ТЕМА 3. ЗАХИСТ ІНФОРМАЦІЇ НА РІВНІ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ

Завдання 1. Оцінка ефективності апаратних ключів

Дослідити роботу апаратних ключів та систем захисту.

Етапи виконання завдання:

- порівняти ключі YubiKey, eToken, RSA SecureID;
- виконати тестування їхньої ефективності в реальному середовищі;
- запропонувати сценарії використання для захисту конфіденційних даних.

Результати виконання завдання оформити у вигляді аналітичного звіту.

Завдання 2. Моделювання атак через фізичні порти

Дослідити методи атак на порти та способи їхнього блокування.

Етапи виконання завдання:

- використати USB Rubber Ducky або BadUSB для моделювання атак;
- виявити можливі сценарії витоку даних через фізичні інтерфейси;
- налаштувати політики безпеки та протестувати ефективність блокування.

Результати виконання завдання оформити у вигляді звіту та відеодемонстрації тестування.

Завдання 3. Проєктування системи фізичної безпеки серверної кімнати

Розробити багаторівневу систему фізичного захисту інформації.

Етапи виконання завдання:

- аналіз вразливостей об’єкта;
- розробка системи сигналізації, відеоспостереження, контролю доступу;
- використання біометричних і RFID-систем.

Результати виконання завдання оформити у вигляді документу проєкту безпеки.