**Міністерство Освіти І НАУКИ України**

**Національний університет "Львівська політехніка"**

Інститут **КНІТ**

Кафедра **ПЗ**

### ЗВІТ

До лабораторної роботи № 4

**З дисципліни:** *“Основи системного адміністрування”*

**На тему:** *“Реалізація механізму групових політик у Windows 10. Аналіз і налаштування безпеки”*

**Лектор:**

проф. каф. ПЗ

Фечан А.В.

**Виконав:**

ст. гр. ПЗ-45

Хруставчук М.Л.

**Прийняв:**

проф. каф. ПЗ

ФечанА.В.

« \_\_\_\_ » \_\_\_\_\_\_\_\_ 2025 р.

∑= \_\_\_\_\_ .

Львів – 2025

**Тема роботи:** Реалізація механізму групових політик у Windows 10. Аналіз і налаштування безпеки.

**Мета роботи:** Ознайомлення зі структурою, принципом роботи та налаштуванням об’єкта групової політики на локальному комп’ютері під управлінням ОС Windows 10. Навчитись використовувати та створювати шаблони безпеки для ефективного налаштування та аналізу типових параметрів безпеки.

**TЕОРЕТИЧНІ ВІДОМОСТІ**

Групові політики (Group Policy) у Windows – це потужний механізм централізованого керування параметрами операційної системи, безпеки та робочого середовища користувачів. Вони дозволяють адміністраторам автоматизувати налаштування системи, контролювати доступ до ресурсів, застосовувати обмеження та політики безпеки для користувачів і комп’ютерів.

Об’єкт групової політики (GPO – Group Policy Object) містить набір параметрів, які поділяються на дві основні категорії:

* Computer Configuration – політики, що впливають на налаштування комп’ютера незалежно від користувача.
* User Configuration – політики, що застосовуються до конкретних облікових записів користувачів.

Основний інструмент для роботи з політиками – оснастка “Local Group Policy Editor” (gpedit.msc). Вона дозволяє змінювати параметри безпеки, доступу, керування обліковими записами, оновленнями, мережевими службами тощо. Наприклад, у гілках Password Policy задаються вимоги до складності паролів, їх мінімальної довжини та часу дії, а в Account Lockout Policy – параметри блокування облікових записів після кількох невдалих входів. Також через User Rights Assignment можна керувати правами користувачів і обмежувати їхні дії. Administrative Templates забезпечують можливість стандартизувати робоче середовище, а політики безпеки – підвищити рівень захисту даних і стабільність системи.

**ЗАВДАННЯ**

1. В оснастці *Group Policy* задати мінімальну довжину пароля та параметри складності, перевіривши неможливість створення пароля, що не відповідає політиці.
2. У політиках безпеки встановити поріг блокування облікового запису, перевірити блокування після кількох помилкових входів і зняти його через *Local Users and Groups*.
3. У *User Rights Assignment* дозволити вимкнення комп’ютера лише адміністраторам та перевірити відсутність цього пункту у звичайного користувача.
4. В *Administrative Templates* увімкнути політику, що видаляє значок «Display» з панелі керування, і переконатись у її застосуванні до всіх користувачів.
5. У *Software Restriction Policies* створити правило, що забороняє запуск програм із усіх томів, крім «C:», та виняток за хешем для дозволеного файлу.
6. Відкрити оснастку *Security Configuration and Analysis* і створити базу даних для аналізу стану політик системи за шаблоном.

