Запорізький національный університет

Основи безпеки інформаційних систем

І.В.Козін

Задачі лекції

1. Об’єкти захисту інформації
2. Задачі захисту інформації
3. Загрози проникнення
4. Комп’ютерні віруси

Об’єкти захисту інформації

- Власники і користувачі
- Носії і засоби обробки
- Системи зв'язку та інформатизації
- Об'єкти органів управління

Задачи захисту інформації

- 1. Не допустити атаки
- 2. Виявити факт атаки
- 3. Усунути наслідки атаки

Конфіденційність інформації

Суб'єктивно обумовлена характеристика інформації, яка вказує на необхідність введення обмежень на коло суб'єктів, що мають доступ до цієї інформації, і забезпечується здатністю системи зберігати зазначену інформацію в таємниці від суб'єктів, які не мають повноважень доступу до неї.

Цілісність інформації

Існування інформації в неспотвореному вигляді, тобто в незмінному по відношенню до деякого фіксованого її стану.

Доступність інформації

Властивість системи, що характеризується здатністю забезпечувати своєчасний і безперешкодний доступ до інформації суб'єктів відповідно до запитів

Загрози проникнення

- Маскарад-користувач маскується під іншого користувача.
- Обхід захисту-використання слабких місць в системі безпеки з метою отримання доступу.
- Порушення повноважень-використання ресурсів не за призначенням.
- Троянські програми-програми, що містять програмний код, при виконанні якого порушується функціонування системи безпеки.

Загрози розкриття параметрів системи

- Визначення типу і параметрів носіїв інформації
- Отримання інформації про програмно-апаратної середовищі, про функції, які виконуються ІС, про системи захисту.
- Визначення способу представлення інформації.
- Визначення якісного змісту даних

Загроза порушення конфіденційності

- Розкрадання носіїв інформації.
- Несанкціонований доступ до ІС.
- Виконання користувачем несанкціонованих дій.
- Перехоплення даних, переданих по каналах зв'язку.
- Розкриття змісту інформації.

Загроза відмови доступу

- Виведення з ладу машинних носіїв інформації.
- Прояв помилок розробки програмного забезпечення.
- Обхід механізмів захисту.
- Спотворення відповідності конструкцій мови.

Загроза порушення цілісності

- Знищення носіїв інформації
- Внесення несанкціонованих змін в програми і дані.
- Установка і використання нештатного програмного забезпечення.
- Зараження вірусами
- Впровадження дезінформації

Поняття комп’ьютерного віруса

Комп’ютерний вірус – це спеціальна програма, що наносить заведому щкоду комп’ютеру, на якому вона запускається на виконання, або іншим комп'ютерам в мережі.

Основною функцією вірусу є його розмноження

Принципи класифікації комп'ютерних вірусів

- ***по природному середовищу;***
- ***по операційним системам;***
- ***за алгоритмом роботи;***
- ***за деструктивними можливостями.***

По природному середовищу:

Файлові віруси

Завдають шкоди файлів. Створюють файл-двійник з ім'ям оригіналу.

Загрузочні віруси

прониають в завантажувальний сектор диска. Операційна система при цьому завантажується з помилками і збоями

Макро-віруси

«Псують» документи Word, Excel і інших прикладних програм операційної системи Windows.

Мережеві віруси

Поширюються по Internet через електронні листи або після відвідування сумнівних сайтів.

По операційним системам

Для кожної операційної системи створюються свої віруси, які будуть «працювати» тільки в ній. Але існують і універсальні віруси, які здатні впроваджуватися в різні операційні системи.

За алгоритмом роботи

Резидент-ність

Віруси, що володіють цією властивістю діють постійно поки комп'ютер включений.

Самошифрування і полімор-фізм

Віруси-полиморфики змінюють свій код або тіло програмі, що їх важко виявити.

Стелс–алгоритм

Віруси-невидимки «ховаються» в оперативній пам'яті і антивірусна програма їх не може виявити.

Нестан-дартные приемы

Принципово нові методи впливу вірусу на комп'ютер.

За деструктивними можливостями

Нешкідливі
не завдають ніякої шкоди ні користувачу, ні комп'ютера, але займають місце на жорсткому диску.

Безпечні
наносять моральну шкоду користувачеві Викликають візуальні графічні чи звукові ефекти.

Небезпечні
знищують інформацію в файлах. «Псують» файли, роблять їх несчітиваемимі тощо

Дуже небезпечні
збивають процес завантаження ОС, після чого потрібно її перевстановленн я; або «псують» вінчестер, що його потрібно форматувати

Шкідливі програми

- ***Троянський кінь -*** це програма, яка містить в собі деяку руйнує функцію, яка активізується при настанні деякого умови спрацьовування. Зазвичай такі програми маскуються під які-небудь корисні утиліти. Види деструктивних дій:
- **Знищення інформації**. (Конкретний вибір об'єктів і способів знищення залежить тільки від фантазії автора такої програми і можливостей ОС. Ця функція є спільною для троянських коней і закладок).
- **Перехоплення і передача інформації**. (Паролів, які набираються на клавіатурі).
- **Цілеспрямована** зміна програми.

- ***Хробаками*** називають віруси, які поширюються по глобальних мережах, вражаючи цілі системи, а не окремі програми. Це найнебезпечніший вид вірусів, так як об'єктами нападу в цьому випадку стають інформаційні системи державного масштабу. З появою глобальної мережі Internet цей вид порушення безпеки представляє найбільшу загрозу, тому що йому в будь-який момент може зазнати будь-який з комп'ютерів, підключених до цієї мережі. Основна функція вірусів даного типу - злом атакується системи, тобто подолання захисту з метою порушення безпеки і цілісності.

А що буде далі…

..ну що, нарешті ...

Пора прощатися.

До побачення!