**Міністерство Освіти І НАУКИ України**

**Національний університет "Львівська політехніка"**

Інститут **КНІТ**

Кафедра **ПЗ**

### ЗВІТ

До лабораторної роботи № 5

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

**На тему:** *“Аудит. Політики аудиту. Робота з журналом безпеки Windows”*

**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:** Аудит. Політики аудиту. Робота з журналом безпеки Windows.

**Мета роботи:** Ознайомлення з політиками та налаштуванням аудиту, аналізом безпеки системи шляхом вивчення журналу подій в Windows 10. Навчитись проводити аудит локальної системи та працювати з журналом безпеки Windows.

**TЕОРЕТИЧНІ ВІДОМОСТІ**

Аудит у Windows – це механізм контролю дій користувачів і системних процесів, який дозволяє відстежувати події, пов’язані з безпекою: спроби входу в систему, доступ до файлів, зміну політик, видалення чи створення об’єктів. Основною метою аудиту є своєчасне виявлення несанкціонованих дій та аналіз активності для забезпечення інформаційної безпеки.

Політики аудиту налаштовуються через локальні або групові політики. Серед основних типів подій аудиту: Logon Events, Account Management, Object Access, Policy Change, Privilege Use, System Events тощо. Для кожного типу можна вказати фіксацію успішних, невдалих або обох типів спроб.

Записи результатів аудиту зберігаються у журналі безпеки (Security Log), який можна переглядати через оснастку Event Viewer. У записах міститься інформація про користувача, дату, тип події, код і опис результату. За допомогою цих даних адміністратор може визначити, хто і коли здійснив певну дію.

Для спостереження за конкретними об’єктами (папками, файлами, реєстром) потрібно у властивостях об’єкта активувати вкладку «Аудит» і вибрати користувачів та типи дій, які контролюються (наприклад, створення, читання або видалення). Аудит ефективно поєднується з правами доступу NTFS і груповими політиками, забезпечуючи комплексний контроль дій користувачів.

Завдяки правильно налаштованому аудиту можна виявляти порушення безпеки, аналізувати інциденти, збирати докази під час розслідування, а також підвищувати загальний рівень захищеності системи.

**ЗАВДАННЯ**

1. Увімкнути аудит доступу до об’єктів у «Груповій політиці» та задати контроль дій користувачів.
2. Створити файл, видалити його під іншим користувачем і перевірити запис у журналі подій.
3. Активувати аудит змін політик, системних подій і входу в систему та переглянути результати в журналі безпеки.
4. Увімкнути політику «Не затирати події», заповнити журнал, перевірити блокування входу й очистити записи адміністратором.

