**Лабораторна робота 6**

**Бурлаченко Єгор**

1. Політика безпеки в Windows - це набір правил та налаштувань, які допомагають забезпечити безпеку комп'ютерної системи. Вона включає в себе правила для керування паролями, доступом до файлів, захистом від вірусів і шкідливих програм, а також багато іншого.

2. Як запустити утиліту "Локальна політика безпеки":

a. Натисніть клавішу "Win + R", щоб відкрити вікно "Виконати".

b. Введіть "secpol.msc" і натисніть "OK".

3. Перерахунок політик паролів:

- Політика мінімальної довжини пароля.

- Політика вимагання використання великих і малих літер.

- Політика вимагання використання цифр та спеціальних символів.

- Політика періодичної зміни паролів.

- Політика заборони використання попередніх паролів.

4. Політика паролів - це набір вимог та обмежень, які визначають, які характеристики повинні мати паролі користувачів системи. Вона спрямована на забезпечення безпеки облікових записів і перешкоджає використанню слабких або легко вгадуваних паролів.

5. Коротка характеристика кожної політики паролів:

- \*Мінімальна довжина пароля\*: Вимагає встановлення пароля з мінімальною кількістю символів.

- \*Вимагання великих і малих літер\*: Забезпечує використання букв верхнього та нижнього регістрів.

- \*Вимагання цифр та спеціальних символів\*: Вимагає використання цифр та спеціальних символів у паролі.

- \*Періодична зміна паролів\*: Змушує користувачів змінювати паролі через певні інтервали часу.

- \*Заборона використання попередніх паролів\*: Забороняє використовувати паролі, які були вже використані.

6. Перерахунок політик блокування облікових записів:

- Політика блокування облікового запису після невдалих спроб входу.

- Політика часового обмеження блокування облікового запису.

7. Політика "Порогового значення блокування" - це налаштування, яке визначає, після скількох невдалих спроб входу в обліковий запис користувача обліковий запис буде заблоковано на певний час або до втручання адміністратора. Наприклад, якщо ця політика встановлена на 3, то після 3 невдалих спроб входу обліковий запис буде заблоковано.

8. Коротка характеристика кожної політики блокування облікових записів:

- \*Політика блокування облікового запису після невдалих спроб входу\*: Визначає кількість невдалих спроб входу, після яких обліковий запис буде заблоковано.

- \*Політика часового обмеження блокування облікового запису\*: Вказує, на скільки хвилин або годин обліковий запис буде заблоковано після досягнення порогового значення невдалих спроб входу.

9. Як поставити правило блокування так, щоб обліковий запис автоматично розблокувався після 2 хвилин:

a. Відкрийте "Політика локальної системи" через "secpol.msc".

b. Перейдіть до "Локальні політики" -> "Безпека" -> "Політика блокування облікового запису".

c. Знайдіть "Часове обмеження блокування облікового запису" та встановіть бажаний час блокування (2 хвилини).

10. Як вручну розблокувати обліковий запис:

a. Відкрийте "Диспетчер завдань" (Task Manager) за допомогою комбінації клавіш "Ctrl + Alt + Delete" або "Ctrl + Shift + Esc".

b. Вкладка "Подробиці" (Details) або "Процеси" (Processes) (залежно від версії Windows).

c. Знайдіть процес "explorer.exe" та виберіть його.

d. Натисніть "Завершити завдання" (End Task).

e. Після цього виберіть "Файл" (File) в верхньому лівому куті і оберіть "Запустити нове завдання" (Run New Task).

f. Введіть "explorer.exe" і натисніть "Enter".

g. Робочий стіл та обліковий запис будуть розблоковані.