексну програму забезпечення інформаційної безпеки;

- визначення відповідальних за просування програми у підрозділи підприємства;
- забезпечення бази для дотримання законів і нормативних актів щодо інформаційної безпеки;
- прийняття управлінських рішень з питань реалізації програми безпеки, які стосуються підприємства в цілому.

Для політики верхнього рівня цілі підприємства в області інформаційної безпеки формулюються в термінах цілісності, доступності і конфіденційності. На верхньому рівні вирішуються питання управління захисними ресурсами, координації використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем, підтримка контактів з іншими організаціями, які забезпечують або контролюють режим безпеки.

До політики середнього рівня відносять питання, що стосуються окремих аспектів інформаційної безпеки:

- опис аспекту;
- область застосування (де, коли, як, до чого застосовується дана політика безпеки);
- позиція підприємства по даному аспекту;
- ролі та обов'язки (особи, що відповідають за впровадження політики безпеки в життя);
- відповідальність (загальний опис заборонених дій і покарання за них);
- точка контакту (посадова особа, до якої можна звертатись за додатковим роз'ясненням).

Політика безпеки нижнього рівня стосується конкретних сервісів. Вона включає в себе всього два аспекти - цілі та правила їх досягнення, вона є набагато більш детальною тому її часом важко відокремити від питань реалізації (надання послуг з інформаційного забезпечення). Специфічні питання

окремих сервісів, не можна єдиним чином регламентувати в рамках всієї організації, тому рішення, які належать до них, повинні прийматися на управлінському, а не технічному рівні. Наприклад:

- Хто має право доступу до об'єктів, що підтримуються сервісом?
- За яких умов можна читати і модифікувати дані?
- Як організований вилучений доступ до сервісу?

При формулюванні цілей, політика нижнього рівня може виходити з міркувань цілісності, доступності та конфіденційності, але її цілі мають бути конкретнішими і повинні пов'язувати між собою об'єкти сервісу та важливі щодо інформаційної безпеки дії з ними. З цілей зазвичай виводяться правила безпеки, що описують, хто, що і за яких умов може робити. Чим детальніше правила, чим більш формально вони викладені, тим простіше підтримувати їх виконання програмно-технічними заходами. З іншого боку, занадто жорсткі правила можуть заважати роботі користувачів, і їх доведеться часто переглядати у зв’язку із будь-якими змінами у динамічній інформаційній системі.

Керівництву необхідно знайти розумний компроміс у питанні забезпечення прийнятного рівня безпеки за прийнятну ціну.

На практиці багато організацій, що впровадили особливо твердий контроль безпеки, кожні 6–12 місяців переглядають теоретичні й практичні аспекти політики.

16.2. Програма управління кібербезпекою

Для реалізації політики і стратегії інформаційної безпеки необхідно розробити програму. Програма інформаційної безпеки будь-якої організації або підприємства повинна включати комплекс технічних, технологічних, адміністративних, економічних, соціальних і психологічних заходів.

Програму інформаційної безпеки потрібно структурувати по рівнях відповідно до структури організації. Найчастіше бувають достатніми два рівні –

верхнього та нижнього. Верхній рівень охоплює всю організацію, нижній – стосується окремих інформаційних послуг або груп однорідних сервісів.

Програма верхнього рівня повинна офіційно затверджуватись і підтримуватись керівництвом організації, мати певний штат і бюджет. Її очолює особа, відповідальна за інформаційну безпеку організації. Головними цілями програми верхнього рівня є наступні:

- керування ризиками, їх оцінка, вибір ефективних засобів захисту;
- координація діяльності в області інформаційної безпеки, поповнення і розподіл ресурсів;
- стратегічне планування;
- контроль діяльності в області інформаційної безпеки.

У рамках програми верхнього рівня приймаються стратегічні рішення щодо забезпечення безпеки, оцінюються нові технологічні рішення з метою їх подальшого впровадження.

Контроль діяльності в області безпеки передбачає два напрямки. Перший – перевірка дій із захисту інформації на відповідність законам, а також контакти із зовнішніми контролюючими організаціями. Другий – постійне відстеження стану безпеки всередині організації, реагування на випадки порушень, доопрацювання захисних заходів у разі потреби.

За програму нижнього рівня відповідають адміністратори сервісів. Програмою нижнього рівня передбачається забезпечення надійного та економічного захисту конкретного сервісу або групи однорідних сервісів. На цьому рівні вирішується, які механізми захисту доцільно використовувати, які необхідно закупити та встановити технічні засоби, як здійснювати повсякденне адміністрування, виявляти слабкі місця.

Програму нижнього рівня необхідно синхронізувати з життєвим циклом захищуваного сервісу, оскільки краще заздалегідь передбачити необхідні зміни у сервісі та зробити відповідні заходи в системі інформаційної безпеки.

У життєвому циклі інформаційного сервісу можна виділити наступні етапи:

- ініціація – виявляється необхідність у придбанні нового сервісу, документально фіксується передбачуване призначення;
- закупівля – складаються специфікації щодо сервісу, аналізуються варіанти придбання, виконується придбання;
- установка – сервіс встановлюється, конфігурується, тестується окремо і в системі, вводиться в експлуатацію;
- експлуатація – сервіс працює, адмініструється, модифікується;
- виведення з експлуатації – відбувається перехід на новий сервіс.

На етапі ініціалізації формується розуміння того, що необхідно придбати новий або модернізувати існуючий сервіс; якщо модернізація, то своїми силами чи запрошувати сторонніх спеціалістів; якими характеристиками і функціями він повинен володіти; які існують фінансові та інші обмеження. Зі сторони безпеки найважливіше оцінити критичність самого сервісу та інформації, яку він буде обробляти. Отже треба відповісти на такі питання:

- Якого роду інформація буде обслуговуватись новим сервісом?
- Які можливі наслідки порушення конфіденційності, цілісності та доступності цієї інформації?
- Які загрози, стосовно яких сервіс та інформація будуть найбільш уразливими?
- Чи є які-небудь особливості нового сервісу, що вимагають прийняття спеціальних процедурних заходів?
- Які характеристики персоналу мають відношення до безпеки?

- Яким законодавчим положенням і внутрішнім правилам повинен відповідати новий сервіс?

За результатами оцінки критичності складаються специфікації нового сервісу.

На етапі закупівлі остаточно формулюються вимоги до захисних засобів нового сервісу, до компанії-постачальника, до кваліфікації персоналу, що буде використовувати або обслуговувати закуплений продукт, до сумісності нового сервісу з існуючою конфігурацією, до документації, обслуговування, навчання персоналу.

На етапі установки необхідно виконати конфігурування нового продукту. Як правило, комерційні продукти постачаються з вимкненими засобами безпеки, їх необхідно увімкнути і налаштувати, що є достатньо відповідальною справою. Далі підключають процедурні регулятори: підготовка документів, що регламентують використання сервісу, приміщення та його охорону, планів дій на випадок екстрених ситуацій, організація навчання користувачів тощо. Після цього необхідно провести тестування, повнота і комплексність якого може бути гарантією безпеки експлуатації в штатному режимі.

На етапі експлуатації найбільшу небезпеку становлять незначні зміни в конфігурації сервісу, оскільки їх наслідки важко відслідковувати, користувачі та адміністратори психологічно не готові змінювати свою поведінку і відношення до оновлених сервісів. Якщо безпеку не підтримувати, вона деградує: користувачі не дотримуються суворо посадових інструкцій, адміністратори менш ретельно аналізують реєстраційну інформацію, непродумано роздаються додаткові привілеї.

Для боротьби з ефектом повільних змін необхідно включати до програми інформаційної безпеки періодичні аудиторські перевірки сервісу безпеки. Коли ж у системі відбуваються значні модифікації, то аудиторські перевірки є обов’язковими.

На етапі виведення сервісу з експлуатації дані переносять на іншу систему, архівують, викидають або знищують. При архівуванні даних для їх подальшого використання необхідно передбачити апаратно-програмну сумісність засобів зчитування й запису, а також, за необхідністю, перезапис на нові носії, з урахуванням вимог конфіденційності. В разі архівування інформації у зашифрованому вигляді необхідно зберегти ключ і засоби дешифрування.

Для підвищення рівня інформаційної безпеки доцільно розбити технологічний процес на ряд самостійних етапів, щоб службовці знали тільки частину конфіденційної інформації, а повною інформацією володіло лише керівництво або вузьке коло осіб. Необхідно створити систему внутрішньофірмової комунікації, що не допускає повної автономності окремих працівників.

16.3. Основні заходів процедурного рівня

Процедурні заходи безпеки орієнтовані на людей, а не на технічні засоби. Саме люди формують режим інформаційної безпеки, вони ж є головною загрозою, тому "людський чинник" заслуговує на особливу увагу.

Виходячи з накопиченого досвіду, компанії повинні з’ясувати степінь залежності від комп’ютерної обробки даних, а суспільство повинне знати не тільки переваги, але й небезпеки, пов’язані з використанням інформаційних технологій.

На **процедурному рівні** можна виділити наступні класи заходів:

- керування персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відновлюваних робіт.

Керування **персоналом** починається зі складання опису посади, приймання на роботу. На цьому етапі бажано підключити спеціаліста з інформаційної безпеки для визначення обов'язків та комп'ютерних привілеїв, асоційованих з посадою. Необхідно дотримуватись таких принципів:

- розподіл обов'язків;
- мінімізація привілеїв.

Принцип розподілу обов'язків визначає, як розподіляти ролі та відповідальність, щоб одна людина не могла порушити критично важливий для організації процес. Наприклад, процедурні обмеження дій суперкористувача: можна штучно розщепити пароль суперкористувача, повідомивши першу його частину одному співробітнику, а другу – іншому. Тоді критично важливі дії з адміністрування ІС вони зможуть виконати тільки удвох, що зменшує ймовірність помилок і зловживань.

За принципом мінімізації привілеїв виділяють користувачам тільки ті права доступу, які необхідні їм для виконання службових обов'язків, щоб зменшити втрати від випадкових або навмисних некоректних дій. Попередній опис посади дозволяє оцінити її критичність і визначити процедуру перевірки та відбору кандидатів. Чим більш відповідальна посада, тим більш ретельною повинна бути перевірка кандидата.

Коли кандидата визначено, його необхідно ознайомити із службовими обов'язками, з нормами і процедурами інформаційної безпеки, завести його системний рахунок із вхідним ім'ям, паролем і привілеями. Після цього розпочинається його адміністрування, а також протоколювання і аналіз дій користувача в умовах постійної зміни середовища, в якому він працює, службових обов'язків тощо. Все це потребує відповідної зміни привілеїв. Технічну складність викликають тимчасові переміщення користувача, виконання його обов'язків замість співробітника, що пішов у відпустку, коли

повноваження треба надати тимчасово. В такі періоди профіль активності користувача змінюється, що заважає виявляти підозрілі ситуації.

Ліквідація системного рахунку, особливо у випадку конфлікту між співробітником і організацією, необхідно проводити максимально оперативно з обмеженням фізичного доступу до робочого місця.

При адмініструванні осіб, що працюють за контрактом, використовується той самий принцип мінімізації привілеїв, за яким надається стільки прав, скільки необхідно, на термін контракту.

Додаткові вразливі місця виникають у випадках, коли на обслуговування і адміністрування важливих компонент комп'ютерної системи беруть зовнішні організації або адміністрування виконується у віддаленому режимі. Їх необхідно компенсувати посиленим контролем засобів віддаленого доступу або навчанням власних співробітників.

Фізичний захист повинен бути безперервним у часі та просторі. Безпека інформаційної системи залежить від прийнятих заходів захисту будівель, території, інфраструктури, обчислювальної техніки, носіїв даних.

Основні напрямки **фізичного захисту**:

- фізичне керування доступом;
- протипожежні заходи;
- захист підтримуючої інфраструктури;
- захист від перехоплення даних;
- захист мобільних систем.

Фізичне керування доступом дозволяє контролювати та, за необхідністю, обмежити вхід і вихід співробітників і відвідувачів.

При проєктуванні та реалізації заходів фізичного керування доступом доцільно застосовував об'єктний підхід. По-перше, визначають периметр

безпеки, визначають зовнішній інтерфейс організації – порядок входу/виходу штатних співробітників і відвідувачів, внесення/винесення техніки.

По-друге, виконується декомпозиція контрольованої території на окремі об’єкти і зв’язки між ними, виокремлюються найбільш критичні з позиції безпеки, щоб забезпечити їм підвищений захист, щоб відвідувачі не мали безпосереднього доступу до комп’ютерів і приміщень, які захищаються, щоб їх можна було відрізняти від співробітників.

Засоби фізичного захисту бажано максимально автоматизувати.

Також необхідно встановити протипожежну сигналізацію та автоматичні засоби гасіння пожеж.

До підтримуючої інфраструктури (системи електро-, водо- і теплопостачання, кондиціонери і засоби комунікацій) застосовуються ті ж вимоги цілісності та доступності, що і до інформаційних система. Для забезпечення цілісності необхідно захищати устаткування від крадіжок і пошкоджень. Для підтримки доступності необхідно обрати устаткування з максимальним часом напрацювання на відмову, дублювати відповідальні вузли та завжди мати запасні частини.

Для захищення від перехоплення даних з монітору, з пакетів, що передаються мережею, від аналізу побічних електромагнітних випромінювань необхідно максимально розширити контрольовану територію, захищати лінії зв’язку.

Не можна залишати без нагляду мобільні та портативні комп’ютери, бажано шифрувати дані на жорстких дисках таких комп’ютерів, а також регулярно копіювати великі бази даних

Обираючи засоби фізичного захисту обов’язково виконувати аналіз ризиків.

Для **підтримки працездатності** інформаційних систем необхідно повсякденно виконувати рутинні заходи, оскільки ненавмисні помилки

системних адміністраторів і користувачів загрожують зіпсування апаратури, руйнуванням програм і даних.

Можна виділити наступні напрямки повсякденної діяльності:

- підтримка користувачів;
- підтримка програмного забезпечення;
- конфігураційне керування;
- резервне копіювання;
- управління носіями;
- документування;
- регламентні роботи.

Підтримка користувачів це консультування та надання допомоги при вирішенні різних проблем. Найчастіше в організаціях ці функції виконує системний адміністратор. Дуже важливо вчасно вирішувати проблеми, пов'язані з інформаційною безпекою. Доцільно фіксувати питання користувачів, щоб виявляти типові помилки і включити рекомендації для виходу з поширених ситуацій до спеціальних пам'яток.

Підтримка програмного забезпечення – найважливіший засіб забезпечення цілісності інформації. Щоб попередити зараження вірусами, не можна дозволяти користувачам самостійно встановлювати чи змінювати програми на свій розсуд. Треба постійно підтримувати еталонні копії програмних систем, а також тестувати робочі версії програм.

Конфігураційне керування дозволяє контролювати і фіксувати зміни у програмній конфігурації. Вони повинні бути продуманими і дозволяти у разі потреби повернутись до попередньої працюючої версії. Фіксування змін дозволить легко відновити поточну версію після аварії. Зменшенню помилок у рутинній роботі сприяє максимальна її автоматизація.

Резервне копіювання необхідне для відновлення програм і даних після аварій. Копії необхідно зберігати на території організації та поза нею у безпечному місці, захищеному від несанкціонованого доступу та аварійних ситуацій.

Керувати носіями необхідно для забезпечення фізичного захисту і обліку дисків, стрічок, друкованих документів тощо. Управління носіями дозволить забезпечити конфіденційність, цілісність і доступність інформації, що зберігаються поза комп'ютерними системами. Управління носіями повинне охоплювати весь життєвий цикл - від закупівлі до виведення з експлуатації.

Документування – невід'ємна частина інформаційної безпеки. У вигляді документів оформлюються майже все – від політики безпеки до журналу обліку носіїв.

До збереження документів застосовні вимоги забезпечення конфіденційності, цілісності та доступності.

Регламентні роботи – дуже серйозна загроза безпеці, оскільки співробітник, задіяний у них, отримує безмежний доступ до системи, його важко проконтролювати, тому до них залучають осіб, що користуються цілковитою довірою керівництва.

Програма безпеки, прийнята організацією, повинна передбачати заходи, спрямовані на **реагування на порушення режиму інформаційної безпеки**, такі, щоб послідовність дій була спланована заздалегідь, оскільки заходи треба реалізувати терміново і скоординовано.

Реакція на порушення режиму безпеки переслідує три головні цілі:

- локалізація інциденту і зменшення шкоди;
- виявлення порушника;
- попередження повторних порушень.

В організації повинна бути особа, до якої можна звертатись цілодобово, який відповідає за реакцію на порушення, координати якого повинні бути відомі всім співробітникам.

Часто вимоги локалізації інциденту і зменшення нанесеної шкоди вступає у конфлікт із бажанням знайти порушника. Отже необхідно вирішити, що є більш важливим у даній ситуації.

Щоб знайти порушника, треба завчасно з'ясувати контактні координати постачальника мережевих послуг і домовитись про можливість і порядок виконання відповідних дій.

Щоб попередити повторні порушення, необхідно аналізувати кожний інцидент, виявляти причини, накопичувати та аналізувати статистику.

Необхідно відслідковувати появу нових вразливих місць і швидко ліквідувати асоційовані з ними вікна безпеки. В організації повинний бути спеціаліст, який курирує цей процес, швидко виконує відновлювані заходи і коригувати програму безпеки для прийняття довгострокових заходів.

Планування відновлюваних робіт дозволяє підготуватись до аварій, зменшити втрати від них і зберегти здібність до виконання основних функцій.

Заходи інформаційної безпеки можна розділити на три групи, в залежності від того, на що вони спрямовані: на попередження, викриття чи ліквідацію наслідків атак. Більшість заходів має попереджувальний характер. Оперативний аналіз зареєстрованої інформації використовується для викриття і відбиття атак. Планування відновлюваних робіт відносять до групи.

Процес планування відновлюваних робіт можна розділити на такі етапи:

- виявлення критично важливих функцій організації, встановлення пріоритетів;
- ідентифікація ресурсів, необхідних для виконання критично важливих функцій;
- визначення переліку можливих аварій;

- розробка стратегії відновлюваних робіт;
- підготовка до реалізації обраної стратегії;
- перевірка стратегії.

Плануючи відновлювальні роботи, треба враховувати, що не завжди можливо відновити всі функції, тому необхідно виявляти критично важливі функції, встановлювати між ними пріоритети, щоб з мінімальними витратами відновити роботу після аварії.

Ресурси, необхідні для виконання критично важливих функцій, повинні охоплювати всі аспекти проблеми, отже для їх ідентифікації потрібно підключати спеціалістів різного профілю. До критичних ресурсів відносять одну з наступних категорій:

- персонал;
- інформаційна інфраструктура;
- фізична інфраструктура.

Складаючи списки відповідальних спеціалістів, необхідно враховувати, що може виникнути необхідність заміни співробітників, які не зможуть виконувати свої професійні обов’язки з якихось причин. Бажано мати деякий резерв спеціалістів, яких можна залучити в разі необхідності.

Інформаційна інфраструктура включає наступні елементи:

- комп’ютери;
- програми і дані;
- інформаційні сервіси зовнішніх організацій;
- документацію.

Необхідно підготуватись до того, що на місці, куди організація буде евакуйована після аварії, апаратна платформа може відрізнятись від попередньої. Відповідно, необхідно подбати про програмну і апаратну

сумісність. Аналізуючи критичні ресурси, доцільно враховувати часовий профіль їх використання.

При визначенні переліку можливих аварій необхідно розробити їх приблизні сценарії розвитку.

Стратегія відновлюваних робіт повинна базуватись на наявних ресурсах, враховувати ризики для критичних функцій та містити найбільш економічне рішення. Вона повинна передбачати не тільки роботу за тимчасовою схемою, але й повернення до нормального функціонування.

Доцільно заключити угоду з постачальниками інформаційних послуг про першочергове обслуговування в критичних ситуаціях або угоду з декількома постачальниками.

Перевірка стратегії виконується шляхом аналізу підготовленого плану, прийнятих і намічених заходів.

16.4. Керування інцидентами кібербезпеки

Будь-яка подія, що може перешкодити виконанню вимог кібербезпеки, класифікується як інцидент. Інциденти кібербезпеки можна вважати окремим підкласом кризових і надзвичайних ситуацій у залежності від масштабу події та об’єкта: тобто вони можуть відбутися в інфо-, соціо-, технічній інфраструктурі держави чи в організаційно-технічних системах та інфокомунікаційних мережах підприємства, впливаючи на стан державних інформаційних ресурсів і національної безпеки, чи на рівень інформаційної безпеки підприємства.

Тому підтримку прийняття рішень під час інцидентів кібербезпеки можна розглядати як частину більш загальної проблеми підтримки прийняття управлінських рішень у кризових ситуаціях.

Державою здійснюються **окремі** організаційні, правові та технічні заходи, **частково** спрямовані на підготовку до реагування, обробки та ліквідації наслідків інцидентів інформаційної безпеки, керування телекомунікаційними

мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану. Зокрема, в рамках Адміністрації Держспецзв'язку України створено підрозділ — Державний центр безпеки інформаційно-телекомунікаційних систем, діяльність якого спрямована на вирішення завдань реагування та обробки інцидентів, що порушили безперебійне функціонування інформаційно-комунікаційних мереж органів державної влади.

Як в Україні, так і в світовій практиці завдання підтримки прийняття рішень й автоматизації керування інцидентами інформаційної безпеки потребує подальшого дослідження. Хоча у міжнародній практиці розроблено достатню кількість нормативних документів різного характеру (стандарти, рекомендовані практики, керівництва тощо), що регламентують питання управління інцидентами інформаційної безпеки, в жодному з міжнародних чи вітчизняних нормативно-технічних документів, які частково або цілком присвячені керуванню інцидентами інформаційної безпеки, не визначений повний перелік функцій та елементів, що забезпечують повну автоматизацію процесу керування інцидентами.

Управління інцидентами є однією з найважливіших процедур управлін-ня інформаційною безпекою. У бібліотеці кращих IT-практик ITIL під поняттям "інцидент" розуміється будь-яка подія, що не є елементом нормального функціонування певного сервісу. Наведемо приклади інцидентів інформаційної безпеки.

Приклади інцидентів інформаційної безпеки і їх причини

Інциденти КБ можуть бути умисними або випадковими (наприклад, бути наслідком помилки або природних явищ) і можуть викликатися як технічними, так і фізичними засобами. Їх наслідками можуть бути такі події, як несанкціоновані зміни інформації, її знищення або інші події, які роблять її недоступною, нанесення збитку активам організації або їх розкрадання. Події

КБ, про які не було повідомлено, які не були визначені як інциденти, не можуть бути досліджені, і не можуть бути застосовані захисні заходи для запобігання повторній появі цих подій.

Відмова в обслуговуванні

Відмова в обслуговуванні є великою категорією інцидентів, що мають одну загальну рису. Подібні інциденти призводять до збоїв в системах, сервісах або мережах, які не можуть продовжувати роботу з колишньою продуктивністю, найчастіше при повній відмові у доступі авторизованим користувачам.

Існує два основні типи інцидентів "відмова в обслуговуванні", створюваних технічними засобами: знищення ресурсів і виснаження ресурсів. Типовими прикладами таких умисних технічних інцидентів "відмова в обслуговуванні" є наступні:

- зондування мережевих широкомовних адрес з метою повного заповнення смуги пропускання мережі трафіком повідомлень у відповідь;
- передача даних в непередбаченому форматі в систему, сервіс або мережу, спроба зруйнувати або порушити нормальну роботу;
- одночасне відкриття декількох сеансів з конкретною системою, сервісом або мережею в спробі вичерпати її ресурси (тобто, уповільнити її роботу, блокувати її або зруйнувати).

Ці технічні інциденти "відмова в обслуговуванні" ініціюються навмисно, щоб зруйнувати систему або сервіс, понизити продуктивність мережі, тоді як інші інциденти є побічними продуктами іншої шкідливої діяльності. Наприклад, деякі найбільш поширені методи прихованого сканування і ідентифікації можуть призводити до повного руйнування старих або помилково конфігурованих систем або сервісів при їх скануванні. Слід зауважити, що багато навмисних технічних інцидентів "відмова в

обслуговуванні" часто виконуються анонімно (тобто, джерело атаки фальшиве).

Випадкові технічні інциденти "відмова в обслуговуванні":

- в результаті помилки в конфігурації, допущеній оператором;
- через несумісність прикладного програмного забезпечення.

Інциденти "відмова в обслуговуванні", створювані нетехнічними засобами, що призводять до втрати інформації, сервісу і (чи) пристроїв обробки можуть бути наслідками наступного:

- Порушення фізичних систем безпеки, що призводять до розкрадань, або умисних нанесень збитку, або руйнування устаткування;
- Випадкове нанесення збитку апаратурі, чи її місцю розташування від вогню або води/повені;
- Екстремальні умови довкілля, наприклад, висока температура (вихід з ладу кондиціонера);
- Неправильне функціонування або перевантаження системи;
- Неконтрольовані зміни в системі;
- Неправильне функціонування програмного або апаратного забезпечення.

Збір інформації

Категорія інцидентів "збір інформації" включає дії, пов’язані з визначенням потенційних цілей атаки і отримання уяви про сервіси, запущені для ідентифікованих цілей атаки. Інциденти такого типу свідчать про проведення розвідки з метою визначення:

- топології мережі;
- потенційних вразливостей мережі або уразливості безпосереднього мережевого середовища, які можна використати.

Типовими прикладами атак, спрямованих на збір інформації технічними засобами являються наступні:

- скидання записів DNS (системи доменних імен) для цільового домена Інтернету (передача зони DNS);
- відправка тестових запитів по випадкових мережевих адресах з метою знайти системи, що працюють;
- зондування системи з метою ідентифікації операційної системи хосту;
- сканування доступних мережевих портів на протокол передачі файлів системі з метою ідентифікації відповідних сервісів (наприклад, електронна пошта, FTP, Web і т. д.) і версій програмного забезпечення цих сервісів;
- сканування одного або декількох сервісів з відомими вразливостями по діапазону мережевих адрес (горизонтальне сканування).

В деяких випадках технічний збір інформації розширюється до несанкціонованого доступу, якщо, наприклад, зловмисник, відшукуючи уразливості, намагається також отримати несанкціонований доступ. Зазвичай це здійснюється автоматично хакерськими приладами, які не лише шукають уразливості, але і автоматично намагаються використати уразливі системи, сервіси чи мережі.

Інциденти, спрямовані на збір інформації, створювані нетехнічними засобами, призводять до наступного:

- прямого або непрямого розкриття або модифікації інформації;
- розкрадання інтелектуальної власності, що зберігається в електронній формі;
- порушення обліковості, наприклад, при реєстрації облікових записів;

- НЕПРАВИЛЬНОГО ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ (НАПРИКЛАД, З ПОРУШЕННЯМ ЗАКОНУ АБО ПОЛІТИКИ БЕЗПЕКИ ОРГАНІЗАЦІЇ);
- ПОРУШЕННЯ ФІЗИЧНОГО ЗАХИСТУ БЕЗПЕКИ, ЩО ПРИЗВОДЯТЬ ДО НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ І РОЗКРАДАННЯ ПРИСТРОЇВ ЗБЕРІГАННЯ ДАНИХ, ЩО МІСТЯТЬ ЗНАЧИМІ ДАНІ, НАПРИКЛАД, КЛЮЧІ ШИФРУВАННЯ;
- НЕКОНТРОЛЬОВАНИХ СИСТЕМНИХ ЗМІН, АБО НЕПРАВИЛЬНОГО ФУНКЦІОНУВАННЯ ПРОГРАМНОГО АБО АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ, ЩО ПРИЗВОДИТЬ ДО ТОГО, ЩО ПЕРСОНАЛ ОРГАНІЗАЦІЇ АБО СТОРОННІЙ ПЕРСОНАЛ ДІСТАЄ ДОСТУП ДО ІНФОРМАЦІЇ, НЕ МАЮЧИ НА ЦЕ ДОЗВОЛУ.

Несанкціонований доступ

ЦЯ КАТЕГОРІЯ ІНЦИДЕНТІВ ВКЛЮЧАЄ ІНЦИДЕНТИ, ЯКІ НЕ УВІЙШЛИ ДО ПЕРШОЇ ДВОХ КАТЕГОРІЇ. ВЗАГАЛІ ЦЯ КАТЕГОРІЯ ІНЦИДЕНТІВ СКЛАДАЄТЬСЯ З ФАКТИЧНИХ НЕСАНКЦІОНОВАНИХ СПРОБ ДОСТУПУ В СИСТЕМУ АБО НЕПРАВИЛЬНОГО ВИКОРИСТАННЯ СИСТЕМИ, СЕРВІСУ АБО МЕРЕЖІ. ДЕЯКІ ПРИКЛАДИ ТЕХНІЧНОГО НЕСАНКЦІОНОВАНОГО ДОСТУПУ ВКЛЮЧАЮТЬ:

- СПРОБИ ВИТЯГНУТИ ФАЙЛИ, ЩО МІСТЯТЬ ПАРОЛІ;
- АТАКИ ПЕРЕПОВНЮВАННЯ БУФЕРА З МЕТОЮ ДІСТАВАННЯ ПРИВІЛЕЙОВАНОГО (НАПРИКЛАД, НА РІВНІ СИСТЕМНОГО АДМІНІСТРАТОРА) ДОСТУПУ ДО МЕРЕЖІ;
- ВИКОРИСТАННЯ ВРАЗЛИВОСТЕЙ ПРОТОКОЛУ ДЛЯ ПЕРЕХОПЛЕННЯ З'ЄДНАННЯ АБО НЕПРАВДИВОГО НАПРЯМУ ЛЕГІТИМНИХ МЕРЕЖЕВИХ З'ЄДНАНЬ;
- СПРОБИ ПІДВИЩИТИ ПРИВІЛЕЇ ДОСТУПУ ДО РЕСУРСІВ АБО ІНФОРМАЦІЇ ПОРІВНЮЮЧИ З ТИМИ, ЯКІ КОРИСТУВАЧ АБО АДМІНІСТРАТОР ВЖЕ МАЮТЬ ЛЕГІТИМНО.

ІНЦИДЕНТИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ, ЩО СТВОРЮЮТЬСЯ НЕТЕХНІЧНИМИ ЗАСОБАМИ, ЯКІ ПРИВОДЯТЬ ДО ПРЯМОГО АБО НЕПРЯМОГО РОЗКРИТТЯ АБО МОДИФІКАЦІЇ ІНФОРМАЦІЇ, ДО ПОРУШЕНЬ ОБЛІКУ АБО НЕПРАВИЛЬНОГО ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ, МОЖУТЬ ВИКЛИКАТИСЯ НАСТУПНИМИ ЧИННИКАМИ:

- РУЙНУВАННЯМ ФІЗИЧНОГО ЗАХИСТУ БЕЗПЕКИ З ПОДАЛЬШИМ НЕСАНКЦІОНОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЇ;
- НЕВДАЛО АБО НЕПРАВИЛЬНО СКОНФІГУРОВАНОЮ ОПЕРАЦІЙНОЮ СИСТЕМОЮ УНАСЛІДОК НЕКОНТРОЛЬОВАНИХ ЗМІН В СИСТЕМІ;
- НЕПРАВИЛЬНИМ ФУНКЦІОНУВАННЯМ ПРОГРАМНОГО АБО АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ, ЩО ПРИЗВОДЯТЬ ДО РЕЗУЛЬТАТІВ, ПОДІБНИХ ДО ПОПЕРЕДНІХ.

Необхідність створення системи управління інцидентами кібербезпеки

Для ефективного управління інцидентами кібербезпеки (УІКБ) необхідно організувати комплекс процесів управління інцидентами, забезпечити його належними ресурсами, відповідною нормативною і робочою документацією, технічними засобами забезпечення механізмів контролю.

Інциденти інформаційної безпеки спричинені багатьма зовнішніми чинниками (загрозами) та внутрішніми вразливостями сучасних інформаційних і телекомунікаційних технологій (обробки, зберігання, передачі інформації). Складний розподілений характер, модульність, помилки та недоліки в програмно-апаратній архітектурі інформаційних систем обробки та зберігання даних створюють додаткові вразливості та можливості для реалізації загроз кібербезпеки у вигляді інцидентів. Крім того, для інформаційного обміну використовують послуги вразливих і не завжди достатньо захищених інформаційно-комунікаційних мереж, наприклад, Інтернет.

Крім того, розвиток високих технологій, таких як нанотехнології, робототехніка, сенсорні мережі, радіочастотна ідентифікація, телебіометрія, штучний інтелект, інформаційна зброя, нові засоби впливу тощо, – додає **нових проблем, ризиків, побічних негативних явищ.** Тому і в найближчому майбутньому інформаційно-комунікаційні мережі виявляться слабо

захищеними від зловживань, вторгнень, зовнішніх і внутрішніх впливів, стаючи ареною інформаційних війн, діяльності кіберзлочинців і хакерів.

Керування інцидентами інформаційної безпеки характеризується множиною критеріїв і показників. Головними комплексними критеріями є якість, надійність і безпечність інформаційного обміну. Можна виділити множину показників, пов'язаних з інцидентами : кількісні (частота й кількість появи інцидентів, середній час реагування, відсоток успішно вирішених інцидентів, величина збитків) і якісні (термінологія, ступінь критичності, перебіг інциденту тощо).

Спостерігається постійне зростання кількості зареєстрованих інцидентів інформаційної безпеки, зокрема в системах, які підключені до мережі Інтернет. У той же час, заходи протидії не встигають за ростом кількості інцидентів. Це свідчить про недостатню ефективність існуючих підходів до захисту інформації та керування інформаційною безпекою і необхідність шукати нові методи вдосконалення процесів реагування, обробки, розслідування та запобігання, які в сукупності складають керування інцидентами інформаційної безпеки.

ОРГАНІЗАЦІЯ ПРОЦЕСУ КЕРУВАННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ

Організувати процес керування інцидентами інформаційної безпеки, не використовуючи засоби **автоматизації,** дуже складно. Необхідно збирати та консолідувати надвелику кількість даних у різних форматах, вести централізований архів. Для ручної обробки даних щодо подій та інцидентів інформаційної безпеки потрібна велика кількість висококваліфікованих фахівців-аналітиків. Через великий обсяг рутинної роботи обробка подій буває неповною, що не відображає всієї поточної ситуації. Може статися, що інциденти інформаційної безпеки, критичні для надійного й захищеного функціонування системи, виявляються поза полем зору аналітиків, і через це не приймаються відповідні превентивні заходи.

Управління інцидентами КБ повинно включати такі дії:

- повідомлення про уразливі місця ІКС та події КБ;
- відповідальність і процедури;
- навчання на інцидентах КБ;
- збір доказів.

Документування подій інциденту КБ необхідне, перш за все, для збору і консолідації технологічних та операційних свідчень розслідування. Документуванню підлягають усі факти та докази зловмисного впливу. Типовою практикою розслідування інциденту є ведення журналу, який не має загальної стандартної форми і розробляється командою підприємства.

Апаратно-програмні засоби моніторингу і аудиту – засоби, що реалізують функції з протоколювання, збору, накопичення та обробки інформації функціонування ІКС організації. Вони складають підсистему збору інформації про інциденти КБ. Результатом їх роботи є дані, на основі яких системою приймається рішення щодо настання інциденту.

У рамках СУІКБ необхідно збирати і обробляти велику кількість подій КБ, які надходять з різних джерел. Ці події мають бути приведені до єдиного вигляду, що дозволяє застосовувати єдині алгоритми обробки та безпомилкового виділення з них саме інцидентів КБ. Необхідно зберігати події КБ протягом часу, достатнього для забезпечення розслідування інцидентів.

Оперативні дані сенсорів безпеки повинні аналізуватися та оцінюватися на предмет наявності відомих інцидентів за допомогою бази знань інформаційної системи підтримки прийняття рішень. Після чого кожний адміністратор, користувач чи співробітник повинен одержати інструкцію, що визначатиме, які повинні бути його дії. Звіт про виявлення та реєстрацію інциденту інформаційної безпеки в організаційно-технічній системі повинен містити докладний опис інциденту, перелік залучених співробітників, прізвище співробітника, що зафіксував інцидент, дату виникнення та реєстрації.

Під час розслідування інциденту інформаційна система підтримки прийняття рішень повинна надавати інформаційно-аналітичну підтримку у вигляді досвіду та знань, що містять у собі визначення винних у виникненні інциденту, збір доказів, визначення дисциплінарних стягнень тощо.

Практично неможливо уникнути небажаних інцидентів у захисті. Кожний інцидент потрібно досліджувати настільки глибоко, наскільки вагомий збиток він спричинив. Регулювання інциденту дає змогу відповідно реагувати на випадкові або навмисні збої нормального режиму роботи системи інформаційних технологій. Отже, проєкт звітності і розслідування інцидентів повинні бути придатними для всієї організації і сервісних служб системи інформаційних технологій. Після цього потрібно об'єднати між організаційні плани звітності для глибшого уявлення про місця виявлення інцидентів безпеки інформаційних технологій і пов'язаних з ними загроз, їх впливу на активи інформаційних технологій та ділову активність.

Основними цілями розслідування інцидентів безпеки інформаційних технологій повинні бути:

- з'ясувати чи було компетентним і ефективним реагування на інцидент;
- зробити висновки з інцидентів, щоб запобігти подібним несприятливим подіям.

Підготовлений план дій із наперед визначеними рішеннями дає змогу організації на прийнятних умовах припинити подальше пошкодження і, якщо можливо, продовжувати ділову активність із запасними засобами. План реагування на інциденти повинен включати вимоги хронологічного документування всіх подій і заходів; це повинно допомогти ідентифікувати джерела інцидентів. Це є передумовою для досягнення іншої мети – зменшення ризику в майбутньому через вдосконалення засобів захисту. Інший позитивний наслідок інцидентів – збільшення готовності інвестувати в засоби захисту.

Важливо також проаналізувати здійснення й документування інциденту, керуючись такими питаннями:

- що сталося і коли саме?
- чи діяв персонал згідно з планом?
- чи вчасно необхідна інформація була в розпорядженні персоналу?
- що персонал запропонував робити інакше наступного разу?

Відповіді на ці питання допоможуть зрозуміти інцидент. Також це допоможе знизити ризик шляхом збільшення релевантності проєктів і методик захисту інформаційних технологій (наприклад, вдосконалення засобів захисту, зменшення уразливості й адаптування програми компетентності в захисті).

Усунення причин, наслідків інциденту і його розслідування.

Інформаційна система підтримки прийняття рішень на підставі звіту повинна надавати інструкцію щодо усунення причин і наслідків інциденту інформаційної безпеки, включаючи опис загальних заходів, які необхідно розпочати, та конкретні дії для кожного інциденту інформаційної безпеки, а також терміни, протягом яких варто усунути наслідки та причини інциденту інформаційної безпеки. Необхідно розробити класифікацію інцидентів інформаційної безпеки – визначити рівні критичності інцидентів, описати інциденти кожного рівня й терміни їхнього усунення.

Коригувальні та превентивні дії.

Після усунення наслідків інциденту й відновлення нормального функціонування бізнес-процесів організаційно-технічної системи, доцільно виконати дії щодо запобігання повторного виникнення інциденту інформаційної безпеки. Для визначення необхідності реалізації таких дій інформаційна система підтримки прийняття рішень повинна провести аналіз ризиків, у рамках якого визначити доцільність коригувальних і превентивних дій.

Для того щоб процедура виконувалася правильно й ефективно, всі ці етапи повинні безупинно й послідовно повторюватися.

Отже, УІКБ – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються інформаційної системи, а на виході цих процесів одержують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, про заходи, які необхідно вжити для того, щоб інцидент не повторився. Таким чином, УІКБ спрямовано на вдосконалення системи забезпечення безпеки організації. Крім того, вихідні дані є, по суті, єдиним об'єктивним параметром у визначенні ймовірності реалізації загроз при аналізі ризиків.

Ефективність процесу УІКБ залежить від:

- координації і узгодженості дій всіх залучених до нього осіб;
- наявних можливостей з отримання та аналізу інформації, пов'язаної з інцидентом;
- оперативності та коректності отриманих результатів.

Підвищення кожного з наведених показників помітно підвищить ефективність всього процесу і, тим самим, дозволить підрозділу КБ організації набути більш значних результатів. Використовуючи СУІКБ можна радикально змінити ситуацію щодо ефективності управління інцидентами. Таким чином, СУІКБ фактично буде системою колективної роботи, яка автоматизує процеси з УПБ за допомогою інтеграції людей і апаратно-програмного забезпечення моніторингу і захисту, а також інформаційної інфраструктури організації.

У загальному випадку, ознаки інциденту поділяються на дві основні категорії - повідомлення про те, що інцидент відбувається в даний момент і повідомлення про те, що інцидент, можливо, відбудеться у майбутньому.

Прийняття рішення про настання інциденту багато в чому залежить від компетентності експертів команди реагування. Вони мають чітко відрізняти

випадкову помилку оператора, наприклад, від зловмисного цілеспрямованого впливу на ІКС.

Розробка методики керування інцидентами кібербезпеки

Процес прийняття будь-якого рішення щодо керування інцидентами інформаційної безпеки супроводжується попереднім аналізом альтернатив можливих варіантів. Під час аналізу альтернатив виникає необхідність розрахунку, порівняння, розподілу ресурсів інформаційної безпеки.

Але пряме використання традиційних математичних підходів, таких як апарат теорії ймовірностей, математична статистика, теорія систем масового обслуговування, теорія черг, марківські процеси, класичні методи багатокритеріальної оптимізації не дає прийнятних результатів під час вирішення завдань інформаційної безпеки, тому що недостатній період спостережень за процесами, відсутність репрезентативних статистичних даних, невідповідність математичного інструментарію рівню складності, невизначеності й нечіткості досліджуваних процесів захисту інформації та керування інформаційної безпеки.