**ХІД ВИКОНАННЯ**

**1. В оснастці *Group Policy* задав мінімальну довжину пароля та параметри складності, перевірив неможливість створення пароля, що не відповідає політиці.**

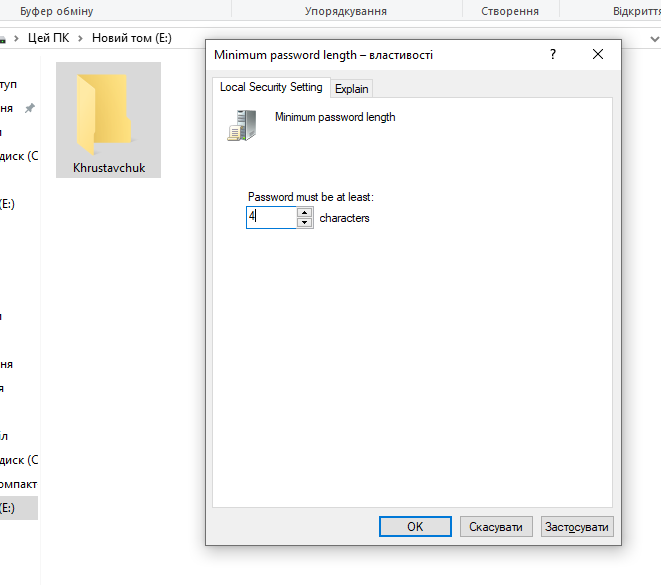


Рис. 1. Властивості параметру безпеки

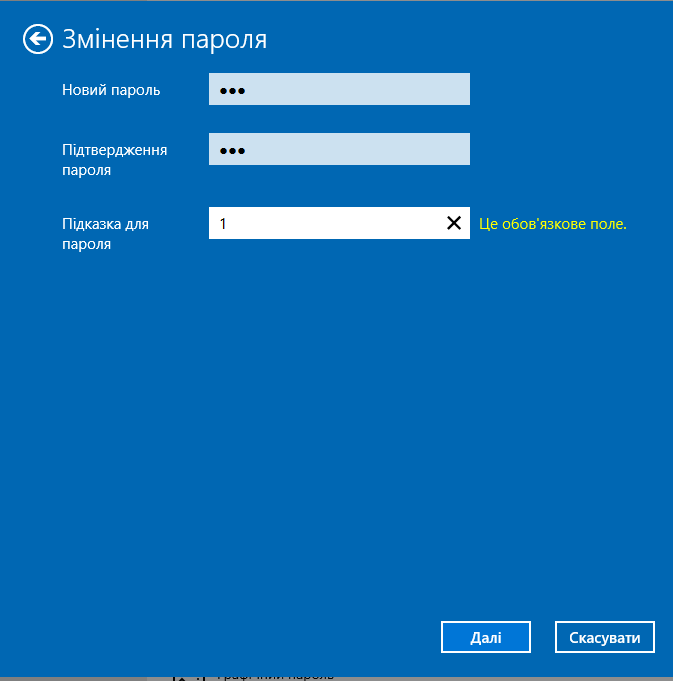


Рис. 2. Зміна паролю

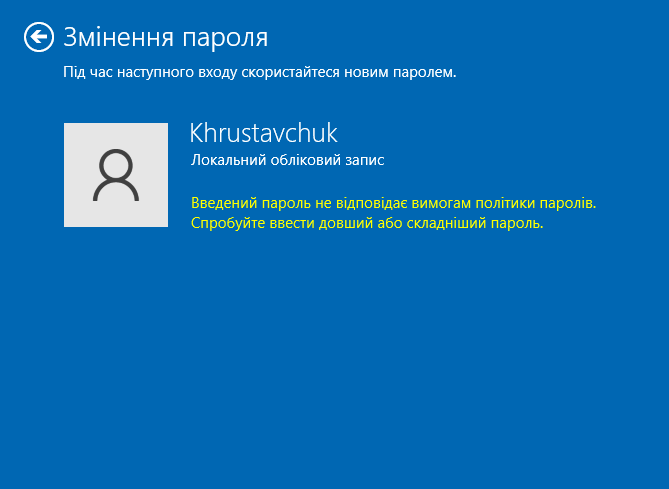


Рис. 3. Повідомлення системи про невідповідність параметру значенню політики

**2. У політиках безпеки встановив поріг блокування облікового запису, перевірив блокування після кількох помилкових входів і зняв його через *Local Users and Groups*.**

