## Розділ 10. Моделі безпеки в інформаційній та/або кібербезпеці.

**10.1. ДСТУ ISO/IEC 15408**
**10.2. Модель порушника.**
**10.3. Модель загроз.**
**10.4. Модель вразливостей**

### 10.1. ДСТУ ISO/IEC 15408

При побудові моделі безпеки в інформаційній та/або кібербезпеці, для аналізу інформаційних ризиків необхідно використовувати моделі системи інформаційної безпеки, засновані на міжнародних стандартах. Для цього як правило використовуються наступні стандарти: ДСТУ ISO/IEC 27002 та ДСТУ ISO/IEC 15408. ДСТУ ISO/IEC 27002 розглядався раніше, тому розглянемо ДСТУ ISO/IEC 15408.

**ДСТУ ISO/IEC 15408. Інформаційні технології. Методи захисту. Критерії оцінки.**

Безпека інформаційних технологій (IT) стоїть у ряду найактуальніших проблем інформатизації суспільства. Її розв'язання значною мірою визначається досконалістю відповідної нормативно-методичної бази. Дана доповідь присвячена одному з найбільш значущих в цьому плані документів – міжнародному стандарту ISO/IEC 15408 "Критерії оцінки безпеки інформаційних технологій "

**Стандарт ISO 15408** – один з найбільш поширених стандартів у галузі безпеки. У його створенні взяли участь організації зі США, Канади, Англії, Франції, Німеччини, Голландії. У стандарті, що отримав назву «Загальні критерії оцінки безпеки інформаційних технологій» (The Common Criteria for Information Technology Security Evaluation), докладно розглянуто загальні підходи, методи та функції забезпечення захисту інформації в організаціях.

Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. **Всі функції представлені у вигляді чотирирівневої ієрархічної структури**: клас – сімейство – компонент – елемент.

За аналогією представлені вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки і зіставити створену модель з поточним станом справ.

**У стандарті виділені 11 класів функцій**:

– аудит;
– ідентифікація та автентифікація;
– криптографічний захист;
– конфіденційність;
– передача даних;
– захист даних користувача;
– управління безпекою;

– захист функцій безпеки системи;
– використання ресурсів;
– доступ до системи;
– надійність засобів.

Оцінка інформаційної безпеки базується на моделях системи безпеки, що складаються з перерахованих у стандарті функцій. У ISO 15408 міститься **ряд зумовлених моделей** (так званих **профілів),** що описують стандартні модулі системи безпеки. З їх допомогою можна не створювати моделі поширених засобів захисту самостійно, винаходячи велосипед, а користуватися вже готовими наборами описів, цілей, функцій і вимог до цих засобів. Простим прикладом профілів може служити модель міжмережевого екрану.

**Сертифікований профіль** являє собою повний опис певної частини (або функції) системи безпеки. У ньому міститься аналіз внутрішнього і зовнішнього середовища об'єкта, вимоги до його функціональності і надійності, логічне обгрунтування його використання, можливості та обмеження розвитку об'єкта.

Стандарт ISO 15408 вигідно відрізняє **відкритість.** Описує ту чи іншу область системи безпеки профіль можна створити самостійно за допомогою розробленої в ISO 15408 структури документа. У стандарті визначена також послідовність дій для самостійного створення профілів.

**Загальні критерії (ЗК) визначені у стандарті ISO 15408 дозволяють підвищити довіру до засобів захисту і самої інформації, що захищається за рахунок трьох основних якостей:**

1. Можливості гнучкого завдання вимог до засобів захисту інформації з урахуванням їх призначення і умов застосування.
2. Більш повного і обґрунтованого набору вимог безпеки.
3. Наявності методології оцінки, що забезпечує об'єктивність і порівнянність результатів.

**Загальні критерії являють собою набір з п'яти окремих взаємопов'язаних частин. До них відносяться:**

– Введення і загальна модель.
– Функціональні вимоги безпеки.
– Вимоги до надійності захисних механізмів.
– Попереднє визначення профілі захисту.
– Процедури реєстрації профілів захисту.

**Основними відмітними рисами ЗК є наступні:**

1. Перш за все, ЗК – це певна методологія та система формування вимог і оцінки безпеки ІТ. Системність простежується, починаючи від термінології та рівнів абстракції представлення вимог аж до їх застосування при оцінці безпеки на всіх етапах життєвого циклу продуктів і систем ІТ.
2. Загальні критерії характеризуються найбільш повною на сьогоднішній день сукупністю вимог безпеки ІТ.
3. У ЗК проведено чіткий поділ вимог безпеки на функціональні вимоги і вимоги довіри до безпеки. Функціональні вимоги (11 класів, 66 родин, 135 компонентів) відносяться до функцій безпеки (ідентифікації, автентифікації, управління доступом, аудиту і т. д.), а вимоги довіри (8 класів, 44 сімейства, 93

компонента) – до досягнення впевненості в коректності реалізації та ефективності функцій безпеки шляхом оцінки технології розробки, тестування, аналізу вразливостей експлуатаційної документації, постачання і супроводу продуктів та систем ІТ.

4. Загальні критерії включають шкалу довіри до безпеки (оціночні рівні довіри – ОРД), яка може використовуватися для отримання різного ступеня впевненості у безпеці продуктів і систем ІТ

5. Систематизація і класифікація вимог щодо ієрархії «клас» – «сімейство» – «компонент» – «елемент»з унікальними ідентифікаторами вимог забезпечує зручність їх використання.

6. Компоненти вимог в родинах і класах ранжовані за ступенем повноти і строгості, а вимоги довіри згруповані в пакети вимог

7. Гнучкість у підході до формування вимог безпеки для різних типів продуктів і систем ІТ та умов їх застосування забезпечується можливістю цілеспрямованого формування необхідних наборів вимог у вигляді певних в ЗК стандартизованих структур (пакетів вимог, профілів захисту і завдань з безпеки).

8. Загальні критерії володіють відкритістю і розширюваністю, тобто дозволяють уточнювати існуючі і вводити додаткові вимоги.

Як показують оцінки фахівців у галузі інформаційної безпеки за рівнем систематизації, повноті і можливостям деталізації вимог, універсальності і гнучкості в застосуванні ЗК представляють найбільш досконалий з існуючих в даний час стандартів. Причому, що дуже важливо, в силу особливостей побудови він має практично необмежені можливості для розвитку і являє собою базовий стандарт, що містить методологію завдання вимог і оцінки безпеки ІТ, а також систематизований каталог вимог безпеки. Як функціональних стандартів, в яких формулюються вимоги до безпеки певних типів продуктів і систем ІТ, передбачається використання профілів захисту (ПЗ), що створюються за методологією і на основі каталогу вимог ЗК. У ПЗ можуть бути включені і будь-які інші вимоги, які є необхідними для забезпечення безпеки конкретного типу продуктів або систем ІТ.

– керівництво з розробки профілів захисту і завдань з безпеки;

– процедури реєстрації профілів захисту;

– загальна методологія оцінки безпеки інформаційних технологій;

– Інструментальні засоби автоматизації розробки профілів захисту і завдань з безпеки.

Загальні критерії отримали широке визнання у світі. У 1998 році урядовими організаціями Канади, Франції, Німеччини, Великобританії і США було підписано угоду про взаємне визнання оцінок (The International Mutual Recognition Arrangement – MRA), отриманих на основі Загальних критеріїв.

У травні 2000 року представниками вже чотирнадцяти країн було підписано більш універсальне (у порівнянні з MRA) угоду CCRA (CC Recognition Arrangement). Угода CCRA значно розширює можливості приєднання нових країн-учасниць. Як очікується, найближчим часом їхня кількість наблизиться до двадцяти.

У країнах, що беруть участь в Угоді з Загальними критеріями (перш за все, в США, Великобританії, Франції та ін), розроблено вже декілька десятків профілів захисту для різних типів продуктів ІТ:

– систем управління доступом;
– операційних систем;
– систем управління базами даних;
– міжмережевих екранів;
– компонентів інфраструктури управління ключами;
– смарт-карт і ін.

Частина з них пройшла експертизу і включена в національні реєстри. Існує міжнародний реєстр сертифікованих профілів захисту, а також знаходяться в процесі оцінки і сертифікованих продуктів ІТ. У рамках ОК пройшли оцінку і сертифікацію більше 40 продуктів і систем ІТ і близько 20 знаходиться в процесі оцінки.

Проблема забезпечення безпеки інформаційних технологій займає усе більш значне місце в реалізації комп'ютерних систем та мереж у міру того, як зростає їх роль в інформатизації суспільства. Забезпечення безпеки інформаційних технологій (ІТ) являє собою комплексну проблему, яка вирішується в напрямках вдосконалення правового регулювання застосування ІТ, вдосконалення методів і засобів їх розробки, розвитку системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. Ключовим аспектом вирішення проблеми безпеки ІТ є вироблення системи вимог, критеріїв та показників для оцінки рівня безпеки ІТ.

ДСТУ ISO/IEC 15408 містить загальні критерії оцінки безпеки інформаційних технологій.