Особливості розробки ефективної та обґрунтованої методики підтримки прийняття рішень щодо керування інцидентами інформаційної безпеки**:**

- недостатність знань про природу та структуру нових інцидентів інформаційної безпеки;
- невизначеність законів розподілу ймовірностей появи інцидентів інформаційної безпеки через нестохастичні чинники та непередбачувані умови їхнього здійснення;
- необхідність врахування надвеликої кількості неістотних на перший погляд чинників, які можуть суттєво вплинути на процес обробки інциденту інформаційної безпеки;

- вирішальний вплив антропогенного фактору на процеси керування інцидентами інформаційної безпеки;
- відсутність репрезентативної кількості інформації стосовно інцидентів інформаційної безпеки;
- недостатньо тривалий період спостережень за інцидентами інформаційної безпеки;
- отримання необхідної інформації виявляється складним, трудомістким або навіть неможливим завданням;
- множина загроз, що можуть спричинити інцидент інформаційної безпеки, постійно розширюється й динамічно змінюється, причому швидшими темпами, ніж множина засобів захисту.

Керування інцидентами інформаційної безпеки є послідовний безперервний процес, що динамічно відбувається в режимі реального часу на всіх етапах життєвого циклу організаційно-технічної системи або інформаційно-комунікаційної мережі, починаючи з розробки вимог безпеки та складання технічного завдання на проєктування комплексної системи захисту інформації, технічної експлуатації, наступної модернізації та вдосконалення.

Сертифікація систем керування інцидентами вітчизняних організаційно-технічних систем за IS0/IEC 27001 могла би підвищити ступінь їхньої привабливості та надійності для іноземних інвесторів і партнерів. Враховуючи це, необхідно використовувати стандарти IS0/IEC та інші як методологічні засади для створення системи керування інцидентами ІБ, яка б цілком вписувалася та була б логічним продовженням уже існуючих і сертифікованих систем керування бізнес-процесами організаційно-технічних систем, зокрема, таких як система технічної експлуатації та система менеджменту якості IS0 9001. Якщо в організаційно-технічній системі уже впроваджено системи менеджменту у відповідності до стандартів 1S0 9001 та IS0 14000, то доцільно

забезпечити виконання вимог стандарту IS0 27001 у рамках існуючих систем менеджменту.

Стандарти IS0 серій 9000, 14000, 20000, 27000 описують правила створення систем керування різними процесами та гармонійно поєднуються один з одним. Усі вони, як основу керування підконтрольними процесами, використовують процесний підхід, що розглядає керування як набір взаємозалежних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, що витрачені для цього.

Узагальненою метою забезпечення КБ організації є зниження ризиків, діючих відносно інформаційних ресурсів, і як наслідок запобігання або мінімізація збитку від можливих інцидентів КБ. Основною задачею процесу УІКБ є усунення інцидентів в гранично стислі терміни. У ході процесу управління інцидентами КБ проводиться виявлення, реєстрація, класифікація і початкова підтримка запитів, а також пошук рішення, його застосування, контроль, інформування і підготовка звітності. Оскільки, інцидентом, в першу чергу, є певна недозволена подія, то вона має бути кимось заборонена. Отже, існує необхідність розробки та затвердження документів, що чітко описують всі дії, які можна виконувати в ІКС і які виконувати заборонено.

Ці документи повинні описувати:

1) визначення інциденту КБ – перелік подій, що є інцидентами КБ саме в цій організації;

2) порядок сповіщення відповідальної особи про виникнення інциденту, формат звіту, контактну інформацію осіб, яких слід оповіщати про інцидент;

3) порядок усунення наслідків і причин інциденту;

4) порядок розслідування інциденту (визначення причин інциденту, винних у виникненні інциденту, порядок збору і збереження доказів);

5) винесення дисциплінарних стягнень;

6) реалізацію коригуючих і превентивних заходів.

Важливо зберігати ці документи, що містять всі дані про інциденти ІБ, адже за допомогою статистики інцидентів можна визначити найбільш актуальні загрози для організації і, відповідно, максимально точно планувати заходи щодо підвищення рівня захищеності інформаційно-комунікаційних систем організації.

16.5. Керування кіберзахистом автоматизованих робочих місць

Діяльність працівників сфери управління (бухгалтерів, плановиків, керівників підрозділів, інспекторів відділу кадрів тощо) орієнтована на використання розвинутих інформаційних технологій. Організація та реалізація управлінських функцій вимагає радикальної зміни як самої технології управління, так і технічних засобів обробки інформації, перш за все, персональних комп'ютерів. Вони все більше перетворюються із систем автоматичної обробки вхідної інформації у засоби накопичення досвіду управлінських працівників, аналізу, оцінки і вироблення найбільш ефективних рішень.

Автоматизоване робоче місце (АРМ) – це сукупність інформаційно-програмно-технічних ресурсів, що забезпечують кінцевому користувачу обробку даних і автоматизацію управлінських функцій в конкретній предметній області.

Створення автоматизованих робочих місць передбачає, що основні операції з накопичення, зберігання і обробки даних покладаються на обчислювальну техніку, а працівник сфери управління виконує частину ручних операцій і операцій, які вимагають творчого підходу при підготовці управлінських рішень. Персональна техніка застосовується користувачем для контролю виробничої діяльності, зміни значень окремих параметрів в процесі рішення задачі, а також введення вхідних даних в автоматизовану інформаційну систему для рішення поточних завдань і аналізу функцій управління.

АРМ створюється для забезпечення виконання деякої групи функцій. Найбільш простою функцією АРМ є інформаційно-довідкове обслуговування. АРМ мають проблемно-професійну орієнтацію на конкретну предметну область. Професійні АРМ є головним інструментом спілкування людини з обчислювальними системами, виконуючи роль автономних робочих місць, інтелектуальних терміналів великих ЕОМ, робочих станцій у локальних мережах.

Локалізація АРМ дозволяє здійснити оперативну обробку інформації зразу ж після її надходження, а результати зберігати як завгодно довго і видавати їх на вимогу користувача.

Метою впровадження АРМ є посилення інтеграції управлінських функцій, і кожне робоче місце повинне забезпечувати роботу у багатофункціональному режимі.

АРМ виконує децентралізовану одночасну обробку інформації на робочих місцях виконавців у складі розподіленої бази даних (БД). При цьому вони мають вихід через системний пристрій і канали зв'язку на комп'ютери і БД інших користувачів, забезпечуючи таким чином спільне функціонування комп'ютерів у процесі колективної обробки.

Технічне, інформаційне, програмне забезпечення АРМ

АРМ, створені на базі персональних комп'ютерів – найбільш простий і поширений варіант автоматизованого робочого місця для працівників сфери організаційного управління. Таке АРМ розглядається як система, яка в інтерактивному режимі роботи надає конкретному працівнику (користувачу) всі види забезпечення монопольно на весь сеанс роботи. Користувач сам виконує всі функціональні обов'язки по перетворенню інформації.

Створення АРМ на базі персональних комп'ютерів забезпечує:

- простоту, зручність і дружність по відношенню до користувача;

- простоту адаптації до конкретних функцій користувача;
- компактність розташування і невисокі вимоги до умов експлуатації;
- високу надійність і живучість;
- більш-менш просту організацію технічного обслуговування.

Ефективним режимом роботи АРМ є його функціонування в межах локальної обчислювальної мережі в якості робочої станції. Особливо доцільним є варіант, коли необхідно розподіляти інформаційно-обчислювальні ресурси між декількома користувачами.

У найбільш складних системах АРМ можуть через спеціальне обладнання підключатись не тільки до ресурсів головної ЕОМ мережі, але й до різних інформаційних служб і систем загального призначення (службам новин, національним інформаційно-пошуковим системам, базам даних і знань, бібліотечним системам тощо).

Можливості створюваних АРМ значною мірою залежать від техніко-експлуатаційних характеристик ЕОМ, на яких вони базуються. У зв'язку з цим на стадії проєктування АРМ чітко формулюються вимоги до базових параметрів технічних засобів обробки і видачі інформації, набору комплектуючих модулів, мережевих інтерфейсів, ергономічних параметрів пристроїв тощо.

Інформаційне забезпечення АРМ орієнтується на конкретну, звичну для користувача предметну область. Обробка документів повинна передбачати таку структуризацію інформації, яка дозволяє здійснювати необхідну маніпуляцію різними структурами, зручне і швидке коригування даних у масивах.

Технічне забезпечення АРМ повинно гарантувати високу надійність технічних засобів, організацію зручних для користувача режимів роботи. З усього сказаного вище можна зробити такі **висновки щодо вимог** до АРМ:

- своєчасне задоволення інформаційної та обчислювальної потреби спеціаліста;

- мінімальний час відповіді на запити користувача;
- простота засвоєння прийомів роботи на АРМ, легкість спілкування, надійність і простість обслуговування;
- терпимість по відношенню до користувача;
- можливість роботи у складі обчислювальної мережі.

Узагальнену схему АРМ представлено на рис. 16.1.

Загальне програмне забезпечення (ПЗ) забезпечує функціонування обчислювальної техніки, розробку та підключення нових програм. До нього належать операційні системи, системи програмування, обслуговуючі програми.

Функціональне ПЗ забезпечує рішення функціональних задач АРМ, обробку регламентних запитів та дії у штатних ситуаціях.

Що стосується захисту АРМ, то різні фірми пропонують свої розробки. Лінійка продуктів "Криптон", була розроблена російською фірмою "Анкад", яка разом з організаційними заходами дозволяє успішно вирішувати найскладніші задачі із захисту інформації з урахуванням її важливості, включаючи інформацію високого рівня секретності.

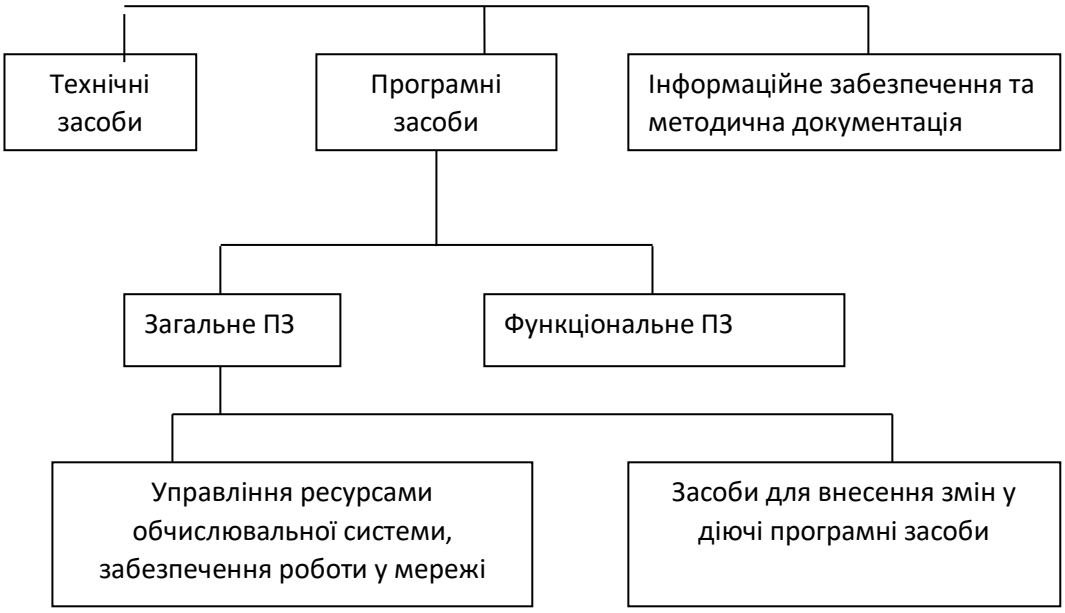


Рис. 16.1. Схема автоматизованого робочого місця

Автоматизоване робоче місце абонента системи "Контур-Экстерн" використовує засоби криптографічного захисту інформації (СКЗІ) для забезпечення цілісності, авторства і конфіденційності інформації, що передається в рамках інформаційної системи.

Продукти Altiris Cisco створювались для рішення задач моніторингу і централізованого управління комп'ютерами користувачів. Програмне забезпечення Altiris Client Management Suite дозволяє автоматизувати типові операції з обслуговування АРМ: вести адміністрування комп'ютерів співробітників, усувати збої, оновлювати програмне забезпечення у віддаленому режимі; створювати та підтримувати в актуальному стані облікову базу наявності та використання програмно-апаратних засобів АРМ. Це надає можливість підвищити оперативність і ефективність роботи IT-служби, знизити вартість обслуговування комп'ютерної інфраструктури, стандартизувати апаратні та програмні засоби і оптимізувати управління життєвим циклом устаткування і ПЗ.

Захист автоматизованого робочого місця

Автоматизоване робоче місце спеціаліста повинне використовувати засоби захисту інформації для забезпечення цілісності, авторства та конфіденційності інформації, що передається в рамках інформаційної системи.

Для цього необхідно, перш за все, розробити **політику захисту АРМ**, основними пунктами якої є:

- допускати до автоматизованих робочих місць, з яких здійснюється доступ в систему (АРМ) лише довірених осіб;
- використовувати на АРМ лише ліцензійне програмне забезпечення;
- використовувати АРМ, на якому встановлена **лише одна операційна система;**
- працювати в операційній системі АРМ під локальним обліковим записом з обмеженими правами доступу;
- встановити на АРМ спеціальні програмні та апаратні засоби захисту (міжмережеві екрани (firewall), антивірусне програмне забезпечення, засоби виявлення шкідливих програм), які повинні регулярно оновлюватись. Також оновлювати файли операційної системи;
- запускати на АРМ програми, отримані лише з довірених джерел (особливу небезпеку можуть становити програми, отримані електронною поштою або з мережі Інтернет);
- періодично, не рідше за один раз на два місяці, проводити контроль цілісності встановленого на АРМ програмного забезпечення;
- не встановлювати на АРМ програмне забезпечення, що містить засоби розробки і налагодження додатків, а також засоби, що дозволяють здійснювати несанкціонований доступ до системних ресурсів;
- встановити парольний захист на вхід в BIOS, в операційну систему та інформаційну систему;
- регулярно проводити зміну паролів;

- не виконувати і не відкривати файли, отримані із загальнодоступних мереж передачі даних, без проведення відповідних перевірок на предмет вмісту в них програмних закладок і вірусів.

Власник сертифіката ключа АРМ зобов'язаний:

- не використовувати для шифрування відкриті й закриті ключі, якщо йому відомо, що ці ключі використовуються або використовувалися раніше;
- зберігати в таємниці закритий ключ;
- негайно вимагати призупинення дії сертифіката ключа за наявності підстав вважати, що таємниця закритого ключа порушена (компрометація ключа).

Для реалізації політики захисту рекомендується:

- встановлення та налаштування захисту на автоматизоване робоче місце повинні виконуватися в присутності адміністратора. Перед установкою необхідно перевірити цілісність програмного забезпечення системи кіберзахисту. Забороняється встановлювати систему захисту, цілісність якої порушена;
- має бути визначено і затверджено порядок обліку, зберігання і використання носіїв ключової інформації з закритими ключами, який повинен повністю виключати можливість несанкціонованого доступу до них;
- повинен бути затверджений список осіб, які мають доступ до ключової інформації;
- для зберігання носіїв закритих ключів та шифрування в приміщеннях повинні встановлюватися надійні металеві сховища (сейфи), обладнані надійними запірними пристроями з двома екземплярами ключів (один у виконавця, інший в службі безпеки);

- використовувати АРМ із вбудованими засобами захисту в режимі **одного** користувача. В окремих випадках, при необхідності використання АРМ кількома особами, ці особи повинні мати рівні права доступу до інформації;
- при завантаженні операційної системи і при поверненні після тимчасової відсутності користувача на робочому місці повинен запитуватися пароль, що складається не менше ніж з 6 символів. В окремих випадках при неможливості використання парольного захисту, допускається завантаження ОС без запиту пароля. При цьому повинні бути реалізовані додаткові організаційно-режимні заходи, що виключають несанкціонований доступ до цих АРМ;
- повинні бути вжиті заходи по виключенню несанкціонованого доступу в приміщення, в яких встановлено технічні засоби АРМ із вбудованими системами захисту;
- мають бути передбачені заходи, що виключають можливість несанкціонованої зміни апаратної частини робочої станції на встановлених системах захисту;
- встановлене на АРМ програмне забезпечення не повинно містити засобів розробки й налагодження додатків, а також засобів, що дозволяють здійснювати несанкціонований доступ до системних ресурсів;
- адміністрування повинно здійснюватися довіреними особами. Засобами BIOS виключити можливість мережного завантаження ОС робочої станції;
- засобами BIOS виключати можливість роботи на ПЕОМ, якщо під час її початкового завантаження не проходять вбудовані тести;
- входження користувачів в режим конфігурування BIOS штатними засобами BIOS має здійснюватися тільки з використанням парольного захисту при довжині пароля не менше 6 символів;
- при використанні ОС Windows всі користувачі робочої станції повинні мати право доступу до всієї конфіденційної інформації, що обробляється на цій станції;

- при використанні ОС Windows NT сімейства вжити заходів, що виключають доступ користувача до системного реєстру;
- обмежити або виключити використання програмного продукту Scheduler (планувальник завдань), що входить до складу ОС Windows. При використанні Scheduler програмне забезпечення на АРМ узгоджується з адміністратором безпеки;
- при використанні ОС Windows виключити можливість віддаленого редагування системного реєстру користувачами (виключаючи адміністратора);
- при використанні ОС Windows NT сімейства перейменувати користувача Administrator, відключити обліковий запис для гостьового входу (Guest);
- у разі звільнення або переведення в інший підрозділ (на іншу посаду), зміни функціональних обов'язків співробітника, що мав доступ до ключових носіїв, повинна бути проведена зміна ключів, до яких він мав доступ.

Не допускається:

- Знімати несанкціоновані копії з ключових носіїв.
- Знайомити із вмістом ключових носіїв або передавати ключові носії особам, до них не допущених.
- Виводити секретні ключі на дисплей (монітор) комп’ютера або принтер.
- Встановлювати ключовий носій у зчитувальний пристрій (дисковод) комп’ютера АРМ, не передбачений функціонуванням системи, а також в інші комп’ютери.
- Записувати на ключовий носій сторонню інформацію.

Дії, пов'язані з експлуатацією системи захисту, **повинні фіксуватися в журналі,** який веде особа, відповідальна за забезпечення інформаційної безпеки. У журнал крім цього записуються факти компрометації ключових документів, позаштатні ситуації, що відбуваються в системі і пов'язані з використанням системи захисту, проведення регламентних робіт, дані про

отримані у адміністратора безпеки організації ключових носіях, позаштатних ситуаціях, що сталися на АРМ, з встановленим ПЗ системи захисту.

У журналі може відображатися наступна інформація:

- дата, час;
- запис про компрометації ключа;
- запис про виготовлення особистого ключового носія користувача, ідентифікатор носія;
- запис про виготовлення копій особистого ключового носія користувача, ідентифікатор носія;
- запис про виготовлення резервного ключового носія користувача, ідентифікатор носія;
- запис про отримання сертифіката відкритого ключа, повний номер ключового носія, відповідний сертифікату;
- записи, що відображають видачу на руки користувачам (відповідальним виконавцям) і здачу ними на зберігання особистих ключових носіїв, включаючи резервні ключові носії;
- події, що відбувалися на АРМ користувача з встановленим ПЗ системи захисту, із зазначенням причин і виконаних дій.

При використанні АРМ підвищується захист корпоративної мережі, надійність її роботи, зменшуються витрати на адміністрування інформаційної системи і усунення наслідків її зараження шкідливим програмним забезпеченням.

Крім того, ці рішення допомагають боротися із "хаосом" у комп’ютерній інфраструктурі компанії, своєчасно встановлювати на комп’ютери співробітників необхідні оновлення системного програмного забезпечення і систем захисту.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Назвіть види моделей політики кібербезпеки.
2. Назвіть цілі програми верхнього та нижнього рівня.
3. В чому полягає життєвий цикл інформаційного сервісу.
4. Які класи заходів можна виділити на процедурному та фізичному рівнях?
5. Що необхідно зробити для захисту бізнес-інформації?
6. Назвіть мету впровадження АРМ.
7. Поняття інциденту кібербезпеки.
8. Нормативне забезпечення інцидентів кібербезпеки.
9. Наведіть приклади інцидентів кібербезпеки.
10. Які ви знаєте інциденти "відмова в обслуговуванні"?
11. Наведіть приклади ІНЦИДЕНТІВ "ЗБІР ІНФОРМАЦІЇ".
12. Наведіть приклади ІНЦИДЕНТІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО СИСТЕМИ.
13. Яким чином можливо організувати процес керування інцидентами інформаційної безпеки?
14. Від яких факторів залежить ефективність процесу УІКБ?

РОЗДІЛ 17. КЕРУВАННЯ КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

17.1. Керування кібернетичною безпекою інформації

Планування і загальний огляд процесів планування і керування

Планування і керування КЗ інформаційних технологій – загальний процес встановлення і підтримування програми КБ інформаційних технологій в організації. На рисунку 17.1 відображено основні елементи цього процесу.

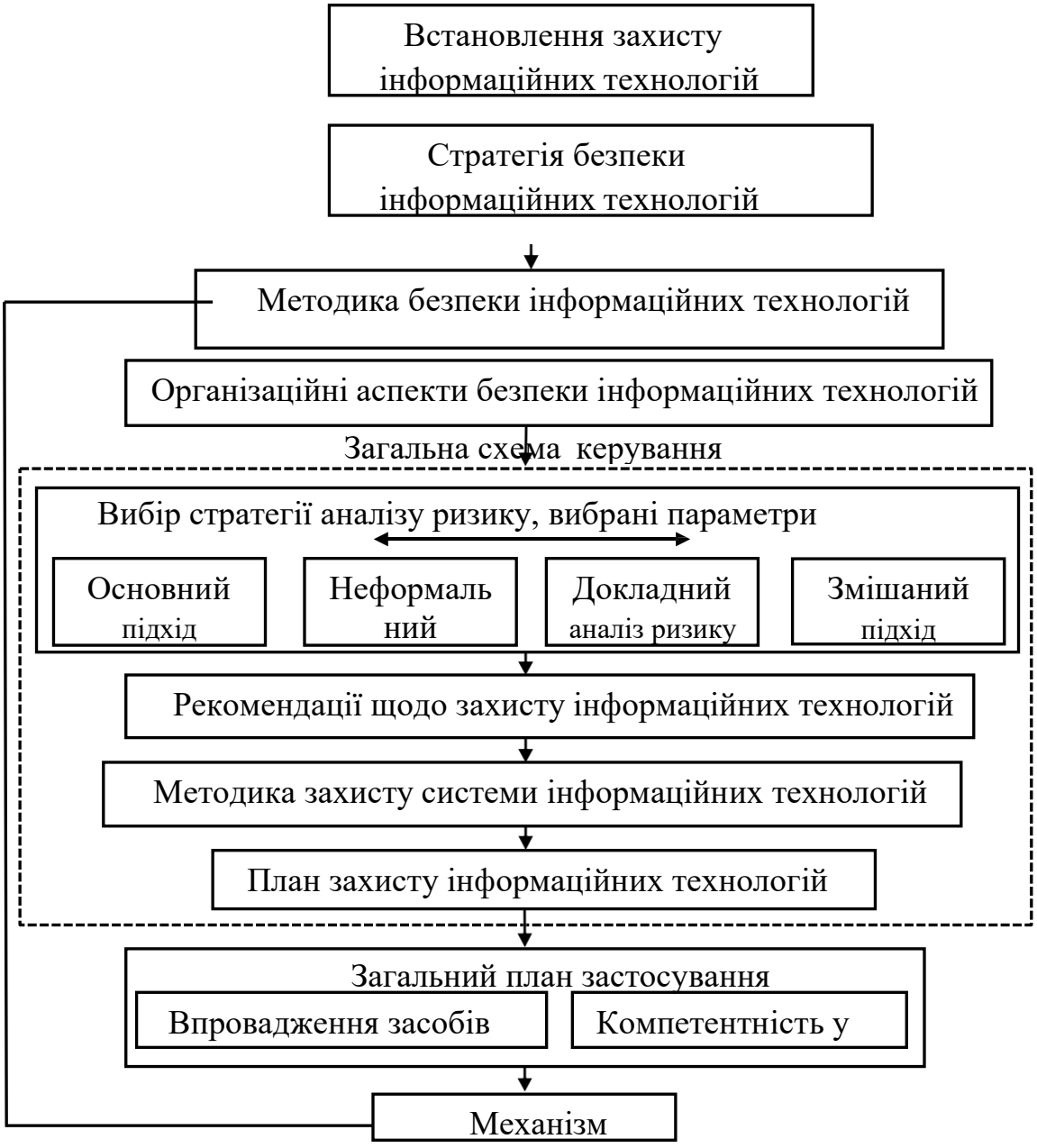


Рисунок 17.1. Загальна схема керування КБ інформаційних технологій

Відмінність типів керування, розмірів і структур організацій зумовлює орієнтацію процесу на середовище. Важливо, що всі аспекти та функції, які зображені на рис. 17.1, пристосовані до типу, розміру і структури організації та способу ведення діяльності. Безумовно, ці елементи керування є лише частиною діяльності організації.

Відправною точкою є встановлення чітких цілей КЗ інформаційних технологій організації. Вони виходять з цілей вищого рівня (наприклад, з цілей ділової активності) і, в свою чергу, визначають стратегію КБ інформаційних технологій організації і корпоративну методику КБ інформаційних технологій. Отже, частиною методики КБ інформаційних технологій є створення відповідної структури організації, яка буде гарантувати досягнення певної мети.

Загальна схема керування ризиком

Керування ризиком складається з чотирьох різних дій:

• визначення загальної стратегії керування ризиком згідно з корпоративною методологією керування КБ інформаційних технологій;

• вибір засобів КЗ для конкретної системи інформаційних технологій згідно з аналізом ризику або відповідно до концепції керування ризиком;

• розробка методик КЗ системи інформаційних технологій, виходячи з рекомендацій КБ, та, в разі потреби, модифікація методологій КЗ інформаційних технологій (і відповідних відомчих методик захисту інформаційних технологій);

• розробка проектів КБ інформаційних технологій щодо застосування засобів КЗ на основі схвалених методик КЗ системи інформаційних технологій.

Загальний план застосування

Застосування необхідних засобів КЗ для кожної системи інформаційних технологій має відповідати проектам КБ інформаційних технологій. Поліпшення загальної компетентності в КЗ інформаційних технологій, чим часто нехтують, є важливим аспектом ефективності засобів захисту. Рисунок 17.1 показує, що ці два завдання, а саме: застосування засобів КЗ і програми компетентності в КЗ – треба розв’язувати паралельно, оскільки звична поведінка конкретного користувача не може бути раптово змінена і для освоєння потрібен певний час.

Загальний огляд функцій механізму доопрацювання

Механізм доопрацювання охоплює:

• обслуговування засобів КЗ для забезпечення їхньої безперервної й ефективної роботи;

• перевірку засобів КЗ, яка гарантує, що вони задовольняють обумовлені методики і проекти;

• контроль активів, загроз, уразливості і засобів КЗ щодо відхилень, щоб виявити зміни, які впливають на ризики;

• відстежування кожного інциденту, щоб гарантувати відповідну реакцію на небажані події.

Механізм доопрацювання – тривалий процес, який повинен містити переоцінювання рішень, прийнятих раніше.

Інтеграція кіберзахисту інформаційних технологій

Усі дії щодо КЗ інформаційних технологій будуть більш ефективними, якщо їх застосовують одночасно в усій організації і з самого початку кожного життєвого циклу системи інформаційних технологій. Процес КЗ інформаційних технологій – це важливий окремий цикл діяльності, який повинен бути інтегрований в усі стадії життєвого циклу системи інформаційних технологій. КЗ найефективніший, якщо його інтегрують у нові системи з самого початку, успадковані системи та їхня діяльність мають користь від інтеграції КЗ протягом усього періоду.

Життєвий цикл системи інформаційних технологій може бути поділений на три базові стадії. Кожна з цих стадій стосується безпеки інформаційних технологій таким чином:

• проектування: КЗ інформаційних технологій треба враховувати протягом усього процесу проектування та прийняття рішень щодо діяльності організації;

• комплектація: вимоги КЗ інформаційних технологій потрібно інтегрувати в процеси проектування, розробки, придбання, оновлювання або в інші конструктивні зміни системи. Інтегрування вимог захисту в ці процеси гарантує оптимальність вартісно-ефективних показників засобів КЗ, задіяних у системі, а також їхню своєчасність і відсутність наслідків;

• дії: КЗ інформаційних технологій необхідно інтегрувати в оперативне середовище. Система інформаційних технологій, яку використовують для виконання визначеної функції, звичайно зазнає ряд оновлень, які охоплюють закупівлю нових апаратних компонентів, зміни або доповнення програмного забезпечення. Крім того, часто змінюється оперативне середовище. Зміни в оточенні (середовищі) можуть створювати нові вразливості системи, які треба аналізувати, оцінювати і відповідно коригувати або сприймати. Також є важливим призначення або зняття захищеності системи.

Убезпечування інформаційних технологій – безперервний процес з багатьма зворотними зв’язками всередині і між стадіями життєвого циклу системи інформаційних технологій. Повний зворотний зв’язок був показаний на рисунок 17.1. У більшості випадків зворотний зв’язок пронизує всю основну діяльність процесу КЗ інформаційних технологій. Це забезпечує

безперервний потік інформації щодо виявлення уразливості, загроз і засобів КЗ системи інформаційних технологій протягом усіх трьох стадій життєвого циклу системи інформаційних технологій.

Також варто зазначити, що кожна зі сфер діяльності організації може визначити унікальні вимоги щодо КЗ інформаційних технологій. Ці сфери повинні взаємно зміцнювати одна одну і весь процес КЗ інформаційних технологій, спільно використовуючи інформацію про стан КБ, що, в свою чергу, може впливати на процес прийняття управлінських рішень.

17.2. Методика безпеки інформаційних технологій

Цілі (які повинні бути досягнуті), стратегії (як досягнути цих цілей) і методики (правила для досягнення цілей) можна визначити для кожного рівня організації і для кожного ділового підрозділу чи відділу. Для досягнення ефективної КБ інформаційних технологій необхідно впорядкувати різні цілі, стратегії і методики для кожного організаційного рівня і ділового підрозділу. Узгодженість між відповідними документами, незважаючи на вплив різних точок зору, дуже важлива, оскільки більшість загроз (таких як злом системи, знищення файлів і пожежі) – загальні проблеми ділової активності.

Взаємозв'язки методик

Методика КБ інформаційних технологій може бути внесена до корпоративного технологічного й методологічного керування, і все це разом формує основу для загальних стратегічних положень в інформаційних технологіях. Ці положення повинні містити певні вагомі твердження на користь КЗ, особливо якщо є необхідність узгодження захисту і стратегії. Рисунок 17.2 показує залежність між різними методиками. Незалежно від документації та адміністративної структури, використованої організації, дуже важливо, щоб різні положення описаних методик, для підтримки узгодженості, були однаково спрямовані.

Інші методики КЗ інформаційних технологій необхідні для певних систем і служб або для групи систем інформаційних технологій і служб. Їх, зазвичай, описують як методики КЗ систем інформаційних технологій. Це важливий аспект керування, оскільки їхній контекст і межі чітко визначені та обґрунтовані діловими і технологічними підставами.

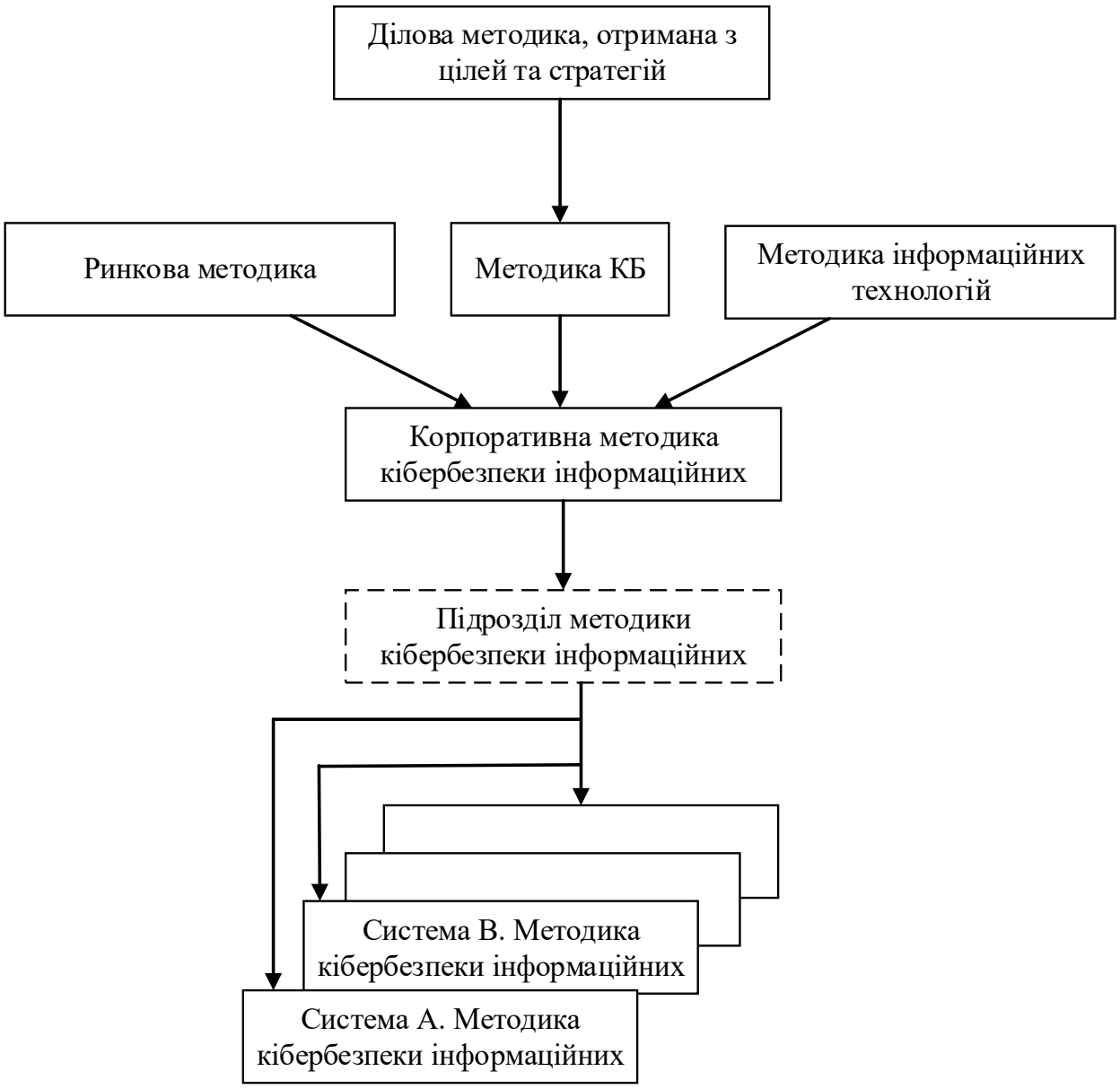


Рисунок 17.2. Залежності між різними методиками

Елементи методики кібербезпеки інформаційних технологій

Методика безпеки повинна охоплювати, принаймні, такі розділи:

- вимоги КБ інформаційних технологій (умови конфіденційності, цілісності, доступності, обліковості, достовірності і надійності, особливо з урахуванням уявлень власників активів);
- інфраструктура організації і розподіл обов'язків;
- інтеграція КЗ в розробці і реалізації системи;
- директиви і процедури;
- визначання класів для класифікації інформації;
- стратегії керування ризиком;

- планування непередбачуваних обставин;
- підготовка персоналу (особлива увага повинна приділятися службовцям відповідних посад, наприклад, технічному персоналу й адміністраторам системи);
- компетентність і навчання;
- юридичні і регуляторні зобов'язання;
- зовнішнє керування й інформаційна взаємодія;
- реакція на інциденти.

17.3. Організаційні аспекти кібербезпеки інформаційних технологій

Функції та обов'язки

КБ інформаційних технологій є міжгалузевою темою і стосується кожного проекту інформаційних технологій, системи і всіх користувачів інформаційних технологій в організації. Відповідний розподіл посад і розмежування обов'язків гарантують, що всі важливі завдання будуть успішно й ефективно виконані.

Цієї мети досягають за допомогою різних організаційних заходів залежно від розміру та структури організації. У кожній конкретній організації мають існувати такі структури:

- рада з КБ інформаційних технологій, яка підсумовує міжгалузеві досягнення та затверджує директиви і стандарти;
- контролер (головний) КБ інформаційних технологій, який діє як центральна ланка всіх аспектів КБ інформаційних технологій в організації.

Як рада з КБ інформаційних технологій, так і контролер КБ інформаційних технологій повинні мати добре визначені та однозначні обов'язки і мати достатній вплив, щоб гарантувати прив'язку до методології КБ інформаційних технологій. Організація повинна забезпечити надійний зв'язок між контролером КБ інформаційних технологій, радою з КБ інформаційних технологій і представниками інших підрозділів в організації, а також визначити повноваження й відповідальність контролера КБ інформаційних технологій. Ці обов'язки повинні бути схвалені радою з КБ інформаційних технологій. Перелік цих обов'язків може бути доповнений шляхом зовнішніх консультацій.

Рисунок 17.3 показує типовий приклад зв'язків між контролером КБ інформаційних технологій, радою з КБ інформаційних технологій і представниками таких підрозділів в організації, як інші відділи КБ, товариства користувачів і персонал інформаційних технологій. Ці стосунки можуть полягати як у безпосередньому керуванні, так і у функціонуванні.

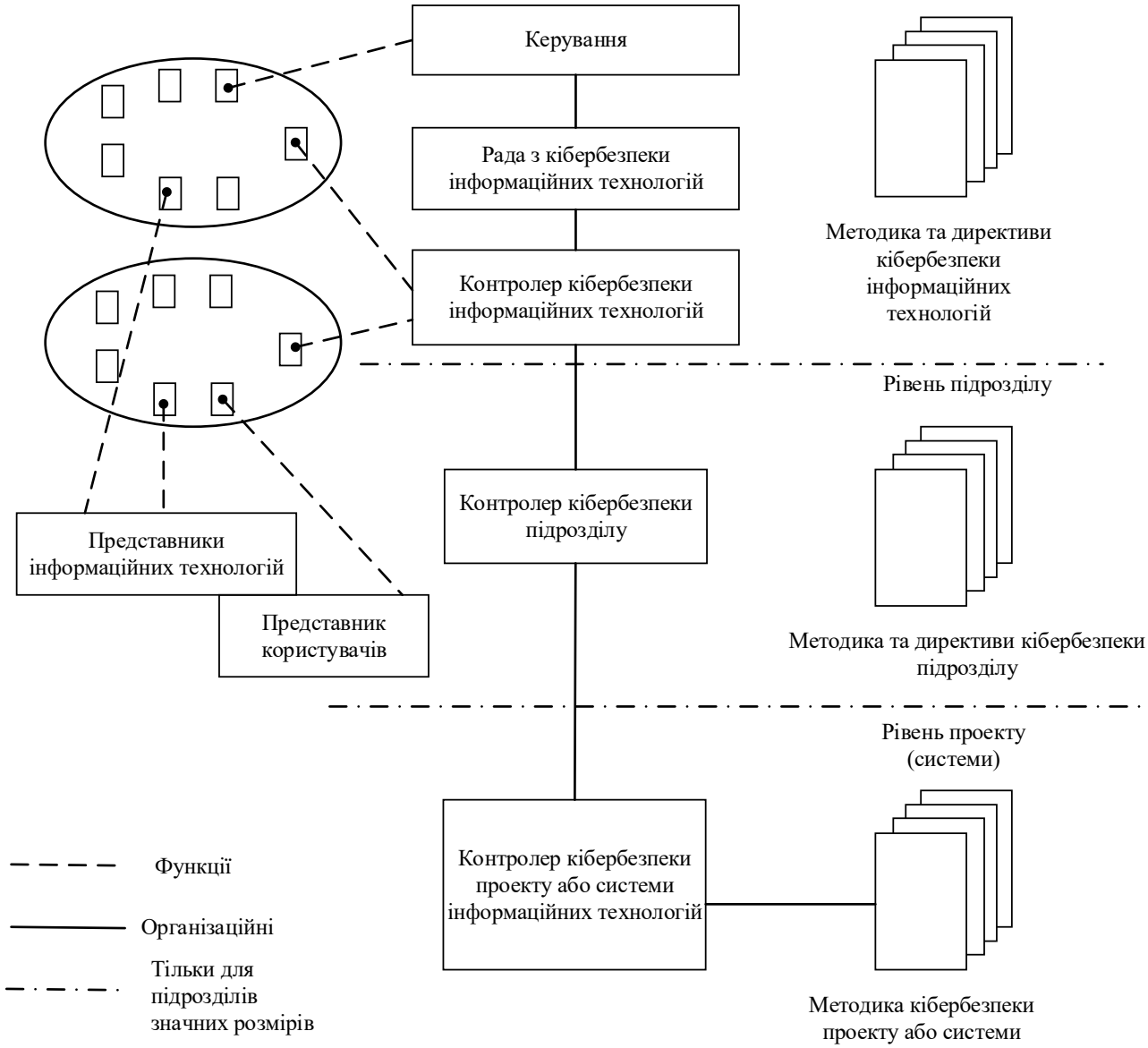


Рисунок 17.3. Приклад організації КБ інформаційних технологій

Наприклад, для організації КБ інформаційних технологій, зображеної на рис. 17.3, використовуються три організаційних рівні. Їх можна легко пристосувати до будь-якої організації, додаючи або вилучаючи відповідні рівні згідно з потребами організації. Невеликі й середні організації можуть мати контролера КБ інформаційних технологій, чиї обов'язки охоплюють всі питання, пов'язані з КБ. Коли функції тісно залежать одна від одної, важливо забезпечити відповідні перевірки й утримання рівноваги, щоб уникнути концентрації дуже великої кількості обов'язків у однієї особи, без можливості впливу на неї або контролю за нею.