**ХІД ВИКОНАННЯ**

**1. Увімкнув аудит доступу до об’єктів у «Груповій політиці» та задав контроль дій користувачів.**

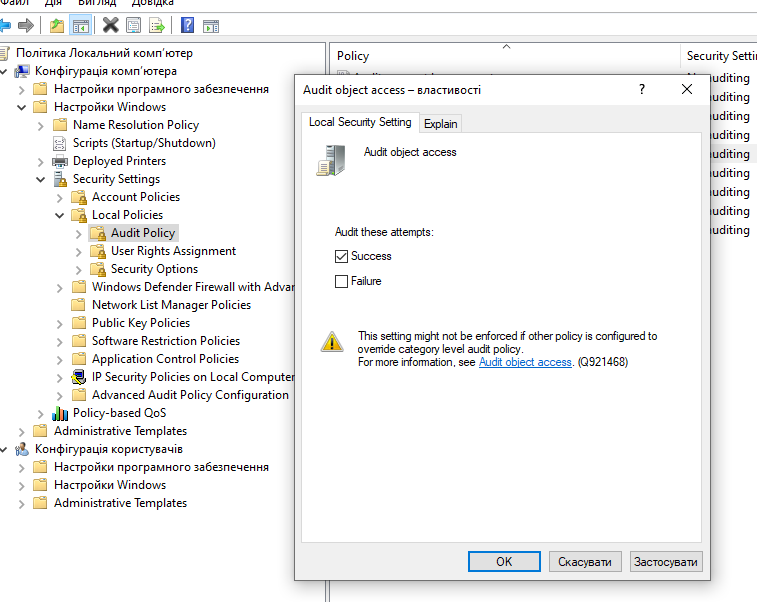


Рис. 1. Включення політики аудиту

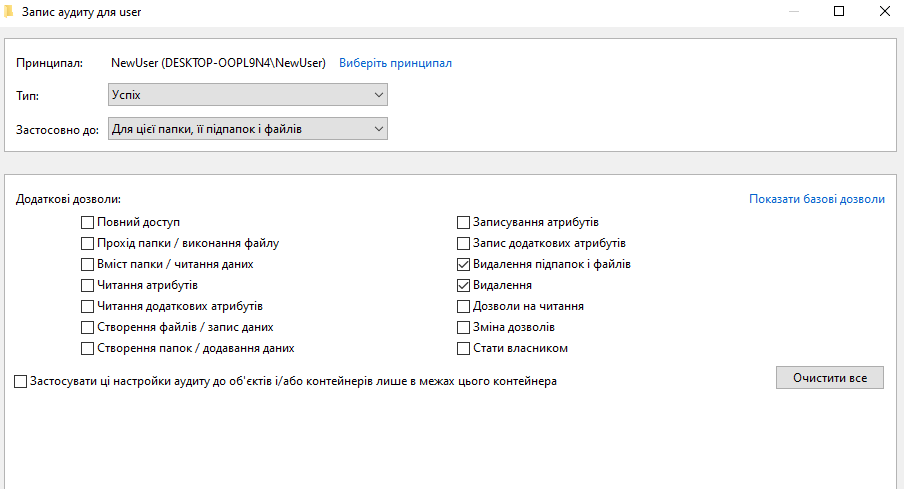


Рис. 2. Налаштування аудиту

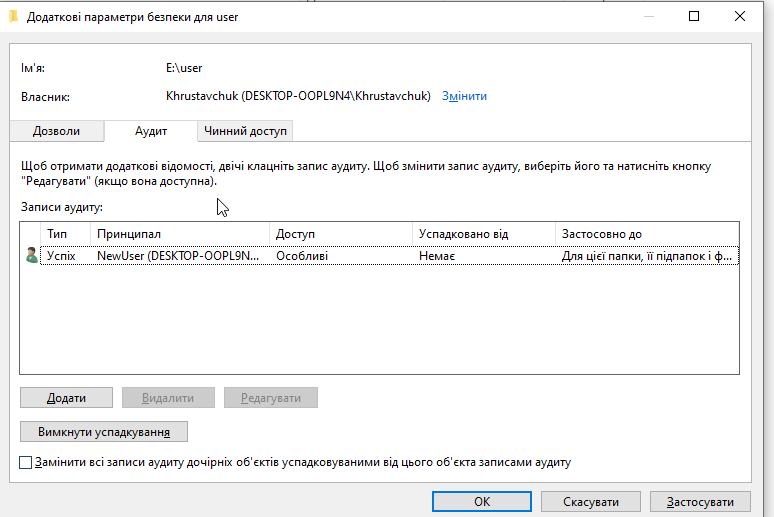


Рис. 3. Повідомлення системи про невідповідність параметру значенню політики

**2. Створив файл, видалив його під іншим користувачем і перевірив запис у журналі подій.**

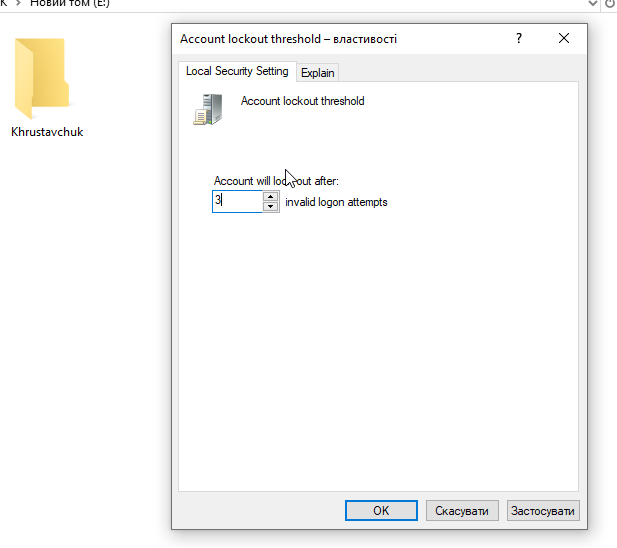


Рис. 4. Встановлення граничного значення блокування облікового запису

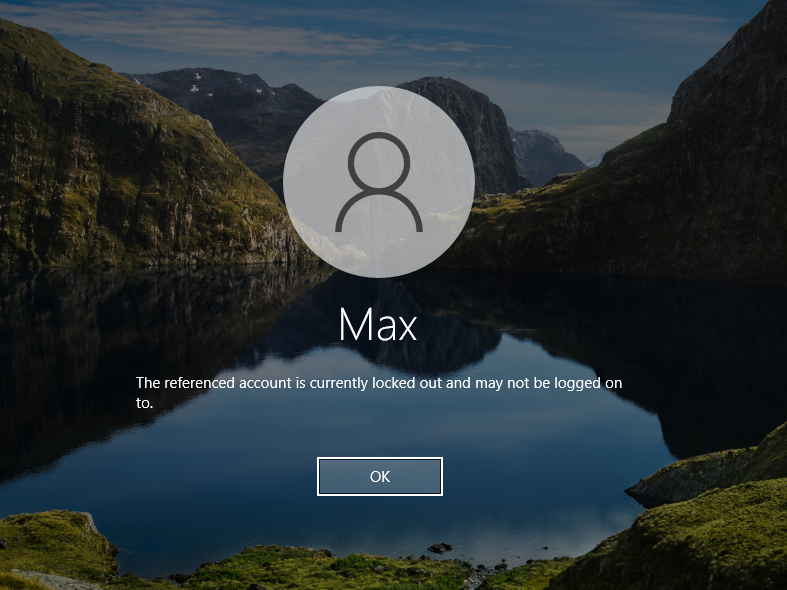


Рис. 5. Повідомлення системи про блокування облікового запису

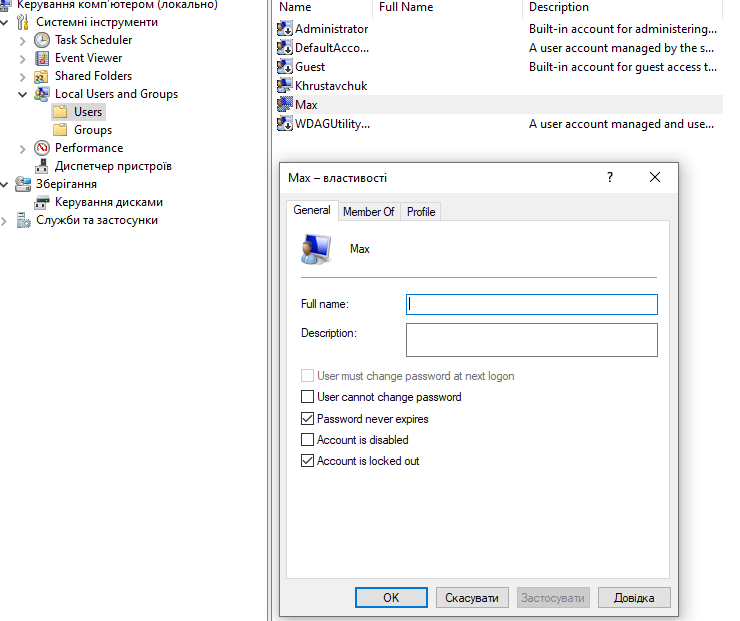