ДСТУ ISO/IEC 15408-1 встановлює загальний підхід до формування вимог до оцінки безпеки (функціональні та довіри), основні конструкції (профіль захисту, завдання з безпеки) подання вимог безпеки в інтересах споживачів, розробників і оцінювачів продуктів і систем ІТ. Вимоги безпеки об'єкта оцінки (00) за методологією Загальних критеріїв визначаються виходячи з цілей безпеки, які, у свою чергу, грунтуються на аналізі призначення 00 і умов середовища його використання (загроз, припущень, політики безпеки).

ДСТУ ISO/IEC 15408-2 містить універсальний систематизований каталог функціональних вимог безпеки і передбачає можливість їх деталізації і розширення за певними правилами.

ДСТУ ISO/IEC 15408-3 включає в себе систематизований каталог вимог довіри, визначають заходи, які повинні бути прийняті на всіх етапах життєвого циклу продукту або системи ІТ для забезпечення впевненості в тому, що вони задовольняють пред'явленим до них функціональним вимогам. Тут же містяться оціночні рівні довіри, що визначають шкалу вимог, які дозволяють з зростаючої ступенем повноти і строгості оцінити проектну, тестову та експлуатаційну документацію, правильність реалізації функцій безпеки 00, вразливості продукту або системи ІТ, стійкість механізмів захисту і зробити висновок про рівень довіри до безпеки об'єкта оцінки.

**Особливості ISO 15408 в порівнянні з іншими стандартами в галузі безпеки:**

– Стандарт дозволяє визначити повний перелік вимог до засобів безпеки, а також критерії їх оцінки (показники захищеності інформації).

– Стандарт визначає повний перелік об'єктів аналізу і вимог до них, не загострюючи уваги на методах створення, управління та оцінки системи безпеки.

– Стандарт дозволяє оцінити повноту системи інформаційної безпеки з технічної точки зору, не розглядаючи при цьому комплекс організаційних заходів щодо забезпечення захисту інформації.

Вивчення існуючих критеріїв оцінки безпеки дозволяє зробити наступні висновки:

1. Для того, щоб результати сертифікаційних випробувань можна було порівнювати між собою, вони мають проводитися в рамках надійної схеми, що встановлюється відповідними стандартами в цій галузі і дозволяє контролювати якість оцінки безпеки.

2. В даний час в деяких країнах існують такі схеми, але вони базуються на різних критеріях оцінки. Однак, ці критерії мають між собою багато спільного, тому що використовують подібні концепції, що дозволяє здійснювати їх порівняння. "Єдині критерії" підтримують сумісність з вже існуючими. Це дозволяє використовувати наявні результати та методики оцінок.

3. Єдині критерії визначають загальний набір понять, структур даних і мова для формулювання питань і тверджень щодо безпеки. Це дозволяє експертам, які проводять оцінку, використовувати вже у цій області досвід.

4. Вимоги, що містяться в "Єдиних критеріях", можуть також використовуватися при виборі відповідних засобів забезпечення безпеки. Потенційні користувачі ІКС, спираючись на результати сертифікації, можуть визначити чи задовольняє даний програмний продукт або система їх вимогам безпеки.

5. Крім цього, "Єдині критерії" покращують існуючі критерії, вводячи нові концепції і уточнюючи зміст наявних.

Розглянемо більш детально стандарт.

**ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2022, IDT)**

Цей документ встановлює загальні концепції та принципи оцінювання безпеки ІТ і визначає загальну модель оцінювання, що надається різними частинами стандарту, який у цілому призначений для використання в якості основи для оцінки властивостей безпеки ІТ-продуктів.

Цей документ містить огляд усіх частин серії ISO/IEC 15408. Він описує різні частини серії ISO/IEC 15408; визначає терміни та скорочення, які слід використовувати в усіх частинах стандарту; встановлює основну концепцію мети оцінювання (TOE); описує контекст оцінювання та описує аудиторію, якій

адресовані критерії оцінювання. Дано вступ до основних концепцій безпеки, необхідних для оцінки ІТ-продуктів.

Цей документ представляє:

– ключові поняття профілів захисту (PP), модулів PP, конфігурацій PP, пакетів, цілей безпеки (ST) і типів відповідності;

– опис організації компонентів безпеки по всій моделі;

– різні операції, за допомогою яких функціональні компоненти та компоненти гарантії, наведені в ISO/IEC 15408-2 та ISO/IEC 15408-3, можуть бути налаштовані шляхом використання дозволених операцій;

– загальну інформацію про методи оцінювання, наведені в ISO/IEC 18045;

– настанову щодо застосування ISO/IEC 15408-4 з метою розробки методів оцінювання (EM) і діяльності з оцінювання (EA), виведених із ISO/IEC 18045;

– загальну інформацію про попередньо визначені рівні гарантії оцінювання (EAL), визначені в ISO/IEC 15408-5;

– інформація щодо обсягу схем оцінювання.

**ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2022, IDT)**

Цей документ визначає необхідну структуру та зміст функціональних компонентів безпеки з метою оцінки безпеки. Він містить каталог функціональних компонентів, який відповідає загальним вимогам безпеки багатьох ІТ-продуктів.

Він включає в себе наступні розділи:

1 Область застосування.

2 Нормативні посилання.

3 Терміни та визначення, умовні позначення та скорочення термінів.

4 Огляд.

4.1 Організація цієї частини ISO/IEC 15408.

5 Парадигма функціональних вимог.

6 Функціональні компоненти безпеки.

6.1 Огляд.

6.2 Каталог компонентів.

7 Клас FAU: Аудит безпеки.

7.1 Автоматична відповідь аудиту безпеки (FAU_ARP).

7.2 Генерація даних аудиту безпеки (FAU_GEN).

7.3 Аналіз аудиту безпеки (FAU_SAA).

7.4 Аудит безпеки (FAU_SAR).

7.5 Вибір події аудиту безпеки (FAU_SEL).

7.6 Зберігання подій аудиту безпеки (FAU_STG).

8 Клас FCO: Комунікація.

8.1 Невідмова від походження (FCO_NRO).

8.2 Невідмова від отримання (FCO_NRR).

9 Клас FCS: Криптографічна підтримка.

9.1 Керування криптографічними ключами (FCS_CKM).

9.2 Криптографічна операція (FCS_COP).
10 FDP класу: Захист даних користувача.
10.1 Політика контролю доступу (FDP_ACC).
10.2 Функції контролю доступу (FDP_ACF).
10.3 Автентифікація даних (FDP_DAU).
10.4 Експорт із TOE (FDP_ETC).
10.5 Політика керування потоком інформації (FDP_IFC).
10.6 Функції керування потоком інформації (FDP_IFF).
10.7 Імпорт із-за меж TOE (FDP_ITC).
10.8 Внутрішня передача TOE (FDP_ITT).
10.9 Захист залишкової інформації (FDP_RIP).
10.10 Відкат (FDP_ROL).
10.11 Цілісність збережених даних (FDP_SDI).
10.12 Захист передавання конфіденційності даних користувача між TSF (FDP_UCT).
10.13 Захист передавання цілісності даних користувача між TSF (FDP_UIT).
11 Клас FIA: Ідентифікація та автентифікація.
11.1 Помилки автентифікації (FIA_AFL).
11.2 Визначення атрибутів користувача (FIA_ATD).
11.3 Специфікація секретів (FIA_SOS).
11.4 Автентифікація користувача (FIA_UAU).
11.5 Ідентифікація користувача (FIA_UID).
11.6 Прив’язка користувача до суб’єкта (FIA_USB).
12 Клас FMT: Управління безпекою.
12.1 Керування функціями в TSF (FMT_MOF).
12.2 Керування атрибутами безпеки (FMT_MSA).
12.3 Управління даними TSF (FMT_MTD).
12.4 Відкликання (FMT_REV).
12.5 Термін дії атрибута безпеки (FMT_SAE).
12.6 Специфікація функцій керування (FMT_SMF).
12.7 Ролі керування безпекою (FMT_SMR).
13 Клас FPR: конфіденційність.
13.1 Анонімність (FPR_ANO).
13.2 Псевдонім (FPR_PSE).
13.3 Від’єднаність (FPR_UNL).
13.4 Неспостережуваність (FPR_UNO).
14 Клас FPT: Захист TSF.
14.1 Захист від помилок (FPT_FLS).
14.2 Доступність експортованих даних TSF (FPT_ITA).
14.3 Конфіденційність експортованих даних TSF (FPT_ITC).
14.4 Цілісність експортованих даних TSF (FPT_ITI)..
14.5 Внутрішня передача даних TOE TSF (FPT_ITT).
14.6 Фізичний захист TSF (FPT_PHP).
14.7 Довірене відновлення (FPT_RCV).