Рада з безпеки інформаційних технологій

Така рада складається з персоналу необхідного рівня кваліфікації для визначання вимог, розробки методик, складання програми КЗ, аналізу здобутків та видачі вказівок (завдань, рекомендацій) контролеру КБ інформаційних технологій. Для цього може використовуватися вже існуюча рада, або має бути створена окрема рада з КБ інформаційних технологій. Ця рада може створюватися в існуючій структурі. В обов'язки ради з КБ інформаційних технологій входить:

- повідомлення керівного комітету інформаційних технологій про стратегічні плани з КБ;
- розробка корпоративної методики КБ інформаційних технологій в межах підтримки всієї стратегії інформаційних технологій і затвердження її керівним комітетом інформаційних технологій;
- перенесення методик КБ інформаційних технологій у програму КБ інформаційних технологій;
- контроль застосування програми КЗ до інформаційних технологій;
- контроль ефективності методик КБ інформаційних технологій;
- підтримування компетентності щодо проблем КБ інформаційних технологій;
- надання консультацій з питань персоналу, фінансів, інформації, знань, іншого, необхідними для підтримування процесів проектування та застосування програми КЗ інформаційних технологій.

Для максимальної ефективності роботи в раду повинні входити спеціалісти з базовою підготовкою з захисту і технічних аспектів системи інформаційних технологій, а також представники постачальників послуг і користувачів системи. Знання і кваліфікація в усіх цих галузях необхідні для розробки практичних методик КБ інформаційних технологій.

Контролер кібербезпеки інформаційних технологій

Оскільки відповідальність за КБ інформаційних технологій розподілена, то існує ризик, що в результаті ніхто не буде відчувати відповідальності взагалі. Щоб уникнути цього, повинен бути призначений відповідальний за всі питання КБ інформаційних технологій. Контролер КБ інформаційних технологій повинен діяти як центральна ланка щодо всіх аспектів КБ інформаційних технологій в організації. Для цього може бути задіяна вже наявна посада, з додатковими обов'язками, або, що найчастіше доцільно, необхідна окрема посада. Треба надавати перевагу особі, що вже має базовий рівень підготовки з питань КЗ інформаційних технологій.

Головні обов'язки контролера КБ інформаційних технологій [53,54]:

- нагляд за реалізацією програми КЗ інформаційних технологій;
- зв’язок і звітування перед органом з КБ інформаційних технологій;
- підтримка корпоративних методик КЗ інформаційних технологій і директив;
- координація розслідувань інцидентів;
- керування ходом проведення програми компетентності КБ на рівні корпорації;
- визначення компетенції системних контролерів КБ проекту (і, за наявності, відповідних контролерів КБ підрозділів інформаційних технологій).

Контролер кібербезпеки проекту інформаційних технологій і контролер кібербезпеки системи інформаційних технологій

Індивідуальні проекти або системи повинні мати відповідального за КЗ, якого називають контролером КБ інформаційних технологій. У деяких випадках це може бути посада за сумісництвом. Обов’язок керування цими контролерами входить до компетенції контролера КБ інформаційних технологій (або, де можливо, контролера підрозділу КБ інформаційних технологій). Контролер КБ в цьому випадку діє як головна ланка всіх аспектів КЗ проекту, системи або групи систем. Головні обов’язки цих посадовців:

- зв’язок та підзвітність корпоративному контролеру КБ (або, де можливо, контролеру підрозділу КБ інформаційних технологій);
- ініціювання і підтримка проекту або методики КЗ системи інформаційних технологій;
- розробка і реалізація проекту безпеки;
- щоденний контроль реалізації та використання захисних засобів інформаційних технологій;
- ініціювання і допомога в запобіганні інцидентам.

Відповідальність

Відповідальність є необхідною для забезпечення ефективного КЗ в інформаційних технологіях, якщо керування на різних рівнях забезпечується зусиллями конкретних осіб. Бізнесова відповідальність охоплює і цілі КБ інформаційних технологій, а саме:

- розуміння глобальних потреб організації;
- розуміння необхідності КЗ інформаційних технологій в організації;
- пояснення зобов’язань щодо КЗ інформаційних технологій;

- готовність приділяти увагу потребам КЗ інформаційних технологій;
- готовність розподіляти ресурси для КЗ інформаційних технологій;
- обізнаність на найвищому рівні, що таке засоби КЗ інформаційних технологій або їхні складові (межі, обсяг).

Цілі КБ інформаційних технологій повинні бути оголошені для всієї організації. Кожний службовець чи субпідрядник повинен знати свої функції та обов'язки, їхній вплив на захист інформаційних технологій і активно брати участь у досягненні цих цілей.

Послідовний підхід

Послідовний підхід до КЗ інформаційних технологій треба застосовувати до процесів проектування, експлуатації й оновлення. КЗ повинен бути невід'ємним складником протягом усього життєвого циклу інформації і системи інформаційних технологій від проектування до знищення.

Організаційна структура, показана на рис. 17.3, може підтримувати узгоджений підхід до КЗ інформаційних технологій у межах організації. Це, однак, потребує прив'язки до стандартів, охоплюючи міжнародні, національні, регіональні, промислові і корпоративні стандарти або правила, які вибирають і застосовують згідно з потребами КЗ інформаційних технологій організації. Технічні стандарти повинні бути доповнені правилами і рекомендаціями щодо їх впровадження, використання і керування ними.

Переваги використання стандартів такі:

- інтегрованість захисту;
- здатність до взаємодії;
- послідовність;
- мобільність;
- економність розмірів (шкали затрат);
- взаємодія між організаціями.

17.4. Рекомендації щодо кіберзахисту інформаційних технологій

Будь-який з підходів повинен надати мінімальний набір рекомендацій для доведення ризику до допустимого рівня. Ці рекомендації повинні бути схвалені адміністрацією та охоплювати:

- критерії для визначення допустимих рівнів ризиків для систем розглянутих інформаційних технологій;
- вибір засобів захисту, які доводять ризики до припустимого рівня;

- переваги, отримані внаслідок застосування цих засобів захисту, і значне зниження ризиків;
- приймання ризиків, що залишаються після застосування всіх засобів захисту.

Вибір засобів кіберзахисту

Є декілька типів засобів КЗ: ті, які попереджають, зменшують, контролюють, виявляють або виправляють небажані інциденти, і ті, які відновлюють засоби КЗ після небажаних інцидентів. Запобігання може охоплювати засоби, які стримують небажані дії і забезпечують краще розуміння захисту. Основні сфери, де можна застосовувати відповідні захисні засоби, і деякі приклади для кожної сфери такі:

- апаратні засоби (резервне копіювання, ключі);
- програмне забезпечення (електронні підписи, реєстрація, антивірусні засоби);
- зв'язок (мережеві пристрої захисту (firewall), кодування інформації);
- фізичне оточення (захисні споруди, контрольні пункти);
- персонал (компетентність персоналу, процедури для швидкого анулювання доступу службовця);
- адміністрування (повноваження, розподіл апаратних засобів, ліцензоване керування).

Засоби КЗ не є незалежними один від одного, і їх часто використовують спільно. Процес вибору повинен враховувати залежність засобів КЗ. У процесі вибору засобів КЗ треба також перевіряти, чи не залишилися прогалини. Такі прогалини роблять можливим обхід наявних засобів КЗ і дають змогу випадковим загрозам викликати пошкодження.

Для нових систем або для тих, де зроблені корінні зміни, вибір засобів захисту повинен враховувати структуру захисту. Структура захисту є частиною загальної структури системи і відображає наскільки задовольняються вимоги безпеки системи інформаційних технологій. Це також стосується і технічних засобів КЗ, навіть коли розглядають нетехнічні аспекти.

Усі засоби КЗ потребують уваги, щоб гарантувати ефективне використання. Багато засобів КЗ для досягнення ефективності потребують підтримки керівництвом. Ці чинники треба враховувати протягом всього процесу вибору засобів захисту.

Дуже важливо, щоб використання засобів КЗ було ефективним і не викликало зайвого втручання користувача або органу керування. Якщо засоби КЗ спричиняють істотні зміни, то їх застосування потрібно враховувати в програмі компетентності КЗ, а також у керуванні змінами і налаштуванням системи.

Врахування ризику

Після застосування вибраних засобів КЗ завжди буде існувати залишковий ризик. Це пов'язано з принциповою неможливістю побудови абсолютно захищеної системи, а також з тим, що деякі активи, можливо, залишаються навмисно незахищеними (наприклад, через низький ризик або високі витрати на засоби КЗ порівняно з розрахунковою вартістю активів, які треба захищати).

Перший крок процесу врахування ризику полягає в оцінцюванні вибраних засобів КЗ, в ідентифікації і визначенні всіх залишкових ризиків. Наступний крок повинен кваліфікувати залишкові ризики як такі, що «можуть бути допущеними», і такі, що «не можуть бути допущеними» організацією.

Очевидно, що неприйнятні ризики не можна допускати і тому необхідні додаткові засоби КЗ, що обмежують ураження або наслідки ризиків. У кожному з цих випадків необхідно прийняти відповідне рішення.

Або ризик треба оцінювати як допустимий, або необхідні додаткові витрати на засоби КЗ, які понизять ризик до припустимого рівня.

17.5. Методика кіберзахисту системи інформаційних технологій

Методики, які розробляються для КЗ системи інформаційних технологій, повинні ґрунтуватись на методиці захисту системи. Ці методики КЗ системи містять багато принципів і правил для убезпечування систем і служб. Методики повинні бути реалізовані у вигляді застосування відповідних засобів КЗ систем і служб, щоб гарантувати, що досягнуто належний рівень захисту.

Методики захисту системи інформаційних технологій повинні бути затверджені вищим керівництвом як обов'язкові набори принципів і правил, щоб гарантувати використання фінансових та трудових ресурсів за призначенням.

Ключові моменти, які треба враховувати під час визначання кожної методики КЗ системи інформаційних технологій, так і:

- визначення характеристик системи інформаційних технологій і її меж;

• визначення бізнесових цілей, яких буде досягнуто системою, оскільки вони можуть впливати на методику КЗ системи, на вибір і застосування засобів КЗ;

• визначення потенційно несприятливих уражень від:

• недоступності, відмови або знищення допоміжних чи основних активів, також інформації;

• несанкціонованої зміни інформації або програмного забезпечення;

• несанкціонованого розголошування даних з наслідками, що їх вимірюють кількісно, такими як прямі або непрямі фінансові втрати, а також з такими якісними наслідками, як втрата престижу, інформації, що викликає збитки або небезпеку, порушення особистої конфіденційності;

• рівень інвестування в інформаційні технології;

• існування істотних загроз системі інформаційних технологій та оброблюваній інформації;

• уразливість через слабкі місця, які дозволяють ідентифікованим загрозам впливати на системи інформаційних технологій;

• необхідність засобів КЗ, адекватних ідентифікованим ризикам;

• витрати на захист в інформаційних технологіях, тобто витрати на КЗ активів інформаційних технологій (кошти, вкладені в захист інформаційних технологій, треба розглядати як частину капіталу власника системи інформаційних технологій);

• структура принципів вибору зовнішніх провайдерів (наприклад, обчислювальні центри, обслуговування інформаційних систем).

КЗ інформаційних технологій вимагає планового підходу і не повинен розглядатися окремо. Це має бути головним питанням у процесі стратегічного планування для гарантування, що захист був запланований та інтегрований в систему з самого початку.

17.6. Впровадження засобів кіберзахисту інформаційних технологій

Після затвердження проекту КБ інформаційних технологій необхідно його впровадити. Як правило, за це відповідає системний контролер КБ інформаційних технологій. У процесі застосування засобів КЗ досягнення цілей повинні гарантуватись такі аспекти:

• вартість засобів КЗ повинна залишитись у прийнятих межах;

• засоби КЗ використовують відповідно до вимог проекту КБ;

• використання і керування засобами КЗ повинно відповідати вимогам проекту КБ інформаційних технологій.

Більшість технічних засобів КЗ потребує експлуатаційного та адміністративного регламентування, їх не можна використовувати як звичайні технічні засоби. Відповідні інструкції повинні бути підтримані і впроваджені керівництвом.

Заходи КБ охоплюють і навчання задіяного персоналу, компетентного у питаннях захисту, а саме:

• персоналу, відповідального за впровадження системи інформаційних технологій;

• персоналу, відповідального за експлуатацією системи інформаційних технологій;

• контролерів КБ проекту і системи інформаційних технологій;

• персоналу, відповідального за керування КБ, наприклад за контролювання доступу.

Після реалізації плану КБ інформаційних технологій треба формально затвердити застосування засобів КБ, зазначених у проекті КБ системи інформаційних технологій. Після затвердження дозвіл передають в систему інформаційних технологій або послуги вводять в дію. Процес затвердження в деяких комітетах проводять як акредитацію.

Будь-які істотні зміни в системі інформаційних технологій або послугах повинні викликати повторну перевірку, повторні випробовування і затвердження системи інформаційних технологій або послуг.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

• Наведіть контрольні питання політики інформаційної безпеки.

• Наведіть контрольні питання організації КБ.

• Наведіть контрольні питання з захисту доступу сторонніх організацій.

• Наведіть контрольні питання класифікації і управління активами.

• Наведіть контрольні питання класифікації інформації.

• Наведіть контрольні питання реагування на інциденти безпеки.

• Наведіть контрольні питання фізичного захисту і захисту середовища.

• Наведіть контрольні питання з безпеки обладнання.

• Наведіть контрольні питання загальних засобів безпеки.

• Наведіть контрольні питання управління діяльністю.

• Наведіть контрольні питання операційних процедур та відповідальність.

• Наведіть контрольні питання планування потужності і приймання систем.

• Наведіть контрольні питання з захисту від зловмисного коду.

• Наведіть контрольні питання управління мережею.

• Наведіть контрольні питання управління доступом.

• Наведіть контрольні питання у правління доступом працівників.

РОЗДІЛ 18. КЕРУВАННЯ КІБЕРЗАХИСТОМ ІНФРМАЦІЙНИХ ТЕХНОЛОГІЙ

Після оцінювання ризику визначають відповідні засоби захисту для кожної системи інформаційної технології, щоб привести ризики до допустимого рівня. Ці засоби захисту впроваджують відповідно до плану безпеки інформаційних технологій. Застосування повинне підтримуватися програмою компетентності і навчання персоналу, які важливі для ефективності засобів захисту.

18.1. Підходи та рекомендації щодо кіберзахисту інформаційних технологій

Будь-який з підходів повинен надати мінімальний набір рекомендацій для доведення ризику захисту до допустимого рівня. Ці рекомендації повинні бути схвалені адміністрацією і включати:

- критерії для визначення допустимих рівнів ризиків для систем інформаційних технологій, що розглянуті;
- вибір засобів захисту, які доводять ризики до припустимого рівня;
- переваги, отримані внаслідок застосування цих засобів захисту, і значне зниження ризиків;
- врахування залишкового ризику, що залишається після застосування всіх засобів захисту.

Ідентифікація наявних і/або вибір запланованих засобів захисту

Засоби захисту, ідентифіковані після аналізування ризику, повинні бути доповненням до вже наявних і запланованих засобів захисту. Важливо, щоб наявні і заплановані засоби захисту були визначені як частина цього процесу, щоб уникнути непотрібної роботи чи витрат, наприклад, під час дублювання засобів захисту. Може виявитися, що для наявних чи запланованих засобів захисту немає обґрунтувань. У цьому випадку потрібно перевірити, чи засіб захисту потрібно вилучити і замінити іншим, більш підхожим, чи треба лишити його для подальшого виконання своїх функцій (наприклад через вартість).

Крім того, треба виконати перевірку, щоб установити після аналізу ризику, чи сумісні обрані засоби захисту з наявними і запланованими засобами захисту, тобто, що обрані та наявні засоби захисту не суперечать один одному.

Під час визначення наявних засобів захисту треба перевірити, чи правильно вони функціонують. Якщо захисний засіб, на який покладено певну функцію захисту, не функціонує в процесі ділової активності, він є джерелом можливої вразливості.

Результат цього кроку – перелік всіх наявних і запланованих засобів захисту і стан їх впровадження і використовування.

Існує декілька типів засобів захисту: ті, які попереджають, зменшують, контролюють, виявляють або виправляють небажані інциденти, і ті, які відновлюють після них. Запобігання може охоплювати засоби, що стримують небажані дії і що забезпечують краще розуміння захисту. Основні сфери, де можна застосовувати відповідні захисні засоби, і деякі приклади для кожної сфери такі:

- апаратні засоби (резервне копіювання, ключі);
- програмне забезпечення (електронні підписи, реєстрація, антивірусні засоби);
- зв’язок (мережні пристрої захисту (firewall), кодування інформації);

- фізичне оточення (огороджувальні споруди, контрольні пункти);
- персонал (компетентність персоналу, процедури для швидкого анулювання доступу службовця);
- адміністрування (повноваження, розподіл апаратних засобів, ліцензоване керування).

Засоби захисту не є незалежними один від одного, і їх часто використовують спільно. Процес вибирання повинен враховувати залежність засобів захисту. У процесі вибирання засобів захисту треба також перевіряти, чи не залишилося прогалин. Такі прогалини роблять можливим обхід наявних засобів захисту і дають змогу випадковим загрозам викликати пошкодження.

Для нових систем або для тих, де зроблені корінні зміни, вибирання засобів захисту повинно враховувати структуру захисту. Структура захисту є частиною загальної структури системи і відображає, наскільки задовольняються вимоги безпеки системи інформаційних технологій. Це також стосується і технічних засобів захисту, навіть коли розглядають нетехнічні аспекти.

Усі засоби захисту вимагають уваги, щоб гарантувати ефективне використання. Багато засобів захисту вимагають підтримки керівництвом для досягнення ефективності. Ці чинники треба враховувати протягом всього процесу вибирання засобів захисту.

Дуже важливо, щоб використання засобів захисту було ефективним і не викликало зайвого втручання користувача або органу керування. Якщо засоби захисту спричинюють істотні зміни, то їх застосування потрібно враховувати в програмі компетентності захисту, а також у керуванні змінами і настроюванням системи.

Врахування ризику

Після застосування вибраних засобів захисту завжди буде існувати залишковий ризик. Це пов’язано з принциповою неможливістю побудови абсолютно захищеної системи, а також з тим, що деякі активи, можливо,

залишаються навмисно незахищеними (наприклад, через низький ризик або високі витрати на засоби захисту порівняно з розрахунковою вартістю активів, які треба захищати).

Перший крок процесу врахування ризику полягає в оцінюванні вибраних засобів захисту, в ідентифікації і визначенні всіх залишкових ризиків. Наступний крок повинен кваліфікувати залишкові ризики як такі, що "можуть бути допущеними", і такі, що "не можуть бути допущеними" організацією.

Очевидно, що неприйнятні ризики не можна допускати і тому необхідні додаткові засоби захисту, що обмежують ураження або наслідки ризиків. У кожному з цих випадків необхідно прийняти відповідне рішення. Або ризик тре-ба оцінювати як допустимий, або необхідні додаткові витрати на засоби захисту, які знизять ризик до припустимого рівня.

18.2. Методика захисту системи інформаційних технологій

Методики, які розробляються для захисту системи інформаційних технологій, повинні ґрунтуватись на методиці захисту системи. Ці методики захисту системи містять багато принципів і правил для убезпечування систем і служб. Методики повинні бути реалізовані у вигляді застосування відповідних засобів захисту до систем і служб, щоб гарантувати, що досягнуто належного рівня захисту.

Методики захисту системи інформаційних технологій повинні бути затверджені вищим керівництвом як обов’язкові набори принципів і правил, щоб гарантувати, що фінансові і трудові ресурси використовують за призначенням.

Ключові моменти, які треба враховувати під час визначання кожної методики захисту системи інформаційних технологій:

- визначання характеристик системи інформаційних технологій і її меж;

- визначання бізнесових цілей, яких буде досягнуто системою, оскільки вони можуть впливати на методику захисту системи, на вибір і застосування засобів захисту;
- потенційно несприятливі ураження від:
    - недоступності, відмови або знищення допоміжних, або основних активів, включаючи інформацію;
    - несанкціонованої зміни інформації або програмного забезпечення;
    - несанкціонованого розголошування даних, з наслідками, що їх вимірюють кількісно, такими як прямі або непрямі фінансові втрати, а також із наслідками якісними, такими як втрата престижу, інформації, що викликає збитки або небезпеку, порушення особистої конфіденційності;
- рівень інвестування в інформаційні технології;
- істотні загрози системі інформаційних технологій та оброблюваній інформації;
- уразливості через слабкі місця, які дозволяють ідентифікованим загрозам впливати на системи інформаційних технологій;
- необхідність засобів захисту, адекватних ідентифікованим ризикам;
- витрати на захист в інформаційних технологіях, тобто витрати на захист активів інформаційних технологій (кошти, вкладені в захист інформаційних технологій, треба розглядати як частину капіталу власника системи інформаційних технологій);
- структура принципів вибору зовнішніх провайдерів (наприклад, обчислювальні центри, обслуговування інформаційних систем).

Захист інформаційних технологій вимагає планового підходу і не повинен розглядатися окремо. Це має бути головним питанням у процесі стратегічного планування для гарантування, що захист був запланований та інтегрований в

систему спочатку. У більшості випадків затримка в застосуванні засобів захисту призводить до більших витрат або стає непрактичним.

18.3. План кіберзахисту інформаційних технологій

План захисту або кіберзахисту інформаційних технологій – документ, який визначає узгоджені заходи, які необхідно здійснити для реалізації методики захисту системи інформаційних технологій. Цей план повинен включати короткі, середні і довго тривкі першорядні заходи з відповідними капіталовкладеннями, строками фінансування, вартістю експлуатації, навантаженнями тощо, а також графіком впровадження. Він повинен містити:

- повну структуру і проєкт захисту;
- короткий розгляд системи інформаційних технологій для узгодження з задачами захисту організації, відображеними в термінах максимальних фінансових втрат, утруднень, іміджу організації тощо;
- визначення засобів захисту, підтриманих і затверджених вищим керівництвом згідно оцінених ризиків;
- оцінку фактичного рівня впевненості в засобах захисту, згідно визначання їхньої ефективності;
- аналіз оцінок залишкового ризику в аспекті системи або її використання;
- ідентифікацію і визначення пріоритетності заходів для впорядкованості впровадження засобів захисту;
- детальний робочий план впровадження засобів захисту, враховуючи пріори-тети, фінансування і часовий графік;
- дії з керування проєктом, що включають:
  - розподіл ресурсів, обов’язків і відповідальності;
  - визначання процедур звітності про хід роботи;

- компетентність у захисті і вимоги до навчання персоналу інформаційних технологій та кінцевих користувачів;
- вимоги до умов експлуатації засобів захисту і процедур керування.

Крім того, план повинен охоплювати заходи, що визначають умови і дії із затвердження кожного з вище перерахованих положень, включаючи і внесення змін до плану.

18.4. Впровадження засобів кіберзахисту

Після затвердження проєкту безпеки інформаційних технологій необхідно його впровадити. Як правило, за це відповідає системний контролер безпеки інформаційних технологій. У процесі застосування засобів захисту досягнення цілей повинно гарантувати, що:

- вартість засобів захисту повинна залишитись у прийнятих межах;
- засоби захисту використовують відповідно до вимог проєкту безпеки;
- використання і керування засобами захисту повинно відповідати вимогам проєкту безпеки інформаційних технологій.

Більшість технічних засобів захисту потребують експлуатаційного й адміністративного регламентування, їх не можна використовувати як звичайні технічні засоби. Відповідні інструкції повинні бути підтримані і впроваджені керівництвом.

Обізнаність в питаннях захисту (компетентність у захисті) і навчання також включають у заходи безпеки. Оскільки весь персонал повинен бути обізнаним у захисті, потрібно провести навчання:

- персоналу, відповідального за впровадження системи інформаційних технологій;
- персоналу, відповідального за експлуатацією системи інформаційних технологій;

- контролерів безпеки проєкту і системи інформаційних технологій;
- персоналу, відповідального за керування безпекою, наприклад за контролювання доступу.

Після реалізації плану безпеки інформаційних технологій треба формально затвердити застосування засобів захисту, зазначених у проєкті безпеки системи інформаційних технологій. Після затвердження дозвіл передають у систему інформаційних технологій або послуги вводять в дію. Процес затвердження в деяких комітетах проводять як акредитацію.

Будь-які істотні зміни в системі інформаційних технологій або послугах повинні викликати повторну перевірку, повторні випробовування і затвердження системи інформаційних технологій або послуг.

18.5. Компетентність у кіберзахисті

Програму компетентності у кіберзахисті треба застосовувати до всіх рівнів організації, від вищого керівництва до користувачів. Без участі персоналу на рівні користувачів програма компетентності у захисті не може бути успішною. Користувачі повинні розуміти своє значення в успіху програми.

Програма компетентності повинна враховувати методики безпеки інформаційних технологій і забезпечувати однозначне розуміння рекомендацій із захисту і відповідних дій. Крім того, програма компетентності у захисті повинна охоплювати цілі проєктів захисту системи. Програма повинна включати принаймні такі розділи:

- основні вимоги захисту інформації;
- залучення користувачів до аналізування інцидентів у безпеці, як і організації в цілому;
- перелік цілей, роз’яснення методик захисту інформаційних технологій та стратегії керування ризиком, інструкції щодо обізнаності з ризиками і засобами захисту;

- плани безпеки інформаційних технологій із застосування і перевірки засобів захисту;
- класифікація інформації;
- обов’язки власників даних;
- обов’язки користувачів, опис задач і процедур;
- необхідність у звітності і розслідуванні порушень безпеки або спроб порушень;
- наслідки некомпетентних дій (включно з дисциплінарними заходами);
- перевірка сумісності захисту;
- керування змінами і настройкою.

Для досягнення ефективності програми компетентності у захисті потрібно використовувати широкий спектр носіїв, наприклад брошури, довідники, плакати, відео, інформаційні листи, практичні вправи, семінари і лекції. Дуже важливо, щоб реалізація програми компетентності враховувала соціальні, культурні і психологічні аспекти значення захисту.

Компетентність у захисті стосується кожного працівника організації і повинна впливати на поведінку та відповідальність усіх працівників. Головним чинником є розуміння адміністрацією потреби у захисті. Адміністративний апарат повинен гарантувати компетентність персоналу у захисті. Тому він повинен планувати відповідні статті в бюджеті. У великих організаціях відповідальність за компетентність у захисті інформаційних технологій треба покласти на контролера безпеки інформаційних технологій. Метою програми компетентності є також необхідність переконати всіх причетних осіб у важливості ризиків для системи інформаційних технологій і в можливих інформаційних втратах або несанкціонованій зміні чи розкритті, які можуть призвести до тяжких наслідків для організації та її службовців.

Для покращення роботи необхідно організовувати навчання з врахуванням реальних умов роботи організації. Необхідно наводити релевантні приклади, які ґрунтуються на реальних випадках в організації, що покращує розуміння суті і розмірів уражень більше, ніж опис цього в засобах інформації. Такі навчання також дають змогу службовцям оптимально взаємодіяти з викладачем. Розуміння службовцями засобів захисту треба контролювати для визначення ефективності процесу підвищення компетентності у захисті і для оцінювання змісту цього процесу. Якщо результат не задовольняє, зміст процесу підвищення компетентності захисту потрібно відповідно коригувати.

Навчання з підвищення компетентності у захисті треба періодично повторювати, щоб оновити знання діючого персоналу й інформувати новий. Крім того, кожний новий службовець чи особа, що здійснила переміщення по службі, або кандидат на посаду повинні бути ознайомлені зі своїми новими обов'язками. Бажано також інтегрувати питання захисту інформаційних технологій в інші навчальні курси. Варто також підкреслити, що компетентність у захисті – це тривалий процес, який ніколи не є повністю завершеним.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

- Чим установлюється порядок проведення робіт з технічного захисту інформації або окремих їхніх етапів?
- Що є метою обстеження організації?
- Ким повинно бути проведено обстеження?
- Що необхідно зробити у ході обстеження?
- Що слід скласти за результатами обстеження?
- Які матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз?
- Що необхідно визначити на підставі матеріалів обстеження та окремої моделі загроз?

РОЗДІЛ 19. МЕТОДИ КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ

В розділі описано методи для успішного керування безпекою інформаційних технологій. Дані методи можна використовувати для визначання необхідних вимог захисту і ризиків; вони допомагають встановлювати і підтримувати відповідні засоби захисту, тобто забезпечувати необхідний рівень безпеки інформаційних технологій. Результати, що отримані таким способом, можна покращити додатковими засобами захисту, на вимогу самої організації та оточення. Це стосується кожного, хто відповідає за керування і (або) реалізацію безпеки інформаційних технологій в організації (ДСТУ ISO/IEC TR 13335-3:2003).

19.1. Методика керування кібербезпекою інформаційних технологій

Керування кібербезпекою інформаційних технологій складається з аналізування вимог захисту, створення плану дотримання цих вимог, виконання цього плану, а також із підтримання і керування здійсненим захистом. Цей процес починається з визначання організацією цілей і стратегій захисту в інформаційних технологіях і розробляння корпоративних методик захисту інформаційних технологій.

Важливою частиною процесу керування безпекою інформаційних технологій є оцінка ризиків і спосіб, яким їх можна привести до допустимого рівня. Необхідно брати до уваги ділові цілі, організаційні аспекти та пов’язані з оточенням і усі визначені вимоги і ризики системи інформаційних технологій.

Після визначення необхідних вимог захисту системи інформаційних технологій і її служб бажано вибрати стратегію аналізування ризику. Рекомендований вибір має керуватися аналізуванням ризику високого рівня для всіх систем інформаційних технологій, щоб ідентифікувати системи з високим ступенем ризику. Ці системи потім досліджують в процесі докладного аналізування ризику, у той час як для інших систем застосовують основний

підхід. Для систем з високим ступенем ризику докладний розгляд активів, загроз і вразливостей приводить до докладного аналізування ризику, що полегшує вибір ефективних засобів захисту у відповідності з оціненими ризиками. Використовуючи отримані показники, процес керування ризиком можна зосереджувати там, де істотні ризики чи високі вимоги, і вся програма може бути зроблена з найефективнішими вартісними і часовими показниками.

Після оцінювання ризику визначають відповідні засоби захисту для кожної системи інформаційної технології, щоб привести ризики до допустимого рівня. Ці засоби захисту впроваджують відповідно до плану безпеки інформаційних технологій. Застосування повинне підтримуватися програмою компетентності і навчання персоналу, які важливі для ефективності засобів захисту.

Крім того, керування безпекою інформаційних технологій містить постійне завдання займатися різною поточною діяльністю, яка може спричинити зміни в раніше отриманих результатах і рішеннях. Дії щодо доопрацювання охоплюють експлуатацію, перевірку надійності засобів захисту, керування змінами, контроль й обробку інцидентів.

19.2. Цілі і стратегії методики кібербезпеки інформаційних технологій

Після затвердження цілей безпеки інформаційних технологій організації потрібно розробити стратегію захисту інформаційних технологій, щоб сформувати основу для розробки методик захисту інформаційних технологій. Розробка корпоративних методик захисту інформаційних технологій повинна гарантувати, що результати процесу керування ризиком є придатними і ефективними. Підтримка процесу керування в усій організації необхідна для розробки й ефективного застосування методики. Найголовніше, щоб методика захисту інформаційної технології брала до уваги цілі і специфічні особливості організації. Вона повинна бути, узгодженою з методикою безпеки і методикою ділової активності. Після узгодження методика захисту інформаційної

технології може забезпечити найефективніше використання ресурсів і буде гарантувати несуперечливий підхід до захисту в усьому оточенні системи.

Може знадобитися розробка окремої спеціальної методики захисту для кожної чи деяких систем інформаційних технологій. Ця методика повинна базуватись на аналізуванні ризику або основних результатів і бути сумісною з методикою безпеки інформаційної технології, а також враховувати рекомендації щодо захисту системи, до якої вона відноситься.

Цілі кібербезпеки

На першому етапі в процесі керування кібербезпекою інформаційної технології треба розглянути питання, який діапазон ризиків є допустимим для організації. Вірно обраний рівень допустимості ризиків, і значить відповідний рівень захисту, є запорукою успішного керування кібербезпекою. Необхідний діапазон рівня захисту визначають цілями безпеки інформаційних технологій, які повинні задовольнити потреби організації. Щоб визначити цілі кібербезпеки, треба розглянути активи і їхню цінність для організації. Вони, головним чином, обумовлені тим, що інформаційні технології важливі для підтримування ділової активності в організації; витрати безпосередньо на інформаційні технології – тільки мала частина їхньої загальної цінності. Щоб оцінити, наскільки ділова активність організації залежить від інформаційних технологій, треба відповісти на наступні питання:

- наскільки важлива частина бізнесової діяльності, яка не може виконуватися без підтримки інформаційних технологій?
- які задачі можуть бути виконані тільки за допомогою інформаційних технологій?
- які важливі рішення залежать від точності, цілісності, доступності чи актуальності інформації, оброблюваної за допомогою інформаційної технології?
- яка оброблювана конфіденційна інформація потребує захисту?

- які приховані передумови небажаних інцидентів безпеки для організації?

Відповіді на ці питання можуть допомогти визначити цілі кібербезпеки організації. Якщо, наприклад, деякі важливі чи дуже важливі частини ділової активності залежать від точності чи актуальності інформації, то однією з цілей безпеки цієї організації є забезпечення цілісності і своєчасності інформації в процесі обробки в системі інформаційних технологій. Також під час оцінки цілей кіберзахисту необхідно врахувати важливість бізнесових аспектів і їхній зв’язок з безпекою.

Залежно від цілей кібербезпеки має бути погоджена стратегія для досягнення цих цілей. Обрана стратегія має відповідати важливості активів, що їх захищають. Якщо, наприклад, відповідь на одне чи кілька цих питань "так", то найймовірніше організація має важливі потреби в захисті і необхідно порекомендувати вибрати стратегію разом з необхідними заходами для реалізації цих потреб.

Стратегія безпеки інформаційних технологій тезисна і в загальних поняттях описує, як організація може досягти цілей безпеки інформаційних технологій. Положення, яких має стосуватися стратегія, будуть залежати як від кількості, типу і важливості цих цілей, так і тих цілей, які організація розглядає як важливі для усіх своїх підрозділів. Положення можуть бути або цілком конкретними або дуже загальними.

У випадку положення стратегії можуть полягати в тому, що всі системи затверджують як такі, безпечність яких визначає третя особа.

Інші можливі положення стратегії безпеки інформаційних технологій, згідно з визначеними цілями чи їхніми комбінаціями, можуть включати:

- стратегію аналізу ризику і методи, що будуть прийняті для всієї організації;

- вимоги методики безпеки системи інформаційних технологій для кожної системи;
- вимоги механізмів захисту для кожної системи;
- схему класифікації критичної інформації для всієї організації;
- вимоги щодо захисту засобів зв'язку; це повинно бути визначено і перевірено до установлення відносин з іншими організаціями;
- схему обробки інцидентів, універсальну у використанні.

Після визначення стратегія безпеки і її положення повинні міститися в методиці безпеки інформаційної технології.

Методика кібербезпеки інформаційних технологій

Методику кібербезпеки інформаційної технології треба створювати на підставі цілей і стратегій безпеки інформаційної технології. Її необхідно затвердити і підтримувати, узгоджуючи з діяльністю, безпекою і методиками інформаційних технологій, а також згідно із законодавчими положеннями та інструкціями.

Важливим фактом, що впливає на методику безпеки інформаційної технології, є залежність організації від використовуваної інформаційної технології. Чим важливішими є використовування інформаційної технології і ступінь залежності організації від неї, тим більший рівень захищеності необхідно забезпечити для реалізації ділових цілей. Під час створення методики безпеки інформаційної технології треба брати до уваги мікро політику, оточення і характеристики організації, тому що вони можуть впливати на підходи щодо безпеки, наприклад, деякі засоби захисту, що можуть бути легко сприйняті в одному оточенні, можуть бути цілком неприйнятні в іншому.

Залежно від захисту діяльність, що описана в методиці безпеки інформаційної технології, може базуватись на цілях і стратегії організації, результатах попереднього аналізу ризику безпеки та оглядах керування,

результатах додаткових заходів, таких як перевірка відповідності вимогам захисту реалізованих засобів захисту, контроль й аналіз захисту в щоденному використовуванні, і складання звітів про доречний захист від інцидентів. Будь-яку серйозну загрозу чи вразливість, виявлену в процесі цих дій, треба враховувати в корпоративній методиці безпеки інформаційної технології, що описує загальний підхід організації до проблем безпеки. Докладні дії описані в різних методиках захисту системи інформаційної технології чи в інших допоміжних документах, наприклад, у робочих процедурах захисту.

У розробці методики кібербезпеки інформаційної технології повинні брати участь представники таких напрямків:

- аудит;
- фінанси;
- інформаційні системи (фахівці і користувачі);
- господарчі структури (особи, відповідальні за приміщення, енергетику, кондиціювання повітря тощо);
- персонал;
- захист;
- старші бізнес-менеджери.

Відповідно до цілей кібербезпеки і стратегії, прийнятої організацією для досягнення цих цілей, вибирають відповідний рівень деталізації методики безпеки інформаційних технологій. Як мінімум, методика кібербезпеки інформаційної технології має описувати:

- галузь і призначення;
- цілі кібербезпеки щодо правових і регуляторних зобов’язань і бізнесових цілей;

- необхідні умови кіберзахисту інформаційної технології щодо конфіденційності, цілісності, доступності, обліковості, достовірності і надійності інформації;
- керування кіберзахистом інформації, з урахуванням обов'язків і повноважень організації та окремих осіб;
- підхід до керування ризиком, прийнятий організацією;
- спосіб, яким можуть бути визначені пріоритети для застосування засобів кіберзахисту;
- загальний рівень захисту і залишкового ризику, до якого прагне керівництво;
- будь-які загальні правила для контролювання доступу (логічний контроль доступу, а також керування фізичним доступом до споруд, кімнат, систем та інформації);
- підхід до компетентності персоналу в захисті і навчання в межах організації;
- різноманітні процедури для перевірки і підтримки захисту;
- загальні проблеми безпеки персоналу;
- способи передачі методик відповідальним особам;
- обставини, за яких методики потрібно переглянути;
- метод контролю змін в методиці.

За необхідності в детальнішій методиці безпеки розглядають і такі питання:

- моделі захисту і процедури в межах організації;
- використання стандартів;
- процедури впровадження засобів захисту;
- підхід до завершальних дій, таких як:
  - перевірка відповідності захисту;
  - контроль засобів захисту;

- обробка інцидентів, пов’язаних із захистом;
- контроль експлуатації системи інформаційних технологій;
- обставини, відповідно до яких треба залучати зовнішніх консультантів із захисту.

Результати попереднього аналізу ризику і огляд керування, перевірка відповідності захисту та інцидентів у захисті може впливати на методику захисту інформаційних технологій. Це, в свою чергу, може потребувати, щоб попередньо була розглянута чи удосконалена визначена стратегія або методика.

Для забезпечення адекватної підтримки і супроводу всіх засобів безпеки методика захисту інформаційних технологій повинна бути затверджена керівництвом.

На основі методики безпеки інформаційних технологій необхідно видати розпорядження, яке об’єднає персонал управління і службовців. Може виникнути необхідність особистого підпису кожного працівника на документі, який підтверджує його відповідальність за безпеку в організації. Крім того, потрібно розробити і реалізувати програми компетентності в захисті і процеси навчання, щоб повідомити ці положення.

Потрібно призначити особу, відповідальну за методику безпеки інформаційних технологій і за забезпечення від слідкування за цією методикою потреб і фактичного стану організації. Це переважно належить до обов’язків контролера безпеки інформаційних технологій, який також відповідає за доопрацювання, що охоплює огляд, перевірку надійності захисту, обробку інцидентів і слабкостей в захисті, а також будь-які зміни в методиці безпеки інформаційних технологій, що потрібні відповідно до результатів цих заходів.

19.3. Варіанти стратегії аналізу ризику

Перед початком будь-якої діяльності, пов’язаної з аналізом ризику, організація повинна мати стратегію щодо здійснення цього аналізу, а її складові

частини (методи, технології тощо) повинні бути відображені в методиці безпеки інформаційної технології. Засоби і критерії для вибору методу аналізу ризику потрібно погодити з вимогами організації. Стратегія аналізу ризику повинна гарантувати, що обраний підхід відповідає оточенню і що він зосереджує зусилля захисту там, де вони необхідні. Варіанти, подані нижче, описують чотири різних підходи до аналізування ризиків. Основна відмінність між цими варіантами – глибина аналізування ризику. Оскільки загальний детальний аналіз ризику всіх систем являється дорогим, а також неефективним є побічне ставлення до суттєвих ризиків, то потрібен баланс між цими варіантами.

Нагадаємо, що між можливістю бездіяльності і визнанням множини ризиків невідомої величини і серйозності, можна виділити чотири основних варіанти методики аналізування ризику:

- використання однакового основного підходу для всіх систем інформаційних технологій незалежно від ризиків, що стоять перед системами, і прийняття того, що рівень захисту ніколи не може бути відповідним;
- використання неформального підходу для аналізування ризику і зосередженість на системах інформаційних технологій, які підпадають під високий рівень ризику;
- проведення детального аналізу ризику використанням формальних підходів;
- використання змішаного підходу для застосування початкового аналізування ризику високого рівня, щоб визначити системи інформаційних технологій з високим рівнем ризику, і є критичними для ділової активності, з детальним аналізуванням ризику для цих систем, і застосуванням основного захисту до всіх інших систем.

