Урок № 2.

Тема уроку: Інструктаж з БЖД. Загрози безпеці інформації в автоматизованих системах.

Сьогодні ти познайомишся з поняттям загрози інформаційної безпеки, різновидами загроз та шляхами їх реалізації.

Правила поведінки за комп'ютером:

Пам’ятай:

- Робоче місце за комп'ютером потрібно тримати у порядку.
- Не клади зайвих речей на стіл біля комп'ютера.
- Прибирай пил з комп'ютера спеціальною ганчіркою, коли він вимкнений.

Виконуй:

- Слідкуй за осанкою (спина повинна бути прямою).
- Очі мають бути на відстані 50 – 60 см від екрану монітору.
- Кожні 30 хвилин роби перерву в своїй роботі.

Під *загрозою* розуміють будь-які обставини та події, що виникають у зовнішньому середовищі, які у відповідних умовах можуть викликати появу небезпечної події.

Інформаційна загроза — це потенційна можливість певним чином порушити інформаційну безпеку та (або) нанесення збитків автоматизованій системі (АС).

Загрози самі по собі не виявляються. Всі загрози можуть бути реалізовані тільки при наявності яких-небудь слабких місць - вразливостей, властивих об'єкту інформатизації.

Вразливість системи: нездатність системи протистояти реалізації певної загрози або сукупності загроз.

Атака на комп'ютерну систему – це дія, що робиться зловмисником для пошуку і використання тієї або іншої вразливості системи. Таким чином, атака – це реалізація загрози безпеки.

Класифікація загроз.

Залежно від обсягів завданих збитків загрози інформаційній безпеці поділяють на:

- Нешкідливі – не завдають збитків;
- Шкідливі – завдають значних збитків;
- Дуже шкідливі – задають критичних збитків інформаційній системі.

Загрози пошкодження даних можна класифікувати *за природою їх виникнення*.

1) *Природні* (об'єктивні, не залежать від людини) стихійні явища, природне старіння обладнання, відмова елементів ОС;
2) *Штучні* (суб'єктивні, залежать від людини):
   • випадкові (вихід із ладу обладнання, помилки персоналу або програмного забезпечення)
   • навмисні (перехоплення даних, маскування під дійсного користувача, фізичне руйнування системи)
3) *Ненавмисні* (випадкові) погрози, помилки програмного забезпечення, персоналу, збої в роботі систем, відмови обчислювальної та комунікаційної техніки.

За *метою впливу* розрізняють наступні основні типи загроз безпеки (відповідно до відомої моделі безпеки даних):

1) Загроза порушення конфіденційності (розкриття) полягає в тому, що дані стають відомими тому, хто не має права доступу до них. Вона виникає щоразу, коли отримано доступ до деяких секретних даних, що зберігаються в комп’ютерній системі чи передаються від однієї системи до іншої. Іноді, у зв’язку із загрозою порушення конфіденційності, використовується термін «витік даних».

2) Загроза порушення цілісності передбачає будь-яку умисну зміну даних, що зберігаються в комп'ютерній системі чи передаються з однієї системи в іншу. Вона виникає, коли зловмисники навмисно змінюють дані, тобто порушується їхня цілісність, може відбутися її повне або часткове знищення, спотворення, фальсифікація, дезінформація). Цілісність даних також може бути порушена внаслідок випадкової помилки програмного або апаратного забезпечення.
3) Загроза відмови служб (загроза доступності) виникає щоразу, коли в результаті навмисних дій, які виконує інший користувач або зловмисник, блокується доступ до деякого ресурсу комп'ютерної системи, відбувається порушення часткове або повне працездатності системи. Блокування буває постійним, якщо доступ до запитуваного ресурсу ніколи не буде отримано, або воно може викликати тільки затримку запитуваного ресурсу, досить довгу для того, щоб він став непотрібним. У цих випадках говорять, що ресурс вичерпано.

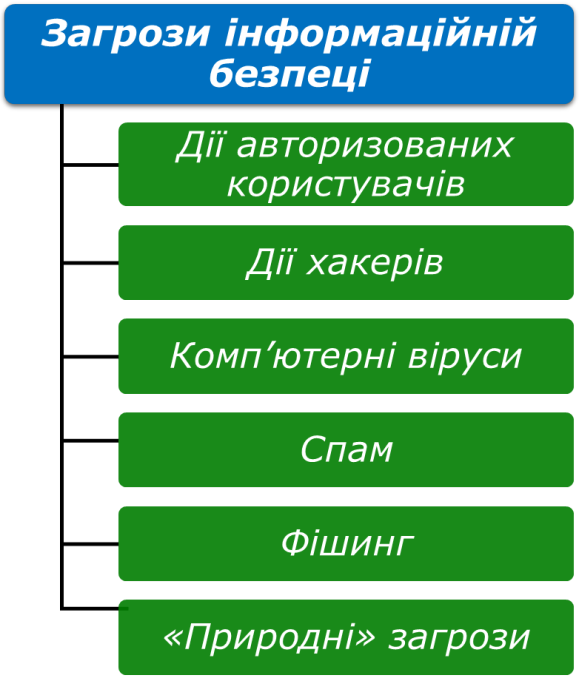
Джерела загроз:

Людський чинник. Ця група загроз пов'язана з діями людини, що має санкціонований або несанкціонований доступ до інформації.

Технічний чинник. Ця група загроз пов'язана з технічними проблемами – фізичне і моральне старіння устаткування, неякісні програмні і апаратні засоби опрацювання інформації.

Стихійний чинник. Ця група загроз включає природні катаклізми, стихійні лиха і інші форс-мажорні обставини, незалежні від діяльності людей.

Загрози, які можуть завдати шкоди інформаційній безпеці організації, можна розділити на кілька категорій:



Додаткове відео до уроку: http://surl.li/rrid.