14.8 Виявлення повтору (FPT_RPL).
14.9 Протокол синхронізації стану (FPT_SSP).
14.10 Мітки часу (FPT_STM).
14.11 Послідовність даних TSF між TSF (FPT_TDC).
14.12 Тестування зовнішніх об'єктів (FPT_TEE).
14.13 Внутрішня узгодженість реплікації даних TSF TOE (FPT_TRC).
14.14 Самоперевірка TSF (FPT_TST).
15 Клас FRU: Використання ресурсів.
15.1 Відмовостійкість (FRU_FLT).
15.2 Пріоритет обслуговування (FRU_PRS).
15.3 Розподіл ресурсів (FRU_RSA).
16 Class FTA: Доступ TOE.
16.1 Обмеження обсягу вибраних атрибутів (FTA_LSA).
16.2 Обмеження на кілька одночасних сеансів (FTA_MCS).
16.3 Блокування та завершення сеансу (FTA_SSL).
16.4 Банери доступу до TOE (FTA_TAB).
16.5 Історія доступу до TOE (FTA_TAH).
16.6 Встановлення сеансу TOE (FTA_TSE).
17 Клас FTP: Довірений шлях/канали.
17.1 Довірений канал Inter-TSF (FTP_ITC).
17.2 Довірений шлях (FTP_TRP).
Додаток A (обов’язковий) Примітки щодо застосування функціональних вимог безпеки.
Додаток B (обов'язковий) Функціональні класи, родини та компоненти.
Додаток C (обов'язковий) Клас FAU: Аудит безпеки.
Додаток D (обов'язковий) Клас FCO: зв'язок.
Додаток E (обов’язковий) Клас FCS: Криптографічна підтримка.
Додаток F (обов'язковий) Клас FDP: Захист даних користувача.
Додаток G (обов'язковий) Клас FIA: Ідентифікація та автентифікація.
Додаток H (обов'язковий) Клас FMT: Управління безпекою.
Додаток I (обов’язковий) Клас FPR: конфіденційність.
Додаток J (обов’язковий) Клас FPT: Захист TSF.
Додаток K (обов'язковий) Клас FRU: Використання ресурсів.
Додаток L (обов'язковий) Class FTA: доступ до TOE.
Додаток M (обов’язковий) Клас FTP: Довірений шлях/канали

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

ISO/IEC 15408-3:2008 визначає вимоги довіри до критеріїв оцінювання. Він включає в себе рівні достовірності оцінки, які визначають шкалу для вимірювання достовірності для цілей компонентів оцінювання (TOE), складені пакети достовірності, які визначають шкалу для вимірювання достовірності для складених TOE, окремі компоненти довіри, з яких складаються рівні та пакети достовірності., а також критерії оцінки профілів захисту та цілей безпеки.

ISO/IEC 15408-3:2008 визначає зміст і представлення вимог довіри у формі класів достовірності, сімейств і компонентів і надає вказівки щодо організації нових вимог довіри. Компоненти впевненості в сімействах впевненості представлені в ієрархічному порядку.

**Моделі безпеки в інформаційній та/або кібербезпеці**

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).

**Інформаційна безпека за сферою застосування**

**Інформаційна безпека держави** – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається заподіяння шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

**Інформаційна безпека організації** – цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток. Здійснюється часто Службою інформаційної безпеки.

**Інформаційна безпека особистості** характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Створення **моделі управління захистом інформації** ґрунтується на послідовному визначенні об’єктів управління, цілей і завдань управління, показників і критеріїв ефективності управління, функцій управління, складу системи та організаційної структури управління, на розробці методів і засобів управління.

Проблеми інформаційної безпеки істотно залежать від типу інформаційних систем і сфери їх застосування. У локальних системах малого масштабу систему захисту побудувати набагато простіше, ніж в системах розподіленого типу, що пояснюється особливостями цих систем, основними з яких є:

– територіальна розосередженість компонентів системи і як наслідок наявність обміну інформацією між ними;

– широкий спектр способів подання, зберігання і передачі інформації;

– одночасна участь в процесах опрацювання інформації великою кількістю користувачів з різними правами доступу;

– використання різнорідних програмно-технічних засобів обробки і систем телекомунікацій.

Саме тому фахівцями була запропонована **структурна модель інформаційної безпеки систем розподіленого типу**, яка відображена на рис. 10.1.

Структурна модель передбачає, що рішення проблеми безпеки в інформаційних системах розподіленого типу полягає в аналізі наступних основних компонентів:

– визначення основних завдань захисту інформації;

– визначенні суб'єктів інформаційних процесів;

– класифікації основних можливих загроз безпеки;

– визначенні рівнів вразливості інформаційних систем;

– визначенні джерел інформації;

– ознайомленні з особливостями джерел загроз;

– дослідженні способів та напрямів захисту та звичайно цілей захисту.

**Забезпечення безпеки інформації** полягає у вирішенні трьох взаємопов'язаних завдань: конфіденційність, цілісність, доступність.

– Завдання забезпечення **конфіденційності** полягає в захисті інформації в процесі її створення, зберігання, обробки та обміну від ознайомлення з нею особами, які не мають права доступу до неї.

– Завдання щодо забезпечення **цілісності** полягає в захисті від навмисної або ненавмисної зміни інформації та алгоритмів її обробки особами, які не мають на те права.

– Забезпечення **доступності** полягає в наданні користувачам всієї наявної в системі інформації відповідно до встановлених їм правам.

**Додатково також використовують такі властивості**:

– Апелювання (англ. non-repudiation) – можливість довести, що автором є саме заявлена людина (юридична особа), і ніхто інший.

– Підзвітність (англ. accountability) – властивість інформаційної системи, що дозволяє фіксувати діяльність користувачів, використання ними пасивних об'єктів та однозначно встановлювати авторів певних дій в системі.

– Вірогідність (англ. reliability) – властивість інформації, яка визначає ступінь об'єктивного, точного відображення подій, фактів, що мали місце.

– Автентичність (англ. authenticity) – властивість, яка гарантує, що суб'єкт або ресурс ідентичні заявленим.

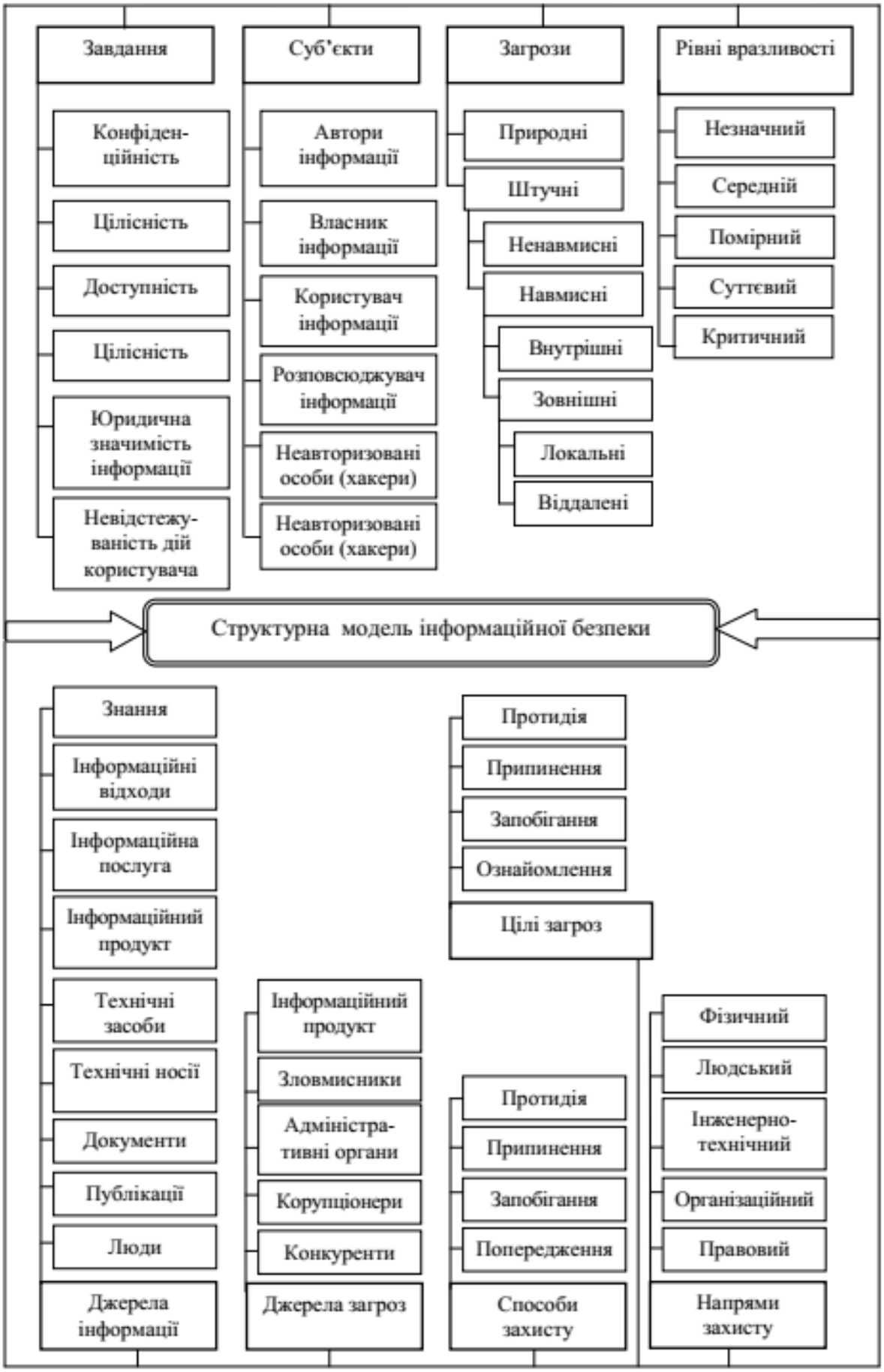


Рисунок 10.1 – Структурна модель інформаційної безпеки

**Основними суб'єктами в інформаційних процесах** є:

– автори і власники інформації;

– авторизовані користувачі інформації;

– неавторизовані особи (особи, які намагаються отримати самовільний доступ до інформації);

– окремі співробітники або колективи;

– які беруть участь в розробці, забезпеченні працездатності програмно-технічних засобів інформаційних систем і наповненні системи інформацією.