Ці різні можливості щодо напрямків аналізу ризиків безпеки обговорюють далі, з рекомендаціями щодо переваги кожного підходу.

Якщо організація вирішує нічого не робити щодо захисту чи відкласти реалізацію заходів захисту, адміністрація повинна знати можливі наслідки такого рішення. Хоча це не вимагає ані часу, ані грошей, ані персоналу, ні інших ресурсів, така пасивність все-таки має безліч недоліків. Якщо організація не впевнена у безпечності своїх систем інформаційних технологій, вона може тривалий час бути відкритою для серйозних впливів. Організація може бути в конфлікті із законами та розпорядженнями, і її репутація може постраждати, якщо цей конфлікт спричинить порушення у захисті і це покаже, що не було ніякої попереджувальної роботи. Якщо організація мало турбується про захист інформаційних технологій або не має інших робочих перевірених систем, тоді це може бути життєва стратегія. Однак, така організація не знає, наскільки добрий чи поганий поточний стан, і для більшості організацій це навряд чи буде прийнятним рішенням.

Основний підхід

Перший підхід полягає в тому, що організація за основу безпеки для всіх систем інформаційних технологій вибирає стандартні засоби захисту. Низку стандартних засобів захисту запропоновано в основних документах і практичних рекомендаціях з їх використання.

Існують такі переваги використання цього підходу:

- потрібно мінімум витрат для детального аналізування ризику і керування під час забезпечення засобами захисту і менше часу і зусиль на вибір засобів захисту;
- основні засоби захисту є рентабельні, ті самі або подібні основні засоби захисту можуть бути легко пристосовані до багатьох систем, якщо багато систем організацій працюють у спільному оточенні і якщо потреби захисту порівнянні.

Недоліки цього підходу:

- якщо основний рівень установлений занадто високим, сила захисту буде надмірною для деяких систем інформаційних технологій;
- якщо основний рівень занадто низький, може виявитися для деяких систем недостатній рівень захищеності;
- можуть виникнути складнощі в керуванні доречними змінами в захисті. Наприклад, якщо система модернізована, може бути важко визначити, чи є первісні основні засоби захисту, як і раніше, ефективними.

Якщо всі системи інформаційних технологій організації мають низький рівень необхідних вимог захисту, тоді це – найрентабельніша стратегія. У цьому випадку основа повинна бути відповідною рівню захисту, необхідному більшості систем інформаційних технологій. Більшість організацій завжди повинна буде вибирати деяку мінімальну кількість стандартів, щоб захистити секретні дані й узгодити із законами та розпорядженнями, наприклад, із законом захисту даних. Однак там, де системи організації відрізняються в діловій активності, розмірі і складності, цей підхід нелогічний і не рентабельно застосовувати загальний стандарт до всіх систем.

Неформальний підхід

Другий підхід полягає в неформальному, прагматичному аналізуванні ризику. Неформальний підхід базується не на структурованих методах, а на поінформованості і досвіді осіб.

Перевага цього підходу – ефективність щодо вартості і часу. Немає потреби набувати додаткових навичок чи навчати виконувати неформальне аналізування, і його проводять значно швидше, ніж детальне аналізування ризику.

Існує, однак, ряд недоліків такого підходу:

- відсутність формального підходу або вичерпного переліку збільшує ймовірність пропустити деякі важливі деталі;

- підтвердження застосування засобів захисту від ризиків у цьому випадку ускладняється;
- особи, що мають незначний досвід в аналізуванні ризиків, можуть мати мало інструкцій, які б допомогли їм у виконанні завдань;
- частина пропозицій у минулому керувалася уразливістю, тобто реалізовані засоби захисту ґрунтувалися на визначеній вразливості, без врахування можливості використання загрозою цієї вразливості, тобто без реальної потреби в засобах захисту;
- оскільки підхід являється неформальним, результатам властива суб'єктивність поглядів і упередженість консультанта;
- виникають проблеми, якщо особа, що проводить неформальне аналізування ризику, іде з організації.

Ґрунтуючись на вище викладених недоліках, цей підхід не вважають ефективним щодо виконання аналізу ризику для багатьох організацій.

Докладне аналізування ризику

Третій підхід полягає в докладних оцінках аналізування ризику для всіх систем інформаційних технологій організації. Докладне аналізування ризику охоплює визначання та оцінювання активів, а також оцінювання рівнів загроз щодо цих активів і їхньої вразливості.

Переваги цього підходу:

- висока ймовірність того, що для всіх систем визначені відповідні засоби захисту;
- результати докладного аналізування можна використовувати в керуванні змінами в захисті.

Недоліки цього підходу:

- він вимагає багато часу, зусиль і спеціальних знань для одержання результатів;

- є ймовірність, що вимоги захисту небезпечної системи будуть враховані занадто пізно;
- усі системи інформаційних технологій треба розглядати докладно, і буде потрібно багато часу, щоб завершити аналізування.

Змішаний підхід

Четвертий підхід у першу чергу передбачає початкове аналізування високорівневих ризиків для всіх систем інформаційних технологій, у кожному випадку зосереджуючись на практичній цінності системи інформаційних технологій і на серії ризиків, пов'язаних з нею. Для систем інформаційних технологій, визначених як важливі для діяльності організації і (або) пов'язаних з високими рівнями ризику, треба проводити докладне аналізування ризику у першу чергу. Для всіх інших систем інформаційних технологій вибирають основний підхід. Цей підхід забезпечує компроміс і мінімізацію часу і зусиль, затрачених на ідентифікацію засобів захисту, у той самий час гарантуючи відповідну захищеність систем з високим ризиком.

Додаткові переваги цього підходу:

- поєднання на початку швидкості і простоти підходу підвищує ймовірність приймання програми аналізування ризику;
- існує можливість побудови безпосередньої стратегічної картини програми безпеки організації, яку можна використовувати як допомогу під час планування;
- ресурси і кошти можуть бути спрямовані на одержання максимальної вигоди, і системи з ймовірно найбільшою потребою в захисті можуть бути враховані на ранніх стадіях;
- наступні дії будуть успішнішими.

Єдиний потенційний недолік такий: оскільки початкове аналізування ризику проводять на високому рівні, який потенційно менш точний, для деяких

систем не можна визначити відповідний рівень деталізації аналізування ризику. Однак ці системи аналізують все-таки на базі основного підходу. Також ці системи можна заново перевіряти кожен раз, коли треба переконатися чи необхідний більший рівень, ніж той, який забезпечується основним підходом.

Прийняття такого підходу аналізування високорівневого ризику, де змішані основний підхід і детальне аналізування ризику там, де необхідно, може бути запропоновано більшості організацій як найефективніше рішення.

19.4. Реалізація змішаного підходу до аналізування ризиків

Цей розділ подає вказівки для реалізації змішаної стратегії аналізування ризику, рекомендовані вище.

Аналізування ризиків високого рівня

Спочатку необхідно провести початкове аналізування ризику високого рівня, щоб вибрати підхід (основне чи докладне аналізування ризику), що відповідає кожній системі інформаційних технологій. Це аналізування ризику високого рівня розглядає практичну цінність системи інформаційних технологій, оброблену інформацію і ризики з погляду ділової активності організації. Вихідні дані для вирішення щодо вибору відповідного для системи інформаційних технологій підходу можна використовувати такі підстави:

- ділові цілі, що їх досягають за допомогою системи інформаційних технологій;
- рівень залежності ділової активності організації від системи інформаційних технологій, тобто, чи впливає функція, яку розглядає організація, на її виживання або ефективність ділової активності, залежної від цієї системи, чи на конфіденційність, цілісність, доступність, обліковість, достовірність і надійність інформації, оброблюваної цією системою;
- рівень інвестування в цю систему інформаційної технології в умовах розробки, підтримування чи заміни системи;

- активи системи інформаційних технологій, для яких організація безпосередньо надала значення.

Коли ці положення оцінені, рішення прийняти легко. Якщо цілі системи важливі для ділової активності організації, якщо витрати на заміну системи високі чи якщо значення активів мають високі рівні ризику, то необхідне детальне аналізування ризику для системи. Кожна з цих умов може бути достатньою для необхідності детального аналізування ризику.

Загальне правило застосування: якщо відсутність захисту системи інформаційних технологій може спричинити істотну шкоду чи ушкодження в організації, її діловим процесам чи її активам, то необхідне докладне аналізування ризику для визначання потенційних ризиків. У всіх інших випадках для досягнення відповідного рівня захисту досить застосування основного підходу.

Основний підхід

Мета основного захисту полягає в тому, щоб встановити мінімальну кількість засобів захисту і захистити всі чи деякі системи інформаційних технологій організації. Використовуючи цей підхід, можна застосувати основний захист у всій організації, і, як відзначено вище, додатково використовувати докладний аналіз ризику для захисту систем інформаційних технологій з високими рівнями ризику чи систем, вирішальних для справи. Використання основного підходу зменшує капіталовкладення, які організація повинна робити у здійснення аналізу ризику.

Відповідний основний захист можна забезпечити, використовуючи каталоги засобів захисту, які містять перелік засобів захисту для системи інформаційних технологій від найзагальніших загроз. Рівень основного захисту може бути відкоригований відповідно до потреб організації. Докладне оцінювання загроз, вразливостей і ризиків не потрібне. Усе, що треба зробити для здійснення основного захисту, – це вибрати ті частини каталогу засобів

захисту, що стосуються розглянутої системи інформаційних технологій. Після визначення засобів захисту уже реалізованих на місці порівнюють із засобами захисту, перерахованими в основному каталозі. Ті, яких немає на місці, повинні бути реалізовані.

Основні каталоги можуть визначити засоби захисту, які потрібно конкретно використовувати, або вони можуть пропонувати перелік необхідних вимог захисту, врахованих в будь-яких засобах захисту, відповідних розглянутій системі. Обидва підходи мають переваги. Одна з цілей основного підходу – узгодженість засобів захисту по всій організації, якої можна досягти обома підходами.

Кілька уже наявних документів надають перелік основних засобів захисту. Також іноді схожі оточення можна спостерігати серед компаній того самого промислового сектора. Після експертизи основних вимог їх можна використовувати для основних каталогів захисту, які можуть використовувати багато різних організацій. Наприклад, каталоги основних засобів захисту могли б бути отримані від:

- міжнародних і державних організацій зі стандартизації;
- стандартів чи рекомендацій промислового сектора;
- іншої організації, бажано з подібними діловими цілями і відповідного розміру.

Організація може, звичайно, також створити власну основу, установлюючи відповідність із типовим оточенням і з діловими цілями.

Докладний аналіз ризику

Докладний аналіз ризику для системи інформаційних технологій містить визначення структури ризиків і оцінку їхніх величин. Необхідність у докладному аналізуванні ризику може бути визначена без зайвих витрат часу і коштів, коли огляди високого рівня проводять для всіх систем, які

супроводжуються докладним аналізом ризику тільки високого рівня чи вирішальних систем.

Аналізують ризик визначанням потенційних несприятливих уражень, небажаних подій і ймовірності їхньої появи. Небажані події можуть впливати на ділову активність службовців чи на будь-який цінний об’єкт організації. Несприятливе ураження в результаті небажаного випадку – складова частина можливих збитків, пов’язаних із значенням активів і їхніх ризиків. Ймовірність появи уражень залежить від того, наскільки привабливі активи для потенційного нападника, від ймовірності появи загроз і легкості, з якою уразливість можна використати. Результати аналізу ризику приведуть до ідентифікації і вибору засобів захисту, що їх можна використовувати для зменшення визначених ризиків до припустимого рівня.

Докладний аналіз ризику містить глибоку перевірку на кожному із кроків, показаних на рис. 15.1. Цим керуються при виборі перевірених засобів захисту як частини процесу керування ризиком. Необхідні вимоги для цих засобів захисту подані в методиці безпеки системи інформаційних технологій і пов’язані з планом безпеки інформаційної технології. Множина інцидентів і зовнішніх чинників, що можуть впливати на необхідні вимоги захисту системи, може спричинити перегляд усього аналізу ризику чи його частини. Це такі впливи: недавні інциденти, істотні зміни системи, заплановані зміни чи наслідки інцидентів, які потрібно розглядати.

Існує ряд методів для ефективного аналізування ризику, починаючи від контрольного переліку основних підходів і закінчуючи основними методами структурованого аналізу. Можна використовувати автоматизовані (за допомогою інформаційної системи) чи звичайні базові інструкції. Незалежно від того, який метод чи інструкцію використовує організація, вони повинні принаймні стосуватися положень, визначених у наступних пропозиціях. Також важливо, щоб методи гармонізували з мікро-політикою організації.

Після завершення детального огляду аналізу ризиків системи результати огляду: активи і їхня значимість, загрози, вразливості і рівні ризиків, а також визначені засоби захисту – повинні бути збережені, наприклад, у базі даних. Очевидно, методи, що використовують засоби програмного забезпечення, здійснюють це набагато простіше. Таке представлення, згадуване іноді як модель, можна використовувати, щоб досягти істотного ефекту, оскільки через якийсь час відбуваються зміни в конфігурації, в оброблюваних типах інформації, у сценаріях загроз тощо. У цьому разі вихідними даними стають тільки самі зміни для визначання впливу на необхідні засоби захисту. Надалі такі моделі можна швидко використовувати для досліджування різних параметрів, обговорювати у процесі розробки нової системи, використовувати для інших подібних систем.

Рис. 19.1. Керування ризиком, з використанням детального аналізу ризику

Визначання меж огляду

Як показано на рис. 19.1, перед збором подібної інформації для ідентифікації активів і їхньої оцінки, потрібно визначити межі огляду. Точне визначання меж у цій стадії дає змогу уникнути непотрібної роботи і поліпшити якість аналізування ризику. Кінцевий опис чітко визначить, що з наведеного

нижче треба розглядати під час огляду аналізу ризиків для розглянутої системи інформаційних технологій:

- активи інформаційних технологій (наприклад апаратні засоби, програмне забезпечення, інформація);
- люди (наприклад персонал, субпідрядники, інший зовнішній персонал);
- оточення (наприклад будівлі, обладнання);
- діяльність (виконувані роботи).

Ідентифікація активів

Актив – це компонент або частина всієї системи, для якої організація безпосередньо визначає цінність, і отже, яка потребує захисту. Для ідентифікації активів треба брати до уваги те, що система інформаційних технологій складається не тільки з апаратних засобів і програмного забезпечення. Наприклад, типи активів можуть бути такими:

- інформація (дані) (наприклад файли, що містять фінансові подробиці, інформація про продукцію);
- апаратні засоби (наприклад інформаційна система, пристрій для друку);
- програмне забезпечення, в тому числі прикладне (наприклад програми оброблення тексту, програми, розроблені для спеціальних цілей);
- апаратура зв’язку (наприклад телефони, мідний кабель, скловолокно);
- програмно-апаратне забезпечення (наприклад диски, постійна пам’ять);
- документи (наприклад контракти);
- грошові засоби (кошти) (наприклад у банкоматах);
- вироблені товари;
- служби (наприклад інформаційні служби, обчислювальні ресурси);
- конфіденційність і служби довіри (наприклад служби оплати);
- устаткування оточення;
- персонал;

- імідж.

Всі активи у встановлених межах огляду повинні бути визначені і навпаки, будь-які активи, що їх вилучають з меж огляду з будь-якої причини, повинні бути вміщені в інший огляд, для впевненості, що їх не зможуть забудути і не пропустять.

Оцінювання активів і встановлювання залежностей між активами

Після досягнення мети щодо ідентифікації активів, за допомогою огляду всіх активів системи інформаційних технологій, треба визначити цінність активів. Ця цінність відображає важливість активів для діяльності організації. Їх можна виразити в термінах захисту, таких як потенційно небажані порушення ділової активності в результаті розкриття, зміни, недоступності і (або) знищення інформації або інших активів системи інформаційних технологій. Отже, ідентифікація активів і їхня оцінка, заснована на ділових потребах організації, є провідними чинниками при визначанні ризиків.

Вихідними даними для оцінювання активів повинні забезпечувати власники і користувачі активів. Особи(-а), що аналізують ризик, повинні формувати перелік активів. Вони повинні звертатися по допомогу до тих, хто займається плануванням ділової активності, фінансами, інформаційними системами та іншою залежною діяльністю, для того щоб визначити цінність кожного з цих активів. Установлення цінності потрібно пов’язувати з вартістю придбання і підтримування активів і з потенційними ураженнями від втрати конфіденційності, цілісності, доступності, обліковості, достовірності і надійності. Кожен з ідентифікованих активів повинен мати цінність для організації. Проте не завжди є прямий або простий спосіб встановлювання фінансової цінності для всіх параметрів. Також необхідно встановити цінність чи ступінь важливості для не фінансових параметрів, тобто для якісних характеристик, строків у організації. Інакше буде важко визначити рівень захисту і кількість ресурсів, які організація повинна залучити, щоб захистити

активи. Наприклад, для подібних визначень цінності можна використовувати шкалу, де виражають її у градації низько, середньо, високо, чи більш детальну: дуже низько – низько – середньо – високо – дуже високо.

Далі детальніше подані можливі шкали для визначення цінності активів з урахуванням можливих збитків.

Оцінювання активів організації – істотний етап всього процесу аналізування ризику. Значення цінності, визначене активам, повинне бути виражене в поняттях, що стосуються майна і об'єктів, залучених у діловій активності. Для оцінювання активів організація повинна спочатку зробити перелік усіх наявних активів. Щоб забезпечити адекватне оцінювання всіх активів, доцільно згрупувати їх за типами, наприклад, інформаційні активи, програмні активи, фізичні активи і служби. Також корисно визначити власника кожного з активів, що буде відповідати за визначення значень цих активів.

Наступним кроком є вибір і погодження використовуваних шкал і критеріїв специфічних оцінок активів. Оскільки в більшості організацій зазвичай є значне різноманіття активів, швидше за все, цінності деяких активів можуть бути виражені у вартісному значенні і будуть оцінені в національній валюті, в той час як інші, виражені в якісному значенні, можуть бути оцінені діапазоном значень від "дуже низько" до "дуже високо". Рішення про використовування шкали кількісних оцінок замість шкали якісних оцінок є компетенцією організації і має залежати від оцінюваних активів. Обидва види оцінок можна використовувати до тих самих активів.

Типові градації, використовувані для якісної оцінки активів, такі: незначно, дуже низько, низько, середньо, високо, дуже високо і критично. Вибір і діапазон значень залежить від вимог організації до безпеки, розміру організації й інших чинників, визначених для організації.

Критерії, що використовуються як основа для надання значень для кожного з активів, повинні бути зафіксовані в однозначних термінах. Це зазвичай один з

найважчих аспектів оцінювання активів, тому що значення деяких активів, ймовірно, доведеться визначити суб'єктивно і швидше за все це буде визначати багато різних осіб. Можливі критерії, використовувані для визначання значень активів, охоплюють вартість їх придбання, заміни чи вартість повторного створення; їхні значення можуть бути абстрактними, наприклад, значення гарного іміджу організації чи її репутації.

Ще однією основою для оцінювання активів є витрати, спричинені втратою конфіденційності, цілісності чи доступності в результаті інциденту. Ця оцінка надає три важливих доповнення значень активів як додаток вартості відшкодування, що оснований на оцінюванні потенційного збитку чи несприятливого зниження ділової активності, що буде випливати з інцидентів захисту з залежною від нього множиною обставин. Треба зазначити, що цей підхід дозволяє врахувати збитки чи інші втрати коштів як необхідну складову формули оцінки ризику.

Багато активів можуть мати декілька наданих значень в процесі оцінювання. Наприклад, план ділової активності може бути оцінений на підставі зусиль, необхідних для розробки плану розвитку, що в свою чергу ґрунтується на зусиллях, пов'язаних з накопичуванням даних, а також на їхньому значенні для конкурентів. Кожна з отриманих оцінок з великою ймовірністю матиме різні значення. Надане значення може бути максимальним серед всіх можливих значень чи може бути сумою деяких чи всіх можливих значень. Остаточний аналіз, що припускає визначання значення чи значень активів, повинний бути чітко детермінованим, тому що надане остаточне значення активів враховують під час визначання ресурсів, що будуть залучені для захисту активів.

Зрештою всі оцінки активів мають бути зведені до спільної основи. Це може бути виконано за допомогою критеріїв. Критерії, що їх можна використовувати для визначання можливих збитків, зумовлюються втратою конфіденційності, цілісності чи доступності активів:

- порушення законів і (або) розпоряджень;
- порушення ділової активності;
- зміна з позитивного на негативний вплив на репутацію;
- порушення, пов’язані з особистою інформацією;
- втрата особистої безпеки;
- несприятливий вплив на законність діяльності;
- порушення комерційної конфіденційності;
- порушення суспільного порядку;
- фінансові втрати;
- збої в діловій активності;
- втрата безпеки стосовно оточення.

Ці критерії – приклади положень, які потрібно враховувати під час оцінювання активів.

Варто підкреслити на цій стадії, метод для оцінювання повинен давати не тільки кількісну оцінку, але і якісну оцінку там, де кількісна оцінка неможлива чи недоцільна (наприклад, існує потенційна можливість втрати життєздатності чи репутації організації). Необхідно надавати чіткі обґрунтування обраних критеріїв оцінки.

Також потрібно визначити залежності одних активів від інших, тому що це може впливати на їхню цінність. Наприклад, конфіденційність даних треба зберігати протягом усього процесу обробки, тобто вимоги програми захисту обробки даних повинні залежати безпосередньо від значення, що відображає конфіденційність оброблюваних даних. Якщо бізнес-процес спирається на цілісність певних даних, вироблених програмою, вхідні дані цієї програми повинні забезпечувати відповідну надійність. Крім того, цілісність інформації буде залежати від апаратних засобів і програмного забезпечення, що використовуються для її зберігання та обробки. Також апаратні засоби залежать

від електроживлення і, можливо, від кондиціонування повітря. Така інформація щодо залежностей буде допомагати під час ідентифікації залежних загроз і особливо вразливостей. Це також допоможе під час визначення дійсних цінностей активів (прямих залежностей відносин) і, отже, гарантувати відповідний рівень захищеності.

Цінність активів, від яких залежать інші активи, може змінюватися так:

– якщо цінність залежних активів (наприклад дані) нижчі чи дорівнюють цінності розглянутих активів (наприклад програмне забезпечення), цінності залишаються незмінними;

– якщо цінність залежних активів (наприклад дані) вища ніж цінність розглянутих активів (наприклад програмне забезпечення), цінність повинно бути збільшена згідно з:

• рівнем залежності;

• цінністю інших активів.

Організація може мати деякі активи, що повинні бути доступними більше одного разу, такі як копії чи програми інформаційних систем, подібні тим, що їх використовують у більшості організацій. Важливо враховувати цей факт під час оцінювання активів. Ці копії легко доступні, тому, з одного боку, треба потурбуватися про визначення всіх шляхів доступу; з іншого – потрібно шукати шляхи зменшення можливостей доступу.

Кінцевим результатом цього є перелік активів і їхніх цінностей щодо розкриття (забезпечення конфіденційності), зміни (забезпечення цілісності), доступності чи знищення (забезпечення доступності) і вартості відшкодування.

Оцінювання загроз

Загроза потенційно може нашкодити системі інформаційних технологій і її активам за умов прояву. Якщо загроза трапиться, то це може вплинути на систему інформаційних технологій і викликати небажані інциденти і, відповідно, порушення. Загрози можуть мати природне чи людське походження

і можуть бути випадковими чи навмисними. Випадкові і навмисні джерела загроз повинні бути визначені, а ймовірність їхньої появи необхідно оцінити. Важливо, щоб ніяка залежна загроза не була пропущена, тому що це може спричинити пошкодження чи ослаблення в системі захисту інформаційної технології.

Вихідні дані для оцінювання загрози треба отримувати від власників активів чи користувачів, від фахівців із планування і фахівців інформаційних технологій, і від людей, відповідальних за кіберзахист.

Оцінювання вразливостей

Ця оцінка містить визначення недоліків у фізичному оточенні, організації, процедурах, персоналі, керуванні, адмініструванні, апаратних засобах, програмному забезпеченні чи апаратурі зв'язку, які можуть використовуватись загрозами для заподіяння шкоди активам і діяльності, яку вони супроводжують. Сама присутність вразливостей не заподіює шкоди, для чого повинна ще існувати загроза, яка використовує цю вразливість. Вразливість, для якої не існує відомих загроз, не вимагає застосування засобів захисту, але вона все-таки повинна бути ідентифікована і контролюватися щодо змін. Треба зазначити, що неправильно реалізовані чи працюючі зі збоями засоби захисту або засоби захисту, що їх використовують неправильно, можуть приховувати в собі вразливості.

Вразливості можуть бути пов'язані з властивостями чи атрибутами активів, які можливо використати у спосіб або з метою, іншими від визначених у момент купівлі чи виготовлення активів. Наприклад, одна з властивостей постійного запам'ятовувача з перезаписуванням – та, що інформація, яка зберігається в ньому, може бути стерта і змінена. Це – один з конструктивних критеріїв постійного запам'ятовування з перезаписом. Проте ця властивість також надає можливість недозволеного знищення інформації на постійному запам'ятовувачі з перезаписуванням. Це може бути вразливістю.

Оцінювання ідентифікує вразливості, що можуть використовуватись загрозами, та оцінює ймовірний рівень їхньої недостатності, тобто легкості використання. Наприклад, деякими активами легко розпоряджатися, їх легко сховати чи транспортувати – ці властивості можуть спричинити вразливості. Вихідні дані для оцінювання вразливості повинні бути отримані від власників активів чи користувачів, від фахівців і експертів з устаткування систем інформаційних технологій по апаратному і програмному забезпеченню. Приклади вразливостей:

- незахищені зв'язки (наприклад Internet);
- непідготовлені користувачі;
- невірний вибір і використовування паролів;
- відсутність відповідного контролю за доступом (логічним і (або) фізичним);
- відсутність резервного копіювання інформації чи програмного забезпечення;
- розташування на ділянках, де можливі повені.

Далі наведено приклади вразливостей в різних зонах захисту, включаючи приклади загроз, що могли б скористатися цими вразливостями. Ці приклади можна використовувати як довідкову інформацію в процесі оцінювання вразливостей. Варто також підкреслити, що в деяких випадках інші загрози також можуть використовувати ці вразливості.

Оточення та інфраструктура:

- відсутність фізичного захисту будівель, дверей і вікон (може використовувати, наприклад, загроза злодійства);
- недостатнє чи недбале використання фізичного контролювання за доступом до будівель, кімнат (може використовувати, наприклад, загроза навмисного пошкодження);

- нестійкість енергосистеми (може використовувати, наприклад, загроза нестабільності енергоживлення);
- розташування в зоні ймовірного затоплення (може використовувати, наприклад, загроза затоплення).

Апаратні:

- відсутність графіка періодичної заміни (може використовувати, наприклад, загроза погіршення носіїв даних);
- чутливість до змін напруги (може використовувати, наприклад, загроза нестабільності енергоживлення);
- чутливість до коливань температури (може використовувати, наприклад, загроза екстремальних значень температури);
- чутливість до вологості, пилу, вогкості (може використовувати, наприклад, загроза запилення);
- чутливість до електромагнітного випромінювання (може використовувати, наприклад, загроза електромагнітного випромінювання);
- недостатній супровід/неправильна інсталяція даних (може використовувати, наприклад, загроза помилки обслуговуючого персоналу);
- відсутність ефективного керування змінами конфігурації (може використовувати, наприклад, загроза помилки експлуатаційного персоналу).

Програмні:

- неповні чи незрозумілі для розробників технічні вимоги (може використовувати, наприклад, загроза програмної помилки);
- відсутність чи недостатність випробовування програмного забезпечення (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженими користувачами);

- складний інтерфейс користувача (може використовувати, наприклад, загроза помилки експлуатаційного персоналу);
- відсутність ідентифікаційних і пізнавальних механізмів, таких як автентифікація користувача (може використовувати, наприклад, загроза нелегального проникнення користувача);
- відсутність контрольних точок (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженим способом);
- відомі "дірки" в програмному забезпеченні (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженими користувачами);
- незахищені таблиці паролів (може використовувати, наприклад, загроза несанкціонованого доступу користувача);
- недостатнє керування паролями (паролі, які легко підібрати, збереження паролів у відкритому вигляді, недостатня частота зміни; може використовувати, наприклад, загроза нелегального проникнення користувача);
- невірний розподіл прав доступу (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженим способом);
- неконтрольоване завантаження і використання програмного забезпечення (може використовувати, наприклад, загроза зловмисної програмної закладки);
- немає механізмів "виходу із системи" у разі від’єднання робочої станції від системи (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженими користувачами);
- відсутність ефективного керування змінами (може використовувати, наприклад, загроза програмної помилки);

- відсутність документації (може використовувати, наприклад, загроза помилки оперативного персоналу);
- відсутність запасних копій (може використовувати, наприклад, загроза зловмисної програмної закладки чи загроза пожежі);
- розповсюджування чи багаторазове використовування носіїв даних без відповідного очищення (може використовувати, наприклад, загроза використовування програмного забезпечення не уповноваженими користувачами).

Зв’язок:

- незахищені лінії зв’язку (може використовувати, наприклад, загроза підслуховування);
- погані кабельні з’єднання (може використовувати, наприклад, загроза витоку даних із каналів зв’язку);
- відсутність ідентифікації і підтвердження відправника й одержувача (може використовувати, наприклад, загроза нелегального проникнення користувача);
- передавання паролів у відкритому вигляді (може використовувати, наприклад, загроза доступу до мережі не уповноваженими користувачами);
- відсутність підтвердження посилання чи одержання повідомлення (може використовувати, наприклад, загроза невизнання участі);
- вилучений доступ (може використовувати, наприклад, загроза доступу до мережі не уповноваженими користувачами);
- незахищений чутливий потік даних (може використовувати, наприклад, загроза підслуховування);
- недостатнє керування мережею (гнучкість маршрутизації; може використовувати, наприклад, загроза перевантаження трафіка);

- незахищені з’єднання загального використання (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженими користувачами).

Документи:

- збереження в незахищеному вигляді (може використовувати, наприклад, загроза злодійства);
- відсутність обережності у використанні (може використовувати, наприклад, загроза злодійства);
- несанкціоноване копіювання (може використовувати, наприклад, загроза злодійства),

Персонал:

- відсутність персоналу (може використовувати, наприклад, загроза, пов’язана з недостатньою кількістю персоналу);
- неконтрольована зовнішня робота некомпетентним персоналом (може використовувати, наприклад, загроза злодійства);
- недостатнє навчання питанням захисту (може використовувати, наприклад, загроза помилки оперативного персоналу);
- відсутність компетентності в захисті (може використовувати, наприклад, загроза помилок користувача);
- неправильне використання програмного забезпечення і устаткування (може використовувати, наприклад, загроза помилки оперативного персоналу);
- відсутність заходів контролю (може використовувати, наприклад, загроза використання програмного забезпечення не уповноваженим способом);
- відсутність методик для правильного використання засобів телекомунікації і пересилання повідомлень (може використовувати, наприклад, загроза використання мережних засобів не уповноваженим шляхом);

- неадекватні процедури прийому на роботу (може використовувати, наприклад, загроза навмисного збитку).

Загальні причини вразливостей:

- окремі місця недоліків (може використовувати, наприклад, загроза недоліків послуг зв'язку);
- неадекватне реагування служб підтримки (може використовувати, наприклад, загроза відмови апаратури).

Можна визначити, наскільки небезпечні вразливості, іншими словами, як легко ними можна скористатися. Вразливість повинна бути оцінена щодо кожної загрози, яка може використовувати вразливість у відповідній ситуації. Наприклад, система може мати вразливість до загроз нелегального проникнення користувача і використовування ресурсів. Вразливість нелегального проникнення користувача може бути високою через відсутність механізмів авторизації користувачів. З іншого боку, вразливість зловживання ресурсами може бути низькою, тому що навіть без механізмів авторизації користувачів, ресурси, якими вони могли б зловживати, обмежені.

Результатом цього кроку повинен бути перелік вразливостей і оцінок легкості їх використовування, наприклад, у градації високо, середньо і низько.

Ідентифікація наявних і (або) запланованих засобів захисту

Засоби захисту, ідентифіковані після огляду аналізування ризику, повинні бути доповненням до вже наявних і запланованих засобів захисту. Важливо, щоб наявні і заплановані засоби захисту були визначені як частина цього процесу, щоб уникнути непотрібної роботи чи витрат, наприклад, під час дублювання засобів захисту. Може виявитися, що для наявних чи запланованих засобів захисту немає обґрунтувань. У цьому випадку потрібно перевірити, чи засіб захисту потрібно вилучити і замінити іншим, більш підхожим, чи треба

лишити його для подальшого виконання своїх функцій (наприклад через вартість).

Крім того, треба виконати перевірку, щоб установити після огляду аналізу ризику, чи сумісні обрані засоби захисту з наявними і запланованими засобами захисту, тобто, що обрані та наявні засоби захисту не суперечать один одному.

Під час визначення наявних засобів захисту треба перевірити, чи правильно вони функціонують. Якщо захисний засіб, на який покладено певну функцію захисту, не функціонує в процесі ділової активності, він є джерелом можливої вразливості.

Результат цього кроку – перелік всіх наявних і запланованих засобів захисту і стан їх впровадження і використовування.

Оцінювання ризиків

Ризики – функція цінності активів стосовно небезпеки, ймовірності загроз, що трапляються і можуть викликати потенційні порушення в діловій активності, легкості використовування вразливості ідентифікованими загрозами, і будь-яких наявних чи запланованих засобів захисту, що можуть зменшувати ризик.

Існують різні напрямки встановлення зв’язків цих чинників; наприклад, значення, надані активам, вразливостям і загрозам поєднуються, щоб одержати значення вимірювань ризику.

Аналізування ризиків складається з багатьох стадій, що були обговорені в цій та інших частинах цього підручника. Стадії:

- визначання і оцінювання активів (оцінювання потенційних порушень ділової активності);
- оцінювання загроз;
- оцінювання вразливостей;
- оцінювання наявних або запланованих заходів захисту;

- оцінювання ризиків.

Заключний етап повинен визначити повноту ризиків. Як відзначено раніше, активи, що мають цінність і певний рівень вразливості, перебувають у небезпеці щоразу, коли з'являється загроза. Оцінка ризиків – комбінація потенційних порушень ділової активності, небажаних інцидентів, рівнів оцінених загроз і вразливості. Ризики – вимір впливів, яким можуть бути піддані система і пов'язана з нею організація.

Мета аналізування ризику полягає в тому, щоб визначити і оцінити ризики, яким піддано системи інформаційних технологій та її активи, щоб визначити і вибрати відповідні і вмотивовані заходи захисту. Під час оцінювання ризиків необхідно враховувати деякі положення, включаючи порушення та ймовірність.

Порушення може бути оцінено кількома способами, з використанням кількісних, наприклад вартісних, і оцінок якості (може бути засноване на використовуванні ознак таких, як помірковано чи несприятливо), чи комбінації обох. Щоб визначити ймовірність прояву загрози, потрібно встановити часовий інтервал, у якому активи будуть мати цінність чи повинні бути захищені. На ймовірність прояву загрози впливають такі фактори:

- привабливість активів, особливо коли розглядають навмисну людську загрозу;
- простота перетворення активів на матеріальну винагороду, особливо якщо розглядають навмисну людську загрозу;
- технічні можливості носія загрози, що використовується для навмисної людської загрози;
- ймовірність загрози;
- чутливість до вразливостей експлуатації щодо технічних і нетехнічних вразливостей.

Визначення засобів захисту

Виміри ризиків, що визначені попередніми кроками, треба використовувати як основу для визначання всіх засобів захисту, потрібних для забезпечення відповідного рівня захисту.

Щоб вибирати засоби захисту, що ефективно захищають від оцінених ризиків, треба розглядати результати аналізу ризику. Вразливості до відповідних загроз показують, де необхідний додатковий захист і яка його форма може знадобитися.

Якщо є ряд альтернатив розглянутих засобів захисту, то їх відсівають відповідно до витрат. Сфера застосування засобів захисту:

- фізичне оточення;
- персонал;
- адміністрування;
- апаратне чи програмне забезпечення;
- комунікації.

Наявні і заплановані засоби захисту треба повторно аналізувати в поняттях порівняльної вартості, включаючи експлуатацію, витрати на вилучення (чи не застосування) чи поліпшення засобів, якщо вони не досить ефективні. Потрібно відзначити, що іноді дорожче вилучити невідповідний засіб захисту, ніж його залишити і, можливо, додати новий захист. Можливо також, що захист може забезпечувати захист активів за межами поточного розгляду.

Для визначення засобів захисту слід розглядати вразливості, які повинні бути захищеними, і пов’язані з ними загрози. Існує багато можливостей зменшити ризики:

- запобігання ризику;
- переміщення ризику (наприклад страхування);
- зменшення загрози;
- зменшення вразливості;

- зменшення можливих втручань;
- виявлення небажаних подій, реакція на них і відновлення після них.

Яка з перерахованих можливостей (чи їхня комбінація) є найвідповіднішою, залежить від обставин. Можуть бути корисними каталоги засобів захисту. Проте після вибору засобів захисту з каталогу також важливо правильно застосувати їх до визначених потреб організації.

Інший важливий аспект вибору засобів захисту – чинник вартості. Було б недоцільно рекомендувати засоби захисту, дорожчі у застосуванні і супроводі, ніж значення самих активів, для захисту яких їх використано. Також недоцільно рекомендувати засоби захисту, вартість яких перевищує фонди, які виділяє організація для забезпечення захисту. У той самий час необхідно уважніше підходити до питань, пов’язаних із застосуванням засобів захисту, якщо бюджет зменшує їх кількість чи якість, тому що це може допустити більший ризик, ніж заплановано. Затверджений бюджет для засобів захисту треба використовувати як обмежувальний чинник з великою обережністю.

Там, де визначено основний підхід для захисту системи інформаційних технологій, вибір засобів захисту відносно простий. Каталоги засобів захисту надають перелік засобів захисту, які забезпечують захист системи інформаційних технологій проти найзагальніших загроз. Ці рекомендовані засоби захисту порівнюють з наявними чи запланованими засобами захисту, і ті, які ще не застосовані чи не заплановані, формують перелік засобів захисту, що будуть впроваджені для забезпечення основного захисту.

Вибір засобів захисту повинен завжди ґрунтуватися на компромісі між операційними (нетехнічними) і технічними засобами захисту. Операційні засоби захисту – ті, які забезпечують фізичний захист, захист персоналу та керівного апарату.

Фізичні засоби захисту – це зміцнення внутрішніх стінок будівлі, блокування дверей за допомогою замків, системи попередження пожеж,

пожежогасіння та інше. Захист персоналу охоплює перевіряння поповнення (особливо на посаду з підвищеною довірою), контролювання персоналу і програми компетентності в захисті.

Процедурний захист містить захист робочих процедур документообігу, процедури розвитку покращення обробки інцидентів. Щодо цієї категорії важливо відзначити, що відповідні процедури, разом з передбаченням випадковостей, відновленням після уражень, стратегію і план(и) розробляють для кожної системи. План повинен містити подробиці ключових функцій і пріоритетів з відновлення, вимоги обробки й організаційні процедури, які активізуються у випадку надзвичайних подій чи перебоїв у роботі служб. Такі плани мають передбачати кроки, необхідні для обробляння вирішальної щодо засобів захисту інформації, у той час як організація може проводити свою діяльність.

Технічний захист охоплює апаратний і програмний захист та захист комунікацій. Ці засоби захисту вибирають відповідно до ризиків для забезпечення функціонування і гарантування захисту. Функціональні можливості включають, наприклад, ідентифікацію та авторизацію, вимоги контролювання за логічним доступом, контролювання шляху, вимог журналу безпеки, безпеку зворотного виклику, авторизацію повідомлень, кодування тощо. Необхідні вимоги документують рівень довіри, необхідної у функціях захисту і, відповідно, кількість і тип перевірянь, випробовувань засобів захисту тощо, необхідних для забезпечення такого рівня. Якщо вирішено поєднати операційні та технічні засоби захисту, необхідно враховувати, що існує ряд різних підходів для забезпечення вимог спеціального захисту. Структура спеціального захисту має бути визначена для кожного підходу, щоб допомогти у визначенні того, як забезпечити необхідний захист, і також що може бути реалізоване з використанням наявних засобів.

Організація повинна зробити вибір на користь використання оцінених продуктів і систем як аспект кінцевого рішення по системі. Оцінені продукти – ті, які були досліджені третьою стороною. Третьою стороною може бути інша частина тієї самої організації чи незалежна організація, що спеціалізується на перевірці систем. Оцінювати можна всупереч множині визначених критеріїв, що створені спеціально для сформованої системи, або може існувати узагальнена множина критеріїв, які можна використовувати в різних ситуаціях. Оцінки можуть визначити необхідні вимоги функціонування і (або) необхідні вимоги гарантування. Деяка кількість проєктів сертифікації вже існує, багато з них підтримуються урядом і міжнародними організаціями зі стандартизації. Організація може вирішити використовувати оцінені засоби і системи, коли є впевненість, що множина їхніх функціональних можливостей – те, що потрібно, і коли є впевненість у правильності і повноті застосування цих функціональних можливостей. Як альтернатива, зосереджені прагматичні тестування захисту можуть дати впевненість у забезпеченні гарантованого захисту.

Під час процесу вибору засобів захисту для застосування потрібно розглядати множину чинників, зокрема:

- легкість у використанні засобів захисту;
- прозорість для користувача;
- довідку, що забезпечує користувачів інформацією про їхні функції;
- відносну міцність засобів захисту;
- типи виконуваних функцій – запобігання, стримування, виявлення, відновлення, корекція, контролювання і навчання персоналу.

