<u>Лекція №1 (НЕ 1.1, 2 год.).</u> Основні поняття та визначення захисту інформації.

План лекції:

1. Інформація як об’єкт захисту. Поняття ІзОД.
2. Властивості інформації, що підлягають захисту.
3. Класифікація загроз інформації.

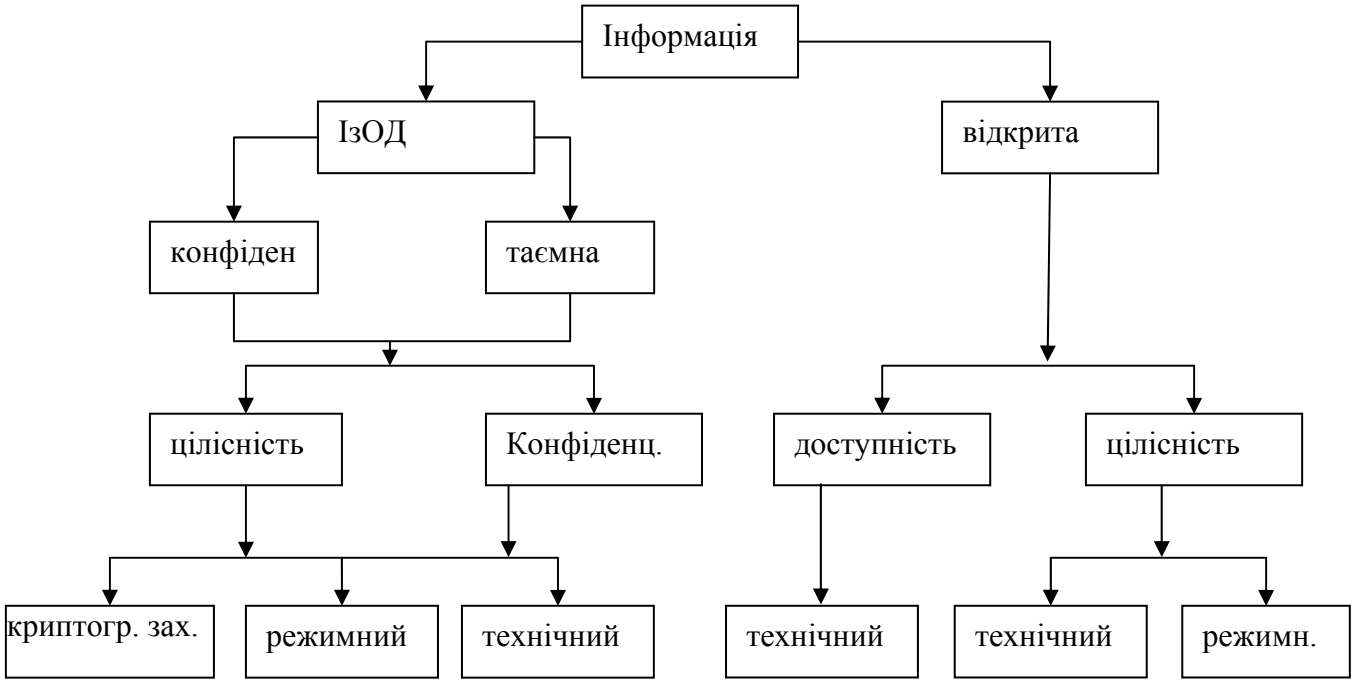
Зміст лекції:

1. Інформація як об’єкт захисту. Поняття про ІзОД.

Захист інформації це діяльність спрямована забезпечення

- конфіденційності;
- цілісності;
- доступності інформації.

Об’єкт захисту це важлива для держави, суспільства та особи інформація.



Інформація з обмеженим доступом (ІзОД) - це така інформація права доступу до якої обмежено встановленими нормами і правилами. До ІзОД відноситься конфіденційна і таємна інформація.

Конфіденційна інформація - це ІзОД, якою володіють, користуються чи розпоряджаються окремі фізичні або юридичні особи чи держава, і порядок доступу до якої встановлюються ними.

Таємна інформація – це ІзОД, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

Типи інформації вУкраїні:

1. Для службового користування (ДСК);
2. Таємна інформація;
3. Цілком таємна інформація;
4. Інформація особливої важливості.

2. Властивості інформації, що підлягають захисту.

Конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення.

Цілісність - властивість інформації бути захищеною від несанкціонованої зміни або зміщення.

Доступність – це властивість інформації бути захищеною від несанкціонованого блокування.