Рис. 6. Властивості заблокованого облікового запису

**3. Активувати аудит змін політик, системних подій і входу в систему та переглянути результати в журналі безпеки.**

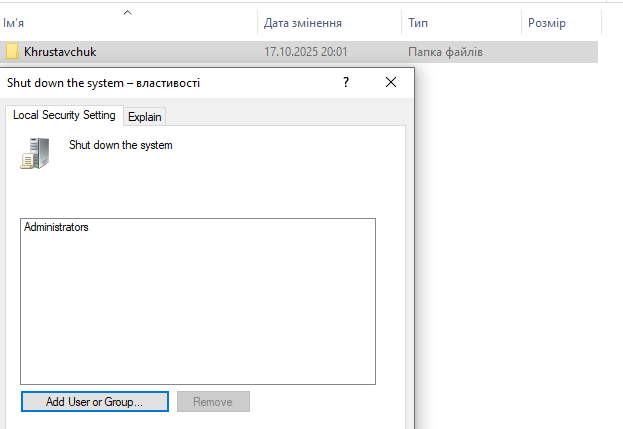


Рис. 7. Властивості параметру прав користувачів на завершення роботи системи

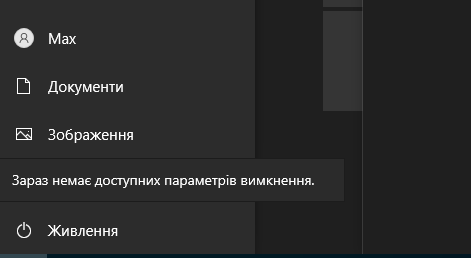


Рис. 8. Результат виконання політики стосовно заборони користувачу завершення роботи системи

**4. Увімкнути політику «Не затирати події», заповнити журнал, перевірити блокування входу й очистити записи адміністратором.**

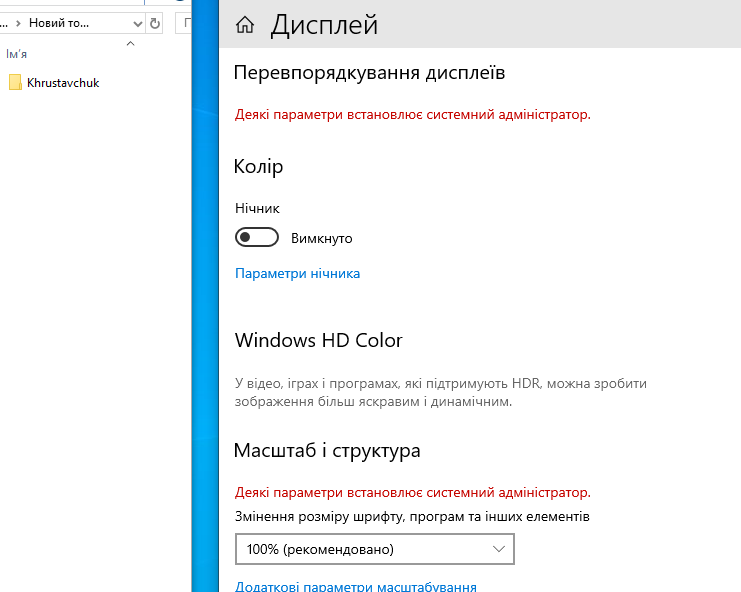


Рис. 9. Повідомлення системи щодо заборони виконання певних налаштувань робочого середовища

**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.