У загальному випадку захисний засіб виконує більше ніж одну з цих функцій, чим більше може виконати, тим краще. Під час дослідження всього захисту чи множини засобів захисту, яку потрібно використовувати, необхідно підтримувати рівновагу між типами функцій, якщо це можливо. Це допомагає

всьому захисту бути ефективнішим і дієвим. Аналіз вартості/вигоди може бути потрібний як пошук компромісу (метод порівняння альтернатив, що конкурують і використовують множину критеріїв, оцінених стосовно кожної конкретної ситуації).

Структура захисту інформаційних технологій

Структура захисту інформаційних технологій описує, як можуть бути задоволені вимоги захисту для системи інформаційних технологій як частина структури всієї системи. Тому важливо розглядати структуру захисту інформаційних технологій у процесі вибору засобів захисту.

Структуру захисту інформаційних технологій треба враховувати в розробці нових систем і коли зроблені великі зміни в наявних системах. Ґрунтуючись на результатах аналізування ризику на основному підході, необхідно визначити вимоги до захисту і співвіднести їх із комплексом технічних служб безпеки системи, що задовольняють ці вимоги. У деяких випадках, зокрема коли було внесено зміни до наявних систем, деякі вимоги можуть бути виражені у формі характеристик засобів захисту, які можуть бути застосовані.

Структура захисту інформаційних технологій зосереджується на технічних службах безпеки і способах досягнення ними цілей безпеки. При цьому беруть до уваги і суміжні нетехнічні засоби захисту. Навіть коли структура формується із множини різних концепцій і підходів, необхідно врахувати такий фундаментальний принцип: структура захисту інформаційних технологій звичайно складається з однієї чи кількох ділянок захисту (угруповань тих чи інших вимог захисту і засобів захисту). У разі порушення захисту однієї дільниці не повинне спричиняти порушення захисту іншої дільниці.

Проблема безпеки системи полягає у формуванні множини унікальних дільниць захисту. Дільниці захисту мають бути похідними від сфер практичної діяльності організації. Ці сфери відповідають специфічним функціональними напрямкам діяльності організації, таким як платіжний, виробничий,

обслуговування споживачів, чи вони можуть бути службами організації, такими як служба електронної пошти, організаційні служби тощо.

Дільниці захисту диференціюють за одним чи кількома такими атрибутами:

- рівні, категорії чи типи інформації, доступної в межах дільниці;
- діяльність стосовно дільниці;
- співтовариства спільних інтересів, пов’язані з дільницею;
- залежності між іншими дільницями та оточенням;
- типи функцій доступу до інформації, необхідні співтовариства спільних інтересів у межах дільниці.

Під час побудови структури захисту інформаційних технологій повинні бути враховані такі положення:

- взаємозв’язки і взаємозалежності між унікальними дільницями захисту;
- порушення чи прихована суть взаємозв’язків і взаємо залежностей, що послаблюють служби захисту;
- додаткові послуги чи запобіжні заходи, необхідні для коригування, контролю чи протистояння будь-якій слабкості.

Опис структури систем захисту інформаційних технологій не є самостійною одиницею, частіше він є залежним і взаємозв’язаним з іншими документами. Найважливіший з них – структурна схема системи та інші залежні структури, такі як апаратні засоби, зв’язки і застосування. Опис структури захисту інформаційних технологій не містить повного опису системи, він лише включає технічні положення та елементи, пов’язані з безпекою. Структура захисту інформаційних технологій має метою зменшити порушення при їх використанні настільки, наскільки це можливо за умови, що оточення вже має оптимальний захист;

Із структурою захисту інформаційних технологій пов’язано чи залежить від неї багато інших документів. До них належать:

- проєкт захисту інформаційних технологій;
- операційна концепція захисту інформаційних технологій;
- план безпеки інформаційних технологій;
- методики безпеки системи інформаційних технологій;
- сертифікація та акредитація системи інформаційних технологій, якщо є потреба.

Ідентифікація або огляд обмежень

Існує множина обмежень, що можуть впливати на вибір засобів захисту. Ці обмеження потрібно взяти до уваги при створенні рекомендацій і при впровадженні. Типові обмеження:

- *часові обмеження*

Існує множина часових обмежень. Наприклад, засоби захисту потрібно реалізувати в межах визначеного періоду часу, встановленого керівним апаратом. Інший тип часових обмежень: чи може захист бути реалізований в рамках життєвого циклу системи. Третій тип часових обмежень – період часу, за який адміністрація визначає допустимий період, на який система буде залишатися відкритою специфічному ризику;

- *фінансові обмеження*

Засоби захисту не повинні бути дорожчими, ніж вартість активів, для захисту яких вони розроблені. Потрібно прикласти значні зусилля, щоб не перевищити виділений бюджет. Проте у деяких випадках неможливо досягти бажаного захисту і рівня допустимого ризику в межах бюджетних обмежень. Тому прийняття рішення в цих умовах є компетенцією адміністрації;

- *технічні обмеження*

Технічних проблем, таких як сумісність програм чи апаратних засобів, можна легко уникнути, якщо їх брати до уваги в процесі вибору засобів захисту. Впровадження засобів захисту для наявної системи часто стримується

технічними обмеженнями. Ці складнощі можуть переміщати баланс засобів захисту до процедурних і фізичних аспектів безпеки;

- *соціологічні обмеження*

Соціологічні обмеження на вибір засобів захисту можуть бути специфічними для країни, області, організації чи навіть відділу в межах організації. Ними не можна нехтувати, тому що багато технічних засобів захисту потребують активного супроводу персоналом. Якщо персонал не розуміє потреби в засобах захисту і психологічно їх не сприймає, ймовірно, що ці засоби захисту стануть неефективними через певний час;

- *обмеження довкілля*

На вибір засобів захисту можуть впливати такі параметри оточення, як доступність у просторі, критичність щодо кліматичних умов і природного довкілля та урбаністичного географічного розташування тощо;

- *юридичні обмеження*

Юридичні аспекти, такі як захист персональних даних чи кримінальна відповідальність за програми з обробки інформації можуть впливати на вибір засобів захисту. Не стосуються інформаційних технологій закони й інструкції, такі як правила пожежної безпеки, положення трудових відносин тощо, які можуть також впливати на вибір захисту.

Визначення залишкового ризику

Після вибору засобів захисту і визначання зменшення ними рівня ризику завжди будуть залишкові ризики: ніяка система не може бути абсолютно захищеною. Ці залишкові ризики мають бути класифіковані для організації як "допустимі" чи "недопустимі". Ця класифікація може бути отримана аналізом потенційних порушень діяльності, пов’язаних із цими ризиками. Очевидно, що з неприйнятними ризиками не можна миритися і їх надалі треба розглядати. Адміністрації треба буде вирішити, чи будуть ці ризики прийняті через інші обставини (такі як витрати чи просто неможливість запобігання як у випадку

можливого руйнування будівель чи землетрусів; проте плани відновлювання після таких подій можуть бути створені), чи додаткові засоби захисту щодо зменшення недопустимих ризиків, можливо, дорогі у реалізації.

Методика керування безпекою системи інформаційних технологій

Методика керування безпекою системи інформаційних технологій повинна містити подробиці про необхідні засоби захисту й описувати їхнє призначення. План безпеки системи інформаційних технологій розглядає особливості їхнього застосування.

Багато систем вимагають власних методик безпеки, що ґрунтуються на аналізуваннях ризику. Це зазвичай актуально для великих і складних систем чи систем, що мають унікальні і специфічні властивості, які відсутні в інших системах організації. Методика безпеки системи інформаційних технологій повинна бути сумісною з методиками безпеки інформаційних технологій, щоб уникнути будь-яких протиріч. Вона повинна стосуватися більш конкретних положень, ніж методики безпеки інформаційних технологій. Методика безпеки системи інформаційних технологій ґрунтується на результатах розгляду аналізу ризику і визначенні засобів захисту для системи і підтримується комплексом засобів захисту, вибраних відповідно до оцінених ризиків. Ці засоби захисту гарантують, що для системи забезпечено належний рівень захисту.

Методика безпеки системи інформаційних технологій повинна ґрунтуватись на інформації, незалежній від використовуваної стратегії аналізування ризику і повинна містити засоби захисту (зокрема процедури), необхідні для досягнення відповідного рівня безпеки для розглянутої системи. Методика безпеки системи інформаційних технологій і всі супровідні документи повинні містити:

- визначення системи інформаційних технологій, опис її компонентів і меж (цей опис повинен охопити всі апаратні засоби, програмне забезпечення, людей, середовище і діяльність системи);

- визначення ділових цілей системи інформаційних технологій, які можуть впливати на методику безпеки інформаційних технологій для цієї системи, на обраний підхід до аналізування ризику, на вибір і пріоритетність реалізації засобів захисту;
- визначення цілей безпеки для системи;
- рівень залежності від системи інформаційних технологій, який визначає, наскільки ділова активність організації залежить від втрати чи потрапляння під загрозу системи інформаційних технологій, завдань, виконуваних цією системою інформаційних технологій, обробки інформації;
- рівень інвестування в інформаційні технології у поняттях вартості розробки, супроводу і заміни системи інформаційних технологій разом з капітальними і поточними витратами, а також витратами на виконання заміни;
- підхід до аналізування ризику, обраний для системи інформаційних технологій;
- активи системи інформаційних технологій, які хоче захистити організація;
- оцінку цих активів у поняттях того, що відбудеться з організацією, якщо ці активи перебувають під загрозою (значення інформації повинне бути описане в поняттях потенційних порушень ділової активності від розкриття, зміни, недоступності і знищення цієї інформації);
- загрози системі інформаційних технологій і оброблюваній інформації, охоплюючи залежність між активами і загрозами і ймовірність прояву загроз;
- вразливості системи інформаційних технологій, охоплюючи опис притаманних недоліків, що можуть використовуватись загрозами;
- загрози безпеці системи інформаційних технологій як результат:
    - потенційних порушень ділової активності організації;
    - ймовірності прояву загроз;

- легкості використовування вразливості;

- перелік засобів захисту, визначених для захисту системи інформаційних технологій;

- оцінену вартість захисту інформаційних технологій.

Якщо для системи виправданим є застосування лише базового захисту, все-таки необхідним є забезпечення інформацією і згідно інших вище вказаних положень, якщо навіть в деяких випадках достатньо меншого рівня деталізації, ніж для систем, де проводять докладне аналізування ризику.

План безпеки інформаційних технологій

План безпеки інформаційних технологій – документ, що визначає дії, потрібні, щоб впровадити необхідні засоби захисту для системи інформаційних технологій. Цей план повинен містити результати розгляду, описаного вище, дії, що будуть початі в межах короткого, середнього і тривалого проміжку часу, щоб досягти і забезпечити відповідний рівень захисту, витрати і план впровадження. Кожний план повинен містити:

- цілі безпеки в поняттях конфіденційності, цілісності, доступності, обліковості, достовірності і надійності;

- варіант аналізу ризику для визначення системи інформаційних технологій:

- оцінювання залишкових ризиків, очікуваних і прийнятих після впровадження засобів захисту;

- перелік обраних засобів захисту, що будуть реалізовані і перелік наявних і запланованих засобів захисту, разом із визначенням їхньої ефективності і необхідними удосконаленнями засобів захисту; цей перелік повинен містити:

  - пріоритети для застосування обраних засобів захисту і модернізацію наявних засобів захисту;

  - інформацію, як ці засоби захисту треба практично використовувати;

- оцінювання інсталяції і поточних витрат для цих засобів захисту;
- оцінювання людських ресурсів для застосування цих засобів захисту і для їх доопрацювання;
- докладний план робіт по впровадженню, що містить:
  - пріоритети;
  - план застосування з урахуванням цих пріоритетів;
  - необхідний бюджет;
  - обов'язки;
  - програму компетентності в захисті і навчання персоналу інформаційних технологій і кінцевих користувачів, що необхідні для гарантії ефективності засобів захисту;
  - графік процедур затвердження, якщо це необхідно;
  - план для процедур доопрацювання.

Крім того, план безпеки інформаційних технологій повинен описувати заходи контролю процесу правильного застосування засобів захисту:

- визначення процедур звітності про хід робіт;
- процедури визначення можливих труднощів;
- процедури затвердження кожного з пунктів, перерахованих вище, включаючи процедури, пов’язані, з можливою зміною деяких частин або всього плану за потреби.

Результатом цього кроку повинен бути детальний план безпеки інформаційних технологій кожної системи, заснований на методиці безпеки системи інформаційних технологій, що враховує результати розгляду. Він повинен гарантувати, що засоби захисту реалізовані вчасно, відповідно до пріоритетів, визначених з ризиків системи інформаційних технологій, і відповідно до опису того, як застосовувати засоби захисту і як досягти

відповідного рівня захисту. Він також повинен містити план процедур доопрацювання для забезпечення необхідного рівня захисту.

19.5. Застосування плану безпеки інформаційних технологій

Правильне впровадження засобів захисту залежить від добре структурованого і задокументованого плану безпеки інформаційних технологій. Компетенцію в захисті і навчання, пов’язані з кожною системою інформаційної технології, треба запроваджувати одночасно. Коли реалізація плану захисту інформаційних технологій закінчена, може знадобитися атестація всіх засобів захисту, перш ніж система чи служба буде передаватися в експлуатацію.

Застосування засобів захисту

Для застосування засобів захисту потрібно виконати всі необхідні кроки, описані в плані безпеки інформаційних технологій. Особа, відповідальна за план (як правило, це старший контролер системи захисту інформаційних технологій), повинна гарантувати, що пріоритети, плани та графік, відображені в плані безпеки інформаційних технологій, виконуються. Документація на засоби захисту для забезпечення безперервності та цілісності є важливою частиною документації захисту інформаційних технологій. Цей процес може бути виконаний різними способами.

Необхідною є така частина документації захисту, а саме: проєкт захисту, план продовження діяльності (при ураженнях), документація аналізування ризику, методики і процедури захисту. Документацію розробляють для забезпечення потреб управління, використання, адміністраторами, обслуговуючим персоналом; вона повинна включати управління змінами й конфігурацією. Документування засобів захисту повинно бути актуальним і досить докладним, щоб допомогти усунути відхилення у захисті й недогляди та подати інформацію, яка буде гарантувати, що захист діє правильно та ефективно. Велика частина документації, особливо про загрози, вразливості і

ризики, є досить важливою і повинна бути захищена від не уповноваженого розкриття. У результаті більшість організацій повинна обробляти цю документацію дуже обережно і може використовувати послуги "довірчих процедур" поширення.

Якщо такі процедури використовують, вони повинні також бути задокументовані з описом того, як важливі частини інформації про засоби захисту будуть зберігатися, як до них доступатися та використовувати. Крім того, процедури повинні визначити, хто є відповідальним за рішення, яким чином захищена інформація буде зберігатися, і хто матиме доступ та користуватиметься нею. Під час розробляння процедур поширення рішення щодо доступності інформації про засоби захисту необхідно врахувати особливі чинники, такі як знаходження і використання сценаріїв ділової активності, включаючи планування випадковостей і відновлення після уражень, стратегію і план(и), випадків уражень чи інших непередбачених обставин, де час є дуже важливим. Нарешті, необхідне чітке керування конфігурацією засобів захисту для гарантування, що ніякі не уповноважені зміни, що можуть ненавмисно чи несвідомо зменшити ефективність засобів захисту, можуть бути зроблені.

Після завершення плану захисту і завершення ключових функцій повинні бути реалізовані засоби захисту, виконана перевірка відповідності засобів захисту і їх випробовування. Має бути проведена перевірка відповідності захисту, щоб визначити правильність застосування засобів захисту, ефективність їх використання та випробовування. Випробовування захисту можна проводити як частину цього перевіряння. Випробовування – важливий захід для впевненості в тому, що впровадження виконано і закінчено правильно. Випробовування захисту повинне керуватися планом проведення випробовувань захисту, де описуються задачі випробовування, графік і умови. Випробовування на проникнення можна проводити, ґрунтуючись на оцінюванні ризиків. Повинні бути написані докладні процедури випробовування захисту і

треба використовувати стандартний звіт про випробовування. Мета його полягає в тому, щоб реалізувати і перевірити способом, який гарантує, що вимоги плану захисту інформаційних технологій виконуються і ризик зменшено, як і було уточнено.

Компетентність у кіберзахисті

Мета програми компетентності в захисті полягає в тому, щоб збільшити рівень розуміння працівників організації до такого, коли процес захисту стає роботою, яку всі працівники можуть легко виконувати. Програма повинна гарантувати, що персонал і кінцеві користувачі інформаційних технологій мають достатні знання про систему інформаційних технологій (апаратні засоби і програмне забезпечення) і що вони розуміють необхідність захисту та як їх правильно використовувати. Тільки засоби захисту, сприйняті персоналом інформаційних технологій і кінцевими користувачами, можуть працювати ефективно.

Вихідні дані для програми компетентності в захисті повинні бути отримані від усіх рівнів організації. Вона повинна також містити методику безпеки інформаційних технологій, що покриває всі цілі плану безпеки інформаційних технологій організації. До групи компетентності необхідно включити керівників від усіх відділів. Наступні положення повинні бути детально розглянуті на курсах, у бесідах чи будь-якими іншими діями, описаними в програмі компетентності захисту:

- план пояснення значення захисту організації та осіб;
- потреби в захисті і цілі для систем інформаційних технологій в термінах конфіденційності, цілісності, доступності, обліковості, достовірності і надійності;
- приховані аспекти захисту для організації та осіб;
- правильне використовування системи інформаційних технологій, включно з апаратними засобами і програмним забезпеченням;

- пояснення цілей, методика безпеки інформаційних технологій, рекомендації та інструкції по захисту, методика керування ризиком, які ведуть до розуміння ризиків і заходів захисту;
- необхідний захист згідно ризиків системи інформаційних технологій;
- обмеження доступу до приміщень інформаційних технологій (допуск персоналу, блокування дверей, реєстрація на вході тощо) і до інформації (логічне контролювання доступу, права на читання/модифікацію) і пояснення причин цих обмежень;
- необхідність повідомляти про спробу порушення або порушення захисту;
- процедури обліковості та опису завдань;
- все, що персонал і кінцеві користувачі інформаційних технологій не повинні робити з погляду кіберзахисту;
- злагодженість дій персоналу, відповідального за порушення захисту;
- плани захисту системи інформаційних технологій щодо застосування і перевіряння засобів кіберзахисту;
- призначення засобів захисту і настанови як їх коректно використовувати;
- процедури, пов’язані з перевірянням відповідності кіберзахисту;
- керування змінами і настроюваннями.

Розробка програми компетентності в захисті починається з перегляду стратегій безпеки, цілей і методик. Цей процес повинна проводити група співробітників, до обов’язків яких належить визначення головних функцій організації і які мають повну підтримку вищим керівництвом.

Група з аналізу повинна встановити порушення вимог відповідно до методики безпеки інформаційних технологій. Це треба проводити в тісному зв’язку із забезпеченням всебічного захисту (не тільки інформаційних

технологій) і висвітлювати в різних формах, таких як наочні плакати, періодичні видання, бюлетені організації і внутрішнє розсилання.

Група повинна провести відповідні інструктажі з питань захисту. Попередньо проводять також повний аналіз вимог, щоб сформувати необхідну інформаційну базу для інструктажу. Кожен інструктаж треба проводити регулярно через певні проміжки часу (наприклад, кожних шість місяців), щоб гарантувати, що весь персонал ознайомлений з ризиками, властивими сучасним інформаційним технологіям.

Відповідальність за визначення цілей і зміст програми компетентності повинна бути розподілена на рівні ради з захисту інформаційних технологій. Відповідальним за її розробку і реалізацію призначають контролера безпеки інформаційних технологій і групу забезпечення компетентності у захисті. Це доцільно виконувати разом з іншими корпоративними заходами по навчанню. Проте до обов'язків кожної особи належить обізнаність у методиках захисту і процедурах їхньої реалізації, отже програма компетентності в захисті має бути впроваджена на всіх рівнях організації.

Для успішної розробки програми компетентності в безпеці мають бути враховані такі компоненти.

Аналіз вимог

Для визначення рівня компетентності уже наявних професійних груп (виконавці, керівництво і службовці) і більш прийнятних способів передачі їм нової інформації, необхідно виконати аналіз вимог обізнаності у захисті. Аналіз вимог охоплює методику, процедури, відношення до поінформованості щодо захисту і порівняно бажаної ефективності з поточною фактичною ефективністю.

Засвоєння програми

Програма компетентності у загальній безпеці має містити інтерактивні і методи підтримки засвоєння. Ця частина програми компетентності повинна зосереджуватися на неточностях, що були визначені в результаті аналізу вимог.

Працівники повинні набувати уміння оцінювати і розуміти цінність активів інформаційних систем і реальність для них загроз.

Одна з переваг такої програми компетентності в захисті організації це, те, що вона надає працівникам можливість брати участь у програмі захисту. Інтерактивні методи (наради персоналу, навчальні курси тощо) забезпечують інший шлях взаємодії, що дозволяє учасникам і персоналу безпеки перевіряти правильність концепцій і вимог, що випливають з аналізу вимог. Заходи підтримки (відео, E-mail-вставки з безпеки в електронну пошту, плакати, публікації) – односторонні засоби зв'язку, що дають змогу керівництву широкомовно повідомляти концепції, інформацію і відносини недорогим способом.

Контролювання програм компетентності в кібербезпеці

Існує дві відмінні складові, які забезпечують ефективний контроль програми компетентності в безпеці:

- періодичні оцінювання продуктивності, які визначають ефективність програми компетентності, контролюючи дії, пов'язані з захистом, і визначають, які зміни, що впливають на засвоєння програми, можуть знадобитися;
- керування змінами у програмі компетентності. Щоразу, коли відбуваються зміни в загальній програмі захисту (тобто в методиці або зміні стратегії, уведення нових активів чи технологій або відбуваються зміни в загрозах та інше), вимагаються відповідні зміни в програмі компетентності в безпеці, щоб поновити наявні знання і рівень навичок, що відображають ці зміни.

Навчання захисту

Крім загальної програми компетентності в безпеці, що повинна бути спрямована на кожного в організації, необхідне особливе навчання захисту персоналу: із завданнями та обов'язками, пов'язаними з безпекою

інформаційних технологій. Рівень поглибленості навчання захисту повинен залежати від загального значення захисту інформаційних технологій для організації і має змінюватись відповідно до вимог захисту. У разі потреби необхідно вдаватися до більш ґрунтовного навчання, такого як відвідування лекцій в університетах, курсів. Програма навчання захисту інформаційних технологій повинна бути розроблена таким чином, щоб вмістити всі вимоги захисту організації.

Під час визначання персоналу, для якого потрібно проводити навчання захисту, необхідно врахувати:

- персонал з головними обов'язками з проєктування і розробки систем інформаційних технологій;
- персонал з головними обов'язками з діяльності системи інформаційних технологій;
- контролерів безпеки, контролерів безпеки проєкту інформаційних технологій і системи інформаційних технологій;
- персонал з обов'язками адміністрування захисту, такими як контроль доступу, організовування каталогів.

Крім того, повинна здійснюватись перевірка, щоб визначити необхідність у спеціальному навчанні захисту для поточних і запланованих задач, проєктів тощо. Коли приступають до завдань чи проєктів зі спеціальними вимогами захисту, потрібно подбати, щоб була розроблена відповідна програма навчання захисту перед безпосереднім початком проєкту і щоб вона була виконана вчасно.

Тематика навчальних курсів із захисту має залежати від ролі і обов'язків осіб, що навчаються. Загальні положення можуть містити:

- що таке безпека:
    - запобігання порушень конфіденційності, цілісності і доступності;

- потенційні порушення ділової активності організації чи особи;
- схему класифікації важливості інформації;

- загальний процес захисту:
  - опис загального процесу;
  - складові аналізу ризику;
- засоби захисту і супровідне навчання застосуванню засобів захисту;
  - ролі та обов’язки;
  - методику захисту системи інформаційних технологій.

Правильне впровадження і використання засобів захисту – найважливіші складові програми навчання захисту. Кожна організація повинна розробити власну програму навчання захисту відповідно до потреб щодо наявних чи запланованих засобів захисту. Такі приклади положень навчання засобам захисту повинні бути розглянуті з врахуванням рівноваги між нетехнічними і технічними засобами захисту:

- інфраструктура захисту:
  - ролі та обов’язки;
  - методика безпеки;
  - регулярне перевіряння відповідності захисту;
  - обробляння інциденту захисту;
- фізичний захист:
  - будівель;
  - адміністративно-службових приміщень;
  - устаткування;
- захист персоналу;
- захист носіїв (даних);
- захист апаратних засобів/програмного забезпечення:
  - ідентифікація та автентифікація;

- контролювання логічного доступу ;
- облік і ревізія захисту;
- рівні допуску до фізичної пам’яті;

- захист комунікацій:
  - мережної інфраструктури;
  - мостів і шлюзів, маршрутизаторів, мережних пристроїв захисту;
  - Internet і інших зовнішніх каналів зв’язку;
- продовження діяльності, охоплюючи планування і відновлення після уражень, стратегії і план(и).

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

- Назвіть цілі стратегії методики кібербезпеки інформаційних технологій.
- Основні аспекти керування ризиком, з використанням детального аналізу ризику.
- Дайте визначення поняття актив.
- Яким чином здійснюється оцінювання загроз?
- Яким чином відбувається визначення засобів захисту?
- Проаналізуйте структуру кіберзахисту інформаційних технологій?

РОЗДІЛ 20. МЕТОДИ ТА ПІДХОДИ У КЕРУВАННІ КІБЕРБЕЗПЕКОЮ

Світовий досвід розвитку управління і науки управління потребує детального вивчення, об’єктивного осмислення для подальшого використання .

У теперішній час зарубіжна наука використовує чотири основних підходи до управління:

- підхід з позицій різних шкіл в управлінні;
- процесний підхід;

- системний підхід;
- ситуаційний підхід.

Існують чотири школи, які відрізняються своїм підходом до управління:

- школа наукового управління;
- адміністративна або класична школа;
- школа людських стосунків та поведінських наук;
- школа науки управління, заснована на кількісному підході.

20.1. Метод наукового управління

Для цього треба фіксувати трудові операції, що виконуються співробітниками шляхом спостережень, вимірів, фото- і відео зйомки, а потім на основі логічного аналізу намагатися їх удосконалити. Таким чином, методологія наукового управління включала дві фази:

1) Аналіз змісту виконуваних працівником трудових операцій і виділення їх основних.

2) Зміна робочих операцій на основі отриманої інформації з метою усунення зайвих, непродуктивних рухів і підняття ефективності роботи в цілому.

Даний підхід не заперечував важливості обліку соціальних аспектів в управлінні, зокрема:

- виділення управлінських функцій від фактичного виконання роботи і визнання того, що управління – це певна спеціальність;
- систематичне використання стимулювання з метою зацікавити працівників в збільшенні продуктивності і об'єму виробництва;
- визначення об'єктивно виконаних норм виробництва і додаткова винагорода персоналу за перевищення в роботі встановленого мінімуму;
- мотивація праці за принципом "більша винагорода за більшу працю";

- професійний підбір людей, які фізично і інтелектуально відповідають виконуваній роботі;
- важливість професійної підготовки (навчання) працівників.

Разом з тим, у поглядах представників цього підходу пануюче положення в управлінській діяльності керівників займає фінансова мотивація праці.

Концепція наукового управління з'явилася серйозним переломним етапом, завдяки якому управління стало широко визнаватися як самостійна область наукових досліджень. Вперше керівники-практики і вчені побачили, що методи й підходи, використовувані в науці і техніці, можуть ефективно застосовуватися для досягнення мети організації. Крім того, вона з'явилася основою наукової організації праці (НОТ) – процесу вдосконалення організації праці на основі досягнень науки і техніки, фізіології і гігієни праці.

20.2. Методи адміністративного управління

Виходячи із соціального положення в суспільстві, їх головною турботою стало підвищення ефективності роботи всієї організації в цілому. "Класики" вивчали організацію з погляду широкої перспективи, намагаючись визначити загальні характеристики і закономірності розвитку організацій. Метою класичної школи було створення універсальних принципів управління, слідуючи яким можна добитися успіху в діяльності організації. Ці принципи зачіпали два основні аспекти:

1) **Розробка раціональної системи управління організацією**. Визначаючи основні функції управління, "класики" були впевнені в тому, що можуть визначити кращий спосіб розділення організації на підрозділи і робочі групи. Головний внесок А. Файоля в теорію управління полягав в тому, що він розглянув управління як універсальний процес, що складається з декількох взаємопов'язаних функцій. За його словами "управляти означає передбачати і планувати, організовувати, розпоряджатися, координувати і контролювати".

2) **Побудова структури організації і управління працівниками**.

Принципи управління, сформульовані А. Файолем, не втратили своєї актуальності і зараз.

Розглядаючи адміністративну школу управління, не можна не згадати про ідеї ідеального управлінського підходу – бюрократії**,** сформульованої німецьким соціологом Максом Вебером (1864-1920), в якій основним суб'єктом управління виступав державний службовець (чиновник).

Іншими словами, М. Вебер запропонував поняття *формальної організації*: це група людей, діяльність яких раціональна (тобто у її основі лежить принцип доцільності, свідомого руху до певної мети); вона безособова, тобто розрахована на індивідів, відносини між якими встановлюються наперед складеною програмою.

Основний внесок представників класичної школи в теорію управління полягав у тому, що вони розглядали управління як універсальний процес, який розвивається в часі і включає реалізацію взаємозв'язаних функцій: планування, організацію, мотивацію і контроль.

20.3. Метод людських відносин

Як ми бачимо, адміністративна школа управління розвернула вектор управлінської думки від техніки виконання трудових операцій до організації виробництва в цілому, але при цьому основний акцент був зроблений на процес реалізації управлінських функцій безвідносно до того, хто їх виконує. Це пояснювалося в першу чергу тим, що на той час психологія – наука про психічне віддзеркалення дійсності в свідомості людини в процесі його життєдіяльності, знаходилася ще в зачатковому стані. Виняток становив психоаналіз, розроблений в працях австрійського лікаря-психіатра і психолога Зигмунда Фрейда (1856-1939 рр.).

У основі психоаналітичної концепції особи З. Фрейда лежить представлення психічної структури людини у вигляді трьох компонент:

1) *Ід* – ірраціональна, біологічно обумовлена, "темна" і "недоступна" частина психіки, складова її несвідомого, нестримно штовхає людину на задоволення її інстинктивних потреб, пристрасті і т.п.

2) *Его* – колишня частина *Ід*, яка під впливом зовнішньої дійсності стала тим, "що може бути назване розумом і здоровим глуздом".

3) *Супер-его* – частина *Его*, в якій відбиваються норми і заборони суспільства.

Психічне життя людини проходить в постійній боротьбі цих компонентів, результатом якої є або придушення руйнівних для особи і суспільства вабления *Ід*, або їх несвідома трансформація в прийнятні для суспільства форми.

З позицій управління психоаналітичні концепції допомагають описати емоційні відносини, що виникають між співробітниками соціальних організацій.

Таким чином, якщо керівництво проявляє велику турботу про свій персонал, то рівень задоволеності співробітників повинен зростати і вести до збільшення продуктивності. Як психологічні методи мотивації рекомендувалося використовувати прийоми управління людськими відносинами, що включають ефективні дії безпосередніх начальників, консультації із співробітниками і надання їм ширших можливостей спілкування на роботі.

Мораль висока, коли людина відчуває, що його особисті потреби і цілі задовольняються оточенням, в якому він працює. Для досягнення високої моралі існує безліч шляхів:

- активна участь в реалізації загальної мети повинна заохочуватися;
- співробітники підрозділу повинні бути психологічно сумісними один з одним;
- робота повинна бути порівну розподілена між співробітниками;

- повинна культивуватися атмосфера свободи і толерантності в підрозділі, правила і покарання повинні бути зведені до мінімуму.

Висока мораль усередині підрозділу виражається в наступному:

- відчуття загальної мети, що розділяється всіма співробітниками;
- віра, що завдання, поставлене перед підрозділом, реальне і мета досяжна;
- протидія виникненню розбіжностей між співробітниками;
- співпраця і відчуття спільності.

Школа поведінкових наук значно відійшла від школи людських відносин, що зосередилася перш за все на методах налагодження між особових відносин. Новий підхід зосередив свої зусилля на наданні допомоги працівникові в усвідомленні своїх власних можливостей на основі застосування концепцій поведінкових наук до побудови і управління організаціями. Основною метою

цієї школи з'явилося підвищення ефективності організації за рахунок ефективного використання її людських ресурсів.

Рис. 20.1. Модель ієрархії потреб

Таким чином, з даної теорії витікає важливий висновок: керівник повинен ретельно спостерігати за своїми підлеглими, щоб вирішити, які активні потреби рухають ними. Оскільки з часом ці потреби міняються, не можна розраховувати, що мотивація, спрацювавши один раз ефективно, працюватиме весь час.

Таким чином, з даної теорії витікає важливий висновок: керівник повинен ретельно спостерігати за своїми підлеглими, щоб вирішити, які активні потреби рухають ними. Оскільки з часом ці потреби міняються, не можна розраховувати, що мотивація, спрацювавши один раз ефективно, працюватиме весь час.

Теорія справедливості постулювала, що люди суб'єктивно визначають відношення отриманої винагороди до витрачених зусиль і потім співвідносять його з винагородою інших співробітників, що виконують аналогічну роботу. Якщо порівняння показує дисбаланс і несправедливість, то у людини виникає психологічна напруга. В результаті необхідного мотивувати цього співробітника, зняти напругу і для відновлення справедливості виправити дисбаланс.

Дослідження показують, що зазвичай, коли люди вважають, що їм недоплачують, вони починають працювати менш інтенсивно. Якщо ж вони вважають, що їм переплачують, вони менш схильні змінювати свою поведінку і діяльність. Основний висновок теорії справедливості для практики управління полягає в тому, що до тих пір, поки люди не почнуть вважати, що вони отримують справедливу винагороду, вони будуть прагнути до зменшення інтенсивності праці.

Важливий внесок поведінкові науки внесли також до **теорії лідерства**, проаналізувавши і склавши класифікацію стилів керівництва.

Стиль керівництва в управлінні – це звична манера поведінки керівника по відношенню до підлеглих, щоб зробити на них вплив і спонукати до досягнення мети організації.

Одним з найдавніших досліджень ефективності, яке було проведено являються стилі лідерства. Його результати звелися до наступних:

1. *Авторитарне керівництво* характеризується високим ступенем одноосібної влади керівника: керівник визначає всі стратегії групи; ніяких повноважень групі не делегується.

2. *Демократичне керівництво* характеризується розділенням влади і участю співробітників в управлінні; відповідальність не концентрується, а розподіляється.

3. *Ліберальне* керівництво (потурання) характеризується мінімальною участю керівника; група має повну свободу ухвалювати власні рішення.

4. Авторитарне керівництво добивається виконання більшого об'єму роботи, ніж демократичне. Проте при цьому низька мотивація, менше оригінальності, менше дружелюбності в групах, відсутність групового мислення, велика агресивність, що проявляється як до керівника, так до інших членів групи, велика пригнічувана тривога і одночасно – більш залежна і покірна поведінка.

5. В порівнянні з демократичним керівництвом, при ліберальному керівництві об'єм роботи зменшується, якість роботи знижується, з'являється більше гри, і в дослідження виражається перевага демократичного керівника.

Ці дослідження дали основу для пошуків стилю керівництва, який може привести до високої продуктивності праці і високого ступеня задоволеності.

Конфлікти в колективі можуть носити як негативний, так і позитивний характер. Деякі конфлікти не тільки можливі, але навіть можуть бути бажаними, оскільки допомагають виявити різноманітність точок зору, дають додаткову інформацію з вирішуваної проблеми, допомагають виявити більше число альтернатив або проблем і т.д. Іншими словами, конфлікт може бути *функціональним* і вести до підвищення ефективності організації або він може

бути *дисфункціональним* і призводити до зниження особистої задоволеності, групової співпраці і ефективності організації.

Роль конфлікту, в основному, залежить від того, наскільки ефективно їм управляють керівники. Щоб управляти конфліктом, необхідно розуміти причини виникнення конфліктної ситуації. Існує чотири основні типи конфлікту:

a) **внутрішньоособовий конфлікт** – пов'язаний з конкретною особою і може приймати різні форми, наприклад, *ролевий конфлікт*, коли до однієї людини пред'являються суперечливі вимоги з приводу того, яким повинен бути результат його роботи, або порушується принцип єдиноначальності. Іншою формою може бути конфлікт, що виникає в результаті *розузгодження вимог* до співробітника і його особистими потребами або цінностями. Внутрішньоособовий конфлікт може також бути реакцією на робоче перевантаження або недовантаження, тобто такий конфлікт пов'язаний з низьким ступенем задоволеності роботою або стресом;

b) **міжособовий конфлікт** – це конфлікт між різними людьми, що проявляється по-різному. Найчастіше це боротьба керівників за обмежені ресурси, час використання устаткування або схвалення проєкту (плану). Кожний з них вважає, що оскільки ресурси обмежені, він повинен переконати вище начальство виділити ці ресурси саме його підрозділу, а не іншому. Такий конфлікт може також виявлятися і як зіткнення осіб. Люди з різними рисами характеру, поглядами і цінностями іноді просто не в змозі ладнати один з одним. Як правило, погляди і цілі таких людей розрізняються в корені;

c) **конфлікт між особою і групою** виникає в тих випадках, коли очікування групи знаходяться в суперечності з очікуваннями окремої особи. Він може виникнути, якщо особа займе позицію, що відрізняється від позиції групи. Аналогічний конфлікт може виникнути і на підґрунті посадових обов'язків керівника: між необхідністю забезпечити відповідний рівень роботи і при цьому

дотримати правила і процедури, прийняті в організації. Керівник може виявитися вимушеним вживати дисциплінарні заходи, які можуть виявитися непопулярними в очах підлеглих;

d) **міжгруповий конфлікт** виникає між формальними, і неформальними групами в організації. Прикладом такого конфлікту можуть служити розбіжності між лінійними і штабними підрозділами в організації. Лінійні керівники можуть відкидати рекомендації штабних фахівців і виражати незадоволеність з приводу своєї залежності від них у всьому, що пов'язане з інформацією.

Причинами конфліктів можуть бути:

- обмеженість розподілених ресурсів;
- взаємозалежність вирішуваних задач;
- відмінності у поставлених, що стоять;
- відмінності в наявних уявленнях і цінностях;
- відмінності в манері поведінки і життєвому досвіді;
- незадовільний стан комунікації та ін.

Таким чином, в складних ситуаціях, де різноманітність підходів і точна інформація є істотними для ухвалення здорового рішення, появу конфліктуючих думок треба навіть заохочувати і управляти ситуацією, використовуючи стиль вирішення проблеми.

Головний постулат школи людських відносин полягає в тому, що правильне застосування науки про поведінку завжди сприятиме підвищенню ефективності як окремого працівника, так і організації в цілому. Іншими словами, цей підхід відстоює "єдиний якнайкращий шлях" вирішення управлінських проблем.

20.4. Метод кількісного підходу в управлінні

Серед численних проблем, виникнення яких обумовлене науково-

технічною революцією, що бурхливо розвивається, найбільш важливою є проблема вдосконалення управління в усіх ланках людської діяльності. Щоб добитися високої якості управління сучасному керівникові далеко не завжди буває достатньо особистого досвіду, інтуїції і організаторських здібностях. При формуванні як стратегічних, так і багатьох тактичних рішень керівник вимушений враховувати численні, нерідко взаємно суперечливі міркування і спиратися на складні критерії ефективності при виборі шляхів досягнення кінцевої мети.

"**Дослідження операцій"** є науковий метод, що дає в розпорядження військового командування або іншого виконавчого органу кількісні підстави для ухвалення рішень дії військ або інших організацій, що знаходяться під його управлінням".

З цього визначення витікають наступні висновки:

1. Це науковий метод, що має визнану і організовану діяльність з певною методикою підходу до вирішення виникаючих проблем і знаходження кінцевого рішення.

2. Цей метод пов'язаний з отриманням кількісних оцінок, на основі яких ухвалюються рішення. Отже, в його основі лежать певні математичні методи.

3. Дослідження операцій є прикладною наукою, що застосовує всі відомі наукові методи для вирішення специфічних проблем, що є основою для ухвалення рішень.

4. Кількісні оцінки і критерії, вживані в дослідженні операцій, безумовно, не є вичерпними даними для ухвалення рішення людиною, але допомагають йому в цьому процесі.

Під *операцією* розуміється всякий захід (або система дій), об'єднаний єдиним задумом і направлений на досягнення якої-небудь мети. Операція є керованим заходом. Вибір певних параметрів, що впливають на операцію, називається *рішенням*. Рішення можуть бути вдалими або невдалими,

розумними або безрозсудними. *Оптимальними* називаються рішення, за тими або іншими ознаками переважні перед іншими. Мета дослідження операцій – попереднє кількісне обґрунтування ухвалення оптимальних рішень.

Саме ухвалення рішення виходить за рамки дослідження операцій і відноситься до компетенції суб'єкту управління, який при виборі може враховувати разом з рекомендаціями, що випливають з математичного розрахунку, ще ряд міркувань (кількісного і якісного характеру), які цим розрахунком не враховані. Останнє зауваження дуже важливе. Недаремно один з великих фахівців з дослідження операцій американець Т.Л. Сааті, визначаючи свій предмет, пише про те, що "*дослідження операцій є мистецтво давати погані відповіді на ті практичні питання, на які даються ще гірші відповіді іншими методами*".

