**Лабораторна робота №2 "Механізми захисту ОС Windows".**

Дана лабораторна робота узагальнює матеріал попередньої роботи по ОС Windows з курсу «Основи технологій захисту інформації».

**Завдання роботи:**

1. Види суб'єктів ОС, ідентифікатори суб'єктів. Процедура автентифікації. Налаштування політики автентифікації.

2. Облікові записи. Атрибути облікових записів. Керування обліковими записами. Політика облікових записів. У чому відмінність можливостей адміністратора системи від непривілейованого користувача.

3. Маркер доступу і дескриптор захисту. Склад параметрів. Права і дозволи (привілеї).

4. Види об'єктів доступу ОС. Дозволи доступу. Стандартні і спеціальні дозволи. Як перевірити дію окремого дозволу? Відмінність дозволів на каталоги і файли. Захист реєстру ОС.

5. Права (user rights) та дозволи (user permissions) користувачів. Керування доступом на об`єкти файлової системи NTFS. Загальні та специфічні дозволи. Права власника. Алгоритм обчислення ефективних дозволів.
Які дозволи (або заборони) мають пріоритет? (явно призначені користувачам, групові або успадковані, права власника). Обмеження спадкування (біти спадкування). Передавання права власника. Пошук об'єктів у ФС за параметрами ACL. Які набори дозволів на файлові об'єкти можуть становити потенційну вразливість?

6. Рівні цілісності суб'єктів і об'єктів. Зміна рівнів цілісності. Вплив рівнів цілісності на ефективні дозволуи.

7. Квоти дискового простору. Керування квотами.

8. Параметри аудиту. Події, що реєстуються. Журнали аудиту. Налаштування та перевірка аудиту ФС.

9. Налаштування параметрів політики безпеки ОС в цілому.

10. Сформулюйте (письмово) політику доступу для вашої ОС.

11. Використовуючи утиліти автоматичної перевірки захищеності системи (наприклад, WinPeas, Microsoft Security Compliance Toolkit, Microsoft Baseline Security Analyzer (MBSA) ) дізнайтеся про можливі вразливості у встановлених програмних продуктах, налаштуваннях, правах доступу тощо. Опишіть методику перевірки захищеності системи, яку вони використовують.