Тема: Об'єкти захисту. Види заходів протидії загрозам безпеки. Переваги та недоліки різних видів заходів захисту. Основні принципи побудови системи безпеки інформації вм автоатизованій системі.

Інформаційна безпека — захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятний збиток суб'єктам інформаційних відносин.

У якості стандартної **моделі безпеки** використовується модель з трьох категорій:

- **конфіденційність** (англ. confidentiality) — стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на неї право;
- **цілісність** (англ. integrity) — уникнення несанкціонованої модифікації інформації;
- **доступність** (англ. availability) — уникнення тимчасового або постійного приховування інформації від користувачів, які отримали права доступу.

Виділяють і інші **не завжди обов'язкові** категорії **моделі безпеки**:

- **аппеліруемость** (англ. non-repudiation) — здатність засвідчувати дію чи подію так, щоб ці події або дії не могли бути пізніше відхилені;
- **підзвітність** (англ. Accountability) — забезпечення ідентифікації суб'єкта доступу та реєстрації його дій;
- **достовірність** (англ. reliability) — властивість відповідності передбаченій поведінці чи результату;
- **автентичність або справжність** (англ. authenticity) — властивість, що гарантує, що суб'єкт або ресурс ідентичні заявленим..

Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова **Системи забезпечення інформаційної безпеки** даного об'єкту. Для побудови та ефективної експлуатації системи забезпечення інформаційної безпеки необхідно:

- виявити вимоги захисту інформації, специфічні для даного об'єкта захисту;
- врахувати вимоги національного та міжнародного Законодавства;
- використовувати напрацьовані практики (стандарти, методології) побудови подібних системи забезпечення інформаційної безпеки;
- визначити підрозділи, відповідальні за реалізацію та підтримку системи забезпечення інформаційної безпеки;
- розподілити між підрозділами області відповідальності у здійсненні вимог системи забезпечення інформаційної безпеки;
  на базі управління ризиками інформаційної безпеки визначити загальні

положення, технічні та організаційні вимоги, що становлять Політику інформаційної безпеки об'єкта захисту;
- реалізувати вимоги Політики інформаційної безпеки, впровадивши відповідні програмно-технічні засоби і способи захисту інформації;
- реалізувати Систему менеджменту (управління) інформаційної безпеки (СМІБ);
- використовуючи СМІБ організувати регулярний контроль ефективності системи забезпечення інформаційної безпеки і при необхідності перегляд і коригування системи забезпечення інформаційної безпеки і СМІБ.

Організаційно-технічні і режимні заходи і методи.

Для опису технології захисту інформації конкретної інформаційної системи зазвичай будується так звана **Політика інформаційної безпеки** або Політика безпеки розглянутої інформаційної системи.

Політика безпеки (інформації в організації) (англ. Organizational security policy) - сукупність документованих правил, процедур, практичних прийомів або керівних принципів у галузі безпеки інформації, якими керується організація у своїй діяльності.

Політика безпеки інформаційно-телекомунікаційних технологій (англ. ICT security policy) - правила, директиви,практика, що склалася, які визначають, як в межах організації та її інформаційно-телекомунікаційних технологій управляти, захищати і розподіляти активи, в тому числі критичну інформацію.

Для побудови Політики інформаційної безпеки рекомендується окремо розглядати такі напрями захисту інформаційної системи:

- Захист об'єктів інформаційної системи;
- Захист процесів, процедур і програм обробки інформації;
- Захист каналів зв'язку (акустичні, інфрачервоні, провідні оптичні, радіоканали та ін.);
- Придушення побічних електромагнітних випромінювань і наведень;
- Управління системою захисту.

При цьому по кожному з перерахованих вище напрямків Політика інформаційної безпеки повинна описувати наступні етапи створення засобів захисту інформації:

- Визначення інформаційних і технічних ресурсів, що підлягають захисту;
- Виявлення повної безлічі потенційно можливих загроз і каналів витоку інформації;
  Проведення оцінки вразливості і ризиків інформації за наявної безлічі загроз і каналів витоку;

- Визначення вимог до системи захисту;
- Здійснення вибору засобів захисту інформації та їх характеристик;
- Впровадження та організація використання обраних заходів, способів та засобів захисту;
- Здійснення контролю цілісності і керування системою захисту.

Політика інформаційної безпеки оформляється у вигляді задокументованих вимог на інформаційну систему. Документи зазвичай поділяють за рівнями опису (деталізації) процесу захисту.

Програмно-технічні засоби і способи забезпечення інформаційної безпеки.

Класифікація засобів захисту інформації.

- Засоби захисту від несанкціонованого доступу (НСД):
  - Засоби авторизації;
  - Мандатне управління доступом;
  - Виборче управління доступом;
  - Управління доступом на основі ролей;
  - Журналювання (так само називається Аудит).
- **Системи аналізу та моделювання інформаційних потоків** (CASE-системи).
- **Системи моніторингу мереж:**
  - Системи виявлення й запобігання вторгнень (IDS / IPS).
  - Системи запобігання витоків конфіденційної інформації (DLP-системи).
- Аналізатори протоколів.
- Антивірусні засоби.
- Міжмережеві екрани.
- **Криптографічні засоби:**
  - Шифрування;
  - Цифровий підпис.
- **Системи резервування**
  - Резервне копіювання
  - Відмовостійкий кластер
  - Резервний Центр Обробки Даних (ЦОД) для катастрофостійкої ІС
- **Системи безперебійного живлення:**
  - Джерела безперебійного живлення;
  - Резервні лінії електроживлення;
  - Генератори електроживлення.
- **Системи аутентифікації на основі:**
  - Пароля;

    - Ключа доступу (фізичного або електронного);
    - Сертифікату;
    - Біометричних даних.
- Засоби запобігання злому корпусів і крадіжок устаткування.
- Засоби контролю та управління доступом в приміщення.
- Інструментальні засоби аналізу систем захисту