Опис будь-якого завдання дослідження операцій включає завдання компонентів (чинників) рішення, обмежень, що накладаються на них, і системи цілей. Кожній з цілей відповідає *цільова функція*, задана на множині допустимих рішень, значення якої виражають міру здійснення мети. Завдання дослідження операцій класифікують за їх теоретико-інформаційними властивостями. Якщо суб'єкт управління в ході ухвалення рішення зберігає свій інформаційний стан, тобто ніякої інформації не набуває і не втрачає, то ухвалення рішення можна розглядати як миттєвий акт. Відповідні завдання називаються *статичними*. Навпаки, якщо суб'єкт в ході ухвалення рішення змінює свій інформаційний стан, отримуючи або втрачаючи інформацію, то в такому динамічному завданні зазвичай доцільно ухвалювати рішення поетапно (багатокрокові рішення). Значна частина динамічних завдань дослідження операцій входить в динамічне програмування.

Відмітними особливостями науки управління як підходу до рішення управлінських задач являються наступні:

- використання наукового методу;

- системна орієнтація;
- використання моделей.

Розвиток логіко-математичних методів управління і засобів обчислювальної техніки привів до появи в середині 60-х років нового класу складних систем – автоматизованих систем управління (АСУ) різного типу і призначення.

АСУ є засобом комунікації, тобто обміну інформацією на всіх стадіях управлінського циклу між носіями управлінських відносин. Кожен суб'єкт управління є вузлом комунікаційної мережі, в якій здійснюється обмін різноманітною інформацією, що поступає від різних джерел і направляється за різними адресами - одержувачами. Розрізняють внутрішні комунікації: горизонтальні (між різними підрозділами) і вертикальні (вихідні і вхідні), тобто між різними ієрархічними рівнями. Особливий різновид внутрішніх комунікацій – це комунікації між керівником і його підлеглими. Специфічним видом внутрішньої комунікації є неформальні комунікації (канал поширення чуток, домислів). Мабуть, найбільш значним компонентом в системі комунікацій в організації є міжособові відносини "керівник - підлеглий". Виділяють комунікації між системою, організацією та її зовнішнім середовищем, в ході яких задовольняються власні інформаційні потреби, забезпечуються зв'язки із споживачами і громадськістю, створюється імідж організації, вирішуються інші завдання і т.д.

Комунікаційний процес не можна зводити до обміну інформацією. У комунікації передається не тільки раціональний, але і емоційний зміст, виявляються в тій чи іншій мірі особові якості, ціннісні орієнтири учасників комунікаційного процесу, сприйняття ними один одного. В процесі обміну інформацією можна виділити чотири основні компоненти:

1) *відправник* – особа, що генерує ідеї або що здійснює пошук інформації і передає її;

2) *повідомлення* – інформація, закодована за допомогою символів певного алфавіту;

3) *канал* – засіб передачі інформації;

4) *одержувач* – особа якій адресована інформація.

Комунікаційний процес зазвичай розділяють на наступні етапи;

- зародження ідеї;
- кодування і вибір каналу;
- передача; декодування.

20.5. Процесний підхід в управлінні

Розробка концепції процесного підходу з'явилася великим поворотом управлінської думки. Уперше вона була запропонована в рамках школи адміністративного управління, що спробувала описати функції керівника в процесі реалізації управління організацією. Однак її автори розглядали ці функції незалежно один від одного. Процесний підхід, на противагу цьому, розглядає функції управління як взаємозалежні.

Управління варто розглядати як процес, тому що робота з досягнення цілей за допомогою інших людей - це не якась одноразова дія, а серія безперервних взаємозалежних дій, що розгортаються в часі й у просторі. Ці дії, кожне з яких саме по собі є процесом, дуже важливі для успіху організації. Їх називають **управлінськими функціями**. Процес управління є інтегральною сумою всіх функцій.

У різноманітних джерелах по теорії управління виділяють наступні функції:

- цілепокладання;
- планування;
- організація;
- розпорядливість (або командування);

- мотивація;
- керівництво;
- координація;
- контроль;
- комунікація;
- дослідження;
- оцінка;
- прийняття рішень;
- підбор і розміщення персоналу;
- представництво;
- ведення переговорів та ін.

Разом з цим, ряд функцій можна об'єднати і вважати, що процес керування складається із чотирьох основних функцій:

- планування;
- організації;
- мотивації;
- контролю.

Ці первинні функції об'єднані сполучними процесами **комунікації** й **ухвалення рішення**. **Управління** (*лідерство*) розглядається як самостійна діяльність, що припускає можливість впливу на окремих підлеглих і групи співробітників таким чином, щоб вони працювали в напрямку досягнення цілей організації.

Розробка і реалізація стратегії - найважливіша функція керівників фірми вищої ланки управління. Стратегія формулює основні цілі фірми і шляхи їхнього досягнення таким чином, щоб забезпечити єдину спрямованість дій усього колективу фірми.

Стратегічне планування визначає характер стратегічного управління. Реалізація стратегічних планів, стратегічний контроль і виявлення проблем, що виникають, відносяться до сфери оперативного управління і тому не можуть розглядатися як стратегічні фактори.

Підкреслимо такі особливості стратегічного планування: воно орієнтується на довгострокову перспективу; стратегічні плани визначають основні напрямки розвитку підприємства з урахуванням внутрішніх і зовнішніх зв'язків і тенденцій їх розвитку; основна мета стратегічного планування полягає в забезпеченні майбутньої успішної діяльності підприємства.

Функція мотивації – це створення таких умов, щоб члени організації виконували роботу відповідно до делегованих їм повноважень й відповідно із планом. Керівник повинен завжди пам'ятати, що навіть прекрасно складені плани й сама зроблена структура організації не мають ніякого змісту, якщо хтось не виконує фактичну роботу.

Поведінка кожної людини визначається мотивами, тобто внутрішніми силами, що спонукають людину до здійснення певних дій. Мотиви проявляються у вигляді реакції людини на фактори її внутрішнього стану або впливу навколишнього середовища, зовнішньої обстановки, ситуацій, умов. Кожна людина має власну структуру мотивів, що формується в процесі її розвитку, прояву й самооцінки своїх здатностей, досягнення яких-небудь результатів. Мотиви визначаються потребами людини, усвідомленням ступеня й можливостей їхнього задоволення. Але, крім цього, людині властиві її інтереси, які відбивають її прагнення до зміни структури своїх потреб за еталоном ідеальної уяви про можливий спосіб життя в сучасних умовах. Інтереси народжують у поводженні людини стимули, тобто мотиви особливого виду – зацікавленість. Реалізація інтересів супроводжує будь-яку діяльність людини. На цьому будується стимулювання.

Функція контролю – це реалізація зворотного зв'язку в управлінському процесі, тобто функція, за допомогою якої визначається, наскільки організація досягла своїх цілей.

Майже все, що робить керівник, звернено в майбутнє. Він планує досягти цілей за якийсь час, використовуючи ресурси. За цей період багато чого може трапитися: непередбачені обставини можуть змусити організацію відхилитися від основного спочатку наміченого курсу. І якщо керівництво виявиться нездатним знайти й виправити ці відхилення, то організації буде нанесений серйозний збиток, досягнення цілей буде поставлено під загрозу. Як указує один із законів Мерфі: "*Події, надані самим собі, мають тенденцію розвиватися в напрямку від поганого до гіршого*".

Основне призначення контролю - вчасно фіксувати відхилення від норми й вносити корективи в хід робіт, виправляючи допущені помилки, щоб досягти намічених цілей.

Існують три аспекти управлінського контролю:

a) *установлення стандартів* – це точне визначення цілей, які повинні бути досягнуті в позначений відрізок часу. Воно ґрунтується на планах;

b) *вимірювання* того, що було досягнуто в дійсності за певний період, і *порівняння* досягнутого з очікуваними результатами. Якщо ці фази виконані правильно, то керівництво організації не тільки знає про те, що в організації існує проблема, але й знає джерело цієї проблеми;

c) *виконання дій*, якщо це необхідно, для корекції серйозних відхилень від первісного плану.

До **основних властивостей** управлінського рішення, що характеризують його якість, відносяться наступні:

1. Надійність рішення – можливість при заданих вихідних припущеннях реалізувати результат з відомою долею ймовірності. При визначенні надійності

завжди враховують такі властивості, як безвідмовність, оперативність (швидкодія), точність, готовність, а також такі умови, як правильність постановки мети й припущень про динаміку станів системи, логічність критерію вибору альтернативи, компетентність кадрів, повноту й вірогідність інформації, ефективність структури управління тощо.

2. Об'єктивність і корисність рішення – дійсно існуюча практична потреба в рішенні та необхідність у ньому для досягнення бажаної мети.

3. Конкретність і гнучкість рішення – означаючі, з одного боку, чітку визначеність змісту рішення (через ясне розкриття його цілей і механізму їхнього досягнення конкретними виконавцями), а з іншого, – здатність внесення коректив в ухвалене рішення залежно від складних обставин його реалізації.

4. Компетентність рішення – правильне (законне) відбиття компетенції приймаючого його суб'єкта управління. Рішення повинне прийматися тим співробітником, що наділений для цього відповідними повноваженнями.

5. Своєчасність рішення – оперативність (швидкість) ухвалення рішення.

6. Контрольованість рішення – здатність спостереження з боку суб'єктів управління за ходом розробки, прийняття й реалізації управлінських рішень як за формою, так і за змістом.

7. Ефективність рішення – означає результативність його застосування по реалізації поставлених цілей і завдань й є інтегральною характеристикою, яка тією чи іншою мірою враховує усі вище описані властивості. Основними шляхами підвищення ефективності рішень являються:

- підсилення наукової обґрунтованості й стратегічного характеру рішень, їх активної цільової орієнтації на рішення вузлових проблем;
- широке використання сучасних методів вибору альтернатив і прийняття рішень, більше органічне зв'язування цільових програм і планів із прийнятими рішеннями;

- оптимальний розподіл функцій прийняття рішень між різними рівнями управління;
- зміцнення виконавчої дисципліни;
- підвищення професійного рівня керівників та ін.

Основною вимогою для прийняття ефективного об'єктивного рішення або для розуміння широкого масштабу проблеми є наявність адекватної точної інформації. Єдиним способом одержання такої інформації є **комунікація – процес обміну інформацією між двома й більше людьми**. Керівник від 50 до 90% свого часу витрачає на комунікації. Це пов'язано з необхідністю реалізації ролі керівника в міжособистісних відносинах, інформаційному обміні й процесах прийняття рішень. Ефективно працюючі керівники - це ті, хто ефективні в комунікаціях. Вони представляють суть комунікаційного процесу, мають добре розвинене вміння усного й письмового спілкування й розуміють, як середовище впливає на обмін інформацією.

Таким чином, підхід до управління, як процесу, що протікає в будь-якій організації, дозволяє в динаміці побачити управлінський цикл, що включає планування, організацію, мотивацію й контроль, об'єднаних один з одним процесами прийняття рішень і комунікації.

20.6. Системний підхід в управлінні

При зміні яких-небудь елементів або структури окремих підрозділів в організації, всі інші деякою мірою також відчувають вплив цих змін. Такого роду зміни можуть позначитися на майбутній ефективності організації в цілому. Щоб наочно уявити собі ці взаємодії й численні наслідки, керівник повинен:

- бачити перспективу для організації в цілому й для зв'язків організації з навколишнім середовищем;
- усвідомлювати безпосередній вплив рішень, прийнятих в організації, і їхній опосередкований вплив на різні аспекти організаційної діяльності;

- брати до уваги вплив навколишнього середовища на організацію й вплив організації на навколишнє середовище.

Споконвічний недолік підходів різних шкіл до управління полягав у тім, що вони зосереджували увагу тільки на якомусь одному важливому елементі, а не розглядали ефективність управління як результат, що залежить від багатьох різних факторів, тобто із системних позицій.

Оформлення системних принципів вважається одним з найбільш значних досягнень наукового знання другої половини XX в., які почали формуватися в США при розробці ядерної зброї. У рамках системних принципів в 60-і роки у зв'язку з необхідністю вирішувати завдання зовсім нового типу, пов'язані з організацією й управлінням складними технічними й соціотехнічними системами, реалізацією економічних і наукових проєктів, виділилися три основних області досліджень, що відрізняються цільовим напрямком і ступенем спільності:

1. Системний підхід – це загальне принципове уявлення про властивості матеріального світу як сукупності систем різної природи, тобто сучасна загальнонаукова методологія дослідження й пізнання складних систем.

2. Загальна теорія систем – методологічне уявлення про найзагальніші поняття системного мислення, системного підходу до реальної дійсності. Воно в найбільш загальному вигляді описує системи різних класів і типів і розробляє специфічні методи їхнього аналізу й синтезу.

3. Системний аналіз – прикладна дисципліна, що надає набір спеціальних методичних засобів, за допомогою яких можна реалізувати принципи системного підходу в конкретних дослідженнях.

Найважливішим елементом системного підходу є **системний аналіз**, що, по своїй суті, представляє реалізацію системного підходу на практиці й дозволяє звести складне до простого, важкорозв'язну й важкозрозумілу задачу перетворити в чітку серію завдань, що мають певний метод рішення. Відповідно

до принципів системного аналізу, що виникає, складна проблема управління повинна розглядатися як щось ціле, як система у взаємодії всіх її компонентів. Для ухвалення рішення про управління цією системою необхідно визначити її ціль, ціль її окремих підсистем і множину альтернатив досягнення цих цілей, які поєднуються за певними критеріями ефективності, і вибрати найбільш прийнятний для даної ситуації спосіб управління. Новим у системному аналізі в порівнянні з відомими методами дослідження є те, що в ньому, по-перше, здійснений синтез взаємозалежного кола понять, методів і прийомів, які раніше використовувалися розрізнено, і, по-друге, цей комплекс системних методів і прийомів поширюється на нові сфери дослідження.

Логічна структура системного аналізу включає наступні компоненти.

1. Вихідним пунктом системного аналізу й розробки альтернативних варіантів управлінських рішень є уявлення про цілісність досліджуваної системи. Звідси випливає, що, по-перше, система може бути створена (або зрозуміла й реконструйована) як щось ціле, що складається з окремих елементів і взаємодіє із зовнішнім середовищем; по-друге, властивості й функції елементів системи визначаються їхнім місцем у рамках цілого; і по-третє, будь-яка система, створювана людиною, завжди являється елементом більш складної системи.

2. Цілісність системи визначається й конкретизується через зв'язки як між елементами, так і із зовнішнім середовищем. Центральне місце належить "системоутворюючим" зв'язкам, що виражають закономірні відносини й визначають структурну організацію системи.

3. Сукупність зв'язків приводить до поняття структури й організації системи, які надають останній стійкості, стабільності, здатності протистояти певним впливам з боку навколишнього середовища.

4. Структура системи характеризується як "по горизонталі", так й "по вертикалі". Вертикальна структура приводить до понять рівнів системи, їхньої співпідпорядкованості й ієрархії.

5. Наявність управління в системі визначає необхідність постановки в процесі аналізу й розробки систем цілей, завдань, розподілу їх між елементами.

6. У зв'язку з управлінням і необхідністю доцільного характеру поведінки системи виникають проблеми співвідношення функціонування й розвитку, стабільності й інновацій з обліком часових і просторових факторів.

Істотними ознаками системи є наступні:

1. Наявність множини взаємозалежних і взаємозалежних елементів. *Елементи* – найбільш дрібні частки системи, яким властиві деякі якісні характеристики всієї системи. Кожен елемент має власну поведінку й стан, власну функцією. У певних умовах (цілях дослідження) елементи можуть виступати у свою чергу як *підсистеми*. Такий підхід до елементів можливий тому, що елемент входить у систему не всією сукупністю своїх властивостей і характеристик, а лише тими властивостями, завдяки яким він несе в системі певне функціональне навантаження.

2. Можливість опису системи через установлення її певної структури. *Структура* – це наявність певного взаємозв'язку, взаєморозташування складових частин (елементів) системи в просторі й часі, що характеризує її будову. У термінах системного підходу структура є не що інше, як сукупність стійких зв'язків елементів системи. Структурна організація є тип, порядок розподілу складових систем як частин у цілому, спосіб їхнього зв'язку, співпідпорядкованості, характер ієрархії, що формується так, щоб щонайкраще відповідати виконуваним системою функціям.

Зв'язок у структурі – це способи впливу, взаємодії або відносини елементів між собою, що обумовлюють структуру системи, її функціонування в просторі й

часі. Зв'язки можуть бути різними за своєю природою: інформаційної, керуючої, причинні, взаємодії, переваги, послідовності й т.д.

Структура системи характеризується рядом властивостей, до основних з яких можна віднести наступні:

- кількість складових елементів системи, їхня розмаїття і неоднорідність;
- порядок розташування (виділення ієрархії рівнів, якісно неоднорідних, однорідність елементів усередині кожного рівня, кількість рівнів ієрархії);
- спрямованість й інтенсивність зв'язків між елементами одного рівня й між рівнями;
- якісна визначеність зв'язків;
- інтенсивність взаємодії між елементами;
- стійкість зв'язків при рухливості елементів;
- можливість виникнення різних структур з однакових елементів й однакових структур з різних елементів.

3. **Цілісність системи**, тобто незвідність властивостей системи до суми властивостей складових її елементів, невиводимість із останніх властивостей цілого. Інакше кажучи, властивість цілісності системи проявляється в *інтегративності* або *емерджентності* – появі в цілого якісно нових властивостей, відсутніх як в окремих елементів, так і в їхній механічній сумі: внутрішньої погодженості у взаємозв'язках частин, координації й субординації між цілим і частинами в їхній взаємодії із зовнішнім оточенням.

У цілісності системи можна виділити два аспекти:

- *зовнішній*, виражений у стійкості лінії поведінки системи в цілому у взаємозв'язку її з іншими однорідними системами або системою більш високого порядку;
- *внутрішній*, що розкриває механізм її функціонування як цілісного утворення.

До основних ознак цілісності системи можна віднести:

- взаємозв'язок складових частин системи;
- детермінацію цілого частинами;
- інтегративні властивості системи, що служать основою об'єднання її частин;
- взаємна відповідність елементів між собою та елементів і цілого;
- автономність окремих елементів;
- відносну самостійність поведінки системи в цілому стосовно поведінки окремих її елементів і до зовнішніх умов.

4. **Можливість опису функціонування системи через зміну її станів**. *Стан* – це відмінна від минулого й майбутнього дійсна ситуація, обумовлена деякою сукупністю кількісних показників й якісних характеристик, тобто миттєвий вертикальний зріз, у якому перебувають окремі елементи й вся система в цілому. Під станом можна розуміти й найбільш істотні параметри системи, що відбивають її кількісно-якісну визначеність у будь-який момент часу.

5. **Цілеспрямованість і стійкість системи**. *Цілеспрямованість* – це здатність соціальної системи до вибору поведінки залежно від поставленої мети, що визначає напрямок її розвитку, темпи використання засобів, ресурсів і потенційних можливостей, інакше кажучи, - виживання. Принциповим моментом у реалізації мети системи – збереженні (виживанні) виступає принцип "*зосередження функцій*", тобто "певна відповідність функцій системи внутрішньому й зовнішньому середовищу існування, при якому всі функції всіх елементів системи зосереджені на її збереженні".

Функціональною умовою виживання є *стійкість* - якісна визначеність системи, що володіє деякими незмінними співвідношеннями (інваріантами). Якісна визначеність означає розвиток системи в тих границях, у яких кількісні

зміни не виходять за межі даної якості. Стійкість системи забезпечується механізмом *гомеостазису*, дія якого полягає в регулюванні функціонування всіх елементів системи, їхній взаємодії один з одним з метою протидії впливам, що обурюють, навколишню систему середовища.

Стійкість може проявлятися в різних формах:

1) Стійкість зберігається, коли зміна істотних властивостей системи під впливом різного роду зовнішніх і внутрішніх збурювань відбувається в рамках припустимих границь.

2) Система тим більше стійка, чим більше рухливі й гнучкі її елементи. При зміні зовнішніх умов більше шансів зберегти колишню якість має така система, серед елементів якої з більшою ймовірністю знайдеться елемент, успішніше пристосований до нових умов.

3) Стійкість системи проявляється в умовах боротьби суперечливих елементів, взаємопогашення протилежних сил. Порушення рівноваги веде до руйнування внутрішньої структури системи, що рівносильно втраті її якісної визначеності.

6. Наявність у системі зворотного зв'язку. Основним механізмом підтримки стійкості й гомеостатичної рівноваги системи є *зворотний зв'язок*, що представляє собою вплив результатів функціонування системи на характер цього функціонування або вплив наслідку на причини. Основна ідея зворотного зв'язку – вимір відхилень стану системи від заданого (певного) з метою формування керуючого впливу, зрівноважування системи із середовищем таким чином, щоб система змінювалася відповідно до змін середовища, не втрачаючи своєї якісної специфіки.

Зворотний зв'язок у соціальній системі виконує наступні функції:

- порівнює передбачуваний і реальний стан виходу (мету або план з результатом);
- виділяє розходження;

- робить його оцінку;
- виробляє відповідне отриманій оцінці рішення;
- формує процедуру введення рішення (втручання у функціонування системи);
- впливає на функціонування, ліквідуючи виявлене розходження.

Виходячи із зазначених властивостей, будь-яку складну систему можна розглядати як сукупність об'єктів (елементів, підсистем і т.д.), призначену для виконання деякого виду робіт або рішення досить чітко обкресленого класу завдань. Відповідно до цього *процес функціонування* складної системи представляється як сукупність дій її елементів, підпорядкованих єдиній меті.

Якщо мета й завдання системи визначені, можна порушувати питання про оцінку якості її функціонування, тобто *ефективності*. **Ефективність** – основна властивість будь-якої системи, створювана людиною, і, що полягає в здатності системи виконувати поставлені перед нею завдання при заданих умовах функціонування.

Якість функціонування системи оцінюється за допомогою *показників ефективності*. Під **показником ефективності** розуміється така числова характеристика системи, що оцінює ступінь пристосованості системи до виконання поставлених перед нею завдань у заданих умовах роботи. Для того щоб показник ефективності досить повно характеризував якість роботи системи, він повинен ураховувати всі основні особливості й властивості системи, а також умови її функціонування і взаємодії із зовнішнім середовищем, тобто він повинен залежати від структури системи, значень її параметрів, характеру впливу зовнішнього середовища, зовнішніх і внутрішніх випадкових факторів. Інакше кажучи, показник ефективності визначається процесом функціонування системи.

Таким чином, управління на основах **застосування системного підходу** включає три послідовних етапи (стадії):

1. Визначення сфери діяльності, уточнення області й масштабів діяльності об'єкта управління, установлення інформаційних потреб.

2. Проведення необхідних досліджень (системного аналізу).

3. Розробка альтернативних варіантів рішення певних проблем і вибір оптимального варіанта по кожному завданню.

Управління на основі системного підходу покликане забезпечувати й удосконалювати структурні й функціональні єдності системи, розкривати й усувати перешкоди на шляху до мети, асимілювати або нейтралізувати впливи, що обурюють, як всередині системи, так і поза нею. У цьому насамперед проявляється принципи системного підходу в управління. У діловій практиці він означає всебічну розробку прийнятих рішень, аналіз всіх можливих варіантів їхньої реалізації, координацію зусиль на різних напрямках. У соціальних системах цей принцип потребує тісного зв'язування рішень економічних, соціально-політичних і культурних проблем у процесі рішення управлінських завдань.

Застосування системного підходу до управління дозволяє керівникові побачити організацію в єдності складових її елементів, які нерозривно переплітаються між собою й із зовнішнім світом. Цей підхід також допомагає інтегрувати внески всіх шкіл, які в різний час домінували в теорії й практиці управління. Розуміння того, що організації являють собою складні відкриті системи, що складаються з декількох взаємозалежних підсистем, допомагає пояснити, чому кожна зі шкіл в управління виявилася практично прийнятною лише в обмежених рамках тому що прагнула зосередити увагу на якійсь одній підсистемі організації. Школа людських відносин в основному займалася соціальною підсистемою. Школи наукового управління й науки управління - головним чином, технічними підсистемами. Отже, вони найчастіше не могли правильно визначити всі основні компоненти організації. Жодна зі шкіл серйозно не замислювалася над впливом зовнішнього середовища на

організацію. Системний же підхід дає основу для інтеграції концепцій, розроблених і запропонованих більш ранніми школами. На системній основі можна синтезувати нові знання й теорії.

20.7. Ситуаційний підхід в управлінні

Традиційні школи управління намагалися визначити принципи, що ставляться до функцій управління – теоретичні знання про те, як повинні працювати керівники. Це розглядалося як науковий компонент управління. Застосування ж цих принципів на практиці розглядалося як мистецтво, тобто як щось, чого можна досягти тільки через досвід, методом "проб і помилок".

Ситуаційним підходом було внесено великий вклад у теорію управління, використовуючи можливості прямого додавання науки до конкретних ситуацій й умов. Він підкреслює значимість "ситуаційного мислення", використовуючи який керівники можуть краще зрозуміти, які прийоми будуть більшою мірою сприяти досягненню цілей у конкретній ситуації.

Ситуація – це конкретний набір обставин, що роблять сильний вплив на організацію в даний конкретний час.

Ситуаційний підхід, що виник наприкінці 60-х років, не заперечує концепцій і методів, розроблених раніше, а навпаки, намагається інтегрувати їх. Разом з тим він не є набором припасів, – це, скоріше, спосіб мислення про організаційні проблеми й шляхи їхнього вирішення. Ситуаційний підхід визнає, що хоча загальний процес проб однаковий, специфічні прийоми, які повинен використати керівник для ефективного досягнення цілей організації, можуть значно змінюватися.

Ситуаційний підхід намагається погодити конкретні прийоми й концепції з певними конкретними ситуаціями для того, щоб досягти цілей організації найбільш ефективно. Він концентрується на ситуаційних розходженнях між організаціями й усередині самих організацій, а також намагається визначити, які

значимі змінні ситуації і як вони впливають на ефективність організації.

В основу побудови технології управління можуть бути покладені наступні принципи:

1) принцип нормативного використання ресурсів (принцип квантифікації управління, дозування ресурсів для розробки рішень певного типу) – визначається тим, що виконання будь-яких операцій і процедур управління пов'язане з використанням обмежених ресурсів (часу, інформації, людей, техніки й т.п.), тому розподіл ресурсів по операціях і стадіях технології управління визначає його ефективність;

2) принцип раціональності інформаційного забезпечення управління – пов'язаний з тим, що в управлінській діяльності більшу долю займають інформаційні операції (добування, пошук, одержання, обробка, передача інформації й ін.), тому технологічні схеми процесу управління повинні бути побудовані з урахуванням максимально можливої доступності необхідної інформації при виконанні операцій, відрегульовані за критеріями цінності інформації, її повноти, вірогідності, своєчасності та ін.;

3) принцип економії часу – вказує на те, що формування управлінського впливу в міру реалізації розвертається в часі й можливі різні варіанти часових характеристик технології управління, тому економія часу стає одним з головних факторів ефективності управління й визначає своєчасність управлінських рішень, оперативність і ритмічність процесів управління;

4) принцип інтенсифікації технології управління – полягає у вимозі найбільш повного використання можливостей і потенціалу наявних ресурсів, скорочення втрат часу, інформації, матеріальних і фінансових засобів тощо;

5) принцип інтеграції технології управління в рамках загального функціонування системи управління – полягає в тім, що керування пов'язане розробкою й прийняттям безлічі різноманітних рішень, у яких використовуються різні технологічні схеми - прості й складні, лінійні, суворо

послідовні й зворотні й т.д. Очевидно, управління буде ефективним тоді, коли досягається інтеграція різних технологічних схем. Факторами досягнення інтеграції технології управління є методологія й організація управління, розподіл функцій у системі управління, структура управління, система мотивації співробітників, регулювання ступеня централізації управління (делегування повноважень), стратегія управління, використання сучасних інформаційних і комп'ютерних технологій;

6) принцип взаємодії ланок системи управління - указує на те, що в розробці важливих управлінських рішень беруть участь багато підрозділів організації й окремих фахівців, тому використовувана технологія повинна бути спрямована на організацію їхньої ефективної взаємодії в структурі операцій і часу виконання. Реалізація на практиці зазначених принципів, по суті, являє собою мистецтво управління, що відображає роль індивідуальних якостей керівника в досягненні успіху: розвиненості інтуїції, досвіду роботи, характеру освіти, професіоналізму, комунікабельності, переконаності, рішучості, ініціативності та ін.

Залежно від органу (підрозділу), рівня управління й стану справ на конкретній ділянці можуть використовуватися наступні технології управління :

- управління за цілями;
- управління за результатами;
- управління на базі потреб й інтересів;
- управління на базі активізації діяльності співробітників;
- управління шляхом постійних перевірок і вказівок;
- управління у виняткових випадках;
- управління на основі кібернетичного підходу.

У рамках будь-якого підрозділу (організації) можуть застосовуватися різні технології управління й навіть їхнє сполучення. Основним регулятором

використання управлінської технології є способи цільового управління.

Управління за цілями реалізується одним з наступних способів:

1) **Просте цільове управління** – передбачає визначення керівником тільки кінцевої цілі управління й строків її досягнення без вказівки механізму, як цю ціль досягти. При цьому передбачається, що ціль може бути досягнута в передбачений термін або раніше, а може й не бути досягнута взагалі. Просте цільове управління відкриває простір для ініціативних рішень підлеглими, але не гарантує досягнення цілі.

2) **Програмно-цільове управління** – передбачає розробку керівником цілей управління й механізму їхнього досягнення, а також строків і проміжних станів процесу. При цьому передбачається, що ціль буде досягнута в передбачений термін.

3) **Регламентне управління** – передбачає розробку керівником кінцевої цілі управління й обмежень на параметри й ресурси, наприклад, рух тільки в напрямку до цілі при заданому обмеженні ресурсів. При цьому передбачається, що ціль буде обов'язково досягнута, але в строки, які заздалегідь важко визначити.

Програмно-цільове й регламентне управління відноситься до наукового управління, а просте цільове – до управління на рівні здорового глузду ("*хотів зробити як краще*"). Управління за цілями включає науковий підхід до рішення проблем, пов'язаних з можливим ризиком. Керування за цілями з урахуванням ризику може включати наступні стратегії:

- відхилення від дій, що містять певний ризик;
- відповідальність за ризик з гарантією повної компенсації за рахунок власних коштів;
- передача відповідальності за ризик іншій особі;

- скорочення можливих негативних наслідків від ризику за допомогою превентивних заходів;
- ставка на ризик, використання всіх ресурсів для рішення проблеми ("*пан або пропав*").

Технологію управління за цілями доцільно застосовувати в тих випадках, коли керівник зіштовхується з декількома (трьома й більше) ситуаціями з наведеного нижче далеко не вичерпного списку:

- не всі цілі й завдання організації є обґрунтованими;
- відсутній науково-обґрунтована методика формування цілей і завдань;
- не накопичується статистика процесу реалізації цілей і завдань, не проводиться глибокий аналіз реалізації ухвалених рішень;
- має місце підміна змісту понять "ціль", "план", "прогноз", "завдання";
- нерідко наради проводяться експромтом, без відповідної підготовки (без "сценарію" проведення);
- постановка деяких цілей і завдань відбувається без попереднього їхнього осмислення, спонтанно, спостерігається дублювання.

Управління за результатами припускає прийняття управлінських рішень після одержання результатів по раніше ухваленому рішенню. Технологія заснована на очікуванні одержання результатів і базується на загальній функції координації. Її застосування доцільне в тих випадках, коли час між прийняттям рішень і результатом їхнього виконання мінімальний (години, кілька днів).

Для реалізації даної технології необхідно здійснити організаційну й функціональну підготовку, що включає створення аналітичної групи (з 2-3-х професійно підготовлених співробітників і психологів) з матричною структурою управління. Завданнями групи будуть:

- аналіз поточної інформації;
- проведення опитувань співробітників;

- визначення проблем і підготовка пропозицій по коректуванню тактичних і стратегічних рішень;
- створення інформаційної бази.

Данна технологія корисна для самонавчання керівника на власних помилках і досягненнях, а також може бути використана в наступних ситуаціях:

- результати роботи для більшості співробітників обмежуються їхнім робочим місцем;
- слабке моральне й матеріальне стимулювання результатів діяльності співробітників;
- співробітники мало цікавляться справами в підрозділі, не проявляють інтересу до своєї роботи, кулуарні розмови й незліченні перекури займають багато часу.

Управління на основі потреб й інтересів засновано на стимулюванні діяльності підлеглих через їхні потреби й інтереси й забезпечується тісна взаємодія керуючих і керованої систем. Активізація діяльності реалізується шляхом стимулювання (моральної й матеріального) і мобілізації.

Теорія потреб вимагає від керівників здійснювати управлінські відносини тільки через інтереси й потреби, тому що інші впливи приводять до протидії. Перелік потреб й інтересів, які необхідно враховувати в управлінській діяльності наступний.

Набір факторів і ситуацій, у яких дана технологія приводить до успіху, зводиться до наступного:

- немає планів формування гнучких структур управління;
- не всі співробітники знають про перспективи розвитку організації;
- занадто велика увага в підрозділі приділяється перекурам і порожнім розмовам;
- існує велика плинність кадрів;

- керівники часто відчувають протидію з боку співробітників й ін.

Управління на основі кібернетичного підходу – це сучасна технологія управління, реалізована за допомогою інформаційних систем. Її успіх заснований на великому обсязі типових процедур при обробці інформації, прийнятті рішень і використанні автоматизованих робочих місць (АРМ), оснащених розвиненими базами даних і знань й інтегрованих за допомогою локальних мереж в об'єднані автоматизовані інформаційні системи (АІС).

Дана технологія найбільшою мірою враховує особливості управлінської праці, обумовлені масштабами використання сучасних технічних засобів й інформаційних технологій, що веде до наступних змін у діяльності керівника:

- основним засобом управлінської праці стає інформація;
- звільняється частина робочого часу за рахунок використання інформаційних систем керування (ІСУ);
- зростає комфортність управлінської праці за рахунок одержання якісної інформації й роботи з пакетами прикладних програм, що імітують інтелектуальний внесок у загальний потенціал підрозділу;
- у керівника з'являється можливість вибору з ряду рішень, на його погляд, правильного, а потім з набору правильних рішень, на його думку, кращого;
- збільшується "вартість" результатів ухваленого рішення. Інформація як управлінське рішення багаторазово збільшує свою "вартість". Невірно ухвалене рішення може привести до більших витрат;
- досягається оптимальне співвідношення між функціями, що сполучаються керівником, (висококваліфікованих професійних фахівців, безпосередніх організаторів діяльності, вихователів та ін.). ІСУ можуть істотно скоротити час, затрачуваний керівником на роботу як фахівцем;
- істотно зростають масштаби "інформаційної насиченості" управлінської праці. Використання сучасних засобів зв'язку, локальних і глобальних

обчислювальних мереж, комп'ютерних конференцій та інших інформаційних технологій дозволяє, не сходячи з робочого місця, одержати всю інформацію, що цікавить.

ІСУ забезпечує керівника достовірною й повною інформацією про стан об'єкта управління для ухвалення рішення й наступної перевірки його виконання. Використання ІСУ дає можливість розширити набір форм реалізації управлінської праці. Як нові форми можна виділити:

- ділові ігри (тренінги) і комп'ютерне моделювання;
- електронні записні книжки й комп'ютерні органайзери;
- проведення колективних заходів (нарад, засідань, конференцій і т.п.) за допомогою сучасних технічних засобів;
- підготовка управлінських рішень, заснованих на попередньому розрахунку й аналізі за допомогою ЕОМ.

Виходячи з аналізу можливих ситуацій, управлінську технологію, засновану на кібернетичному підході, доцільно використати в наступних випадках:

- наявність у підрозділі складної системи документообігу й відсутність оперативності в обробці документів;
- у підрозділі мало досвідчених співробітників і керівників;
- багато часу йде на збори й наради;
- робочий день більшості керівників перевищує норму;
- у підрозділі розроблені й апробовані алгоритми прийняття рішень по найбільш важливих питаннях;
- підрозділ добре укомплектовано обчислювальними засобами й підготовленими до роботи на них співробітниками.

В основі використання будь-якої технології лежить інформація, тим більше, що зараз науковою думкою запропоноване поняття "інформаційного

суспільства", що може служити орієнтовною моделлю, для технологічних перетворень. Прояви інформаційного суспільства характеризується такими **критеріями:**

- **технологічний** – ключовий фактор – інформаційна технологія, що широко застосовується у виробництві, установах, системі освіти й побуту;
- **соціальний** – інформація виступає як важливий стимулятор зміни якості життя, формується й затверджується "інформаційна свідомість" при широкому доступі до інформації;
- **економічний** – інформація становить ключовий фактор в економіці як ресурс, послуг, товару, джерела доданої вартості й зайнятості;
- **політичний** – доля інформації, що веде до політичного процесу, що відрізняється зростаючою участю й консенсусом між різними класами й соціальними верствами населення;
- **культурний** – визнання культурної цінності інформації за допомогою сприяння твердженню інформаційних цінностей в інтересах розвитку окремого індивіда та суспільства в цілому.

Аналіз розглянутих технологій управління показує, що не існує універсальної технології, ефективної в будь-яких ситуаціях. Та й такого бути не може, коли мова йде про управління в соціальній сфері. Кожна з них має певні переваги й недоліки, обумовлені обмеженістю можливостей.

Системний підхід розглядає організацію як відкриту систему, що складається з декількох взаємозалежних підсистем. Організація одержує ресурси із зовнішнього середовища, обробляє їх і видає продукцію в зовнішнє середовище. Теорія систем допомагає керівникам зрозуміти взаємозалежність між окремими частинами організації й між організацією й середовищем, що оточує її.

Ситуаційний підхід розширив практичне застосування теорії систем, визначивши основні внутрішні й зовнішні змінні, які впливають на організацію.

Оскільки відповідно до цього підходу методики й концепції повинні бути застосовні до конкретних ситуацій, то ситуаційний підхід дозволяє вибрати найбільш доцільне управління, у тому числі й управлінські технології.

Підприємницька діяльність здійснюється на основі одноразових угод. Підприємницька діяльність спрямована на досягнення комерційного успіху, одержання прибутку, або підприємницького доходу. Найкраще використання капіталу: власності, іншого майна, фінансових, матеріально-технічних, трудових ресурсів.

20.8. Використання методів і підходів в управлінні кібербезпекою

Управління кібербезпекою є невід'ємною частиною управління будь-якою системою чи об'єктом, оскільки для них інформація стала таким самим ресурсом, як матеріальні, фінансові, трудові та інші ресурси. Тому до управління кібербезпекою використовуються процесний, системний та ситуаційний підходи, як і до будь-якої іншої системи управління. Однак, як з'ясувалося, особливості самої інформації та інформаційних технологій потребують зовсім інших методів, засобів і заходів для їх захисту. Отже управління кібербезпекою є тією сферою, необхідність теоретичного та практичного вивчення якої стала очевидною. Перші дослідження в цій області почалися наприкінці 1980-х рр., а до кінця 1990-х рр. з'явилися перші національні й міжнародні стандарти (ISO/IEC 17799). Однак стандарти в області управління кібербезпекою не вирішують усіх проблем. Навпаки, завдання управління кібербезпекою ускладнюються разом із усе більш інтенсивним використанням інформаційних комп'ютерних технологій практично в усіх сферах людської діяльності. Це обумовлює необхідність узагальнення досвіду управління кібербезпекою, розробки теорії, вирішення практичних аспектів управління кібербезпекою.

Необхідно відзначити й те, що лише кілька років назад, говорячи про управління кібербезпекою, мали на увазі лише рівень великої організації. Останнім часом усе частіше мова йде про управління безпекою регіональних і національних інформаційних інфраструктур, усе частіше виникає потреба в забезпеченні та управлінні кібербезпекою на середніх, малих підприємствах та в некомерційних організаціях.

Таким чином, забезпечення інформаційної безпеки є необхідною умовою функціонування будь-якої компанії, а створення політики безпеки - одна з перших вимог до організації інформаційної безпеки підприємства.

Політика інформаційної безпеки є однією з декількох політик, якими звичайно керується організація. Інші, як правило, регулюють такі важливі галузі, як кадрова політика, розпорядження виробничими потужностями й фінансовою діяльністю. Політика інформаційної безпеки повинна доповнювати інші політики й сприяти їхньому виконанню. Для кожної інформаційної системи політика інформаційної безпеки повинна бути індивідуальною.

У зв’язку з розширенням сфери використання інформаційних систем й їхнього ускладнення, проблема забезпечення інформаційної безпеки загострюється. Безпеку вже неможливо забезпечити одним лише набором технічних засобів і підтримувати тільки силами підрозділу безпеки. Відсутність регулярної оцінки інформаційних ризиків, недостатня інформованість співробітників про правила роботи із інформацією, що захищається, і дотриманні режиму інформаційної безпеки, відсутність формалізованої класифікації інформації зі ступеня її критичності й уявлень про те, скільки коштують інформаційні активи, - все це може звести нанівець зусилля компанії по забезпеченню інформаційної безпеки. З підвищенням ролі інформаційних систем у підтримці основних бізнесів-процесів компанії до цих проблем додаються питання забезпечення безперервності функціонування бізнесу в критичних ситуаціях. Ігнорування проблем інформаційної безпеки, практика

"латанія дір" сьогодні можуть обійтися компанії дуже дорого. Вирішити ці питання можна шляхом побудови ефективної системи управління кібербезпекою (СУКБ).

Завданнями СУКБ є систематизація процесів забезпечення ІБ, розміщення пріоритетів компанії в області ІБ, досягнення адекватності системи інформаційної безпеки існуючим ризикам, досягнення її "прозорості". Останнє особливо важливо, тому що дозволяє чітко визначити, як взаємозалежні процеси й підсистеми інформаційної безпеки, хто за них відповідає, які фінансові й людські ресурси необхідні для їхнього забезпечення й т.д. Створення СУКБ дозволяє також забезпечити ефективне відстеження змін, внесених у систему інформаційної безпеки, відслідковувати процеси вироблення та виконання політики безпеки, ефективно управляти системою в критичних ситуаціях.