Системи захисту повинні забезпечувати захист прав авторів і власників інформації та одночасно надавати доступ до інформації користувачам відповідно до їх прав.

Під **загрозою безпеки** інформаційних систем розуміється потенційно можлива дія, подія або процес, який за допомогою впливу на інформацію та інші компоненти системи може завдати шкоди інтересам суб'єктів.

**Джерелами загроз** виступають конкуренти, злочинці, корупціонери, адміністративно-управлінські органи.

Джерела загроз переслідують при цьому наступні цілі:

– ознайомлення з відомостями, що охороняються;

– їх модифікація в корисливих цілях;

– знищення для нанесення прямих матеріальних збитків.

**Неправомірне заволодіння конфіденційною ін**формацією можливо шляхом її розголошення джерелами відомостей, за рахунок витоку інформації через технічні засоби та через несанкціонований доступ до відомостей, що охороняються.

**Джерелами конфіденційної інформації** є:

– люди;

– їх знання;

– документи;

– публікації;

– технічні носії інформації;

– технічні засоби забезпечення виробничої та трудової діяльності;

– продукція;

– послуги і відходи виробництва.

**Основними напрямками захисту інформації** є:

– правовий;

– організаційний;

– інженерно-технічний;

– людський;

– фізичний захист інформації

як індикатори комплексного підходу до забезпечення інформаційної безпеки.

**Засобами захисту інформації** є:

– фізичні засоби;

– апаратні засоби;

– програмні засоби;

– криптографічні методи, які можуть бути реалізовані як апаратно, програмно, так і змішано-програмно-апаратними засобами.

В якості **засобів захисту** виступають всілякі заходи, шляхи, способи і дії, що забезпечують попередження протиправних дій, їх запобігання, припинення та протидію несанкціонованому доступу.

Окрім системного підходу, доцільно врахувати і положення процесного підходу до моделювання систем інформаційної безпеки. **Сутність процесного підходу до формування моделі інформаційної безпеки** полягає в тому, що захист інформації розглядається як особливий вид діяльності в організації, який здійснюється при моделюванні, проектуванні як сукупність процесів захисту інформації:

– наявність мети процесу, тобто бажаного результату захисту інформації, що досягається при здійсненні процесу;

– зміни предметної області, в якій реалізується процес. За суттю, реалізація процесу завжди пов'язана зі зміни системи та є цілеспрямованим переходом цієї системи з існуючого в бажаний стан;

– обмеженість необхідних ресурсів на виконання операцій і дій, що складають процес; безперервність процесу. Процес є модель функції захисту, яка здійснюється

– організацією протягом усього свого існування;

– комплексність та розмежування процесу. Комплексність процесу передбачає врахування всіх внутрішніх і зовнішніх факторів, які прямо або опосередковано впливають на розвиток процесу і результати процесу.

У той же час кожен **процес** має чітко визначені **межі предметної області**, наприклад процес аналізу загроз, процес сертифікації засобів захисту, процеси стратегічного управління безпекою тощо.

**Формалізуючи модель інформаційної безпеки** у математичному вигляді, доцільно визначити її функціональну залежність від завдань захисту інформації, суб’єктів інформаційних процесів, загроз безпеки, рівнів вразливості інформаційних систем, джерел інформації, джерел загроз, способів захисту, напрямів захисту, цілей захисту:

– стан системи інформаційної безпеки;

– сукупність суб’єктів системи інформаційної безпеки;

– сукупність завдань системи інформаційної безпеки;

– сукупність загроз системи інформаційної безпеки;

– рівні вразливості системи інформаційної безпеки;

– сукупність джерел інформації системи інформаційної безпеки;

– сукупність джерел загроз системи інформаційної безпеки;

– сукупність способів захисту інформаційних ресурсів;

– сукупність напрямів захисту інформаційних ресурсів;

– сукупність цілей захисту інформаційних ресурсів.

**Інформаційна безпека** є функцією з множини області значень складових системи інформаційної безпеки. Постійне зростання потреби в інформації обумовлює необхідність нарощування та ефективного використання інформаційних ресурсів, формування інформаційного потенціалу організаційних утворень, що виступає основною передумовою зміни стану системи інформаційної безпеки, перебудови або вдосконаленні її моделі.

## 10.2. Модель порушника

**Модель порушника** – це всебічна структурована характеристика порушника, яка використовується сумісно з моделлю загроз для розробки політики безпеки інформації. В Україні прийнята така структура моделі порушника:

Категорія осіб, до якої може належати порушник:

– внутрішні порушники;
– користувачі;
– інженерний склад;
– співробітники відділів, що супроводжують ПЗ;
– технічний персонал, що обслуговує будинок;
– співробітники служби безпеки;
– керівники;
– зовнішні порушники.

Мета порушника:

– отримання необхідної інформації;
– отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами;
– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Повноваження порушника в ІКС:

– запуск фіксованого набору задач (програм);
– створення і запуск власних програмних засобів;
– керування функціонуванням і внесення змін у конфігурацію системи;
– підключення чи зміна конфігурації апаратних засобів.

Технічна оснащеність порушника:

– апаратні засоби;
– програмні засоби;
– спеціальні засоби.

Кваліфікація порушника: для аналізу загроз завжди приймається висока кваліфікація.

## 10.3. Модель загроз

**Загроза** (англ. – Threat) – це будь-які обставини чи події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитку ІКС. Тобто, загроза – це будь-який потенційно можливий несприятливий вплив. **Несприятливий вплив** – це вплив, що призводить до зниження цінності інформаційних ресурсів.

**Атака (**англ. – Attack) – це навмисна спроба реалізації загрози. Якщо атака є успішною (здійснено подолання засобів захисту), це називають **проникненням** (англ. – Penetration). Наслідком успішної атаки є порушення безпеки інформації в системі, яке називають **компрометацією (**англ. – Compromise).

Слід звернути увагу на те, що при комплексному підході до захисту інформації ми повинні розглядати не лише впливи, спрямовані на інформаційні ресурси, але й будь-які впливи, що можуть нанести збитки ІКС.

Загроза часто може бути слідством наявності вразливих місць системи. Визначимо терміном «**вразливість системи»** (англ. – System vulnerability) – нездатність системи протистояти реалізації визначеної загрози чи сукупності загроз.

Розповсюдженим випадком вразливостей систем є вади захисту. **Вади захисту** (англ. – Security flaw) – сукупність причин, умов і обставин, наявність яких може призвести до порушення нормального функціонування системи або до порушення політики безпеки інформації. Здебільшого, під вадами захисту розуміють особливості побудови програмних (а іноді і апаратних) засобів захисту, через які останні за певних обставин не здатні протистояти загрозам і виконувати свої функції. Тобто, вади захисту є окремим випадком вразливостей системи.

В літературі іноді зустрічається інше трактування термінів, яке не є коректним. Наприклад, іноді замість терміну “загроза” вживають термін “атака”. Однак, враховуючи визначення наведені вище, слід розрізняти атаку, яка є дією, спробою реалізувати певну загрозу, і загрозу, яка є потенційною можливістю здійснення несприятливого впливу. Зазначимо, що атака – це здебільшого цілеспрямований вплив, як правило, умисний. Загрози можуть бути випадковими, але від цього втрати внаслідок їх реалізації не стають меншими. Тому захищати інформацію необхідно саме від загроз, а не лише від атак.

Особи, які реалізують загрози називають порушниками. **Порушник** (англ. – User violator) – фізична особа (у загальному випадку не обов’язково користувач системи), яка здійснює порушення політики безпеки системи. Треба розрізняти терміни «порушник» та «**зловмисник**». Останній термін підкреслює умисність порушення, тоді як у загальному випадку порушник може здійснювати порушення неумисно (наприклад, через необережність або недостатню обізнаність).

Широко уживаний термін “**хакер**” (англ. – hacker) є досить неоднозначним тому ми не будемо використовувати його як синонім терміну “порушник”.

**Класифікація загроз інформаційної безпеки**

Історія розвитку інформаційних систем свідчить про те, що нові вразливості систем з'являються регулярно. З такою ж регулярністю, але ж з певним запізненням вони нейтралізуються. У проміжок часу між появою нової вразливості та її нейтралізацією система є особливо вразливою і може бути скомпрометованою. Особливо небезпечним є випадок коли нова вразливість вперше виявляється потенційним порушником. Тому, такий **«послідовний»** підхід до забезпечення інформаційної безпеки **не є ефективним**.

