## Урок № 5

## Тема. Об’єкти захисту. Види заходів протидії загрозам безпеки. Основні принципи побудови системи безпеки інформації в автоматизованій системі.

**Мета:**

- ✓ ***навчальна:*** ознайомитися з різними видами заходів безпеки інформації, визначити їх переваги і недоліки, визначити об’єкти захисту, принципи побудови системи інформаційної безпеки;

Досвід показує, що забезпечення безпеки інформації не може бути одноразовим актом. Це неперервний процес, який полягає в комплексному використанні методів, способів захисту. Найбільший ефект досягається тоді, коли всі використовувані засоби, методи і заходи поєднуються в єдиний цілісний механізм – *систему захисту інформації* (СЗІ).

### Вивчення нового матеріалу

В основі комплексу заходів щодо інформаційної безпеки повинна бути стратегія захисту інформації. У ній визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи захисту. Найважливішою особливістю загальної стратегії інформаційного захисту є дослідження системи безпеки. Можна виділити **два основних напрямки**:

• аналіз засобів захисту;

• визначення факту вторгнення.

На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації, а далі – політика безпеки інформації

Розробку ***концепції захисту*** рекомендується проводити **в три етапи**:

І етап – визначення цінності об’єкта захисту інформації.

ІІ етап – аналіз потенційних дій зловмисників

ІІІ етап – оцінка надійності встановлених засобів захисту інформації на об’єкті.

На **першому етапі** повинна бути чітко визначена цільова установка захисту, тобто які реальні цінності, виробничі процеси, програми, масиви даних необхідно захищати. На цьому етапі доцільною диференціювати за значимістю окремі об'єкти, що вимагають захисту, та, у відповідності до цього, встановлення ступенів захисту об’єктів і елементів технічного і програмного забезпечення ІАС (файлів, програм, пакетів дисків, ПЕОМ в цілому).

Об’єктом спільного використання є пам’ять, пристрої введення-виведення (наприклад, диски, принтери), програми, дані.

На **другому етапі** повинен бути проведений аналіз злочинних дій, що потенційно можуть бути зроблені стосовно об'єкта, що захищається, визначення усіх можливих загроз та каналів витоку інформації. Важливо визначити ступінь реальної небезпеки таких найбільш широко розповсюджених злочинів, як економічне шпигунство, саботаж, крадіжки зі зломом. Потім потрібно проаналізувати найбільш ймовірні дії зловмисників стосовно основних об'єктів, що потребують захисту.

Головною метою **третього етапу** є аналіз обставин, у тому числі місцевих специфічних умов, виробничих процесів, уже встановлених технічних засобів захисту. Визначаються вимоги до системи захисту, здійснюється вибір заходів, методів і засобів захисту інформації та їх впровадження і організація використання.

У загальному випадку існують **чотири стратегії захисту**.

1. *Нікого не впускати*. Це повна ізоляція. Вона забезпечує найкращий захист, але перешкоджає використанню інформації або послуг від інших, і передачі їх іншим користувачам. Це непрактично для всіх.

2. *Не впускати порушників*. Програми всередині цього захисту можуть бути легковірними. Це дозволяє зробити електронні цифрові підписи програм і міжмережеві екрани (МЕ).

3. *Пустити порушників, але перешкодити їм в заподіянні шкоди*. Традиційним способом захисту служить динамічне ПЗ типу sandboxing, що створює в комп'ютері захищений простір (sandbox), в якому може виконуватися підозрілий код, і в типовому випадку використовує контроль доступу до ресурсів, щоб визначити порушення.

4. *Захопити порушників і переслідувати їх*. Це роблять аудит і силові структури

### *Види заходів протидії загрозам безпеки*

Всі заходи протидії комп'ютерним злочинам, що безпосередньо забезпечують безпеку інформації, можна підрозділити на:

- правові;
- організаційно-адміністративні;
- інженерно-технічні.

До *правових* заходів варто віднести розробку норм, що встановлюють відповідальність за комп'ютерні злочини, захист авторських прав програмістів, удосконалювання карного і цивільного законодавства, а також судочинства.

До *організаційно-адміністративних* заходів відносяться: охорона комп'ютерних систем, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною, наявність плану відновлення працездатності центру після виходу його з ладу, обслуговування обчислювального центру сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення роботи центру, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво), покладання відповідальності на осіб, що повинні забезпечити безпеку центру, вибір місця розташування центру і т.п.