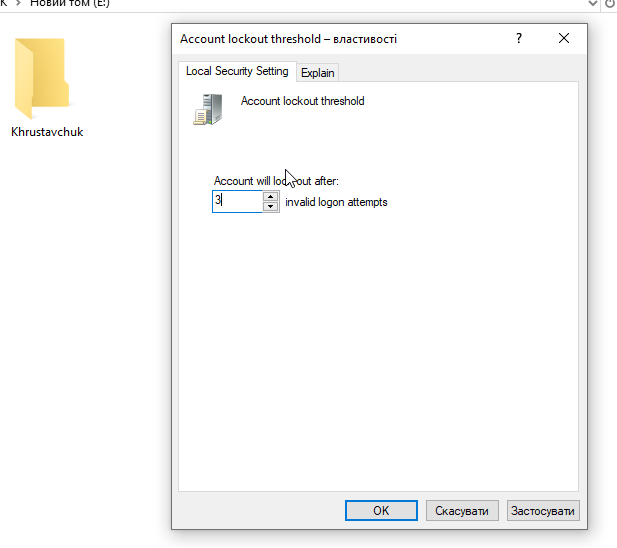


Рис. 4. Встановлення граничного значення блокування облікового запису

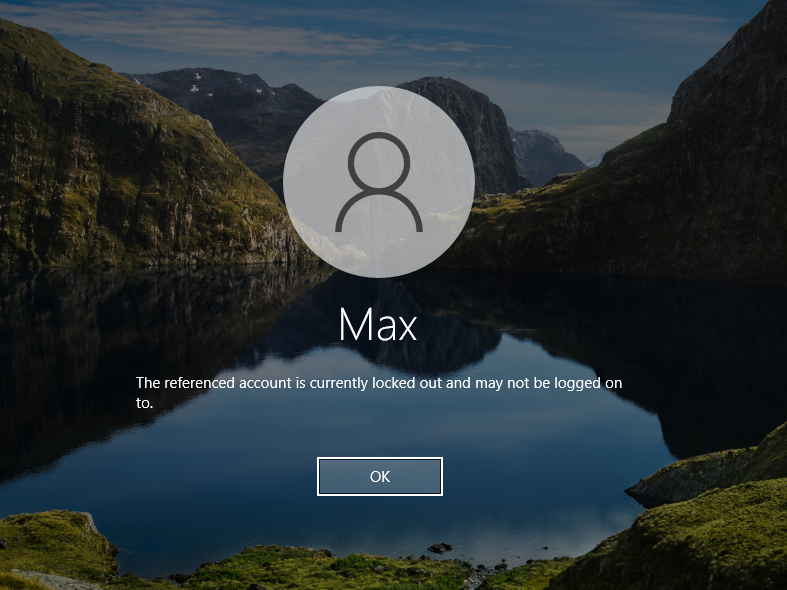


Рис. 5. Повідомлення системи про блокування облікового запису

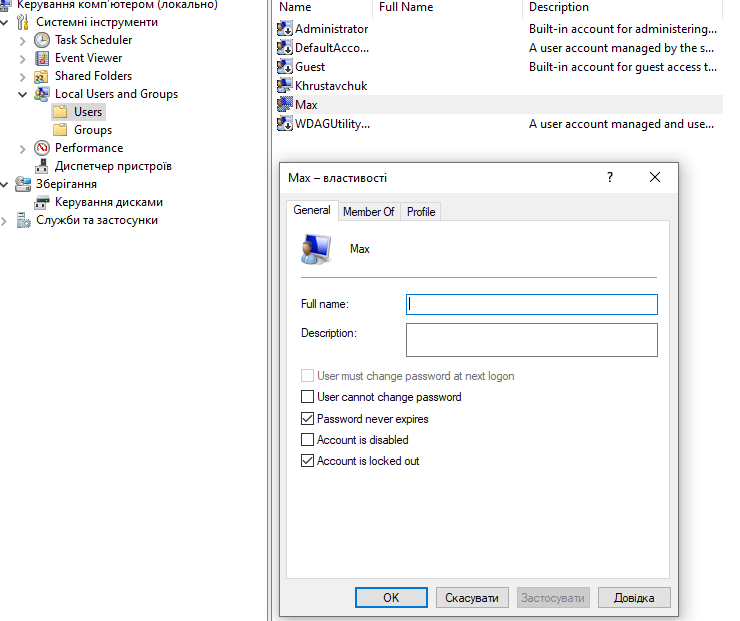


Рис. 6. Властивості заблокованого облікового запису

**3. У *User Rights Assignment* дозволив вимкнення комп’ютера лише адміністраторам та перевірив відсутність цього пункту у звичайного користувача.**

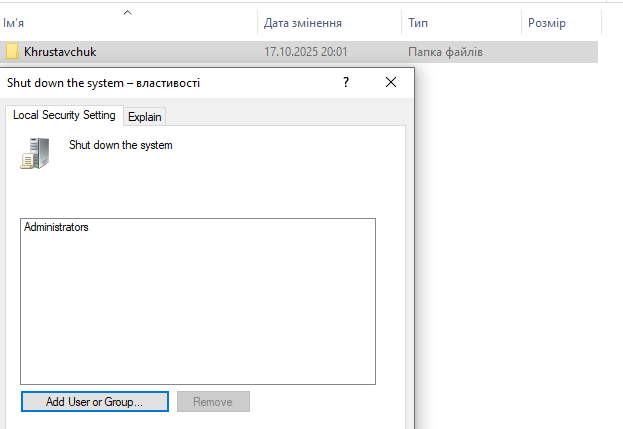