Більш ефективним є підхід **упередженого** захисту інформації, який базується на передбаченні всіх можливих, передбачуваних та потенційних загроз та розробці **комплексної системи захисту інформації** (повне визначення буде наведено пізніше). Найбільш ефективний та економічний варіант комплексної системи захисту інформації базується на аналізі всіх можливих загроз інформації та вразливостей інформаційної системи та передбаченні дій потенційного порушника. Тому, розглянемо їх змістовніше.

Загрози інформаційної безпеки класифікуються за низькою ознак:

– за складовими інформаційної безпеки;

– за компонентами інформаційних систем, на які загрози націлені;

– за характером впливу;

– за розміщенням джерела загроз.

**Класифікація загроз інформаційної безпеки за її складовими**

Класифікація загроз інформаційної безпеки за її складовими полягає у визначенні загроз (загрози), які безпосередньо направлені на таки складові інформаційної безпеки, як **конфіденційність, доступність, цілісність**. Усі загрози, що класифікуються за іншими ознаками можуть впливати на усі складові інформаційної безпеки.

**Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які вони націлені**

Класифікація загроз інформаційної безпеки за компонентами інформаційних систем, на які загрози націлені полягає у визначенні загроз (загрози), які безпосередньо направлені на таки складові інформаційної системи, як інформація, що обробляється в обчислювальної системі, обчислювальна система, програмне забезпечення, апаратура, персонал та інші.

В якості прикладів загроз компонентам інформаційних систем, що суттєво впливають на стан захищеності інформації, можна навести такі:

- зміна архітектури системи;
- зміна складу та/або можливостей апаратних і програмних засобів;
- підключення до мережі (особливо глобальної);
- відмінності в категорії та/або кваліфікації персоналу.

**Класифікація загроз інформаційної безпеки за характером впливу**

Загрози інформаційної безпеці за характером впливу класифікують як **випадкові та навмисні** дії природного або техногенного характеру.

**Випадкові загрози**

Випадкові загрози – це загрози, які не пов'язані з умисними діями зловмисників та реалізуються у випадкові моменти часу. Випадкові загрози поділяють на загрози від аварій та стихійних лих, збоїв та відмов технічних засобів, помилок при розробці елементів інформаційної системи, алгоритмічні та програмні помилки, помилки користувачів чи обслуговуючого персоналу та інші (за статистикою – до 65% збитків у порівнянні з іншими загрозами). Реалізація цих загроз веде до найбільшої втрати інформації (за статистикою – до 80% збитків у порівнянні з іншими загрозами). Це – знищення, порушення цілісності, доступності, інколи – конфіденційності інформації.

Треба зазначити, що механізм реалізації випадкових загроз є добре вивченим та існують добре апробовані методи протидії (нейтралізації) таким загрозам. З найефективніших методів протидії випадковим загрозам є спеціальні методи управління якістю розробки та експлуатації програмно-апаратних засобів, методи резервування інформації та інші.

**Навмисні загрози**

Навмисні загрози – це цілеспрямовані дії зловмисника. Цей клас загроз динамічний, постійно оновлюється новими загрозами, як правило, недостатньо вивчений. Навмисні загрози поділяють на:

– «спеціальні впливи»;
– несанкціонований доступ до інформації;
– використання технічних каналів витоку інформації;
– несанкціоновану зміну структури;
– та інші.

Спроба реалізації будь якої навмисної загрози по відношенню до об'єкту інформаційної діяльності підпадає під дію відповідних статей Карного кодексу України.

**«Спеціальні впливи»**

«Спеціальні впливи». Загрози інформаційної безпеці від традиційних «спеціальних впливів» до цього часу залишаються актуальними. Частіше за все їх використовують для отримання інформації про систему захисту інформації або її знищення з метою подальшого проникнення до інформаційної системи.

Методами «спеціальних впливів» є:

– підслуховування;
– візуальне спостереження;
– викрадення документів або носіїв інформації;
– викрадення програм або атрибутів системи захисту інформації;
– підкуп або шантаж співробітників;
– сбір та аналіз відходів машинних носіїв інформації;
– підпалення
– та інші.

Підслуховування може здійснюватись на відстані починаючи з одиниць метрів до десятків кілометрів від об'єкту. В приміщеннях підслуховування найбільш часто здійснюється за допомогою мініатюрних магнітофонів або мікрофонів (закладок, радіозакладок, жучків та ін.). Мікрофони фіксують інформацію та здійснюють подальшу її передачу по радіо- чи іншим каналам зв'язку. Суттєвим недоліком цього методу є необхідність попереднього фізичного проникнення на об'єкт з метою розміщення там необхідного обладнання.

Існують засоби зняття інформації (підслуховування) за відбитим від віконного скла променем лазерного випромінювача (відстань – до 1км.). При цьому для підслуховування попереднє проникнення у приміщення не потрібне.

Розмови у сусідніх приміщеннях можуть контролюватись за допомогою стетоскопічних мікрофонів (можлива товщина стін – 50 – 100см.). Для прослуховування розмов у приміщення крім того може використовуватись метод високочастотного нав'язування. Цій метод базується на впливі високочастотного електромагнітного випромінювання на елементи, які здатні модулювати ці поля сигналами, що містять мовну інформацію. Такими елементами можуть бути порожнини з електропровідними поверхнями, телефонний апарат та інше.

Поза приміщеннями підслуховування проводиться за допомогою зверхчутливого мікрофону (відстань – 50 – 100м.).

Порушення інформаційної безпеки може здійснюватись методами та засобами візуального спостереження (дистанційної відеорозвідки). Ці методи використовується не часто та мають допоміжний характер. Засобами візуального спостереження є теле-, фото-, кіно- апаратура. Існують зразки мобільних (у тому числі літаючих) мікроботів візуального спостереження.

Інші методи «спеціальних впливів» характеризувати не будемо.

**Несанкціонований доступ до інформації**

Несанкціонований доступ до інформації. Серед найбільш розповсюджених загроз інформації є загроза несанкціонованого доступу до інформації (НСД). Несанкціонований доступ до інформації – це доступ до інформації, який порушує правила розмежування доступу (ПРД) з використанням штатних засобів обчислювальної техніки або автоматизованих систем.

**Правила розмежування доступу** – це сукупність положень, які регламентують права доступу осіб або процесів (суб'єктів доступу) до одиниць інформації (об'єктів доступу). Права доступу до інформаційних ресурсів визначається керівництвом щодо кожного співробітника у відповідності до його функціональних обов'язків.

Виконання правил розмежування доступу реалізується **системою розмежування доступу (СРД)**. Несанкціонований доступ до інформації можливий лише з використанням штатних засобів обчислювальної техніки або автоматизованих систем. Розрізняють наступні джерела виникнення НСД:

– відсутність або помилки СРД;
– збої чи відмова в роботі обчислювальної системи;
– помилкові дії користувачів чи обслуговуючого персоналу;
– фальсифікація повноважень;
– та інші.

**Технічні канали витоку інформації**

Технічні канали витоку інформації. Технічні канали витоку інформації являють собою небезпечне джерело загроз інформації. Технічні канали витоку інформації – це сукупність об'єкту інформаційної діяльності, технічного засобу зняття інформації та фізичного середовища, в якому розповсюджується інформаційний сигнал.

В основі процесів витоку інформації по технічним каналам є:

– перетворення фізичних величин;

– випромінювання електромагнітних коливань;

– паразитні зв'язки та наведення на дроти та елементи електронних пристроїв.

Процес обробки та передачі інформації технічними засобами супроводжується електромагнітними випромінюваннями в оточуючий простір та наведення електричних сигналів в мережах електричного живлення, лініях зв'язку, сигналізації, заземлення та інших дротах. Таки процеси отримали назву **побічних електромагнітних випромінювань та наведень (ПЕМВН)**. За допомогою спеціального обладнання таки сигнали приймаються, виділяються, підсилюються та можуть спостерігатись чи записуватися. Отримати таки сигнали можна з використанням спеціальних приймачів електромагнітного випромінювання чи приєднавшись безпосередньо до мереж електричного живлення, ліній зв'язку, сигналізації, заземлення та інших. Зняття інформації частіше за все проводиться поза периметром контрольованого доступу об'єкту інформаційної діяльності.

Наведемо таки приклади. Дальність сталого прийому з використанням дипольної антени складає 50 метрів, використання направленої антени та підсилювача може збільшити відстань прийому випромінювання збільшується до 1 кілометра. Прийом та відтворення інформації, яку випромінює неекранований електричний кабель, може здійснюватись на відстані до 300 метрів.

Зловмисник також має можливість знімати та відтворювати «наведену» інформацію безпосередньо підключаючись до мереж електричного живлення, ліній зв'язку, сигналізації, заземлення та інших дротів

Загрози інформації по технічним каналам витоку, у випадку їх реалізації, направлені на **конфіденційність** інформації.

