7

Основи інформаційної та кібербезпеки

Лекція 7.
Захист в операційних системах

1. Поняття захищеної операційної системи і принципи її створення
2. Управління доступом
3. Автентифікація
4. Аудит і виявлення вторгнень

1 Поняття захищеної операційної системи

Будемо вважати **захищеною** таку ОС, яка передбачає захист від основних загроз:

- Сканування файлової системи
- Викрадення ключової інформації
- Підбирання паролів
- Збирання сміття
- Перевищення повноважень
- Програмних закладок
- Жадібних програм

1 Поняття захищеної операційної системи

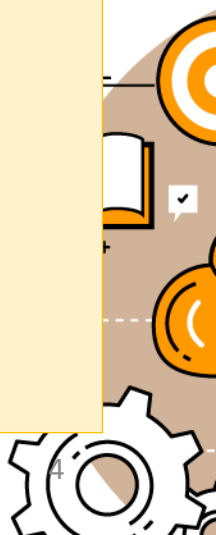
Підходи до створення захищених ОС:

- ✓ **Фрагментарний**
- ✓ **Комплексний**

Фрагментарний:

- антивірус
- система шифрування
- система реєстрації дій користувачів

…



1 Поняття захищеної операційної системи

Комплексний: *розроблення захищених систем “з нуля”*

- При розробці захищених систем “з нуля” на етапі проектування закладаються усі функціональні можливості та архітектурні рішення, що розраховані на сертифікацію за встановленим класом вимог
- Головною рисою цього підходу є розробка методів гарантованої реалізації встановлених вимог
- Застосовується класична схема проектування захищених систем:
  - **визначення вимог безпеки;**
  - **розробка моделі безпеки;**
  - **визначення об’єктів взаємодії;**
  - **визначення правил керування доступом;**
  - **вибір механізмів керування доступом;**
  - **вибір методів ідентифікації й автентифікації сторін, що взаємодіють;**
  - **визначення множини подій, що підлягають аудиту;**
  - **реалізація системи**

1 Поняття захищеної операційної системи

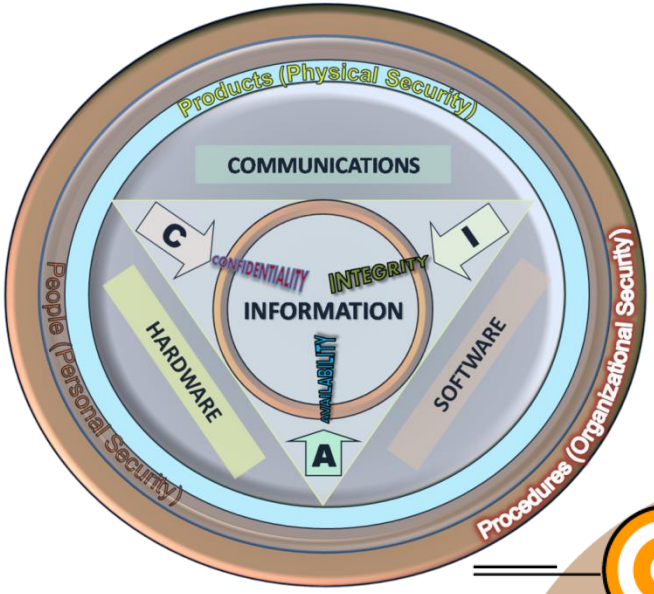
Прикладів розроблення захищених систем “**з нуля**” небагато через складність і значну вартість проведення таких робіт

- системи, які в подальшому були сертифіковані на відповідність найвищим класам вимог: Trusted Xenix, Trusted Mach, Harris CX/SX, XTS 300 STOP

Перевагою побудови “**довірених**” версій шляхом модернізації існуючих систем є економічна ефективність

1 Принципи створення захищених систем

- Принцип інтегрованості
- Принцип інваріантності
- Принцип уніфікації
- Принцип адекватності
- Принцип коректності



1 Принципи створення захищених систем

❑ Принцип інтегрованості

Засоби захисту повинні бути вбудовані в систему таким чином, щоби усі без виключення механізми взаємодії знаходились під їх контролем:

- Найпростішим методом, що реалізує цей принцип при створенні ОС, є максимальне обмеження числа механізмів взаємодії та інтеграція засобів захисту безпосередньо в ці механізми

1 Принципи створення захищених систем

❑ Принцип інваріантності

- Засоби захисту не повинні залежати від особливостей реалізації утиліт і прикладних програм, і не повинні враховувати логіку їх функціонування;
- Засоби захисту повинні бути універсальними для усіх типів взаємодій;

  Для ОС інваріантність засобів захисту може бути досягнута шляхом застосування строго регламентованої парадигми функціонування програм, що обмежує способи взаємодій

1 Принципи створення захищених систем

❑ Принцип уніфікації

- Засоби захисту мають бути універсальними, що дозволяє використовувати їх без змін як для реалізації різних моделей безпеки, так і для керування доступом до об’єктів різної природи:

Повинна існувати однозначна відповідність між взаємодіями суб’єктів і об’єктів, що контролюються, та операціями доступу, керування якими описується моделями безпеки.