Рис. 7. Властивості параметру прав користувачів на завершення роботи системи

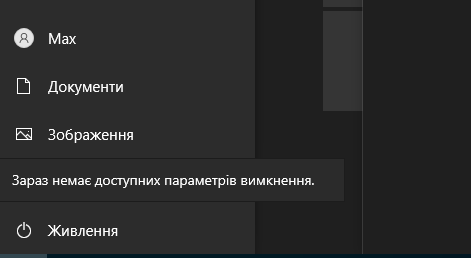


Рис. 8. Результат виконання політики стосовно заборони користувачу завершення роботи системи

**4. В *Administrative Templates* увімкнув політику, що видаляє значок «Display» з панелі керування, і переконався у її застосуванні до всіх користувачів.**

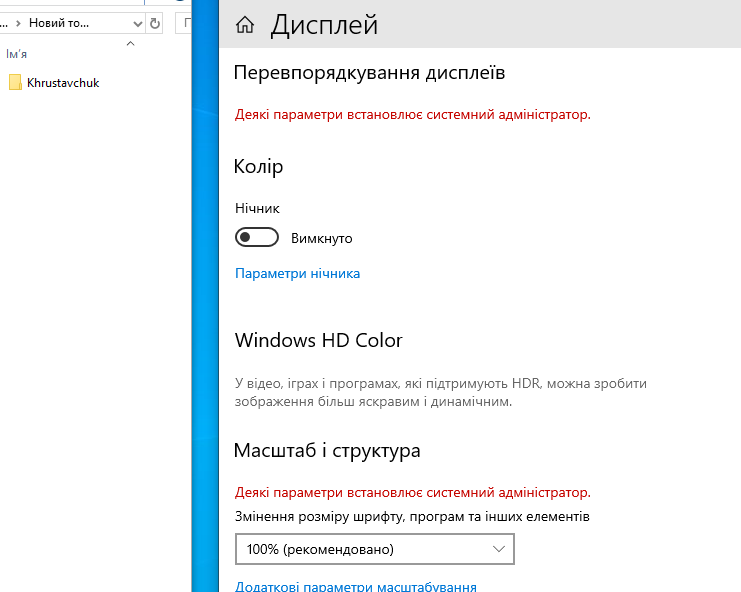


Рис. 9. Повідомлення системи щодо заборони виконання певних налаштувань робочого середовища