Разом з тим високочастотний електромагнітний імпульс великої потужності може знищити інформацію на магнітних носіях на відстані десятків метрів. Пристрій, здатній генерувати такий імпульс здатний розміщуватись у звичайному дипломаті. Така загроза інформації направлена на **цілісність** інформації. Електромагнітне випромінювання високої потужності може також загрожувати **доступності** інформації, яка передається по каналах мобільного безпровідного зв'язку.

**Несанкціонована модифікація структури**

Несанкціонована модифікація структури. Цей клас загроз інформації може бути реалізованим на алгоритмічному, програмному або апаратному рівнях на будь якому етапі життєвого циклу обчислювальної системи. Несанкціонована модифікація структури апаратного або програмного засобу на етапах розробки або модернізації отримало назву «закладка».

Програмні або апаратні закладки, призначені для несанкціонованого входу до системи шляхом обходу її засобів захисту отримали назву «люки».

Закладки впроваджують з метою прямого шкідливого впливу на засіб, несанкціонованого входу до системи, дискредитації засобу конкурентом та за іншими міркуваннями.

Закладки, здійсненні на етапі розробки апаратного або програмного засобу виявити дуже важко у зв'язку складності сучасних технологій та високої кваліфікації розробників.

**Шкідливі програми**

Шкідливі програми. Це один класів загроз інформації, який реалізується шляхом розробки та використання спеціальних програм. У залежності від механізму дії шкідливі програми поділяють на декілька класів. Серед найбільш розповсюджених класів є:

– логічні бомби;

– хробаки;

– троянські коні;

– комп'ютерні віруси та інші.

**Логічні бомби** – це спеціальні програми, або їх частини, які постійно знаходяться в комп'ютерній системі і активізуються лише за наявності певних умов (наприклад, досягнення певного часу події).

**Хробаки** – це спеціальні програми, які знаходяться в комп'ютерній системі, здатні до переміщення та самовідтворення. Неконтрольоване розмноження хробаків в комп'ютерній системі, або мережі веде до перевантаження останніх, переповненню пам'яті та блокуванню системи.

**Троянські коні** – це модифіковані користувацькі програми, які разом з визначеними функціями можуть виконувати додаткові несанкціоновані шкідливі функції.

**Комп'ютерні віруси** – це невеликі спеціальні програми, здатні до самовідтворення шляхом копіювання та переміщення. За певних обставин віруси можуть бути шкідливими. Вірусам притаманні ознаки майже всіх шкідливих програм. Тому, часто, шкідливі програми називають вірусами.

**Класифікація загроз інформаційної безпеки за розміщенням їх джерела**

Розрізняють два класи загроз інформації за розміщенням їх джерела в середині інформаційної системи, або поза неї.

Найбільш небезпечною загрозою вважається **внутрішня загроза**, джерелом якої є співробітники установи – користувачі інформаційної системи. Серед користувачів є специфічна категорія – керівництво. Часто, керівники

вимагають собі підвищені привілеї в системі, а також не визнають щодо себе жодних обмежень. До того ж, адміністратори системи формально підпорядковані керівництву, а не навпаки.

Потенційні можливості легального користувача в ІКС значно більші, ніж у будь-якого зовнішнього порушника. Користувач має в системі певні повноваження. Користувач має багато інформації про систему, а іншу інформацію може порівняно легко отримати (когось спитати, підслухати, "неформально" проконсультуватись – йому це значно простіше, ніж будь-якій сторонній особі). Користувач, як правило, незадоволений обмеженнями своїх прав у системі. Користувач цікавиться інформаційними технологіями і бажає перевірити свої досягнення на практиці. Часто користувач не дуже кваліфікований, і все, що він буде робити, фактично зведеться до методу спроб і помилок.

Саме легальні користувачі є найбільшою проблемою адміністраторів, постійно створюючи реальні загрози порушення безпеки інформації. Але, з іншого боку, не користувачі створені для того, щоб заважати адміністраторам, а адміністратори – для того, щоб обслуговувати користувачів. Єдиним можливим виходом з цього становища є взаємна повага і співпраця. Але на це не варто покладатись без відповідного документування прав і обов'язків всіх категорій користувачів і адміністраторів.

Особливості поведінки користувачів (в тому числі керівників) повинні бути враховані ще на стадії проектування КСЗІ в ІКС під час розробки моделі порушника.

**Зовнішні загрози** визначаються застосуванням обчислювальних мереж. Враховуючи те, що окремі компоненти обчислювальних мереж розподілені у просторі, місце розташування зловмисника за визначенням невідомо.

**Поняття порушника інформаційної безпеки**

В подальшому будемо використовувати терміни **"порушник" і "зловмисник"** у тих значеннях, які було наведено вище.

Нагадаємо, що **порушниками** називають особи, які реалізують загрози. **Порушник** – фізична особа (у загальному випадку не обов'язково користувач системи), яка здійснює порушення політики безпеки системи. Треба розрізняти терміни «порушник» та «**зловмисник**». Останній термін підкреслює умисність порушення, тоді як у загальному випадку порушник може здійснювати порушення неумисно (наприклад, через необережність або недостатню обізнаність).

Іноді будемо використовувати термін **"хакер"** (англ. – hacker) по відношенню до тих, хто глибоко розуміє принципи роботи обчислювальних систем, особливо ПЗ. Ці знання дозволяють їм виявляти вразливості систем. Тобто, хакери – це ті, хто знаходять вразливості і знають, як їх використати.

Погляди на застосування терміну "хакер" різняться. Деякі фахівці вважають, що справжні хакери – це ті, хто діє виключно в інтересах безпеки інформації (так звані "білі хакери", англ. – "white hats"). Про виявлені вразливості такі хакери повідомляють лише тих, хто повинен виправити помилки

ПЗ, які і спричинили наявність вразливості. Такі хакери можуть тісно співпрацювати з розробниками ПЗ і з експертами з комп'ютерної безпеки.

Існують люди, які мають кваліфікацію хакерів, але використовують свої знання і уміння або з корисливою метою, або взагалі з метою вандалізму. Згадані вище фахівці вважають, що називати хакерами таких зловмисників некоректно. Їх пропонують називати іншими термінами, як, наприклад, **"кракер"** (англ. – "cracker"), що іноді перекладають як **"зломник"**.

У масовій свідомості, саме зі словом "хакер" пов'язані всі комп'ютерні зловмисники. До речі, існує значна частина зловмисників, які не мають високої кваліфікації. Для здійснення атаки достатньо знайти необхідний інструментарій і інструкції з його використання, все це доступно в Інтернет будь-кому.

Результатом аналізу можливих загроз є **модель загроз** – абстрактний структурований опис загроз.

Нормативними документами України рекомендовано таку структуру опису загрози:

На порушення яких властивостей інформації або ІКС спрямована загроза:

– порушення конфіденційності,
– порушення цілісності,
– порушення доступності інформації,
– порушення спостереженості та керованості ІКС.

Джерела виникнення загрози:

– які суб'єкти ІКС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу (див. вище модель порушника).

Можливі способи здійснення загрози:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– 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 з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Перші два способи за принципом відносяться до фізичного доступу, останній – до логічного доступу.

## 10.4. Модель вразливостей

У комп'ютерній безпеці термін «**вразливість**» (англ. *vulnerability*, на сленгу – *дірка*) використовується для позначення нестачі в системі, використовуючи який можна навмисно порушити її цілісність і викликати неправильну роботу. Вразливість може бути результатом помилок програмування, недоліків, допущених при проектуванні системи, ненадійних

паролів, вірусів та інших шкідливих програм, скриптових та SQL-ін'єкцій. Деякі вразливості відомі тільки теоретично, інші активно використовуються і мають відомі експлойти.

Зазвичай вразливість дозволяє атакуючому «обдурити» додаток – виконати непередбачені творцем дії або змусити програму вчинити дію, на яку той не повинен мати рацію. Це робиться шляхом впровадження у програму даних або коду в такі місця, що програма сприйме їх як «свої». Деякі вразливості з'являються через недостатню перевірку даних, що вводяться користувачем, і дозволяють вставити в інтерпретований код довільні команди (SQL-ін'єкція, XSS, SiXSS). Інші вразливості виникають через складніші проблеми, такі як порушення безпеки при роботі з пам'яттю, наприклад переповнення буфера. Пошук вразливостей іноді називають *зондуванням*, наприклад коли говорять про зондування віддаленого комп'ютера – мають на увазі, пошук відкритих мережевих портів і наявність вразливостей, пов'язаних із додатками, які використовують ці порти.

Метод інформування про вразливість є одним із пунктів суперечки у спільноті комп'ютерної безпеки. Деякі фахівці відстоюють негайне повне розкриття інформації про вразливість, як тільки їх знайдено. Інші радять повідомляти про вразливості лише тим користувачам, які наражаються на найбільший ризик, а повну інформацію публікувати лише після затримки або не публікувати зовсім. Такі затримки можуть дозволити тим, хто був повідомлений, виправити помилку за допомогою розробки та застосування патчів, але також можуть збільшувати ризик для тих, хто не посвячений у деталі.

Існують інструментальні засоби, які можуть допомогти у виявленні вразливостей у системі. Хоча ці інструменти можуть забезпечити аудитору хороший огляд можливих вразливостей, які у системі, вони можуть замінити участь людини у оцінці.