У цілому, процес управління безпекою відповідає за планування, виконання, контроль і технічне обслуговування всієї інфраструктури безпеки. Організація цього процесу ускладняється також тією обставиною, що забезпечення інформаційної безпеки компанії пов'язано не тільки із захистом інформаційних систем, а і з бізнес-процесами, які підтримуються цими інформаційними системами. На підприємстві існують бізнеси-процеси, не пов'язані з інформаційними технологіями, але вони підпадають у сферу інформаційного забезпечення, наприклад, процеси кадрової служби з найму персоналу.

У світовій практиці є розроблені моделі систем управління ІБ, наприклад, "Information Security Management Maturity Model" (ISM3 від ISECOM) або "The Systems Security Engineering Capability Maturity Model" або стандарт NIST SP800-33. Існує також ряд міжнародних стандартів. Однак пряме використання цих моделей і стандартів утруднене. Вони або занадто конкретизовані, а в будь-якій організації, як правило, уже існує певна система процесів, ролей,

організаційно-розпорядницьких документів інформаційної безпекою, які необхідно інтегрувати в систему управління кібербезпекою. При цьому не визначаються пріоритети, так званої "ваги директив", які звичайно застосовуються в стандартах аудита. Або, навпроти, рекомендації носять занадто загальний характер. Наприклад, стандарти містять або набір контрольних директив, або загальний підхід до систем менеджменту, тобто визначають, що потрібно зробити, але не визначають, як це зробити.

Процесуальна модель СУКБ будь-якої компанії містить три рівні процесів.

- Процеси стратегічного рівня – керування ризиками, керування безперервністю ведення бізнесу, розробка й розвиток політики ІБ верхнього рівня.
- Тактичні процеси – розробка й розвиток процедур інформаційної безпеки, технічної архітектури системи інформаційної безпеки, класифікація ресурсів, моніторинг і керування інцидентами та інші.
- Процеси операційного рівня – керування доступом, керування мережною безпекою, перевірка відповідності та ін.

Стандарти безпеки містять рекомендації з управління кібербезпекою, призначені для співробітників, відповідальних за створення, впровадження й підтримку заходів, що забезпечують безпеку в організації. Вони повинні послужити основою для розробки стандартів безпеки й ефективних методів управління безпекою в конкретній організації. Крім того, допоможуть підтримати взаємну довіру при контактах між організаціями.

ISO/IEC 27002:2007 призначений для використання будь-якою організацією, котра планує встановити систему ефективного інформаційного захисту або покращувати існуючі методи інформаційного захисту.

Однак, це не свідчить, що всі рекомендації стандарту повинні бути обов’язково прийняті. Все залежить від конкретних інформаційних ризиків та вимог підприємства чи організації.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

- Назвіть чотири основних підходи до управління.
- Що являє собою метод кількісного підходу в управлінні?
- Що таке теорія інформації?
- Охарактеризуйте процес ний підхід в управлінні.
- Що являє собою функція планування.
- Охарактеризуйте метод наукового управління.
- Охарактеризуйте метод адміністративного управління.
- Охарактеризуйте метод людських відносин.
- Охарактеризуйте процесний підхід в управлінні.
- Охарактеризуйте системний підхід в управлінні.
- Охарактеризуйте ситуаційний підхід в управлінні.
- Охарактеризуйте методи і підходи в управлінні кібербезпекою.

РОЗДІЛ 21. ШТУЧНИЙ ІНТЕЛЕКТ ТА КІБЕРБЕЗПЕКА

21.1. Штучний інтелект та кіберзахист у кібербезпеці

Кібербезпека була першою сферою IT, у якій почали застосовувати технології штучного інтелекту. Розробникам рішень у кібербезпеці доводилося шукати способи автоматизації боротьби з масовими загрозами – скамом, спамом, фішингом та трохи пізніше – зі складними вірусами, хробаками тощо. Коли кількість таких атак стала вимірюватися не десятками штук, а сотнями мільйонів на добу, то аналіз та підвищення рівня кібербезпеки вже не є завданням людського масштабу.

Передумови використання штучного інтелекту обумовлені перш за все двома факторами: необхідністю оперативного реагування на кіберінциденти та нестачею кваліфікованих фахівців з кіберзахисту. Усе масове має розбирати

штучний інтелект, а функція людини стає постійне донавчання штучного інтелекту і покращення його можливостей до самонавчання.

Сучасний розвиток кіберпростору та штучного інтелекту означає близький кінець кібербезпеки у тому вигляді, в якому вона існувала до сьогодення. Кібербезпека тривалий час базувалась на концепції «закритих кордонів», коли загрози блокувались за допомогою брандмауерів, антивірусного програмного забезпечення, захисту паролем тощо. Ці методи виявилися неадекватними протягом останнього десятиліття, тому що кількість порушень збільшується у всіх секторах. Відбувається експоненційне зростання обсягу даних, що обробляється, та кількість підключених до інтернету пристроїв і сервісів. Така швидкість обумовлена в тому числі і розвитком інструментів створення нових технологій та нових, досконаліших інструментів. Широке використання високорівневих та надвисокрівневих мов програмування, потужних фреймворків та середовищ розробки, розвиток хмарних інфраструктур та технологій віртуалізації та контейнеризації дозволяє «збирати» новий додаток у безпрецедентно короткі терміни.

З такою ж швидкістю множаться і кіберзагрози, оскільки зловмисники використовують самі високоефективні інструменти розробки на базі штучного інтелекту, але у своїх цілях: відомі шахрайські прийоми використання Deep fake (створення реалістичного віртуального образу людини) для обману антифрод систем, підробки голосів для шахрайських дзвінків родичам атакованих осіб із проханням переказати гроші, застосування телефонних IVR-технологій для фішингу та розкрадання коштів. У шкідливому ПЗ також використовуються елементи штучного інтелекту, які дозволяють атакуючим набагато швидше підвищувати свої привілеї, переміщатися по корпоративній мережі, а потім знаходити і викрадати дані, що їх цікавлять.

Це виводить рівень кіберпротидії на новий рівень: якщо раніше протистояння зі зловмисниками можна було описати як боротьбу розумів та

налаштованих засобів захисту інформації, то тепер це вже можна назвати повноцінною «війною машин», у якій борються штучні кіберінтелекти. На ринок дані інструменти вийшли тоді, коли зрілість таких продуктів дозволила застосовувати їх у корпоративних середовищах, точність роботи стала виправдовувати їхню вартість, а можливості зловмисників стали широкими настільки, що ефективно та оперативно протистояти їм стало можливо лише із застосуванням даної технології.

Останні 5 років технології штучного інтелекту постійно прогресували. Проте, виник і негативний тренд – курс розподілу Мережі на сегменти, які жорстко контролюються конкретними країнами. Це призвело до того, що, наприклад, у Китаї, практично немає складних масових і глобальних рішень у галузі кібербезпеки – всі вони локальні, навчаються на локальних даних і не віддають висновки з них у загальний котел. Аналогічна ситуація у США: всі платформи, за винятком американських, вилучені з ринку. Все це йде на руку хакерам, які не обмежені географією – вони атакують корпоративні мережі, незалежно від юрисдикції організації. Відмова від міжнародного обміну даними та досвідом у галузі протидії кіберзагрозам на руку хакерам.

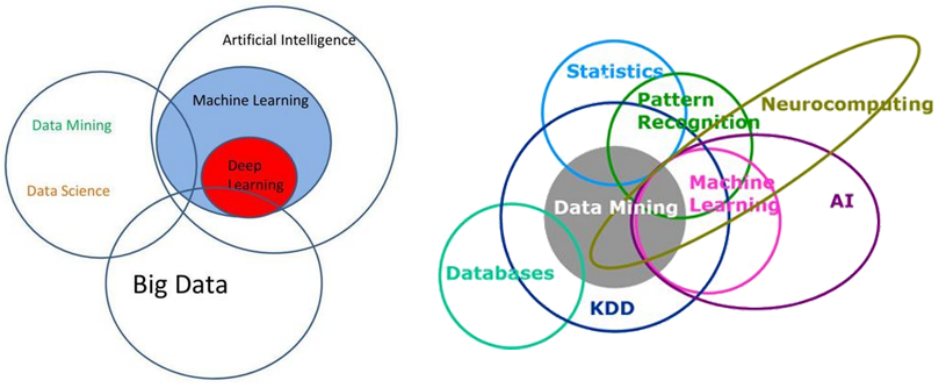
Таким чином, технології, що стали доступними широкому загалу, використовуються як на благо, так і на шкоду, що означає, що боротися з такими підготовленими кіберзлочинцями можна і потрібно із застосуванням найдосконаліших засобів і методів захисту.

21.2. Штучний інтелект: екскурс в історію

Якщо ж звернутися до історії, то передумовами створення концепції штучного інтелекту стали наукові дослідження у сфері побудови математичної моделі штучного нейрона і нейронної мережі на базі спостережень за живими організмами і природними нейронами.

У 1943 році американські нейрофізіологи Уоррен Маккаллок і Вальтер Піттс у своїй науковій статті «Логічне обчислення ідей, що належать до нервової активності» припустили, що мережа, яка складається з природних штучних нейронів, може виконувати логічні та математичні операції. Видатний британський учений Алан Т'юрінг (він був також відомим криптоаналітиком - під час Другої світової війни брав участь у дешифруванні криптограм німецької шифрувальної машини «Єнігма») у 1948 опублікував статтю «Розумні машини» (англ. "Intelligent Machinery"), а в 1950 році - роботу "Обчислювальні машини і розум" (англ. "Computing Machinery and Intelligence"), в яких описуються концепції машинного навчання та штучного інтелекту.

Сам термін «Штучний інтелект» запроваджено американським вченим-інформатиком Джоном Маккарті 1956 року. Він здійснив одну з перших спроб «оцифрувати» живий організм і уявити живу істоту як набір алгоритмів, які можна проаналізувати та відтворити.



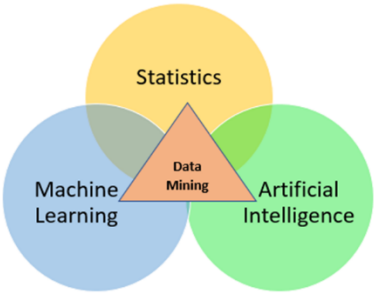


Рис.21.1. *Діаграми Ейлера з різноманітностю існуючих відносин між поняттями штучний інтелект, машинне навчання та інтелектуальний аналіз даних*

З того часу визначення штучного інтелекту неодноразово змінювалося залежно від рівня розвитку інформаційних технологій. Тому зазвичай його тлумачать залежно від контексту та рівня розвитку технологій. Такі визначення отримали назву *парадигм штучного інтелекту*, а процес їх зміни - *зсув парадигми* штучного інтелекту. Наприклад, Давід Аербах виділяв п’ять парадигм штучного інтелекту (AI - Artificial intelligence):

- Speculative (до 1940);
- Cybernetic (1940–1955);
- Symbolic AI (1955–1985), Artificial intelligence winter (1974–80);
- Subsymbolic AI (1985–2010), 2nd Artificial intelligence winter (1987–1993);
- Deep Learning (2010—...).

Щоб переконатися в цьому, достатньо загуглити терміни Artificial Intelligence (AI, штучний інтелект), Machine Learning (ML, машинне навчання) та Data Mining (DM, інтелектуальний аналіз даних), і ви отримаєте безліч діаграм Ейлера, що показують відносини між цими науковими напрямками, причому всі різні (рис.21.1).

Існує дві полярні думки. Згідно з першою, тільки Artificial General Intelligence (AGI, загальний/повний/сильний штучний інтелект), який має такі ж пізнавальні здібності, як і людина, може називатися справжнім штучним інтелектомю. Таким чином, лише такі алгоритми машинного навчання, які служать меті AGI, можуть почесно іменуватися штучним інтелектом. Таку ж позицію мали парадигми середини минулого століття.

У 1950 році Алан Тьюрінг у своїй знаменитій роботі "Обчислювальні машини і розум" запропонував тест для відповіді на запитання «Чи може

машина думати?». Суть тесту, який називався «гра в імітацію», зводилася до почергового ставлення питань людині та машині і спроби визначити за допомогою їхніх відповідей, з ким зараз відбувається спілкування. Його конвенція штучного інтелекту звучить так: «Якщо машина діє так само розумно, як людина, вона так само розумна, як і людина».

Стів Возняк (співзасновник фірми Apple, українець за походженням) згодом запропонував свій варіант тесту під назвою «Coffee», суть якого полягала в тому, що машина (робот), зайшовши в незнайомий американський будинок, зможе знайти всі необхідні інгредієнти та прилади та приготувати каву.

Через сім років, у 1957-му, Франк Розенблатт створив перший персептрон (найпростіша штучна нейронна мережа), давши американським військовим надію на створення машини, яка зможе ходити, говорити, бачити, писати, відтворювати себе і усвідомлювати своє існування.

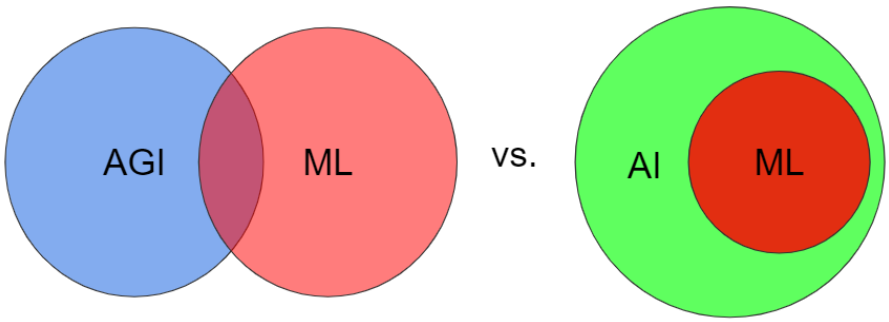


Рис.21.2. ***Діаграми Ейлера, що ілюструють різницю в парадигмах «загального» (AGI, зліва) та прикладного (праворуч) штучного інтелекту***

Іншу, більш практичну позицію зайняли вчені, які займались прикладними дослідженнями в галузі штучного інтелекту (Applied AI). У рамках цієї парадигми машинне навчання є підмножиною штучного інтелекту. Штучний інтелект можна визначити як алгоритм, який знаходить патерн (шаблон) у

вхідних даних або робить їхню оцінку. У подальшому алгоритм використовує отримані результати для прийняття рішень, як би це була людина. У рамках такої моделі штучного інтелекту і розглядаються сьогодня проблеми виявлення та блокування кібератак.

З того часу наука значно просунулась у питаннях створення штучного інтелекту: знаковими подіями можна назвати шахову перемогу суперкомп'ютера IBM Deep Blue над гросмейстером Гаррі Каспаровим у 1997 році та перемогу у грі го програми AlphaGo розробки Google DeepMind над професійним гравцем Лі Седолем в 2000. При цьому перша перемога була досягнута в шахової грі, що добре алгоритмізується, де для виграшу достатньо знати всі можливі комбінації і ходи, а друга - за рахунок машинного навчання, який застосовувався AlphaGo для самонавчання грі в го.

Дамо сучасні визначення кільком термінам, що пов'язані із штучним інтелектом.

Штучний інтелект (англ. ***Artificial intelligence***, AI) передбачає виконання інформаційними системами завдань прийняття рішень та навчання, за аналогією з інтелектом живих істот.

Нейронна мережа (англ. ***Neural network***) - взаємозалежне множина штучних нейронів, що виконують прості логічні операції та здатні до машинного навчання.

Машинне навчання (англ. ***Machine learning***, ML) - це техніка навчання інформаційної системи на основі наданих наборів даних (англ. ***dataset***) без використання зумовлених правил, є окремим випадком штучного інтелекту. Загальним завданням машинного навчання є побудова алгоритму (програми) на підставі наданих вхідних даних та заданих вірних/очікуваних результатів - таким чином, процес роботи ML-системи поділений на початкове навчання на заданих датасетах і на подальшому прийнятті рішень вже навченою системою.

Існує кілька способів машинного навчання, наприклад:

Навчання з вчителем (англ. ***Supervised learning***) - це спосіб машинного навчання, в якому використовуються розмічені набори даних (прокласифіковані об'єкти з виділеними характерними ознаками), для яких «вчитель» (людина чи навчальна вибірка) вказує правильні пари «питання-відповідь», на підставі чого потрібно побудувати алгоритм надання відповідей на подальші аналогічні питання.

Навчання без вчителя (англ. ***Unsupervised learning***) - це спосіб машинного навчання, в якому не використовуються розмічені набори даних, не вказані правильні пари «питання-відповідь», а від інформаційної системи потрібно на підставі відомих властивостей об'єктів знайти різні взаємозв'язки між ними.

Навчання з частковим залученням вчителя (англ. ***Semi-supervised learning***) - спосіб машинного навчання, в якому комбінується невелика кількість розмічених наборів даних та велика кількість нерозмічених. Такий підхід виправданий тим, що отримання якісних розмічених дата-сетів є досить ресурсомістким та тривалим процесом

Навчання з підкріпленням (англ. ***Reinforcement learning***) - окремий випадок навчання з вчителем, при якому «вчителем» є середовище функціонування, що дає зворотний зв'язок інформаційній системі залежно від прийнятих нею рішень. При цьому, в машинному навчанні можуть використовуватися інші алгоритми, такі як байєсовські мережі, ланцюги Маркова, градієнтний бустинг тощо.

Глибоке навчання (англ. ***Deep learning***) - це окремий випадок машинного навчання, в якому використовується складна багатошарова штучна нейронна мережа для емуляції роботи людського мозку та обробки мови (англ. ***natural language processing***), звукових (англ. ***speech recognition***) та візуальних образів (англ. ***англ. computer vision***). Машинний зір (англ. ***computer vision***) в даний час широко використовується в системах забезпечення безпеки, контролю

транспорту та пасажирів. Системи обробки мови (англ. ***natural language processing***) та розпізнавання слів (англ. ***speech recognition***) допомагають голосовим асистентам Siri чи Alice відповідати на запитання користувачів смартфонів.

Великі дані (англ. ***Big Data***) - великий обсяг структурованих та неструктурованих даних у цифровому вигляді, що характеризується обсягом (англ. ***volume***), швидкістю зміни (англ. ***velocity***) та різноманітністю (англ. ***variety***). Для обробки Big Data можуть застосовуватись спеціалізовані програмні інструменти, такі як Apache Hadoop, Storm, Spark, Kaggle, СУБД класу NoSQL. Вважається, що для підвищення business-value під час використання Big Data потрібно перейти від різнорідних даних до структурованої інформації, та потім - до знань. Оброблений, структурований та розмічений dataset, отриманий з релевантного масиву Big Data, є необхідним (і найціннішим) компонентом для машинного навчання у сучасних системах.

Глибокий аналіз даних (англ. ***Data mining***) – структурування та виділення корисної інформації з різнорідної та неструктурованої маси даних, у тому числі з Big Data.

Нечітка логіка (англ. ***Fuzzy logic***) - застосування нестрогих правил та нечітких відповідей для вирішення завдань у системах штучного інтелекту та нейронних мережах. Може застосовуватися для моделювання поведінки людини, наприклад, для звуження або обмеження умов пошуку відповіді питання залежно від контексту.

21.3. Можливості посилення кібербезпеки штучним інтелектом

Загалом використання ШІ в кібербезпеці може підвищити ефективність та швидкість виявлення загроз і дозволити швидше реагувати на кібератаки. Існує безліч сценаріїв використання штучного інтелекту в галузі інформаційної безпеки, наприклад:

– виявлення аномалій у мережевому трафіку та раннє попередження про можливі атаки;
– автоматичне виявлення та аналіз уразливостей у додатках та операційних системах;
– пошук витоків конфіденційних даних та моніторинг їх використання;
– використання машинного навчання для аналізу великих обсягів даних, пов'язаних із безпекою, для виявлення прихованих трендів та загроз;
– автоматичне створення звітів про безпеку та аудитів, на основі даних зібраних із різних джерел;
– аналіз хмарних середовищ та контроль відповідності політикам безпеки;
– використання ШІ для захисту від атак соціальної інженерії та фішингу;
– перевірка відповідності мережевих пристроїв політикам безпеки та виявлення порушень.

Приклади використання ШІ в ІБ включають системи управління погрозами, системи моніторингу безпеки, системи виявлення вторгнень, системи аналізу вразливостей і системи аутентифікації користувача. Більш того, штучний інтелект може використовуватися для навчання співробітників організації правильним методам роботи з інформацією та дотримання правил безпеки, я також ШІ може допомогти створити безпечніше програмне забезпечення, надаючи розробникам зворотний зв'язок у режимі реального часу про те закритий їх код чи ні.

Області застосування штучного інтелекту в кібербезпеці включають:

Виявлення кіберзагроз. *Машинне навчання* (ML) дає можливість виявляти кіберзагрози в режимі реального часу на основі аналізу інформації з різних джерел даних. Алгоритми машинного навчання постійно адаптуються та оновлюються, щоб виявляти загрози для вашої системи до того, як зловмисники зможуть виявити вразливість у захисті мережі компанії та реалізувати загрози. Алгоритми "розуміють" усі нюанси інфраструктури та мережі організації, а

також можливі сценарії атак. Завдяки навчанню, аналізу даних та розумінню моделей поведінки алгоритми можуть виявляти аномалії в системі та запобігати їх до того, як буде здійснено повноцінну атаку. Штучний інтелект служить допоміжним, але дуже надійним інструментом для фахівця з кібербезпеки.

Аналіз мережевої безпеки. У багатьох випадках мережева безпека базується на двох основних аспектах:

– по-перше, це *розробка безпекової політики*. Вона дає можливість виявляти легальні та не дуже мережеві підключення. Якщо компанія не особливо велика, то проблем із аналізом даних небагато. Але для середніх і великих компаній все ускладнюється, адже створювати, керувати і підтримувати політику безпеки для величезної інфраструктури складно. Тому штучний інтелект стає надійним та ефективним інструментом вирішення таких проблем. Він допомагає підприємствам відстежувати та застосовувати правила та нормативи, а також контролювати відповідність складних мереж встановленим нормам. У випадку застосування штучного інтелекту усе це відбувається набагато ефективніше, ніж у разі "ручної" праці, тобто залучення фахівців без ШІ-інструментів.

– по-друге, це *аналіз мережного середовища*. Велика кількість компаній не має достатньо чіткої системи моніторингу різних робочих навантажень. Підрозділу інформаційної безпеки, відповідно, доводиться витрачати багато часу та енергії на визначення того, яка група робочих навантажень яким застосункам належить. Штучний інтелект здатний оптимізувати виконання цього завдання, тут машина справляється значно краще за людину.

Поведінковий аналіз. Йдеться мова про моніторинг дій користувачів у режимі реального часу. При виявленні аномалій система спрацьовує, використовуючи один із сценаріїв захисту. Будь-яка аномалія позначається як підозріла, так що загрозу з високим ступенем ймовірності виявляють. Алгоритми моніторінгу працюють з різною інформацією, включаючи, робочі

години співробітників (якщо хтось заходить з незвичного місця, дія позначається як підозріла), географічне розташування, яке використовується для входу в мережу, ідентифікатори пристроїв, шаблони введення тощо. Для того щоб алгоритми діяли ефективно, команді з інформаційної безпеки необхідно завантажувати в систему еталонні дані, за якими проводиться звірка.

Безпека хмарної інфраструктури. І тут штучний інтелект приходить на допомогу. Справа в тому, що кібербезпеку складніше забезпечувати при переході компаній в "хмару". Рішення, призначені для локальних мереж, не дуже добре справляються з цим завданням. А ось гібридні рішення з використанням штучного інтелекту, які дають можливість відстежувати та аналізувати дані в найрізноманітніших середовищах, працюють дуже ефективно. Дедалі більше організацій застосовують спеціалізований підхід, коли корпоративні дані витягуються з різних архітектур, компілюються та аналізуються програмною платформою. Гібридні системи здатні невтомно вести моніторинг того, що відбувається.

Виявлення фроду. Термін "fraud" (від англ. fraud) використовують для позначення різних видів злочинів, у тому числі для шахрайства в IT-сфері. Чимало користувачів банківських послуг стикалися з незручностями при спробі банку захистити кошти клієнта. Блокуються рахунки, користувачі не можуть використовувати додаток банку, перебуваючи за кордоном – подібних випадків багато. Все тому, що деякі організації використовують досить жорсткий алгоритм розпізнавання підозрілих операцій. Щойно не так - і все блокується. ШІ діє гнучкіше. Помилкових спрацьовувань при інтеграції рішень штучного інтелекту стає набагато менше. Більше того, ШІ оперативно виявляє джерело проблеми, тож правоохоронці вчасно отримують необхідні дані.

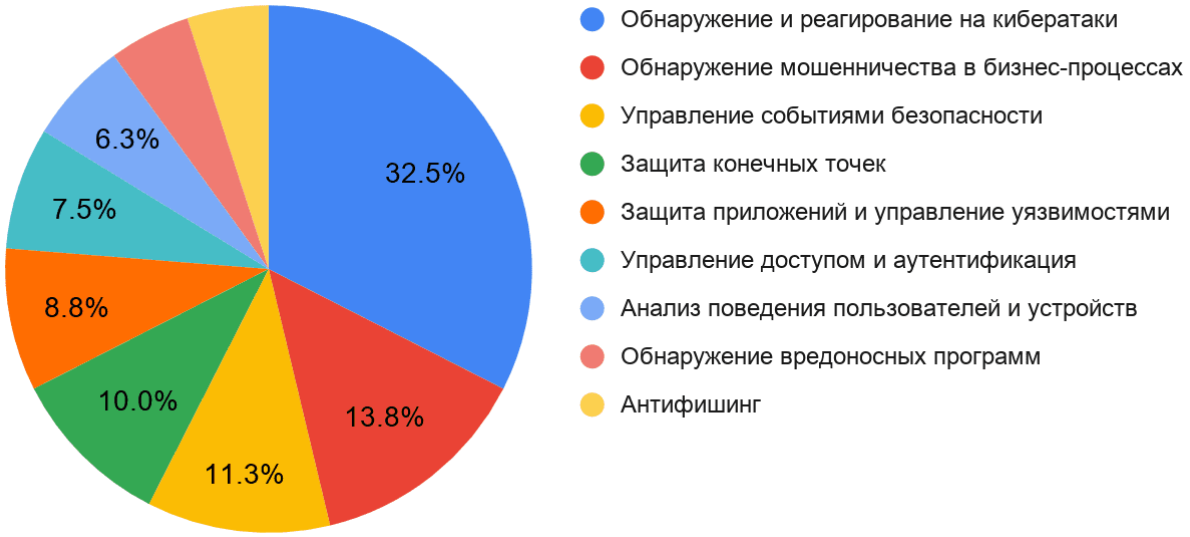


Рис.21.3. Розподіл продуктів із застосуванням технологій ШІ за сценаріями використання

Продукти кібербезпеки зі штучним інтелектом класифікують за сценаріями використання. Перечислимо основні типи:

1. *EDR (Endpoint Detection and Response)* — платформа виявлення атак на робочі станції, сервери, будь-які комп'ютерні пристрої (кінцеві точки) та оперативного реагування на них. За допомогою технологій ШІ продукти цієї категорії можуть знаходити невідомі шкідливі програми, автоматично класифікувати загрози і самостійно реагувати на них, передаючи дані в центр управління. ШІ приймає рішення на основі загальної бази знань, накопиченої від збору даних від безлічі пристроїв. Деякі продукти цього типу використовують технології ШІ для розмітки даних на кінцевих точках і подальшого контролю їх переміщення, щоб виявити внутрішні загрози.

2. *NDR (Network Detection and Response)* — пристрої та аналітичні платформи, які виявляють атаки на мережному рівні та дозволяють оперативно на них реагувати. Використовуючи накопичену статистику та базу знань про загрози, продукти даного типу виявляють за допомогою технологій ШІ загрози у мережевому трафіку та можуть автоматично на них реагувати належним

чином, змінюючи конфігурацію мережевих пристроїв та шлюзів. Частина продуктів цього типу спеціалізується на захисті хмарних провайдерів та їх інфраструктури. Додатковий сценарій використання ШІ в мережевому захисті – це аналіз поштового трафіку щодо фішингу.

3. *UEBA (User and Entity Behavior Analytics)* — системи поведінкового аналізу користувачів та інформаційних сутностей. Вони виявляють випадки незвичайної поведінки та використовують їх для детектування внутрішніх та зовнішніх загроз. Основний сценарій застосування ШІ-технологій у продуктах типу UEBA – це автоматичне виявлення аномалій у поведінкових моделях (відхилення від норми або відповідність шаблону-патерну загрози) для користувачів та різних сутностей інформаційних систем. Виявлені аномалії класифікуються за допомогою ШІ як різні загрози та ризики для бізнесу. Аномальна поведінка може виявлятися з метою моніторингу та управління доступом, виявлення шахрайства серед клієнтів або співробітників (антифрод), захисту конфіденційних даних, перевірки дотримання тих чи інших регламентів та нормативних актів.

4. *TIP (Threat Intelligence Platform)* — платформи раннього детектування загроз та реагування на них, що діють на основі великої кількості різних даних (Data Lake) та індикаторів компрометації (IoC). Застосування ШІ дозволяє підвищити ефективність виявлення невідомих загроз на ранніх етапах; сценарій дуже схожий з роботою SIEM-систем, але орієнтований на зовнішні джерела даних та зовнішні загрози.

5. *SIEM (Security Information and Event Management)* — рішення, які здійснюють моніторинг інформаційних систем та у режимі реального часу аналізують події безпеки, що надходять від мережевих пристроїв, засобів захисту інформації, IT-сервісів, інфраструктури систем і додатків та допомагають виявити інциденти інформаційної безпеки. У системах такого класу накопичується величезна кількість даних із різних джерел, а застосування

технологій ШІ дає можливість виявлення аномалій евристичними методами та скорочення хибних спрацьовувань при зміні патернів та моделей даних. Застосування ШІ у SIEM-системах дозволяє досягти дуже високого рівня автоматизації.

6. *SOAR (Security Orchestration and Automated Response)* — системи, що дозволяють виявляти загрози інформаційній безпеці та автоматизувати реагування на інциденти. У рішеннях цього типу, на відміну від SIEM-систем, ШІ допомагає не тільки проводити аналіз, а й автоматично реагувати належним чином на виявлені загрози.

7. *Засоби захисту додатків (Application Security)* — системи, що дозволяють визначати загрози безпеці додатків, керувати подальшим циклом моніторингу та усунення таких загроз. Основний сценарій застосування технологій ШІ в системах захисту додатків — автоматичний збір інформації про вразливості, атаки та зараження, яка доступна у відкритих джерелах, та заснована на його результатах автоматизація захисних дій: сканування на вразливості, зміни правил захисту для веб-додатків, виявлення загроз та зміни ризикової моделі.

8. *Антифрод (Antifraud)* — системи, що дозволяють виявляти загрози у бізнес-процесах та запобігати шахрайським операціям в режимі реального часу. У системах захисту від шахрайства технології ШІ застосовуються для визначення відхилень від встановлених бізнес-процесів, тим самим допомагаючи швидко реагувати на можливий фінансовий злочин чи вразливість процесів. Застосування ШІ в таких системах є особливо актуальним, оскільки дозволяє швидко адаптуватися до зміни логіки та різних метрик бізнес-процесів, а також використовувати кращі практики в індустрії.

Штучний інтелект робить помітний внесок у боротьбу з сучасними інформаційними загрозами. Зокрема, здебільшого впровадження технологій ШІ в інформаційній безпеці організації скорочує час виявлення проблем та реагування на інциденти, а також витрати на управління персоналом. При

впровадженні технологій штучного інтелекту зростає ефективність детектування невідомих загроз, а також швидкість аналізу та виявлення шкідливої активності на кінцевих точках та у додатках.

21.4. Машинне навчання в задачах кібербезпеки

Роль машинного навчання в запобіганні кіберзлочинам стає все більш важливою, оскільки загрози цифровій безпеці стають все більш складними. Машинне навчання – це тип штучного інтелекту, який дозволяє комп'ютерам навчатися на основі даних і ідентифікувати закономірності. У контексті запобігання кіберзлочинам цю технологію можна використовувати для виявлення зловмисної діяльності, виявлення аномалій і запобігання кібератакам.

Алгоритми машинного навчання можуть виявляти кіберзагрози та реагувати на них шляхом розпізнавання зловмисних моделей поведінки та реагування на них. Наприклад, ці алгоритми можуть аналізувати мережевий трафік для виявлення шкідливих дій, таких як зловмисне програмне забезпечення, фішингові атаки та витоки даних. Виявляючи підозрілу поведінку, алгоритми машинного навчання можуть попередити персонал служби безпеки про потенційні загрози та дозволити їм вжити відповідних запобіжних заходів.

Крім того, машинне навчання можна використовувати для виявлення нових кіберзагроз і реагування на них. Аналізуючи дані попередніх атак, алгоритми машинного навчання можуть ідентифікувати нові шаблони зловмисної поведінки та своєчасно попереджати персонал служби безпеки. Це допомагає організаціям реагувати на загрози швидше й ефективніше.

Нарешті, алгоритми машинного навчання можна використовувати для виявлення та пом'якшення внутрішніх загроз. Аналізуючи поведінку користувачів і розпізнаючи шаблони підозрілої активності, ці алгоритми можуть попередити співробітників служби безпеки про потенційні внутрішні

загрози та дозволити їм вжити необхідних заходів до того, як загроза буде реалізована.

Таким чином, машинне навчання є цінним інструментом у боротьбі з кіберзлочинністю. Виявляючи зловмисну діяльність і реагуючи на неї, виявляючи нові загрози та пом’якшуючи внутрішні загрози, ця технологія може допомогти організаціям ефективніше запобігати кібератакам і реагувати на них.

Для виявлення кібератак традиційно виділяють два підходи: детерміністичний та імовірнісний. У рамках першого зазвичай використовують сигнатури - унікальні послідовності байтів, що описують шкідливі об'єкти (файли, процеси, мережеві з'єднання, ключі у системному реєстрі Windows, об'єкти синхронізації тощо), які дозволяють однозначно ідентифікувати відомі кібератаки в автоматичному режимі.

Другий підхід здебільшого використовується для блокування невідомих погроз або погроз нульового дня при таргетованих атаках, коли ми заздалегідь не знаємо індикаторів компрометації. Цей підхід дозволяє виявляти нові кібератаки з певною ймовірністю, залишаючи останнє слово за користувачем системи або фахівцем з кібербезпеки. Якраз імовірнісний підхід і відкриває широке поле для використання штучного інтелекту з машинним навчанням.

Як відомо, у рамках машинного навчання існує три основні підходи:

1. *Навчання з вчителем* (Supervised Learning). Основні сфери застосування:
   - класифікація та розпізнавання;
   - виявлення патернів та аномалій;
   - прогнозування.
2. *Навчання без вчителя* (Unsupervised Learning). Основні сфери застосування:
   - кластеризація;
   - виявлення патернів та аномалій.

3. *Навчання із підкріпленням* (Reinforcement Learning). Основні сфери застосування:
   - керування роботами;
   - теорія ігор, алгоритми для го (AlphaGo), шахи (AlphaZero), шашки, нарди. Штучний шнтелект спочатку знає лише правила гри, а алгоритми та стратегії він створює в процесі гри із самим собою;
   - виявлення аномалій.

   Є ще два підходи:
4. *Гібридний підхід* (Semi-Supervised Learning) — навчання з частковим залученням вчителя, коли вхідні дані можуть бути як маркованими, так і такими, що не містять мітку класу.
5. *Самостійне навчання* (Self-Supervised Learning). Його особливістю є те, що мітки класів вже знаходяться у вхідних даних. Наприклад, для вибірки довільних зображень ми генеруємо нові зображення шляхом повороту на 90, 180 або 270 градусів. Завдання моделі – навчитися розгортати зображення у вихідне положення. Інший приклад - збирання пазла після розрізання зображення на частини. В обох завданнях ми знаємо результат і вчимо модель знаходити його.

Найпопулярнішим завданням у сфері кібербезпеки є *бінарна класифікація*, тобто розподіл об'єктів на шкідливих та доброякісних з метою виявлення та блокування кібератак. При цьому мається на увазі, що крім самих класів, ми вже знаємо критерії, за якими проводимо атрибуцію об'єктів. Щоб виробити ці критерії, ми повинні мати знання про загрозу.

Тобто у даному випадку ми маємо схему дедектування кібератак з вчителем. Інакше кажучи, методи класифікації дозволяють виявляти відомі типи загроз і вектори атак, але не дають можливості виявляти нові кібератаки, які не використовують традиційні техніки і не містять відомі нам індикатори.

Крім цього, створення бінарного класифікатора пов'язане з низкою проблем, таких як відсутність розмічених даних та вилучення ознак.

Перша проблема якраз пов'язана з відсутністю великої кількості класифікованих даних, які вже мають мітку (наприклад, об'єкт шкідливий або доброякісний, є індикатором атаки або нормальної активності), які могли б підійти для навчання з учителем.

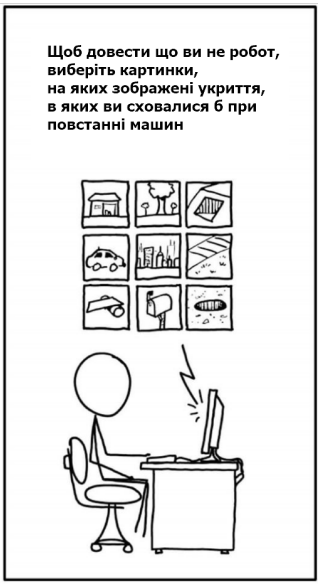


Рис.21.4. *Отримання даних для навчання з вчителем за допомогою CAPTCHA*

Наприклад, щоб натренувати нейронну мережу відрізняти котів від собак, необхідно спочатку надати розмічені зображення. Таке маркування зазвичай здійснюється вручну і на великих кількостях даних це буде с трудомістко. Якщо говорити про кішок та собак, то, на щастя, вже існують готові набори даних від Kaggle, що містять 25 000 класифікованих зображень. Також можна використовувати CAPTCHA (рис.21.4) для того, щоб користувачі класифікували зображення при проходженні тесту, що виявляє інтернет-роботів (Internet crawlers).

Однак обидва ці варіанти не працюють, коли йдеться про кібератаки. По-перше, техніка кібератак еволюціонують швидше за котів і собак, тому модель необхідно регулярно навчати на нових зразках атак. По-друге, звичайних

користувачів не можна залучити до класифікації кіберзагроз через нетривіальність цієї дії.

Тому перспективнішим є підхід «навчання без вчителя» (коли не потрібно попередньо розмічати дані для навчання) або «навчання з підкріпленням» (коли є можливість отримати зворотний зв'язок від експерта).

Детектування фішингу з вчителем

Проте не варто скидати з рахунків навчання з вчителем. Вдалим застосуванням, наприклад, може бути детектування фішингових посилань.

По-перше, існує база валідованих фішингових посилань на Phishtank.org, куди завантажують нові зразки посилань антивірусні компанії, так і індивідуальні дослідники. Білі посилання одержати теж нескладно. Для цього можна скористатися сервісом Alexa.com, де є адреси найпопулярніших веб-сайтів.

По-друге, різноманітність технік запуску фішингових веб-сайтів обмежена можливостями хостингу та реєстратора доменного імені, і за останні 15–20 років мало що змінилося, хіба що почали більше використовувати сертифікати. Зловмисники досі реєструють співзвучні доменні імена, що атакуються сервісу, на мінімально можливий термін. Хостинг для фішингової сторінки також вибирається локальний або використовується зламаний сервер. У більшості атак зазвичай застосовується протокол HTTP без шифрування та сертифікатів. Таким чином, як атрибути достатньо взяти доменне ім'я, WhoIs-інформацію, геолокацію сервера, тип мережного протоколу (HTTP або HTTPS) та наявність сертифіката та його параметрів.

Завдання визначення фішингових посилань можна вирішити за допомогою бінарного класифікатора. Причому необов'язково використовувати складний апарат глибоких нейронних мереж (DNN), який потребує великої кількості даних якісного навчання. Достатньо скористатися традиційними інструментами

класифікації (дискримінантний аналіз, метод опорних векторів, дерева прийняття рішення, випадковий ліс, регресійний аналіз [передбачення]) або створення репутаційної моделі (scoring system) на основі статистичного розподілу атрибутів між двома класами посилань та експертної оцінки.

Розглянемо завдання детектування фішингових посилань на основі наступних атрибутів: реєстратор домену, період реєстрації домену, геолокація хостинг-сервера та наявність захищеного з'єднання з валідним сертифікатом.

Після частотного аналізу двох вибірок з фішинговими (Phishing) і доброякісними (Benign) посиланнями ми бачимо (табл.21.1), що атрибути реєстратора і геолокації буде складно використовувати для бінарної класифікації, оскільки серед значень, що найчастіше зустрічаються, є багато збігів. Відмінності за цими двома атрибутами носять більш тонкий характер і можуть бути виявлені на вибірках більшого розміру. Однак атрибут Lifetime, що відповідає терміну, на який реєструється домен, показує, що серед посилань фішингу існує тенденція реєструвати домени на більш короткий термін. Наприклад, 37% фішингових доменів було зареєстровано на 1 рік, на відміну від доброякісних доменів, які зазвичай реєструються на більш тривалий термін - 10 років і більше.

Табл.21.1. *Приклад вибірки посилань з атрибутами та міткою класу*

#	URL	IP address	Registrar	Lifetime	Country	Class
1	[http://]admin.palmariguani.com/...	192.186.205.8	godaddy	2	US	phishing

2	[http://]www.whoes.info/docs/fox/dropbox/	107.180.26.63	godaddy	1	Murrica	phishing
3	[http://]www.apple-id.ldn-app.mobi/apple	208.109.255.48	godaddy	1	US	phishing
4	[http://]v01-apple.co.uk	45.79.129.214	godaddy	1	UK	phishing
5	[https://]www.bth.se/	194.47.131.132	SE Direkt	14	SE	benign
6	[https://]wikipedia.com	208.80.154.238	MARKMONITOR INC.	16	US	benign
7	...	...	...	...	...	...