При розробленні ОС слідування цьому принципу приводить до необхідності створення універсального інтерфейсу доступу, що об’єднує всі способи взаємодій між суб’єктами й об’єктами, всі функції якого однозначним чином відображаються на множину операцій, що описуються моделлю безпеки

1 Принципи створення захищених систем

❑ Принцип адекватності

- Для забезпечення реальної здатності протидіяти атакам необхідно виключити усі чинники, які спричиняють виникнення вразливостей:

Усі механізми реалізації атак базуються на використанні наявних вразливостей;

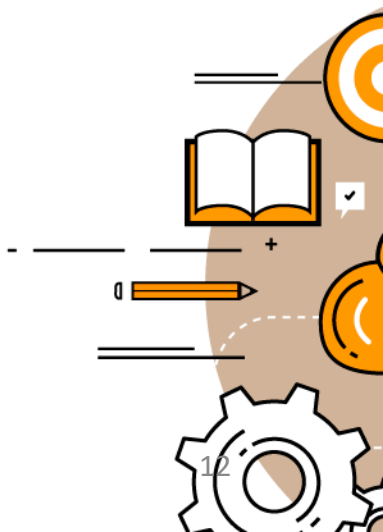
Головною причиною появи вразливостей є непослідовність в реалізації контролю доступу;

Переважну більшість причин появи вразливостей можна усунути, реалізувавши в системі керування доступом на основі універсального інтерфейсу та єдиного механізму взаємодії без будь-яких виключень

1 Принципи створення захищених систем

❑ Принцип коректності

- Засоби захисту повинні реалізовувати керування доступом відповідно до формальних моделей:



1 Принципи створення захищених систем

Типова архітектура комплексу засобів захисту операційних систем

Керування політикою безпеки ОС

Ідентифікація й автентифікація

Розмежування доступу

Реєстрація й облік (аудит)

Криптографічні функції

Забезпечення цілісності

Антивірусний захист

Апаратні засоби

2 Управління доступом

Складові операційної системи

Ядро ОС

- Ядро - Центральна частина операційної системи, що керує процесом Виконання програм та їх доступом до ресурсів комп'ютера
- Функції: жодна програма не може виконуватись без ядра ОС, оскільки саме воно вказує процесору, коли яку програму слід запустити; визначає, якій програмі та до якого ресурсу можна надати доступ

Драйвери

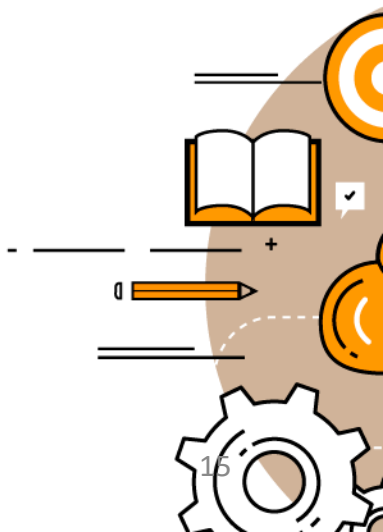
- Драйвер - програмний модуль, що використовується іншими програмами для керування роботою пристроїв
- Функції: програма перетворює стандартні команди операційної системи на специфічні команди конкретної моделі пристроїв.

Файлова система

- Файлова система- набір правил, що визначає спосіб організації, зберігання та іменування данних, розташованих на запам'ятовуючих пристроях.
- Файл - найменша неподільна одиниця данних на запам'ятовуючому пристрої, яка має власне ім'я та з якою метою користувач може виконувати операції.
- Каталог - це елемент файлової системи, який має власне ім'я та може містити файли й інші каталоги.

2 Управління доступом

- Об'єкт доступу
- Метод доступу
- Суб'єкт доступу



2 Управління доступом

Вимоги до правил розмежування:

- Правила розмежування доступу, прийняті в ОС, повинні відповідати аналогічним правилам, прийнятим в організації, в якій встановлена ця ОС.
- Правила розмежування суб'єктів ОС не повинні діяти руйнуюче на ОС, а саме є недопустимою є несанкціонована зміна, видалення або інший вплив на об'єкти, які життєво важливі для нормальної роботи ОС.
- Будь-який об'єкт доступу повинен мати власника. Неприпустимо присутність нічийних об'єктів - об'єктів, що не мають власника.
- Неприпустимо присутність недоступних об'єктів - об'єктів, до яких не може звернутися жоден суб'єкт доступу ні по одному методу доступу.
- Неприпустимий витік конфіденційної інформації.