3. Класифікація загроз інформації

Прийнято вважати що основними джерелами загроз є наступні:

№	Джерела	Мотивація
1	Інші держави	а) Економічні переваги б) Політичні переваги в) Військові переваги
2	Конкуренти (економ.)	а) Переваги в конкурентній боротьбі б) Економічні переваги
3	Фізичні особи	а) Гроші б) Самоствердження
4	Політичні партії	а) Боротьба за владу б) Політичні переваги
5	Злочинні угрупування	а) Нанесення шкоди б) Економічні переваги
6	Помилки персоналу	а) Образа б) Зрада в) Примушення
7	Стихійні лиха, наслідки терактів	

Класифікації загроз інформації:

1. Стихійні лиха, технологічні катастрофи
   Боротьба:
   а) Резервування апаратного забезпечення
   б) Резервні копії інформації
2. Відмови обладнання
   Боротьба:
   а) Резервування апаратного забезпечення
   б) Резервні носії інформації
   в) Вибір «правильного» постачальника
3. Наслідки помилок проектування
   Боротьба:
   а) Залучення ліцензіатів до проектування
   б) Експертиза проекту та системи безпеки.
   в) Аудит системи безпеки (1 раз на 1-2 роки)
4. Наслідки помилок персоналу
   Боротьба:
   а) Підбір персоналу
   б) Підготовка персоналу
   в) Створення нормального робочого клімату в колективі
   г) Адміністративно-організаційні засоби, стягнення
5. Навмисні дії порушників

В теорії захисту інформації доводиться, що якщо пункти 3 і 4 реалізовано повністю то навмисні дії порушників неможливі. З аналізу усіх загроз стає зрозуміло, що **ніяка система захисту не може довгий час протистояти цілеспрямованим діям озброєного сучасними технологіями кваліфікованого порушника**.

2) Найбільш небезпечні загрози сучасних комп'ютерних систем.

1. ***Мережева розвідка (прослуховування) sniffing***

Мета:

1) Вияснити діапазон легальних IP-адрес.
2) Імена та паролі користувачів.
3) Ресурси спільного користування.

Боротьба:

1) Криптографія.
2) Ідентифікація не лише за IP-адресами.
3) Програми антисніфери.

2. ***„Маскарад" (підміна IP-фдреси - IP-spoofing).***

Основною метою підміни IP-адреси є можливість проникнення в локальну мережу за допомогою підміни адреси відправника такою, яку пропускають засоби захисту. Як правило „маскарад" використовують як підготовчу операцію для наступних атак.

Боротьба:

1) Додаткова аутентифікація, наприклад „Kerberos".

3. ***Парольні атаки.***

а) Перебір паролів.

б) Атаки за словником.

Боротьба:

1) Одноразові паролі.
2) Обмеження спроб введення пароля + блокування облікових записів.
3) Обмеження часу на введення пароля.
4) Створення сильних паролів.
5) Пароль + „сіль".

4. ***DoS-атаки:***

Denial of Service } Відмова в обслуговуванні

Distributed Denial of Service } Розподілена DoS-атака

Якщо атака виконується з однієї IP-адреси то DoS, якщо з багатьох - DDoS.

Основна мета DDoS-атак – це блокування доступу до інформації. В цьому випадку легальні користувачі не можуть отримати послугу, таким чином це атака проти доступності інформації.

Боротьба:

1) Інтелектуальні маршрутизатори та міжмережеві екрани з можливістю блокування DoS-атак.

5. ***Посередництво (Man-In-Middle).***

Мета: заволодіти паролями при обміні даними між користувачами.

Боротьба: Аутентифікація учасників обміну ключами

6. ***Зловживання довірою***

DNS, WEB, Поштовий сервер часто знаходяться за брандмауером. Між ними та внутрішньою частиною мережі встановлюються т.зв. довірчі відносини, коли не відбувається ретельної аутентифікації.

Мета: проникнення в мережу за допомогою одного з довірчих серверів

Боротьба: максимальне зменшення рівня довіри, особливо по різні боки міжмеревого екрана.

Застосування додаткової аутентифікації (не тільки за IP-адресами).

7. ***Комп'ютерні віруси:***

Боротьба:

1) Антивіруси;
2) Регулярне оновлення ПЗ;
3) Відслідковування бюлетенів безпеки з метою блокування нових вразливостей.

8. Атаки на рівні застосувань:

Боротьба:

a. Аналіз log-файлів за допомогою аналітичних програм.
b. Відслідковування даних про нові вразливості системи.
c. Використання ліцензійного програмного забезпечення.
d. Регулярне оновлення ПЗ.
e. Використання аналізаторів безпеки.

Причини виникнення загроз

1. Відсутність в протоколі TCP-IP будь яких засобів захисту.
2. Загальнодоступні канали передачі інформації.
3. Відсутність (складність) контролю за трафіком і маршрутами проходження сигналу мережею Internet, що робить віддалені атаки безкарними.