**5. У *Software Restriction Policies* створити правило, що забороняє запуск програм із усіх томів, крім «C:», та виняток за хешем для дозволеного файлу.**

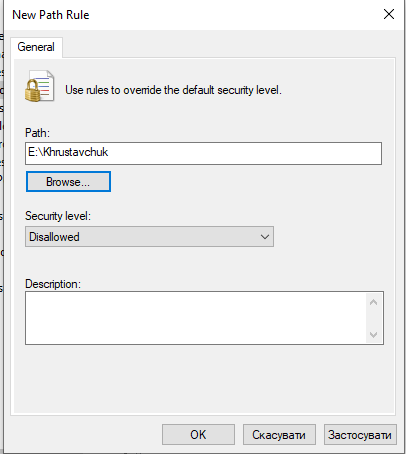


Рис. 10. Властивості правила обмеженого використання програм

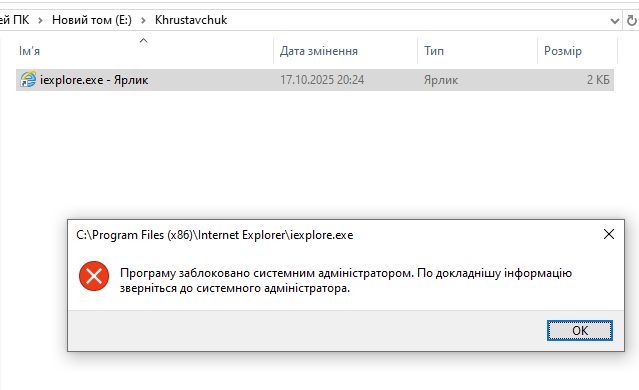


Рис. 11. Повідомлення системи про заборону виконання програми

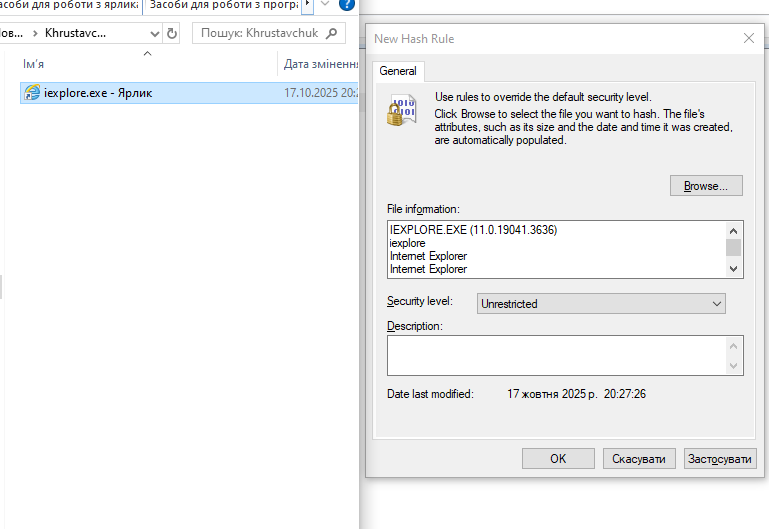


Рис. 12. Створення правила для хешу

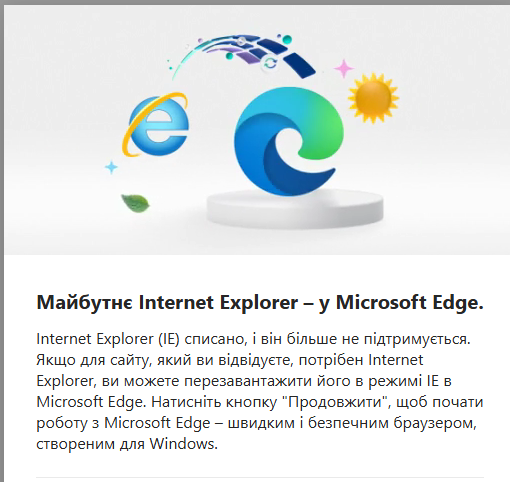


Рис. 13. Виконання файлу

**6. Відкрив оснастку *Security Configuration and Analysis* і створив базу даних для аналізу стану політик системи за шаблоном.**