2 Управління доступом

Основні моделі розмежування доступу:

- ***Вибіркове керування доступом*** (Discretionary Access Control),

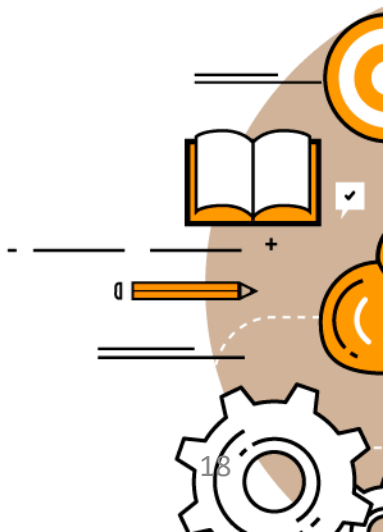
При вибірковому керуванні доступом до певних операцій над певним об'єктом забороняються або дозволяються визначеним суб'єктам або групам суб'єктів.

- **Повноважне керування доступу** (Mandatory Access Control).

При повноважному керуванні доступом, об'єкти можуть мати рівні секретності, а всі суб'єкти поділяються на групи, що утворюють ієрархію відповідно до рівня допуску до інформації. Іноді цю модель називають моделлю багаторівневої безпеки, призначеної для зберігання секретної інформації

2 Управління доступом у Windows

Усі об'єкти є об'єктами доступу:



2 Управління доступом у Windows

Суб'єкти доступу:

1. **Користувачі**
2. **Групи користувачів**
3. **Спеціальні групи**
4. **Відносні суб’єкти**

2 Управління доступом у Windows

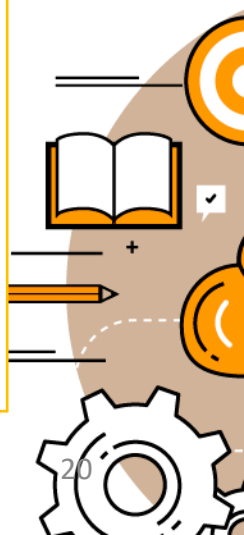
Методи і права доступу:

1. **Стандартні методи:**

   видалення, отримання атрибутів захисту, зміна списку доступу, зміна власника, отримання і зміна параметрів аудиту, очікування

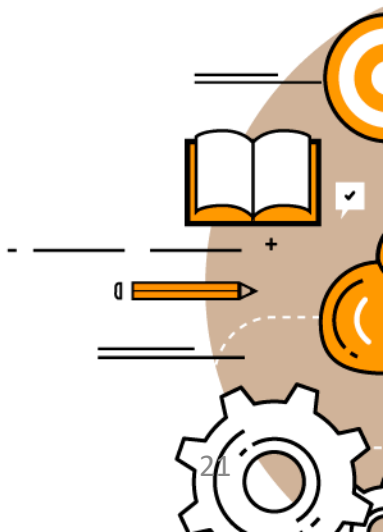
2. **Специфічні методи (16):**

   читання, запис,виконання …



2 Управління доступом у Windows

Мандатний контроль цілісності:



2 Управління доступом в Unix

Об'єкти доступу:

Суб'єкти доступу:

1. **Користувачі**
2. **Групи користувачів**

2 Управління доступом в Unix

Методи доступу:

1. **Read**
2. **Write**
3. **Execute**

В MacOS додатково: delete, append, …

2 Управління доступом в Unix

Методи доступу:

1. **Read**
2. **Write**
3. **Execute**

В MacOS додатково: delete, append, …

3 Автентифікація

- Ідентифікація та автентифікація за допомогою імені та пароля; (***слово, PIN-код, код для замка, графічний ключ***)

- Ідентифікація та автентифікація за допомогою зовнішніх носіїв ключової інформації; (***пластикова карта, ключ від замка, USB-ключ)***

- Ідентифікація та автентифікація за допомогою біометричних характеристик користувачів. (***відбиток пальця, обличчя, сітківка ока)***

3 Автентифікація

- Unix

- Windows

4 Аудит і виявлення вторгнень

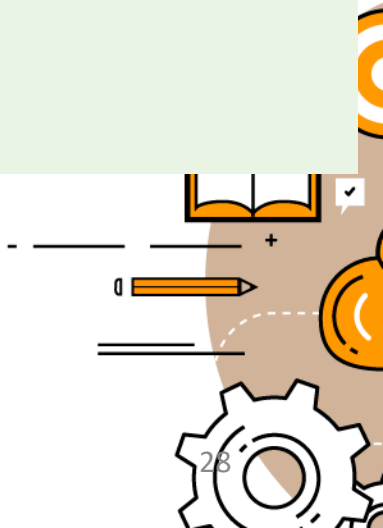
Процедура аудиту безпеки ОС – це реєстрація в спеціальному журналі (журналі безпеки), подій, які можуть становити небезпеку для операційної системи.

Для чого потрібен аудит:

- Виявлення спроб вторгнення;
- Збір інформації про методи вторгнення, як успішні так і неуспішні;
- Аналіз кількості неправильних спроб введення паролю;
- Аналіз попереднього стану системи в контексті виявлених помилок;
- Фіксація входу і виходу з системи;
- Реєстрація зміни атрибутів файлів ОС.

4 Аудит і виявлення вторгнень

- **Windows**
  - ***Event Viewer***
- **Unix**
  1. **syslogd klogd**
  2. **auditd (типу Windows)**



...

- СИСТЕМА БЕЗПЕКИ ОС ANDROID
- Віртуалізація операційних систем