Що ж до захищеного з'єднання, то переважна більшість фішингових посилань (96%) не використовують HTTPS-протокол, тобто це один із суттєвих критеріїв, який можна застосовувати для детектування фішингу. Для HTTPS-посилань можна додатково проводити аналіз сертифіката на основі його атрибутів: наприклад, ким і кому видано адресу реєстрації компанії, якій було видано сертифікат. Хакери можуть реєструвати сертифікати на неіснуючі компанії, як це було у випадку з компанією шифрувальника LockerGoga, файли якого були підписані цифровими сертифікатами, випущеними Sectigo RSA Code Signing CA для фейкових компаній Alina Ltd, Kitty's Ltd., Mikl Limited та AB Simba Limited.

Під час підготовки вибірки для навчання нам необхідно всі строкові значення перевести в категоріальні та закодувати їх числовими значеннями; для категорії можна використати порядковий номер. У такому разі значення атрибуту можна буде у числовому просторі. Наприклад, для категоріального атрибуту Country створимо новий числовий атрибут Country_code з порядковим номером країни, що зустрічається у вибірці (1 Australia, 2 Bangladesh, 3 Canada, ... , 28 USA).

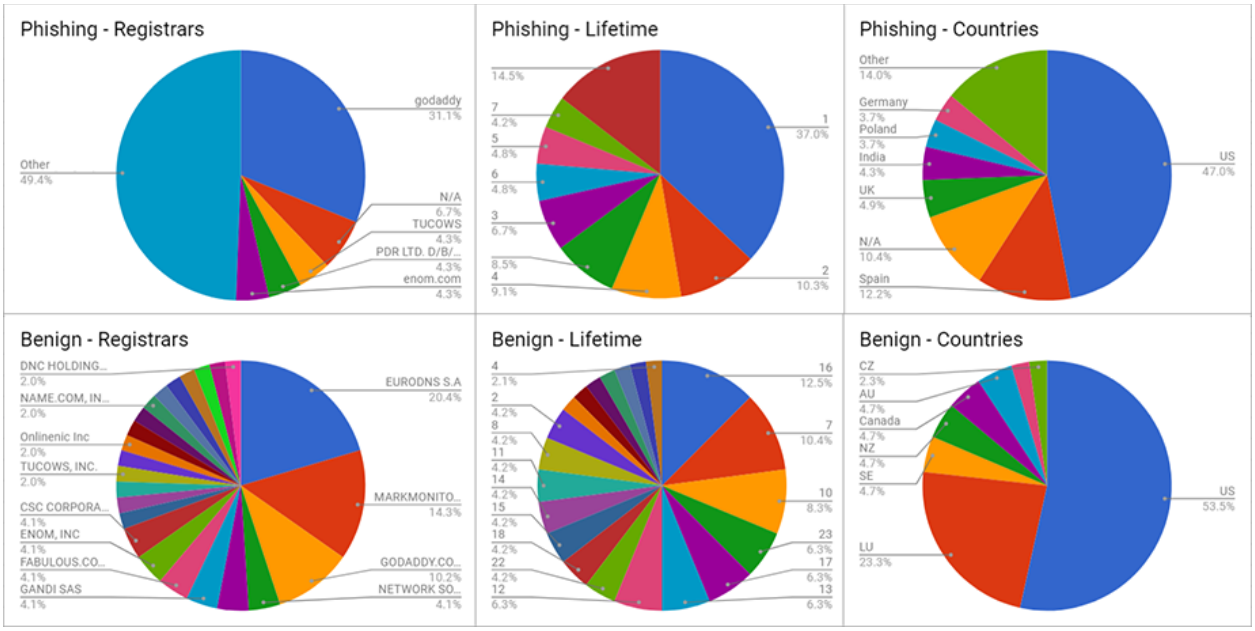


Рис.21.5. *Діаграми, що показують частоту значень трьох атрибутів: а) назву реєстратора (Registrar), б) період реєстрації домену (Lifetime), в) геолокація хостинг-сервера (Countries) для фішингових і доброякісних посилань*

На рис.21.5 видно кілька тенденцій у розподілі даних:

- велика кількість (47% фішингових та 53% доброякісних) IP-адрес знаходиться в США (Country_code = 28);
- переважна більшість фішингових посилань (96%) використовують HTTP-, тоді як усі доброякісні посилання використовують HTTPS-протокол;

- період реєстрації доменів фішингових посилань загалом значно менше, ніж у доброякісних посилань. На більшій вибірці ця тенденція буде краще виражена та приблизно дорівнює 1 року.

Тепер скористаємося методом *k*-найближчих сусідів (англ. k-nearest neighbors algorithm, k-NN) для класифікації посилань. При класифікації метод присвоює об'єкту клас, який є найбільш поширеним серед *k*-сусідів даного об'єкта, класи яких вже відомі.

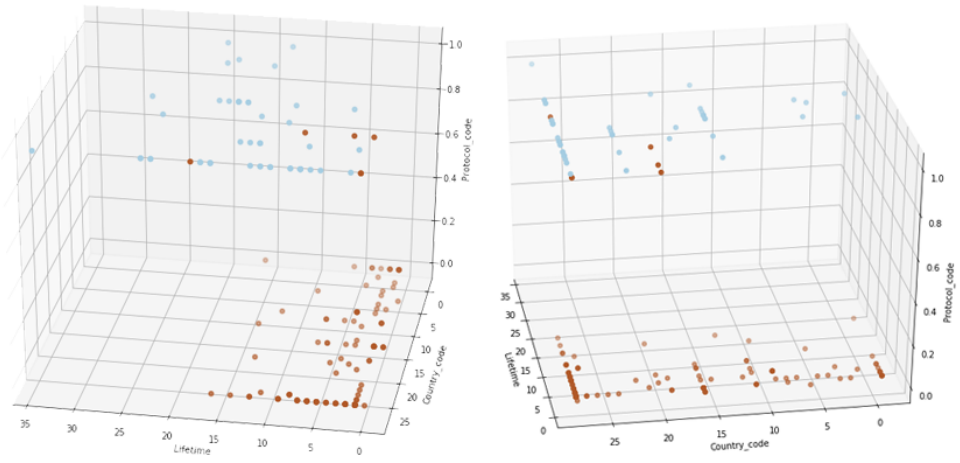


Рис.21.6. *Розподіл фішингових (коричневі точки) та доброякісних (блакитні точки) посилань залежно від періоду реєстрації (lifetime), геолокації (Country_code) та типу протоколу (Protocol_code: {0 - http, 1 - https})*

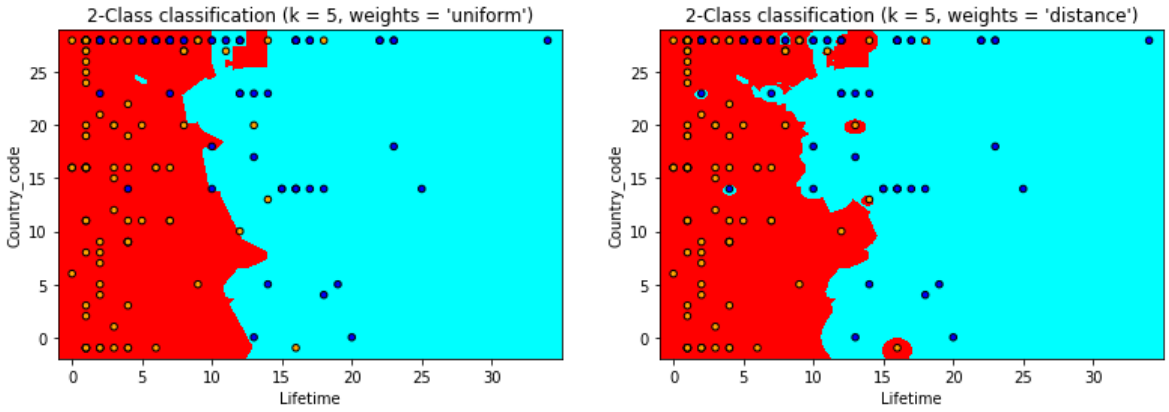


Рис.21.7. *Бінарний класифікатор з урахуванням методу k-найближчих сусідів. Параметри: кількість сусідів k = 5; вагові функції: ліворуч — uniform (усі точки в кожному околиці мають однакову вагу) і праворуч — distance (ближчі сусіди точки запиту матимуть більший вплив, ніж сусіди, які знаходяться далі)*

Спочатку навчимо нашу модель, після чого побудуємо карту класифікатора, щоб побачити межу ухвалення рішення. Якщо нове посилання потрапить у блакитну зону, то воно буде класифіковане як доброякісне, якщо помаранчеве — як фішингове. Точність класифікатора буде тим вищою, чим більше маркованих посилань міститиме тренінгова вибірка. Крім того, можна експериментувати з параметрами моделі, такими як кількість найближчих сусідів, вагова функція, алгоритм знаходження найближчих сусідів та інші.

Далі навчений класифікатор ми можемо використовувати для визначення фішингових посилань. Наприклад, hxxps://www.ebay.com.items-checkout.us/item=2328358263481rt= nctrksid=p2328358263481/ (джерело: Phishtank) - посилання, що веде на підроблену сторінку Ebay з наступними атрибутами: домен зареєстрований на 1 рік (27.01.2019 - 27.01.2020), сервер знаходиться в США, протокол HTTPS. Тому наш класифікатор задедектує реєстратор NameCheap,Inc. як фішинг. У випадку якщо б домен був зареєстрований не на 1 рік, а на 3, то наш класифікатор визначив би сайт як доброякісний.

Для оцінки класифікатора необхідно провести його крос-валідацію (перехресну перевірку) на тестовій вибірці з відомими класами. Результатом тестування буде виявлення відсотка помилкових спрацьовувань. Зокрема, для оцінки класифікатора можуть бути використані такі базові метрики:

- True positive (TP) – кількість фішингових посилань, визначених як фішингові;

- True negative (TN) – кількість доброякісних посилань, визначених як доброякісні;
- False positive (FP) – кількість доброякісних посилань, визначених як фішингові;
- False negative (FN) – кількість фішингових посилань, визначених як доброякісні.

І похідні від них:

- True positive rate (TPR) або Recall = TP/(TP+FN);
- True negative rate (TNR) = TN / (TN+FP);
- False positive rate (FPR) = FP/(FP+TN);
- False negative rate (FNR) = FN / (FN+TP);
- Precision або Positive predictive value (PPV) = (TP+TN) / (TP+TN+FP+FN);
- Negative predictive value (NPV) = TN / (TN+FN);
- F-measure - гармонійне середнє між Recall (TPR) і Precision (PPV) = 2 * Precision * Recall / (Precision + Recall).

У контексті завдання виявлення кібератак найважливішою є метрика FN/FNR, яка дає кількісну оцінку пропущеним атакам.

Візуалізація та зменшення мірності

Оскільки кількість ознак (атрибутів) у моделі найчастіше більша, ніж 2 або 3 (у реальних моделях — 1000 і більше), виникає питання: як уявити об'єкти чи спостереження у дво- чи тривимірному просторі, щоб побачити закономірності їх розподілу для оцінки можливості подальшої класифікації чи кластеризації. Для цього можна скористатися методами зменшення розмірності. Далі ми розглянемо дві техніки – лінійного (PCA) та нелінійного (t-SNE) зменшення розмірності.

Метод головних компонентів (англ. Principal component analysis, PCA) здійснює лінійне відображення даних у простір меншої розмірності таким чином, що дисперсія даних у малорозмірному поданні максимізується.

У нашому випадку зменшення розмірності до двох компонентів маємо такі значення:

- компонента 1: −0.998 x Registrar_code + 0.065 x Lifetime + −0.022 x Country_code + 0.006 x Protocol_code
- компонента 2: 0.020 x Registrar_code + −0.035 x Lifetime + −0.999 x Country_code + −0.005 x Protocol_code

Ми бачимо, що основний внесок у компоненту 1 робить реєстратор домену, а в компоненті 2 — країна, де знаходиться сервер. Це можна пояснити тим, що ці дві величини є категоріальними і після кодування з використанням порядкового номера значення атрибута мають велику дисперсію; розкид значень в інтервалах значень атрибутів (Registrar_code: [1,92], Country_code: [1, 28], Lifetime: [1,34], Protocol_code: [0,1]).

У даному випадку варто поекспериментувати з алгоритмами кодування категоріальних даних, наприклад використовувати one-hot-кодування.

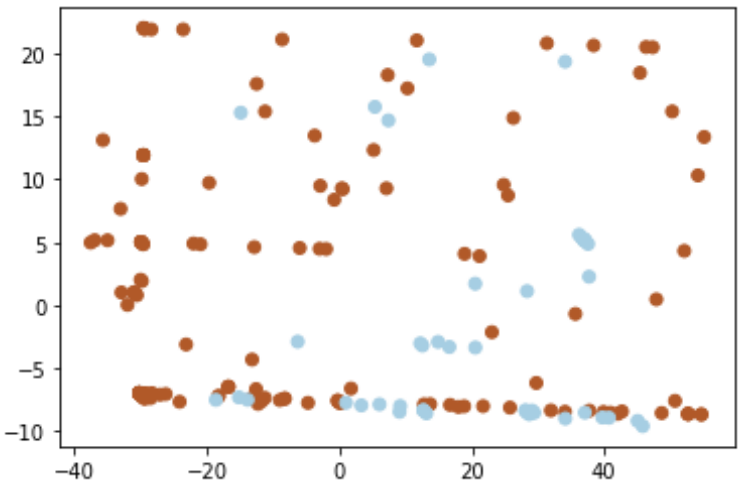


Рис.21.8. *Візуалізація інтернет-посилань у двовимірному просторі після застосування техніки PCA (фішингові посилання – коричневі точки, доброякісні посилання – блакитні точки)*

На рис.21.8 складно виділити окремі групи доброякісних та фішингових посилань. Ця техніка для нашого випадку неефективна.

Іншим алгоритмом є стохастичне вкладення сусідів з *t*-розподілом (T-distributed Stochastic Neighbor Embedding, t-SNE), що представляє нелінійну техніку зменшення розмірності даних. Цей алгоритм є технікою нелінійного зниження розмірності, що добре підходить для вкладення даних високої розмірності для візуалізації в простір низької розмірності (дво- або тривимірний). Зокрема, метод моделює кожен об'єкт високої розмірності дво- або тривимірною точкою таким чином, що схожі об'єкти моделюються близько розташованими точками, а несхожі точки моделюються з великою ймовірністю точками далеко один від одного віддаленими.

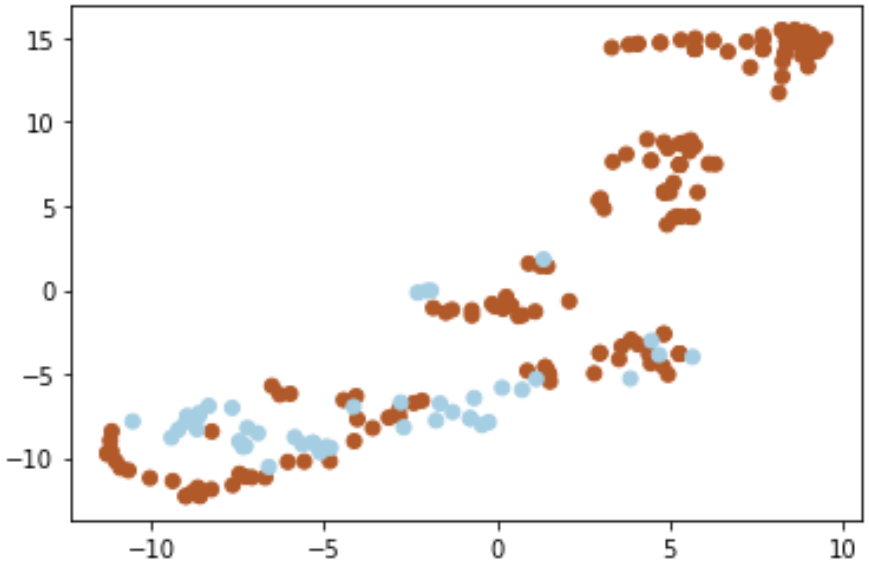


Рис.21.9. *Візуалізація інтернет-посилань у двовимірному просторі після застосування техніки t-SNE (фішингові посилання – коричневі точки, доброякісні посилання – блакитні точки)*

І тут ми можемо побачити скупчення посилань різних класів; це говорить про те, що існують ознаки або їхня сукупність, значення яких можна використовувати для визначення належності об'єктів до одного з класів.

Навчання без вчителя. Кластерний аналіз.

Припустимо, що у нас немає міток класів (фішингові та доброякісні) для інтернет-посилань. У такому разі ми можемо використовувати навчання без вчителя, зокрема кластерний аналіз. Кластеризація дозволяє згрупувати об'єкти невідомих класів за спільністю ознак.

Для цього скористаємося популярним методом кластеризації *k*-середніх (англ. K-means). K-means прагне мінімізувати сумарне квадратичне відхилення точок кластерів від центрів цих кластерів. У нашому випадку кількість кластерів дорівнює двом. Використовуючи техніку t-SNE для проекції даних на двовимірну площину отримуємо наступні візуалізовані результати.

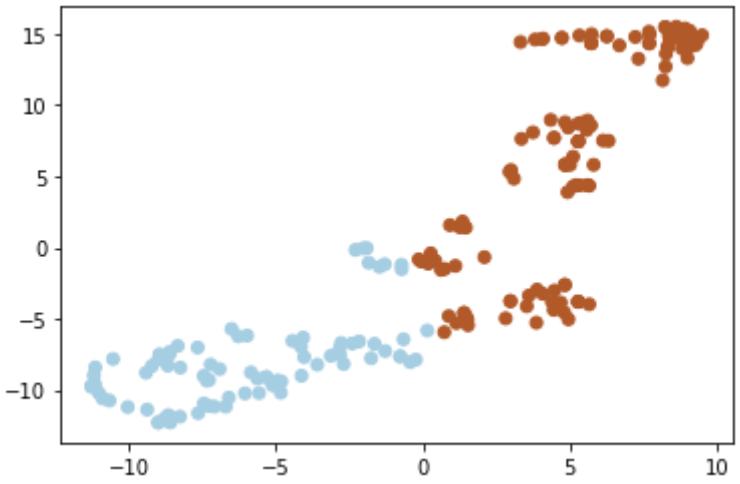


Рис.21.10. *Візуалізація інтернет-посилань у двовимірному просторі після кластерного аналізу за допомогою методу K-means*

Отримані кластери можна порівняти з розміченими даними на малюнку, щоб отримати уявлення про точність кластерного аналізу.

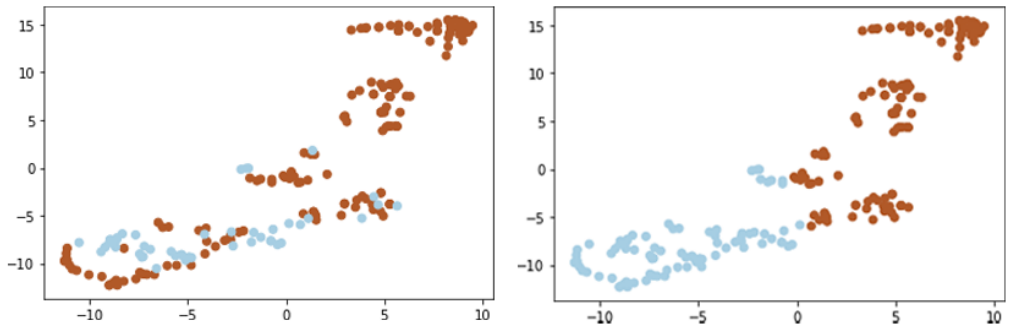


Рис.21.11. *Навчальна вибірка з позначеними мітками класів (ліворуч) та після кластеризації (праворуч)*

Точнішу оцінку ефективності кластеризації можна отримати, використовуючи описані вище метрики: TPR, TNR, FPR, FNR, PPV, NPV, F-measure:

TP = 110, TN = 41, FP = 7, FN = 44;

TPR (Recall) = 71%;

TNR = 85%;

FPR = 15%;

FNR = 29%;

PPV (Precision) = 0.75;

NPV = 0.48;

F-measure = 0.73.

Очевидно, що такої точності класифікатора недостатньо для самостійного використання у продакшен-системах. Однак, враховуючи той факт, що у нас не було позначок класів і ми не навчали нашу модель, це добрий результат. Даний класифікатор може бути затребуваний як додатковий механізм у рамках евристичного підходу для виявлення підозрілих посилань, на які слід звернути увагу і, можливо, подати більш глибокий аналіз або сканування іншими сервісами, наприклад Phishtank або Virustotal. Також можна вдатися до кластеризації для допомоги в маркуванні об'єктів, які надалі, після перевірки

експертом, будуть використовуватися для навчання моделі класифікатора (навчання з учителем) або для детерміністичних методів – пошуку однозначної відповідності з виявленим фішинговим посиланням.

Вище показано на прикладі як застосовують інструменти машинного навчання для виявлення фішингових атак. Навчання без вчителя, незважаючи на невисоку точність, зараз є найперспективнішим напрямом наукових досліджень. Такі моделі не вимагають розмічених даних і тому мають великий потенціал для застосування, у тому числі в галузі кібербезпеки.

Одним із таких перспективних напрямів є детектування аномалій без вчителя. Сьогодні цей підхід активно впроваджується у системи моніторингу та керування подіями інформаційної безпеки (англ. Security Information and Event Management, SIEM) та дозволяє виявляти аномальну активність користувачів та систем, яка може сигналізувати про цільову кібератаку на організацію.

Цікавим, також є можливості застосування генетичних алгоритмів (англ. Genetic Algorithms) та навчання з підкріпленням (англ. Reinforcement Learning) на додаток до популярних Fuzzing та Symbolic Execution для тестування безпеки програмних продуктів (англ. Security Testing) та виявлення вразливостей у них (англ. Vulnerability Testing). Для детектування та аналізу шкідливих програм (malware) може виявитися корисним Smart Pattern Matching. І нарешті, всемогутній Deep Learning, який поки що не набув широкого застосування в кібербезпеці, проте вже успішно використовується в суміжних галузях, зокрема в медіабезпеці для детектування фейкових новин.

21.5. Зростаюча загроза кібератак на основі ШІ

Оскільки світ продовжує ставати все більш оцифрованим, загроза кібератак зростає. За оцінками експертів, зловмисники часто перебувають на кілька кроків попереду фахівців з інформаційної безпеки та правоохоронців. З розвитком технологій хакери стають все більш досконалими у своїх методах і тепер

використовують штучний інтелект (ШІ) для запуску автоматизованих складних атак, які важко виявити і ще важче захиститися.

Кібератаки на основі штучного інтелекту можуть завдати значно більшої шкоди, ніж традиційні кібератаки. ШІ можна використовувати для автоматизації таких завдань, як пошук вразливостей, пошук інформації та запуск цілеспрямованих атак. Це збільшує швидкість і масштаб атак, дозволяючи хакерам запускати одночасні атаки на кілька цілей. ШІ також можна використовувати для створення великих обсягів даних, які можна використовувати для обходу систем безпеки та проникнення в мережі.

Останніми роками атаки програм-вимагачів за допомогою штучного інтелекту стали частішими та завдають більшої шкоди. Ці атаки використовують ШІ для швидкого виявлення вразливих систем і розгортання програм-вимагачів, які можуть швидко поширюватися в мережі. Зловмисне програмне забезпечення на основі штучного інтелекту також можна використовувати для проникнення в мережі, викрадення даних і зриву операцій.

Еволюція штучного інтелекту може бути небезпечною в галузі інформаційної безпеки з кількох причин.

- По-перше, ШІ може бути використаний зловмисниками для створення більш досконалих та ефективних кібератак. Використання ШІ в кіберзлочинах може призвести до більш складних і тонких атак, які будуть важче виявити та запобігти.
- По-друге, з розвитком ШІ можуть виникнути нові вразливості, які можуть бути використані для атак на інформаційну систему. Наприклад, ШІ може бути навчений шукати та використовувати вразливості в системі безпеки, щоб отримати доступ до захищених даних.
- По-третє, ШІ може бути використаний для створення підроблених даних, що може призвести до серйозних наслідків.

Як хакери можуть використовують ШІ для проведення кібератак?

Наприклад, в останій час найбільшою загрозою було визнано дипфейки. Вони дозволяють обійти аутентифікацію обличчям, голосом тощо. Такі рішення можуть використовуватися для дезінформації та маніпуляції.

Також ШІ дозволяє простіше і швидше зібрати важливу інформацію про об'єкт, що атакується. Візьмемо, наприклад, FindFace: фотографуєте обличчя людини, і мобільний додаток знаходить суб'єкт у соцмережах. Виходить, що деанонімізацію, аналіз соцмереж жертви можна провести плюс/мінус безкоштовно.

Насамперед, ШІ використовується для розвідки та збору даних з відкритих джерел – соціальних мереж, месенджерів, інтернет-магазинів, форумів у даркнеті. Дані такої розвідки безцінні під час підготовки атак. Хакер також навчає ШІ виконувати рутинні зломи. Вже зараз хакери щосили експериментують з імперсонацією – використовуючи фото та відео людей у Мережі можна збирати ШІ-ботів, що виглядають та говорять, умовно, як керівник якоїсь компанії начальник. Потім можна використовувати такий бот для соціальної інженерії, обманом змушуючи співробітників цієї компанії зробити потрібні шахраям дії. Це теж форма атак, які без ШІ були неможливі.

Хакери використовують ШІ для проведення кібератак, включаючи вразливості та обходу механізмів безпеки, аналізу даних та розпізнавання образів. Наприклад, ШІ може використовуватися для створення фішингових листів, які є більш ефективними в обмані користувачів. Для боротьби з хакерами, що використовують ШІ, можна використовувати різні техніки, такі як моніторинг мережного трафіку та виявлення аномалій, а також навчання алгоритмів ШІ для виявлення атак та прийняття контрзаходів. Крім того, важливо проводити навчання користувачів та забезпечувати хорошу кібербезпеку, щоб знизити ризики кібератак, у тому числі з використанням ШІ.

Як можна протистояти таким загрозам?

Необхідно використовувати багатофакторну автентифікацію для доступу до корпоративних програм; обмежити доступ до фото- та відеоматеріалів за участю перших осіб компанії; використовувати обробку фото спеціальними програмами, що ускладнюють використання дипфейків.

Зростаюча загроза кібератак на основі штучного інтелекту спонукала уряди та організації вжити заходів для свого захисту. Багато організацій застосували рішення кібербезпеки на основі штучного інтелекту для виявлення загроз і захисту своїх мереж. Крім того, організації збільшили свої бюджети безпеки та інвестують у навчання та навчання, щоб допомогти співробітникам розпізнавати потенційні загрози та реагувати на них.

Загалом зловмисники створюють нові продукти для атаки, а сторона, що захищається, – інструменти для протистояння їм. І, можливо, незабаром ми побачимо, як один ШІ нападає, а інший – захищається без участі людей.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

- Як вплинуло застосування штучного інтелекту на кібербезпеку?
- Дайте визначення штучного інтелекту. Що таке парадигми штучного інтелекту?
- Які існують способи машинного навчання?
- Дайте класифікацію продуктів кібербезпеки, що застосовують технології штучного інтелекту.
- Які нові тренди та можливості посилення кібербезпеки штучним інтелектом?
- Опишіть схему дедектування фішингових кібератак з вчителем.

Література

1. Бабак В.П., Ключников А.А. Теоретические основы защиты информации. – Чернобыль: Ин-т проблем безопасности АС, 2012. – 776с.
2. Браіловський М.М., Зибін С.В., Пискун І.В. та інш. Технології захисту інформації. – К: ЦП «Компрінт», 2021. – 296с.
3. Бобало Ю.Я., Дудикевич В.Б., Микитин В.Г. Стратегічна безпека системи «об'єкт – інформаціна технологія.» - Львів: Вид. Львівської політехники, 2020. – 260с.
4. Браіловський М.М., Зибін С.В., Кобозева А.А., Хорошко В.О., Хохлачова Ю.Є. Аналіз кіберзахищеності інформаційних систем: монографія – К: ФОП Ямчинський О.В., 2021. – 360с.
5. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є. Технології захисту інформації: підручник – К: ЦП «Компрінт», 2021. – 296с.
6. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформація та кібербезпека: соціотехнічний аспект - К: ДУТ, 2015. – 288с.
7. Бурячок В.Л. Основи формування державної системі кібернетичної безпеки. – К: НАУ, 2013. – 432с.
8. Бутузов В.М. Протидія комп'ютерній злочинності в Україні. – К: КИТ, 2010. – 408с.
9. Гайворонський М.В., Новіков О.М. Безпека іноформаційно-комунікаційних систем. – К: Вид. група BHV, 2009. – 608с.
10. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії дифіренціальних ігор та диференціальних перетворень: монографія. – Житомир: Рута, 2010. – 280с.
11. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: монографія. - Житомир: ЖНАЕУ, 2016. – 636с.
12. Грабар І.Г., Грищук Р.В., Молодецька К.В. Беспекова синергетика: кібернетичний та інформаційний аспекти. – Житомир: ЖНАЕУ, 2019. – 280с.
13. Домарев В.В. Безопасность информационных технологий. Системный подход. – К: ООО «ТИД «ДС»», 2004. – 992с.
14. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К: Изд. «ТИД «ДС»», 2001. – 688с.
15. Дубов Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України. – К: НІСД, 2011. – 30с.
16. Дудикевич В.Б., Хорошко В.О., Яремчук Ю.Є. Основи інформаційної безпеки. – Вінниця: ВНТУ, 2018. – 316с.
17. Єжова Л.Ф., Корченко А.О., Мачалін І.О., Скачек Л.М., Хорошко В.О. Управління інформаційною безпекою. В 2-х томах. – К: Вид. НАУ, 2012.

18. Катренко А.В., Пасічник В.В., Пасько В.П. Теорія прийняття рішень. К: Вид. група BHV, 2009. – 448с.

19. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем. – К: ДУІКТ, 2010. – 316с.

20. Козюра В.Д., Хорошко В.О., Шелесм М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ТПК «Орхідея», 2020. – 236с.

21. Козюра В.Д., Скачек Л.М., Ткач Ю.М. та інші. Процеси та технології в інформаційних системах. - Ніжин: ТПК «Орхідея», 2020. – 278с.

22. Кузнецов О.О., Євсеєв С.В., Король О.Г. Захист інформації в інформаційних системах: методи традиційної криптографії. – Харків: Вид. ХНЕУ, 2010. – 316с.

23. Лаптєв О.А. Методичні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К: Міленіум, 2020. – 326с.

24. Мухин В.Е. Риск – ориентированная информационная безопасность. – К: НТТУ «КПИ», 2011. – 292с.

25. Проблемы защиты информации от утечки и пути её решения / С.Л. Емельянов. - Одесса: Феникс, 2011. – 624с.

26. Павлов І.М., Хорошко В.О. Проектування комплексних систем захисту інформації. – К: ВІТІ, ДУІКТ, 2011. – 245с.

27. Поповский В.В., Персиков А.В. Защита информации в телекоммуникационных системах. В 2-х томах. – Харьков: СМИТ, 2006.

28. Томашевський В.М. Моделювання систем. – К: Вид. група BHV, 2005. – 352с.

29. Хорошко В.О., Павлов І.М., Бобало Ю.Я., Дудикевич В.Б., Опірський І.Р., Пархуць Л.Т. Проектування комплексних систем захисту інформації. - Львів: Вид Львівської політехники, 2020. – 320с.

30. Фельдман Л.П., Петренко А.І., Дмітрієва О.А. Чисельні методи в інформатиці. – К: Вид. група BHV, 2006. – 480с.

31. Хорошко В.О., Хохлачова Ю.Є., Козловський В.В. та інш. Новітні технології захисту інформації. – К: НАУ, 2023. – 312с.

32. National Strategy to Secure Cyberspace. U.S. government via Department of Homeland Security. February 2003. p. 16. Retrieved 2008-05-18. [Електронний ресурс]. – Режим доступу: ttp://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

33. ITU's Global Cybersecurity Agenda: An International Framework for Cybersecurity. - Geneva: ITU, 2007. - 46 pp.. [Електронний ресурс]. – Режим доступу: http://www.itu.int/osg/csd/cybersecuritv/gca/index.html.

34. C. E. Shannon Communication Theory of Secrecy Systems // Bell System Technical Journal, vol.28, issue 4, oct. 1949. - pp. 656-715.

35. Phitzmann B. Information hiding terminology // Information Hiding: First International Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science, vol.1174, 1996. - pp. 374-350.

36. Young A., Yung M. Kleptography: using Cryptography against Cryptography // In book: EURO-CRYPT'97 (series: Lecture Notes in Computer Science). Springer, 1998. – vol.1233. – pp. 62–74.

37. Young A., Yung M. Malicious Cryptography. Exposing Cryptovirology. Wiley Publishing, Inc. 2004.

38. Kovalenko B. Methods and models for developing cryptosystems resistant to kleptographic modifications / Dis. ktn for specialty 05.13.21. - National Aviation University. - Kiev, 2019.

39. Kovalenko B., Kudin A. "Kleptography trapdoor free cryptographic protocols", Cryptology ePrint Archive, Report 2018/989, https://eprint.iacr.org/2018/989.

40. Operation Rubikon (нім.). ZDFmediathek. 11 February 2020 https://www.zdf.de/politik/frontal/operation-rubikon-100.html

41. National Institute of Standards and Technology. Escrowed Encryption Stand-ard. - NIST FIPS PUB 185, U.S. Department of Commerce, 1994.

42. National Institute of Standards and Technology. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. – NIST Spe-cial Publication 800-90A, Rev. 1, 2012. First version June 2006, second ver-sion March 2007, http://csrc.nist.gov/publications/ PubsSPs.html#800-90A.

43. ISO/IEC 18031:2005. Information technology – Security techniques – Ran-dom bit generation.

44. Matthew Sparkes Mathematician warns US spies may be weakening next-gen encryption // NewScientist, 10 October 2023 / https://www.newscientist.com/ article/2396510-mathematician-warns-us-spies-may-be-weakening-next-gen-encryption

45. G. Simmons The Prisoners' Problem and the Subliminal Channel // Plenum Press. In Proceedings of Crypto '83, 1984. – pp. 51-67.

46. C. Ajluni, "Two New Imaging Techniques Promise To Improve IC Defect Identification", Electronic Design, Vol. 43(14), July 1995, pp. 37-38.

47. R. Anderson, M. Kuhn, "Tamper Resistance – A Cautionary Note", 2nd USENIX Workshop on Electronic Commerce, Nov 1996, pp 1-11, ISBN 1-880446-83-9.

48. E. Biham, A. Shamir, "Differential Fault Analysis: A New Cryptanalytic Attack on Secret Key Cryptosystems", 1997, Springer LNCS 1294, pp. 513.

49. R. Anderson, M. Kuhn, "Low Cost Attacks on Tamper Resistant Devices", in Security Protocols (Proceedings of the 5th International Workshop (1997) Springer LNCS vol 1361 pp 125–136.

50. Oliver Kommerling. Design Principles for Tamper-Resistant Smartcard Processors / Oliver Kommerling, Markus G. Kuhn. – USENIX Workshop on Smartcard Technology, – Chicago, Illinois, USA, May 10–11, 1999.

51. Paul Kocher, Joshua Jaffe, Benjamin Jun. Differential Power Analysis (англ.) // Proc. of Advances in Cryptology (CRYPTO '99), LNCS : збірник. — 1999. — Vol. 1666. — DOI:10.1.1.40.1788.

52. Mike Bond. Attacks on Cryptoprocessor Transaction Sets (англ.) // Springer-Verlag London, UK ©2001. — ACM Digital Library, Pages 220-234 - CHES '01 Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems - May 14 - 16, 2001.

53. Mike Bond, Ross Anderson. API-Level Attacks on Embedded Systems (англ.) // IEEE Computer Society Press Los Alamitos, CA, USA. — ACM Digital Library, Volume 34 Issue 10, Page 67-75, October 2001.

54. Jean-Jacques Quisquater, Francois Koeune. Side Channel Attacks. State-of-the-art (англ.) // October 2002 (перевірено October 2017).

55. S. Skorobogatov, R. Anderson, “Optical Fault Induction Attacks”, Cryptographic Hardware and Embedded Systems Workshop, CHES 2002, Springer LNCS 2523, pp. 2-12.

56. SP Skorobogatov, \Low temperature data remanence in static RAM", Technical report UCAM-CL-TR-536, university of Cambridge Computer Laboratory, June 2002.

57. JJ Quisquater and D Samyde, \Eddy Current for Magnetic Analysis with Active Sensor", Proceedings of ESmart 2002, pp 185-194, Eurosmart.

58. David Samyde, Sergei Skorobogatov, Ross Anderson and Jean-Jacques Quisquater. On a New Way to Read Data from Memory (англ.) // 1: Universit_e catholique de Louvain, UCL Crypto Group Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium, — 2: Computer Laboratory, JJ Thompson Avenue, Cambridge CB3 0FD, England — November 28, 2002.

59. Kevin Magee, Prof. Kris Gaj. Timing Cryptanalysis (англ.) // AC-2_slides - ECE Department - George Mason University, ECE 646, Fall 2003.

60. Kevin Magee, Prof. Kris Gaj. Timing Cryptanalysis Final Report (англ.) // AC-2_report - ECE Department - George Mason University, ECE 646, Fall 2003.

61. J. Clulow, “The Design and Analysis of Cryptographic APIs for Security Devices”, MSc Thesis, University of Natal, SA, 2003.

62. Mike Bond and Jolyon Clulow. Encrypted? Randomised? Compromised? (When Cryptographically Secured Data is Not Secure) (англ.) // Computer Laboratory, University of Cambridge, JJ Thompson Av., CB3 0FD, UK. — In Cryptographic Algorithms and Their Uses, Eracom Workshop 2004.

63. S. Skorobogatov, “Semi-Invasive Attacks – A New Approach to Hardware Security Analysis”, PhD Thesis, University of Cambridge, September 2004.

64. YongBin Zhou, DengGuo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing (англ.) // Information Security Seminar WS 0607. — 2006.

65. Anderson R., Bond M., Clulow J., Skorobogatov, S. Cryptographic processors – a survey (англ.) // Proceedings of the IEEE : журнал. — 2006. — Vol. 94, fasc. 2. — P. 357—369. — ISSN 0018-9219. — DOI:10.1109/JPROC.2005.862423.

66. YongBin Zhou, DengGuo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing (англ.) // Information Security Seminar WS 0607. — 2006.

67. Adam Matthews. Low Cost Attacks on Smart Cards The Electromagnetic Side-Channel (англ.) // Next Generation Security Software Ltd. — September 2006.

68. Eric Peeters, Fran.cois-Xavier Standaert, Jean-Jacques Quisquater. Power and Electromagnetic Analysis: Improved Model, Consequences and Comparisons (англ.) // UCL Crypto Group, Place du Levant, 3, B-1348 Louvain-La-Neuve, Belgium. — May 24, 2007.

69. Elke De Mulder. Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices. – Dissertation presented in partial fulfillment of the requirements for the degree of Doctor in Electrical Engineering (англ.) // Arenberg Doctoral School of Science, Engineering & Technology Faculty of Engineering Department of Electrical Engineering (ESAT), Katolieke Universiteit LEUVEN. — November 24, 2010.

70. Dr Sergei Skorobogatov. Side-channel attacks: new directions and horizons (англ.). Design and Security of Cryptographic Algorithms and Devices (ECRYPT II) (3 June 2011).

71. Dr Sergei Skorobogatov. Fault attacks on secure chips: from glitch to flash (англ.) // Design and Security of Cryptographic Algorithms and Devices (ECRYPT II) Albena, Bulgaria, 29 May – 3 June 2011.

72. Joe Grand. Practical Secure Hardware Design for Embedded Systems (англ.) // Grand Idea Studio, Inc. — Black Hat DC 2011 Workshop — www.grandideastudio.com.

73. Joe Grand. Hardware Reverse Engineering: Access, Analyze, & Defeat (англ.) // Grand Idea Studio, Inc. — Black Hat DC 2011 Workshop — www.grandideastudio.com.

74. Mohammad Tehranipoor. Crypto Processor Design and Trusted Platform Modules (англ.) // ECE 4095: Hardware Security & Trust — University of Connecticut, ECE Department. — 2012.

75. Mehmet Meral. Cryptoprocessors (англ.) // Grand Idea Studio, Inc. — RSA Conference 2015, San Francisco, April 20-24, Moscone Centre.

76. Joe Grand. Tools of the Hardware Hacking Trade (англ.) // Grand Idea Studio, Inc. — RSA Conference 2015, San Francisco, April 20-24, Moscone Centre.

Навчальне видання

Баланюк Юрій Вікторович, Козловський Валерій Валерієвич,
Лисецький Юрій Михайлович, Моркляник Богдан Васильйович, Хорошко
Володимир Олексійович, Хохлачова Юлія Євгенівна,
Шелест Михайло Євгенович

КІБЕРБЕЗПЕКА

Підручник

Літературний редактор, коректор – Ю. Хохлачова
Комп'ютерна верстка, макетування – А.О. Брем
Технічний редактор – В.Ю. Бихун

Підп. до друку 10.05.2024. Формат 64x90/16.
Папір офсетн. Друк цифровий.
Ум. друк. арк. 9,36. Наклад 1000 прим. Зам. № 25/12

Видавець Бихун В.Ю.
Видавництво «ЛАТ&К»
вул. Леонтовича, 9, к. 18, м. Київ, 01054
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
ДК № 5366 від 26.06.2017 р.
тел./факс: +38 044 235 000 9
моб.: +38 050 310 22 04
e-mail: lk@ukr.net