

Урок 18

Тема уроку: Технології забезпечення безпеки інформаційних систем

Мета уроку:

- ✓ **навчальна:** сформувати уявлення про інформаційні системи, їх види та складові;
- ✓ **розвивальна:** розвивати світоглядні уявлення про пізнаваність явищ і процесів у навколошньому світі, логічне мислення через установлення причинно-наслідкових зв'язків, інформаційну культуру особистості.
- ✓ **виховна:** виховувати уважність та відповідальність, бажання мати глибокі та якісні знання.

Матеріал уроку:

Складові безпеки. Поняття загрози і атаки

За даними європейських Узгоджених Критеріїв Оцінки Безпеки Інформаційних Технологій (Information Technology Security Evaluation Criteria, ITSEC), безпека включає в себе наступні складові:

- 1) конфіденційність - інформацією в системі можуть оперувати лише користувачі з відповідними повноваженнями;
- 2) цілісність - наявна в системі інформація не має пошкоджень, є повною та достатньою;
- 3) доступність - при володінні відповідними правами користувач системи повинен безперешкодно отримати необхідну інформацію в стислі терміни.

Відповідно до цих складових, існують специфікації функцій безпеки:

- о ідентифікація та аутентифікація;
- о управління доступом;
- о протоколювання;
- о аудит;
- о повторне використання об'єктів;
- о точність комунікацій;
- о надійність обслуговування;
- о обмін даними.

Набір функцій безпеки може спеціалізуватись з використанням посилань на класи функціональності, за якими визначається ступінь потрібного захисту системи. ITSEC визначає 10 класів функціональності, причому класи F-C1, F-C2, F-B1, F-B2, F-B3 відповідають аналогічним класам безпеки, які зазначені в американських Критеріях (DOD, Orange Book - OK).

Перед подальшим викладанням матеріалу наведемо декілька означень.

Ідентифікація - надання при вході в систему свого імені або реєстраційного номера, що одержується користувачем при попередній реєстрації в системі

Аутентифікація - підтвердження права на доступ, відповідності наданої ідентифікаційної інформації і користувача

В сучасних системах існують різноманітні засоби для реалізації механізмів ідентифікації та аутентифікації, такі як:

- о пароль;
- о відбитки пальців, сітківка ока, зовнішність, голос, ДНК;
- о наявність ключа чи магнітної картки;
- о ідентичність апаратного забезпечення (контрольна сума BIOS, фізичний номер мережної карти);
 - о відповідна поведінка у реальному часі (швидкість натискання клавіш, швидкодія зворотної реакції на запити, тощо).

Як і більшість сучасних методів дослідження складних систем, аналіз систем захисту використовує ієрархічну декомпозицію:



Рис.16.1. Схема ієрархічної декомпозиції аналізу захищенності складних інформаційних систем

Даний підхід лежить в основі багатьох стандартів для систем захисту та дозволяє проводити аналіз та атестацію захищенності ІС.

Політика безпеки - це набір законів, правил та норм для окремої комп'ютерної системи, що визначають весь процес обробки, поширення та захисту даних в ній

Згідно ОК, метою аналізу захищенності є гарантована відсутність простих шляхів обходу механізмів захисту (рис.16.1, рівень 3). Як правило, кожна сучасна система захисту проходить тестування з допомогою спеціалістів та спеціальних програм на наявність таких шляхів.

Якщо інформація в комп'ютерній системі має цінність, то необхідно визначити, в якому сенсі цю цінність необхідно зберігати. Відповідно до попередньо розглянутих інформаційних характеристик, загрози у комп'ютерній системі можна класифікувати наступним чином:

- о коли цінність інформації втрачається при її розповсюджені - це загроза конфіденційності (секретності) інформації;
- о якщо при зміні або знищенні інформації завдаються збитки, тоді це є загрозою її цілісності;

- о коли цінність інформації визначається оперативністю її використання, то загроза буде у порушенні доступності інформації;
- о якщо цінність втрачається при відмовах самої комп'ютерної системи, тоді є небезпека втрати стійкості до помилок.

Як правило, розглядають три перші загрози, хоча із розвитком складних комп'ютерних систем все частіше стає актуальною і четверта загроза.

Загрози - це шляхи реалізації впливів на інформацію, які вважаються небезпечними

Наприклад, загроза перехоплення інформації через випромінювання монітора може привести до втрати секретності, загроза пожежі може спричинити втрати цілісності інформації, зникнення зв'язку між компонентами системи загрожує доступності. Наслідками вимкнення струму буде хибна оцінка ситуації в АСУ і т.д.

Аналіз загроз для інформації в системі повинен показати, де і коли в системі з'являється цінна інформація, і в якому місці системи вона може втратити цінність. Загроза реалізується через атаку в певному місці і в певний час.

Атака - будь-які зовнішні дії з можливим негативним наслідком для системи, в тому числі і дії користувачів

Написати конспект, відповідно до поданого матеріалу. Виконати домашнє завдання:

Описати наступні інформаційні загрози: 1) логічні бомби; 2) неуважність користувачів.

Фото конспекти надсилали на адресу olia.dubina2017@gmail.com

У темі листа вказати номер групи, прізвище та ім'я.