Для забезпечення захищеності та цілісності системи необхідно постійно стежити за нею: встановлювати оновлення, використовувати інструменти, які допомагають протидіяти можливим атакам. Вразливості виявлялися у всіх основних операційних системах, включаючи Microsoft Windows, Mac OS, різні варіанти UNIX (у тому числі GNU/Linux) та OpenVMS. Так як нові вразливості знаходять безперервно, єдиний шлях зменшити ймовірність їх використання проти системи – постійна пильність та використання оновлених версій програмного забезпечення.

**Виявлення вразливостей**

Для виявлення вразливостей проводяться пентести, в ході яких зазвичай визначається перелік систем, що перевіряються, і конкретна мета, а потім аналізується доступна інформація і підбираються засоби для досягнення цієї мети. Метою тесту проникнення може бути " *білий ящик* " (про який попередня і системна інформація надається тестувальнику заздалегідь) чи " *чорний ящик* " (про який надається лише основна інформація – якщо така є – крім назви компанії).

**Система управління інформаційною безпекою**

Набір політик, що стосуються системи менеджменту інформаційної безпеки (ISMS), був розроблений для управління контрзаходами, щоб стратегія безпеки була реалізована відповідно до правил і положень, що застосовуються до цієї організації.

**Моделі вразливості та факторів ризику**

Ресурс (фізичний чи логічний) може мати одну або кілька вразливостей, якими може скористатися зловмисник. Результат може потенційно поставити під загрозу конфіденційність, цілісність чи доступність ресурсів, що належать організації та/або іншим залученим сторонам (клієнтам, постачальникам).

**Приклади вразливостей**

Поширені типи вразливостей включають:

– Порушення безпеки доступу до пам'яті, такі як:
  - Переповнення буфера. **Переповнення буфера** (англ. *Buffer Overflow*) – явище, що виникає, коли комп'ютерна програма записує дані поза виділеного у пам'яті буфера. Переповнення буфера зазвичай виникає через неправильну роботу з даними, отриманими ззовні, і пам'яттю, за відсутності жорсткого захисту з боку підсистеми програмування (компілятор або інтерпретатор) та операційної системи. В результаті переповнення можуть бути зіпсовані дані, розташовані за буфером (або перед ним). Переповнення буфера є одним з найбільш популярних способів злому комп'ютерних систем, оскільки більшість мов високого рівня використовує технологію стекового кадру – розміщення даних у стеку процесу, змішуючи дані програми з керуючими даними (у тому числі адреси початку стекового кадру та адреси повернення з виконуваної функції). Переповнення буфера може викликати аварійне завершення або зависання програми, що веде до *відмови обслуговування* (Denial of Service, DoS). Окремі види переповнень, наприклад, переповнення в стековому кадрі, дозволяють зловмиснику завантажити і виконати довільний машинний код від імені програми та з правами облікового запису, від якого вона виконується.
  - Висячі покажчики. **Висячий покажчик** або **висяче посилання** (англ. *Dangling pointer, wild pointer, dangling reference*) – покажчик, що не вказує на допустимий об'єкт відповідного типу. Це особливий випадок порушення безпеки пам'яті. Висячі покажчики виникають тоді, коли об'єкт видалений або переміщений без зміни значення покажчика на нульове, так що покажчик все ще вказує область пам'яті, де раніше зберігалися дані. Оскільки система може перерозподілити раніше звільнену пам'ять (у тому числі в інший процес), то обірваний покажчик може призвести до непередбачуваної поведінки програми. Якщо програма записує дані в пам'ять, використовуючи такий покажчик, дані можуть непомітно руйнуватися, що призводить до тонких помилок, які дуже важко

знайти. Цей вид помилок дуже небезпечний, і поряд з витоком пам'яті трапляється досить часто. Ряд мов знижують ймовірність появи висячих покажчиків, зокрема, використовуючи автоматичне складання сміття або іншими методами, підвищуючи безпеку доступу до пам'яті.

- Помилки перевірки даних, такі як:
  - Помилки форматуючого рядка.
  - Неправильна підтримка інтерпретації метасимволів командної оболонки.
  - SQL-ін'єкція. **Впровадження SQL-коду** (англ. *SQL injection/SQLi*) – один із поширених способів злому сайтів і програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL -коду. Впровадження SQL, залежно від типу використовуваної СУБД та умов впровадження, може дати можливість атакуючому виконати довільний запит до бази даних (*наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані*), отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері, що атакується. Атака типу застосування SQL може бути можлива через некоректну обробку вхідних даних, що використовуються в SQL-запитах. Розробник прикладних програм, що працюють з базами даних, повинен знати про такі вразливості та вживати заходів протидії впровадженню SQL.
  - Ін'єкція коду.
  - Ін'єкція E-mail. **E-mail-ін'єкція** – це техніка атаки, яка використовується для експлуатації поштових серверів і поштових додатків, що конструюють IMAP/SMTP вирази з введеного користувачем, який не перевіряється належним чином. Залежно від типу операторів, які використовуються зловмисником, виділяють два типи ін'єкцій: **IMAP ін'єкція** та ін'єкція **SMTP**. IMAP/SMTP ін'єкції дозволяють отримати доступ до поштового сервера, якого раніше доступу не було. У деяких випадках ці внутрішні системи не мають такого самого рівня безпеки, що й решта інфраструктури. Таким чином, зловмисники можуть виявити, що поштовий сервер дає найкращі результати з точки зору експлуатації. Цей метод дозволяє уникнути можливих обмежень, які можуть існувати на рівні додатків (CAPTCHA, максимальна кількість звернень тощо).
  - Обхід каталогів.
  - Міжсайтовий скриптинг у веб-додатках. **XSS** (англ. *Cross-Site Scripting* – «міжсайтовий скриптинг ») – тип атаки на веб-системи, що полягає у впровадженні у сторінку шкідливого коду, що видається веб-системою (який буде виконаний на комп'ютері користувача при відкритті ним цієї сторінки) і взаємодії цього коду з веб-сервер зловмисника. Є різновидом атаки «Впровадження коду». Специфіка подібних атак полягає в тому, що шкідливий код

може використовувати авторизацію користувача у веб-системі для отримання до неї розширеного доступу або отримання авторизаційних даних користувача. Шкідливий код може бути вставлений у сторінку як через вразливість у веб-сервері, так і через вразливість на комп'ютері. Для терміну використовують скорочення XSS, щоб не було плутанини з каскадними таблицями стилів, що використовують скорочення CSS. XSS знаходиться на третьому місці в рейтингу ключових ризиків Web-додатків, згідно з OWASP 2021. Довгий час програмісти не приділяли їм належної уваги, вважаючи їх безпечними. Однак це думка помилкова: на сторінці або в HTTP-Cookie можуть бути дуже вразливі дані (наприклад, ідентифікатор сесії адміністратора або номери платіжних документів), а там, де немає захисту від CSRF, атакуючий може виконати будь-які дії, доступні користувачеві. Міжсайтовий скриптинг може бути використаний для проведення DoS-атаки.

- Міжсайтовий скриптинг за наявності SQL-ін'єкції. **SiXSS** (англ. *Sql Injection Cross Site Scripting* – "Міжсайтовий скриптинг за наявності SQL-ін'єкції") - тип атаки на вразливі інтерактивні інформаційні системи в Інтернеті; впровадження виконуваних на клієнтському комп'ютері шкідливих скриптів у сторінку, що видається системою, за допомогою впровадження коду в SQL-ін'єкцію. Як правило, дана вразливість виникає на стороні клієнта за наявності виведення принтабельних полів за допомогою виконання SQL-ін'єкції.

– Стан гонки, (англ. *race condition*), також **конкуренція** – помилка проектування багатопоточної системи або програми, при якій робота системи або програми залежить від того, в якому порядку виконуються частини коду. Свою назву помилка отримала від схожої помилки проектування електронних схем. Термін *стан гонки* відноситься до інженерного жаргону і виник внаслідок неакуратного дослівного перекладу англійського еквівалента. У суворішому академічному середовищі прийнято використовувати термін **невизначеність паралелізму**. Стан гонки – "плаваюча" помилка (гейзенбаг), що виявляється у випадкові моменти часу і "зникла" при спробі її локалізувати. До них відносяться вразливості такі як:

- Помилки часу-перевірки-до-часу-використання.
- Перегони символьних посилань.

– Помилки плутанини привілеїв, такі як:

- Підробка міжсайтових запитів у веб-додатках. **CSRF** (англ. *cross-site request forgery* – «міжсайтова підробка запиту», також відома як XSRF) – вид атак на відвідувачів веб-сайтів, що використовує недоліки протоколу HTTP. Якщо жертва заходить на сайт, створений зловмисником, від її особи таємно надсилається запит на інший сервер (наприклад, на сервер платіжної системи), який здійснює якусь шкідливу операцію (наприклад, переказ грошей на рахунок зловмисника). Для здійснення даної атаки жертва повинна бути автентифікована на сервері, на який надсилається запит, і цей запит

не повинен вимагати будь-якого підтвердження з боку користувача, яка не може бути проігнорована або підроблена атакуючим скриптом. Даний тип атак, всупереч поширеній помилці, з'явився досить давно: перші теоретичні міркування з'явилися в 1988, а перші вразливості були виявлені в 2000. А сам термін запровадив Пітер Уоткінс у 2001 році. Основне застосування CSRF – вимушення виконання будь-яких дій на вразливому сайті від імені жертви (зміна пароля, секретного питання відновлення пароля, пошти, додавання адміністратора тощо. буд.). Також за допомогою CSRF можлива експлуатація відбитих XSS, виявлених на іншому сервері.

