Безпека операційних систем і комп'ютерних мереж

Лекція 1

Основні питання

- Спочатку нагадаємо концептуальний підхід до захисту інформації
- А потім розберемось із структурою курсу

Інформаційно-телекомунікаційна система (ІТС)

- До інформаційно-телекомунікаційних систем відносять будь-яку систему, яка відповідає одному з трьох видів автоматизованих систем:
  - інформаційна система – організаційно-технічна система, що реалізує технологію оброблення інформації за допомогою засобів обчислювальної техніки і програмного забезпечення;
  - телекомунікаційна система – організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання й приймання інформації у вигляді сигналів, знаків, звуків, зображень або іншим способом;
  - інтегрована система – сукупність двох або кількох взаємопов'язаних інформаційних і (або) телекомунікаційних систем, в якій функціювання однієї (або кількох) з них залежить від результатів функціювання іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Політика безпеки [інформації]

сукупність

- законів,
- правил,
- обмежень,
- рекомендацій,
- інструкцій і т.д.,

що регламентують порядок обробки інформації

і спрямовані на захист інформації від певних загроз

Властивості інформації

- Конфіденційність
  - лише уповноважені користувачі можуть ознайомитись з інформацією
- Цілісність
  - лише уповноважені користувачі можуть модифікувати інформацію
- Доступність
  - уповноважені користувачі можуть отримати доступ до інформації, не очікуючи довше за заданий (малий) час

Безпека інформації

- Стан інформації, в якому забезпечується збереження властивостей інформації, визначених політикою безпеки

Загроза, атака, вразливість

- Загроза:

  будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації та (або) нанесення збитків ІТС

- Атака:

  спроба реалізації загрози

- Вразливість системи:

  нездатність системи протистояти реалізації певної загрози або сукупності загроз

Моделі

- Модель [політики] безпеки:
  - Абстрактний формалізований або неформалізований опис політики безпеки
- Модель загроз:
  - Абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз
- Модель порушника:
  - Абстрактний формалізований або неформалізований опис порушника

Захист інформації в ІТС

- діяльність, спрямована на забезпечення безпеки інформації, що обробляють в ІТС, і ІТС в цілому, яка дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційного збитку в результаті реалізації загроз
- Захищена ІТС:

  ІТС, що здатна забезпечувати захист інформації, що обробляється в ній, від певних загроз

План лекційного курсу

1) Безпека операційних систем
   1) Модель загроз для ОС
   2) Концепція розробки захищених ОС
   3) Комплекс засобів захисту ОС
   4) Стандарти оцінювання безпеки ОС (НД ТЗІ, ISO 15408)
   5) Засоби захисту ОС Windows
   6) Засоби захисту UNIX-подібних ОС
   7) Апаратні засоби як основа механізмів захисту ОС (на прикладі архітектури процесорів x86)
2) Безпека комп'ютерних мереж і розподілених систем
   1) Розподілені атаки і безпека Інтернету
   2) Стандарти безпеки мереж (X.800)
   3) Вразливості протоколів Інтернету
   4) Міжмережне екранування (Firewalling)
   5) Віртуальні приватні мережі (VPN)
   6) Системи виявлення атак і запобігання вторгненням (IDS, IPS)