Основні ненавмисні і навмисні штучні загрози.

Цілі:

- ✓ ***навчальна***: дати уявлення про основні ненавмисні і навмисні штучні загрози;
- ✓ ***розвивальна***: розвивати логічне мислення, пам'ять; формувати вміння узагальнювати;
- ✓ ***виховна***: виховувати інформаційну культуру, формування бережливого ставлення до обладнання комп'ютерного кабінету, виховання уміння працювати в групі; формування позитивного ставлення до навчання.

Тип уроку: Комбінований.

Обладнання та наочність: дошка, комп'ютери з підключенням до мережі Інтернет.

Програмне забезпечення: браузер, офісні програми.

Хід уроку

І. Організаційний етап

- привітання
- перевірка присутніх
- перевірка готовності учнів до уроку

ІІ. Актуалізація опорних знань

Фронтальне опитування

ІІІ. Мотивацій навчальної діяльності

IV. Вивчення нового матеріалу

Підручник В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест. Основи інформаційної безпеки http://www.dut.edu.ua/ua/lib/1/category/729/view/1365

Під безпекою ІС розуміється захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого отримання) інформації, модифікації або фізичного руйнування її' компонентів, тобто здатність протидіяти різним підбурює впливів на ІС.

Основні ненавмисні штучні загрози

Основні ненавмисні штучні загрози АС (дії, що здійснюються людьми випадково, через незнання, неуважність або недбалості, з цікавості, але без злого наміру):

1) ненавмисні дії, що приводять до часткової або повної відмови системи або руйнуванню апаратних, програмних, інформаційних ресурсів системи (ненавмисне псування обладнання, видалення, спотворення файлів з важливою інформацією або програм, в тому числі системних і т. п.);

2) неправомірне відключення обладнання або зміна режимів роботи пристроїв і програм;

3) ненавмисне псування носіїв інформації;

4) запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання або зациклення) або що здійснюють безповоротні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних і т. п.);

5) нелегальне впровадження і використання неврахованих програм (ігрових, повчальних, технологічних і інш., що не є необхідними для виконання порушником своїх службових обов'язків) з подальшим необґрунтованим витрачанням ресурсів (завантаження процесора, захват оперативної пам'яті і пам'яті на зовнішніх носіях);

6) зараження комп'ютера вірусами;

7) необережні дії, що приводять до розголошування конфіденційної інформації, або що роблять її загальнодоступної;

8) розголошування, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, пропусків і т. п.);

9) проектування архітектури системи, технології обробки даних, розробка прикладних програм, з можливостями, що представляють небезпеку для працездатності системи і безпеки інформації;

10) ігнорування організаційних обмежень (встановлених правил) при роботі в системі;

11) вхід в систему в обхід коштів захисту (завантаження сторонньої операційної системи зі змінних магнітних носіїв і т. п.);

12) некомпетентне використання, настройка або неправомірне відключення коштів захисту персоналом служби безпеки;

13) пересилка даних за помилковою адресою абонента (пристрої);

14) введення помилкових даних;

15) ненавмисне пошкодження каналів зв'язку.

Основні навмисні штучні загрози

1) фізичне руйнування системи (шляхом вибуху, підпалу і т. п.) або висновок з ладу всіх або окремих найбільш важливих компонентів комп'ютерної системи (пристроїв, носіїв важливої системної інформації, осіб з числа персоналу і т. п.);

2) відключення або висновок з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолоджування і вентиляції, ліній зв'язку і т. п.);

3) дії по дезорганізації функціонування системи (зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка могутніх активних радіоперешкод на частотах роботи пристроїв системи і т. п.);

4) впровадження агентів в число персоналу системи (в тому числі, можливо, і в адміністративну групу, що відповідає за безпеку);

5) вербування (шляхом підкупу, шантажу і т. п.) персоналу або окремих користувачів, що має певні повноваження;

6) застосування підслуховувальних пристроїв, дистанційна фото- і відео-зйомка і т. п.;

7) перехоплення побічних електромагнітних, акустичних і інших випромінювань пристроїв і ліній зв'язку, а також наводок активних випромінювань на допоміжні технічні засоби, що безпосередньо не беруть участь в обробці інформації (телефонні лінії, сели живлення, опалювання і т. п.);

8) перехоплення даних, що передаються по каналах зв'язку, і їх аналіз з метою з'ясування протоколів обміну, правило входження в зв'язок і авторизації користувача і подальших спроб їх імітації для проникнення в систему;

9) розкрадання носіїв інформації (магнітних дисків, стрічок, мікросхем пам'яті, що запам'ятовують пристроїв і цілих ПЕВМ);

10) несанкціоноване копіювання носіїв інформації;

11) розкрадання виробничих відходів (роздруків, записів, списаних носіїв інформації і т. п.);

12) читання залишкової інформації з оперативної пам'яті і із зовнішніх запам'ятовуючих пристроїв;

13) читання інформації з областей оперативної пам'яті, що використовуються операційною системою (в тому числі підсистемою зашиті) або іншими користувачами, в асинхронному режимі використовуючи нестачі мультизадачних операційних систем і систем програмування;

14) незаконне отримання паролів і інших реквізитів розмежування доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом підбору, шляхом імітації інтерфейсу системи і т. д.) з подальшим маскуванням під зареєстрованого користувача ("маскарад");

15) несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізична адреса, адреса в системі зв'язку, апаратний блок кодування і т. п.;

16) розкриття шифрів криптозащити інформації;

17) впровадження апаратних "спецвкладень", програмних "закладок" і "вірусів" ("троянских коней" і "жучків"), тобто таких дільниць програм, які не потрібні для здійснення заявлених функцій, але що дозволяють долати систему зашиті, потайно і незаконно здійснювати доступ до системних ресурсів з метою реєстрації і передачі критичної інформації або дезорганізації функціонування системи;

18) незаконне підключення до ліній зв'язку з метою роботи "між рядків", з використанням пауз в діях законного користувача від його імені з подальшим введенням помилкових повідомлень або модифікацією повідомлень, що передаються;

19) незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його фізичного відключення після входу в систему і успішної аутентифікація з подальшим введенням дезінформації і нав'язуванням помилкових повідомлень.

За способом отримання інформації потенційні канали доступу можна розділити на:

- фізичний;

- електромагнітний (перехоплення випромінювань);

- інформаційний (програмно-математичний).

V. Засвоєння нових знань, формування вмінь

VI. Підсумки уроку