– Ескалація привілеїв, **Підвищення привілеїв** – це використання комп'ютерного бага, вразливостей, помилок у конфігурації операційної системи або програмного забезпечення з метою підвищення рівня доступу до обчислювальних ресурсів, які зазвичай захищені від користувача. У результаті, додаток, що має більші повноваження, ніж передбачалося системним адміністратором, може здійснювати неавторизовані дії. "Підвищенням привілеїв" називають ситуацію, коли користувач комп'ютерної системи якимось чином підвищує свої повноваження в цій системі (іншими словами: отримав можливість робити те, чого раніше робити не міг). Така помилка в програмі, як використання коду через переповнення буфера, завжди небажана. Однак, серйозною цю помилку можна вважати лише в тому випадку, якщо вона підвищує привілеї користувача. Зокрема, якщо використання коду відбувається на локальній машині, це привілей не підвищує: користувач і без цього може виконувати файли, що виконуються. Якщо ж вдається впровадити код через мережу, то це вже підвищення привілеїв: у користувача з'явилася можливість виконувати машинний код. До цього типу відносяться вразливості такі як:

- Шатерна атака. **"Підривна атака"** (англ. *shatter attack*) – програмна технологія, яка використовується хакерами для обходу обмежень безпеки між процесами одного сеансу в операційній системі Microsoft Windows. Вона спирається на брак архітектури системи передачі повідомлень і дозволяє одному додатку впровадити довільний код в будь-який інший додаток або службу, що працюють у тому самому сеансі. В результаті може статися несанкціоноване підвищення привілеїв.

– Вразливість нульового дня. **0-day** (англ. *zero day*) – термін, що позначає неусунені вразливості, а також шкідливі програми, проти яких ще не розроблені захисні механізми. Сам термін означає, що у розробників було 0 днів на виправлення дефекту: вразливість або атака стає публічно відома до моменту випуску виробником ПЗ виправлень помилки (тобто потенційно вразливість може експлуатуватися на копіях, що працюють, програми без можливості захиститися від неї).

– Недекларовані можливості. У контексті інформаційної безпеки в центрі уваги виявляються функціональні можливості програмного забезпечення, використання яких може порушити його правильну роботу, а також цілісність, доступність або конфіденційність інформації. Вітчизняні стандарти

інформаційної безпеки для таких недокументованих можливостей запроваджують спеціальне поняття – **недекларовані можливості** (скор. **НДМ**), що застосовується, зокрема, під час сертифікації програмного забезпечення.

**Аналіз вразливостей**

Під аналізом вразливостей розуміються процеси, спрямовані на пошук будь-яких загроз, вразливих точок та ризиків потенційного несанкціонованого проникнення зловмисників у ІС (інформаційну систему).

Вразливість – слабкий компонент ІС будь-якої організації. Загроза – можливість негативного впливу з боку зловмисників, що може спричинити компрометацію комерційної та іншої конфіденційної інформації. Третя особа у такому аналізі – зловмисник, який використовує вразливість для реалізації загроз.

Якщо присутні вразливості, це негативно позначається на роботі всього підприємства, оскільки воно стає менш захищеним перед несумлінними конкурентами, це спрощує роботу зловмисників із заподіяння шкоди та дозволяє третім особам отримати доступ до конфіденційних даних.

Джерело загрози може бути як випадковим, так і навмисним. Третій варіант – техногенні та природні фактори, які ніколи не варто виключати.

Кожна загроза має свій список вразливостей, за допомогою яких зловмисник може реалізувати свої плани.

**Аудит інформаційної безпеки**

**Аналіз вразливостей у галузі інформаційної безпеки (ІБ)**

Ефективна ІБ забезпечує як захист від крадіжки будь-яких даних із мережі підприємства, а й фінансову захист бізнесу загалом. Підприємства, які хочуть відрізнятися якісною ІБ, постійно працюють над запобіганням:

– витоків будь-яких корпоративних даних;
– віддаленого редагування захищеної інформації;
– зміни рівня захисту від загроз, які можуть спровокувати втрату довіри інвесторів, постачальників, контрагентів тощо.

Загрози можуть мати кілька джерел, тому дуже важливо своєчасно їх класифікувати та створити схему їхнього аналізу. Це дозволить отримати найбільше охоплення потенційних вразливостей у бізнес-процесах підприємства.

В ІБ вкрай важливо дотримуватися чотирьох принципів:

– конфіденційність;
– цілісність;
– доступність;
– достовірність.

**Різновиди аналізованих загроз**

Щоб провести якісний аналіз вразливостей інформаційної структури, необхідно розрізняти види загроз, які можуть виникнути у системі конкретної організації. Такі небезпеки поділяються на окремі класи.

1 клас. Потенційне джерело загрози, яке може бути:

- безпосередньо в інформаційній системі (ІС);
- в межах видимості ІС (наприклад, пристрої для несанкціонованого звукозапису);
- поза зоною видимості ІС (перехоплення даних у процесі їх відправлення кудись).

2 клас. Вплив на ІС, що може нести:

- активну загрозу (троян, вірус);
- пасивну загрозу (копіювання конфіденційної інформації зловмисником).

3 клас. Метод забезпечення доступу, який може бути реалізований:

- безпосередньо (крадіжка паролів);
- за допомогою нестандартних каналів зв'язку (наприклад, вразливості операційної системи).

Головні цілі атаки на ІТ-інфраструктуру компанії:

- отримання контролю над цінними ресурсами та даними;
- організація несанкціонованого доступу до корпоративної мережі;
- обмеження діяльності підприємства у певній галузі.

Другий метод найчастіше реалізується на замовлення недобросовісних компаній-конкурентів чи політичними діячами.

Що конкретно може загрожувати інформаційній безпеці будь-якого підприємства:

- шкідливе програмне забезпечення;
- шахраї-хакери;
- інсайдери-працівники, які діють зі злими намірами або з необережності;
- природні явища.

Реалізувати загрозу можна кількома способами. Наприклад, організувати перехоплення даних, залишити програмну чи апаратну «закладку» або порушити роботу локальних бездротових корпоративних мереж, організувати доступ до інфраструктури компанії для інсайдерів.

**Оцінка ймовірності загроз**

Для оцінки ймовірності настання загрози професіоналами застосовується якісна шкала, що складається із трьох рівнів. Розглянемо їх докладніше.

**Рівень 1 – Н («низька ймовірність»)**

Відрізняється мінімальною ймовірністю появи. Така загроза не має жодних передумов (минулих інцидентів, мотивів) для того, щоб вона була реалізована. Загрози рівня Н, як правило, виникають не частіше ніж 1 раз на 5 – 10 років.

**Рівень 2 – С («середня ймовірність»)**

Така загроза ймовірність виникнення трохи вища, ніж попередня, тому що в минулому, приміром, вже були подібні інциденти або відомо, що атакуюча

сторона має плани щодо реалізації такої загрози. Загрози з рівнем З призводять до реальних інцидентів приблизно на рік.

**Рівень 3 – В («висока ймовірність»)**

Загроза має найвищі шанси на реалізацію. На підтвердження цього – статистична інформація, наявність подібних інцидентів у минулому, серйозна мотивація зловмисників. Ймовірна частота виникнення загроз рівня В – раз на тиждень чи частіше.

**Методики аналізу вразливостей**

Існує кілька способів, за допомогою яких можна провести аналіз вразливостей системи. Один із них заснований на ймовірнісній методиці, і при його застосуванні потрібно спиратися на такі фактори:

– потенціал зловмисника (виявляється шляхом оцінок експертів);
– джерело загрози (де можлива атака – в зоні видимості або за її межами);
– метод впливу (мережевий, апаратний чи соціальний);
– об'єкт загрози (корпоративні дані, засоби для шифрування, передачі, роботи з ними чи співробітники компанії).

У процесі аналізу вразливостей в інформаційній системі дуже важливо враховувати можливі місця дислокації. Щоб це реалізувати, потрібно оперативно виявити та усунути помилки в операційній системі та програмному забезпеченні, а пізніше систематично встановлювати всі патчі безпеки від розробників.

Аналіз вразливостей, які пов'язані з неправильним настроюванням захисних засобів, повинен проводитись регулярно. Ідеальне рішення – налаштувати безперервний моніторинг ІС щодо виникнення вразливостей. Окремо від вищеописаного аналізу обов'язково необхідно проводити певні заходи з робочим персоналом компанії: видавати права доступу до даних та ресурсів, права на встановлення спеціалізованого програмного забезпечення, а також права на копіювання інформації та застосування зовнішніх носіїв даних.