ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ТЕМА 3. ЗАХИСТ ІНФОРМАЦІЇ НА РІВНІ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ

План

1. Апаратні засоби контролю доступу та захисту інформації
2. Системи фізичної безпеки та сигналізації як елемент захисту наукової інфраструктури
3. Обмеження та блокування пристроїв та інтерфейсів вводу-виводу інформації

Апаратний захист – це система технічних рішень, що фізично обмежують або контролюють доступ до інформаційних ресурсів незалежно від програмного середовища.

Функції апаратного захисту:

- забезпечення фізичної ізоляції критичних ресурсів;
- унеможливлення несанкціонованого доступу до серверів і лабораторного обладнання;
- запобігання витоку даних через фізичні канали;
- мінімізація ризиків внутрішніх загроз;
- підвищення доказовості у разі інцидентів.

Актуальність апаратного захисту:

- наявність унікального обладнання;
- зберігання результатів багаторічних досліджень;
- обробку персональних або чутливих даних;
- інтеграцію з міжнародними дослідницькими мережами.

Апаратні засоби контролю доступу – це сукупність технічних пристроїв та електронних механізмів, які забезпечують фізичне або логіко-фізичне обмеження доступу до інформаційних ресурсів, обладнання та приміщень на рівні апаратури.

На відміну від програмних засобів, апаратний контроль:

- функціонує незалежно від операційної системи;
- складніше піддається несанкціонованому втручанню;
- дозволяє реалізувати принцип «security by design»;
- забезпечує базовий рівень довіри до інфраструктури (root of trust).

Для наукових установ це критично, оскільки:

- дослідницьке обладнання має високу вартість;
- експериментальні дані часто є унікальними;
- можливе зберігання конфіденційних або чутливих даних (персональні дані, результати оборонних або біомедичних досліджень).

Принципи функціонування апаратного контролю:

- Принцип мінімальних привілеїв (Least Privilege) – користувач або пристрій отримує доступ лише до необхідних ресурсів.
- Принцип багатофакторності – комбінація: того, що користувач знає (PIN), того, що має (токен),того, ким є (біометрія).
- Принцип апаратної довіри (Hardware Root of Trust) – безпечний запуск системи з перевіркою цілісності прошивки та ОС.
- Принцип ізоляції – фізичне розмежування доступу до різних сегментів інфраструктури.

Роль апаратних засобів у забезпеченні цілісності наукових даних:

- запобігання фізичному втручанню у сервери дослідницьких баз;
- захист ключів шифрування;
- унеможливлення копіювання даних через USB-інтерфейси;
- гарантування доказової сили електронних даних;
- підтримка відповідності міжнародним стандартам (ISO/IEC 27001, 27002, 27005).

Наукова інфраструктура включає:

- лабораторії та дослідницькі центри;
- серверні приміщення;
- архіви, репозитарії;
- обладнання високої вартості;
- спеціалізовані установки;
- системи зберігання біологічних або хімічних матеріалів.

Особливості наукової інфраструктури:

- висока концентрація матеріальних активів;
- обмежений доступ;
- підвищені вимоги до контролю середовища (температура, вологість);
- можливість цілеспрямованого впливу.

Загрози фізичній безпеці наукових об’єктів

Тип загрози	Приклад	Наслідки
Несанкціоноване проникнення	стороння особа у лабораторії	викрадення, фальсифікація
Внутрішні порушення	зловживання співробітником	витік інформації
Техногенні ризики	пожежа, затоплення	знищення даних
Диверсії	умисне пошкодження обладнання	зрив досліджень

Система фізичної безпеки – це комплекс:

- організаційних заходів;
- інженерно-технічних засобів;
- систем сигналізації;
- засобів контролю доступу;
- засобів відеоспостереження.

Принципи системи фізичної безпеки:

1. **Багаторівневість** – система фізичної безпеки будується за принципом «глибокої оборони», коли захист організовано на зовнішньо, внутрішньому та локальному рівнях;
2. **Безперервність моніторингу** – фізична безпека передбачає постійне спостереження за територією, приміщеннями і об’єктами та включає відеоспостереження; датчики руху, диму, вологи, відкриття дверей; системи тривожного оповіщення;
3. **Інтеграція з ІТ-системами** – фізична безпека ефективна, якщо її компоненти інтегровані з інформаційними системами;
4. **Пропорційність ризику** – заходи фізичної безпеки мають відповідати рівню реальних загроз і цінності об’єктів.

Фізичні методи блокування інтерфейсів введення / виведення інформації – це сукупність інженерних засобів, які унеможливлюють або суттєво ускладнюють використання портів вводу-виводу на рівні апаратної інфраструктури.

Механічні засоби блокування:

– Заглушки USB (USB Port Blockers) – унеможливлюють підключення флеш-накопичувачів; запобігають підключенню зовнішніх жорстких дисків; блокують ін’єкцію шкідливого ПЗ через USB.

– Замки для портів – повністю фізично блокування підключення; надають контрольований доступ лише через відповідального адміністратора.

– Опечатування серверів – забезпечує контроль факту втручання.

– Фізичне вилучення портів

Апаратний рівень контролю – це фундаментальний рівень безпеки, який функціонує ще до запуску операційної системи, призначенням якого є унеможливлення несанкціонованої модифікації середовища запуску, обхід політик безпеки та фізичні атаки через альтернативні способи завантаження.

Цей рівень критично важливий для захисту:

- серверів наукових баз даних;
- робочих станцій дослідників;
- лабораторного обладнання з вбудованими ОС;
- систем обробки чутливих експериментальних результатів.

Складові апаратного контролю

1. BIOS / UEFI як первинна точка контролю – це програмно-апаратне середовище, яке ініціалізує обладнання перед запуском ОС.
2. TPM (Trusted Platform Module) – це апаратний криптографічний модуль, інтегрований у материнську плату.
3. Secure Boot – це механізм перевірки цифрового підпису програм, що запускаються під час старту системи.

Програмні механізми контролю – це інструменти управління використанням пристроїв та каналів передачі даних на рівні операційної системи, корпоративної політики та спеціалізованого захисного ПЗ.

На відміну від фізичних методів, вони:

забезпечують централізоване адміністрування;

дозволяють гнучке налаштування доступу;

формують журнал подій;

інтегруються в системи аудиту та доказування.

Складові програмних механізмів контролю

1. Group Policy (GPO) – централізована політика контролю – це механізм управління параметрами безпеки в середовищі Windows через Active Directory.
2. Endpoint Protection – контроль на рівні кінцевої точки – це комплекс програмного захисту робочих станцій та серверів.
3. DLP-системи (Data Loss Prevention) – це найбільш складний і інтелектуальний механізм захисту для запобігання витоку інформації, що дає можливість диференційованого контролю.

Контроль бездротових каналів

Бездротові інтерфейси – найбільш складні для контролю, оскільки:

- вони не мають фізичного обмеження;
- можуть працювати приховано;
- використовуються як альтернативний канал витоку.

Заходи бездротового захисту

1. Відключення Bluetooth
2. Сегментація Wi-Fi, що мінімізує горизонтальне переміщення зловмисника у разі компрометації.
3. Шифрування WPA3 – сучасний стандарт захисту Wi-Fi.
4. Ізоляція гостьових мереж, що запобігає витоку даних через відвідувачів, партнерів або тимчасових дослідників.

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ДЯКУЮ ЗА УВАГУ!!!