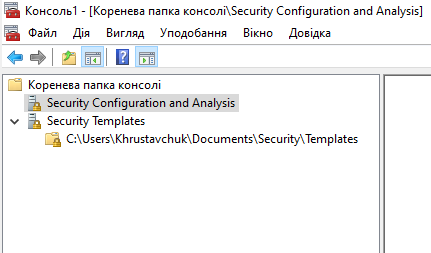


Рис. 14. Оснащення "Security Configuration and Analysis"

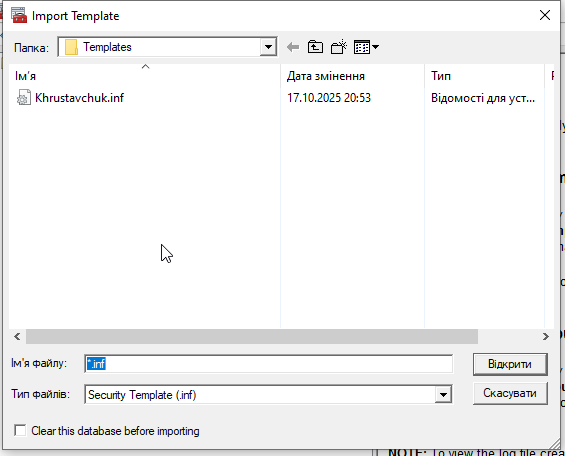


Рис. 15. Створення власних шаблонів

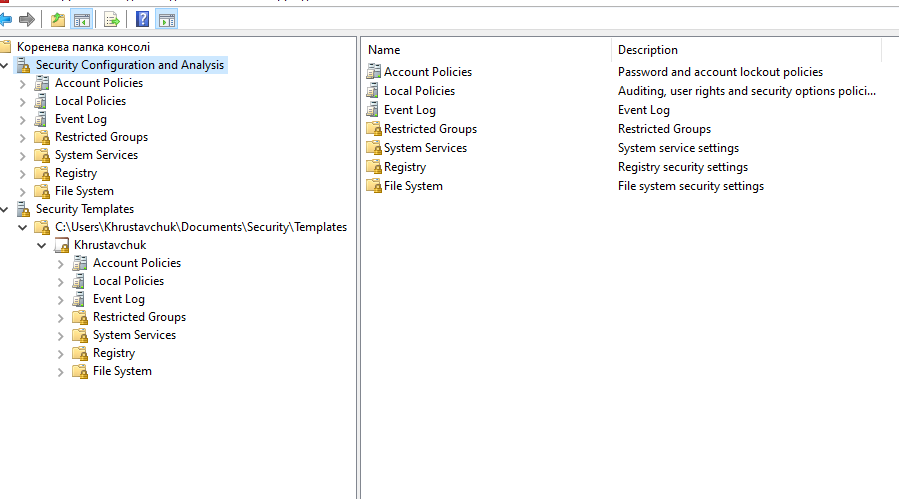


Рис. 16. Результат аналізу безпеки системи

**ВИСНОВКИ**

У ході лабораторної роботи було вивчено механізм групових політик Windows 10 та принципи їх застосування для керування безпекою системи. Практично налаштовано політики паролів, блокування облікових записів, привілеї користувачів і адміністративні шаблони. Продемонстровано, як за допомогою групових політик можна централізовано контролювати параметри системи та обмежувати дії користувачів. Отримані навички є основою для ефективного адміністрування і захисту інформації у корпоративному середовищі.