До *інженерно-технічних заходів* можна віднести:

1) захист від несанкціонованого доступу до комп'ютерної системи,
2) резервування важливих комп'ютерних систем,
3) забезпечення захисту від розкрадань і диверсій,
4) резервне електроживлення, розробку і реалізацію спеціальних програмних і апаратних комплексів безпеки тощо.

*Фізичні засоби* містять у собі різні інженерні засоби, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту, що захищають персонал (особисті засоби безпеки), матеріальні засоби і фінанси, інформацію від протиправних дій.

До *апаратних засобів* відносяться прилади, пристрої, пристосування та інші технічні рішення, які використовуються в інтересах забезпечення безпеки. У практиці діяльності будь-якої організації знаходить широке застосування різна апаратура: від телефонного апарату до розроблених автоматизованих інформаційних систем, що забезпечують її виробничу діяльність. Основна задача апаратних засобів - стійка безпека комерційної діяльності.

*Програмні засоби* - це спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і засобах обробки даних.

*Криптографічні засоби* - ця спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по мережах зв'язку, збереженої та обробленої на комп'ютерах з використанням методів шифрування.

Всі заходи являють собою складну систему захисту, визначаються та проводяться в тісному взаємозв'язку на всіх етапах розробки, створення та функціонування ІАС.

### *Основні принципи побудови системи безпеки інформації*

Загальновідомо, що відділам безпеки, які займаються захистом інформації, протистоять різні організації і зловмисники, як правило, оснащені апаратними засобами доступу до інформації. Виходячи з цього, основу захисту інформації повинні складати принципи, аналогічні принципам отримання інформації, а саме:

- *безперервність* захисту інформації. Характеризується постійною готовністю системи захисту до відбиття загроз інформаційній безпеці в будь-який час;
- *активність*, яка передбачає прогнозування дій зловмисника, розробку і реалізацію випереджаючих захисних заходів;
- *скритність*, що виключає ознайомлення сторонніх осіб із засобами і технологією захисту інформації;
- *цілеспрямованість*, яка передбачає зосередження зусиль щодо запобігання загроз найбільш цінної інформації
- *комплексне використання* різних способів і засобів захисту інформації, що дозволяє компенсувати недоліки одних перевагами інших.

При **побудові системи захисту** інформації потрібно враховувати також наступні принципи:

- мінімізація додаткових завдань і вимог до співробітників організації, викликаних заходами щодо захисту інформації;

- надійність в роботі технічних засобів системи, що виключає як не реагування на погрози (пропуски загроз) інформаційної безпеки, так і помилкові реакції при їх відсутності;

- обмежений і контрольований доступ до елементів системи забезпечення інформаційної безпеки;

- безперервність роботи системи в будь-яких умовах функціонування об’єкта захисту, в тому числі, наприклад, короткочасному відключенні електроенергії;

- адаптованість (пристосовність) системи до змін навколишнього середовища.

Система захисту інформації повинна задовольняти такі **умови**:

- охоплювати весь технологічний комплекс інформаційної діяльності;
- бути різноманітною за використовуваними засобами, багаторівневою з ієрархічною послідовністю доступу;
- бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;
- бути нестандартною, різноманітною. Вибираючи засоби захисту не можна розраховувати на непоінформованість зловмисників щодо її можливостей;
- бути простою для технічного обслуговування і зручною для експлуатації користувачами;
- бути надійною. Будь-які несправності технічних засобів є причиною появи неконтрольованих каналів витоку інформації;
- бути комплексною, мати цілісність, що означає, що жодна її частина не може бути вилучена без втрат для всієї системи.

До системи безпеки інформації висуваються також певні **вимоги**:

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

## Формування практичних умінь і навичок

**Увага!** ***Під час роботи з комп'ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.*** (Інструктаж з правил техніки безпеки)

**Завдання 1.** Виконайте інтерактивну вправу "Організаційні принципи" https://learningapps.org/3944154

**Завдання 2.** Створіть текстовий документ, що містить відомості про систему інформаційної безпеки. Подайте знайдені відомості в текстовому документі у зручному вигляді (таблиці, схеми тощо). Розмісіть роботу на Google-диску, наддайте доступ, для перегляду і редагування учителю і 2 однокласникам. Перегляньте проектну роботу своїх друзів

## Домашнє завдання

1) Опрацювати **конспект**