**Міністерство Освіти І НАУКИ України**

**Національний університет "Львівська політехніка"**

Інститут **КНІТ**

Кафедра **ПЗ**

### ЗВІТ

До лабораторної роботи № 3

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

**На тему:** *“Дозволи та квоти NTFS. Шифрування файлів: EFS”*

**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:** Дозволи та квоти NTFS. Шифрування файлів: EFS.

**Мета роботи:** Навчитись ефективно налагоджувати систему логічного розділення доступу до об’єктів файлової системи в ОС Windows 10; управляти квотами на томах NTFS та використовувати шифровану файлову систему EFS.

**TЕОРЕТИЧНІ ВІДОМОСТІ**

Встановлюючи користувачам певні дозволи на доступ до файлів і каталогів (папок), адміністратори системи можуть захищати конфіденційну інформацію від несанкціонованого доступу. Кожен користувач має певний набір дозволів на доступ до кожного об’єкту файлової системи.

Адміністрування великих комп’ютерних мереж, де сервери підтримують роботу сотень користувачів, зв’язане з рядом складнощів. Одна з них – облік дискового простору серверу, зайнятого файлами співробітників компанії. Як правило, користувачі, що зберігають свої файли на сервері, мало піклуються про актуальність інформації і про знищення застарілих або непотрібних даних.

Безліч тимчасових файлів і копій одного й того ж файлу, що знаходяться в різних папках, лише посилюють ситуацію. В результаті в лічені місяці навіть на великих жорстких дисках серверу може не виявитися необхідного для роботи вільного простору.

Після установки квот дискового простору користувач зможе зберігати на томі обмежений об’єм даних, тоді як на цьому томі може залишатися вільний простір. Якщо користувач перевищує видану йому квоту, в журнал подій вноситься відповідний запис. Потім, залежно від конфігурації системи, користувач або зможе записати інформацію на том («м’який» режим обмежень), або йому буде відмовлено в записі через відсутність вільного простору («жорсткий» режим). Квоти можна використовувати на локальних і спільних мережних дисках (в цьому випадку загальний доступ повинен бути дозволений на рівні кореневого каталогу тому). Стиснення файлів не має значення при обчисленні зайнятого простору – завжди враховується розмір початкового нестиснутого файлу.

**ЗАВДАННЯ**

1. Створити на томі NTFS папку, налаштувати дозволи через вкладку "Безпека", щоб дозволити створення файлів і папок, але заборонити видалення.
2. Увійти під іншим користувачем, створити підпапку, перевірити доступи, заборонити групі «Administrators» доступ.
3. Увійти як адміністратор, перевірити доступ до підпапки, змінити власника та переглянути зміни в списку доступу.
4. Використати "Замінити всі дозволи дочірнього…" для синхронізації дозволів із батьківською папкою.
5. Включити квоти на тому NTFS і створити індивідуальний запис квоти для користувача.
6. Створити агента відновлення шифрованих даних.
7. Зашифрувати файли для кількох користувачів, перевірити доступ до шифрованих файлів і створення сертифіката EFS.

**ХІД ВИКОНАННЯ**

1. **Створив на томі NTFS папку, налаштував дозволи через вкладку "Безпека", щоб дозволити створення файлів і папок, але заборонити видалення.**

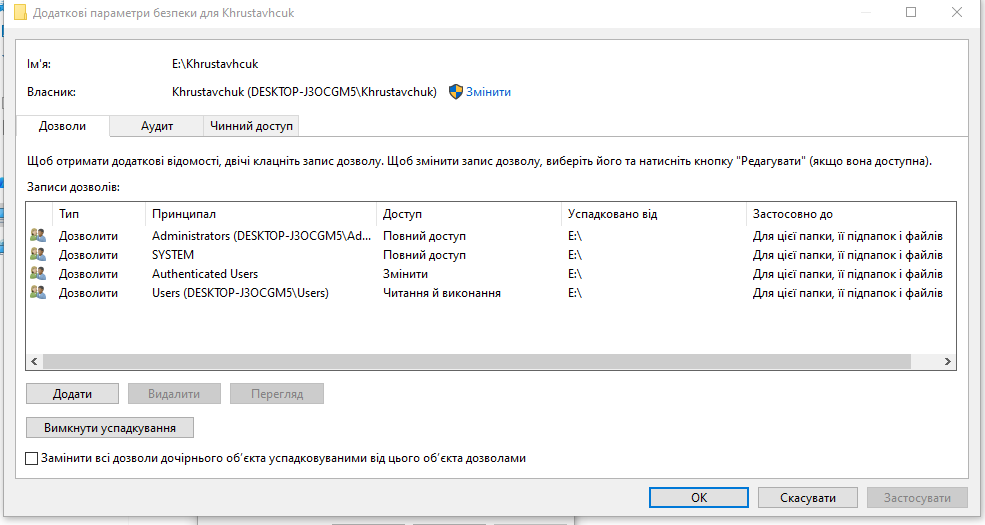


Рис. 1. Додаткові параметри налаштувань безпеки

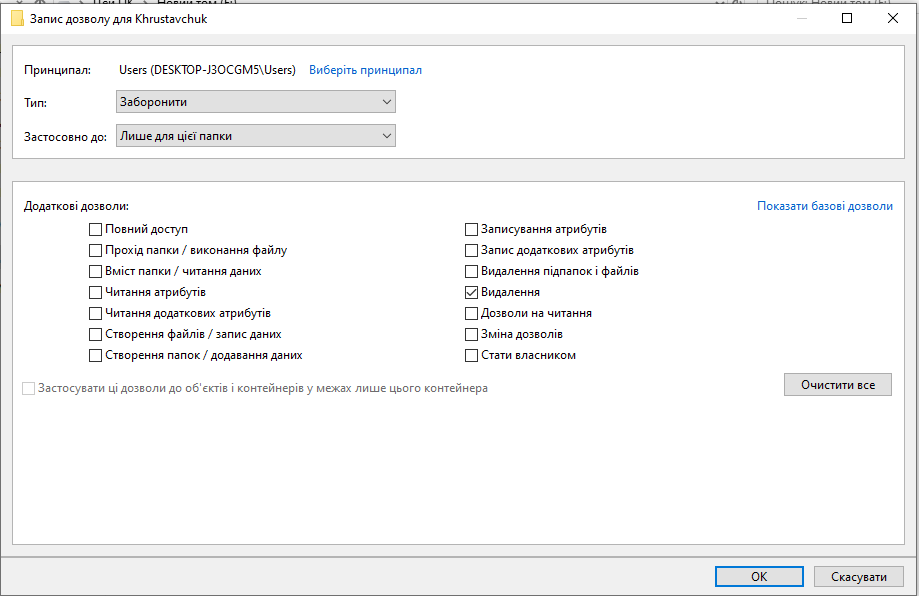


Рис. 2. Задання дозволів

1. **Увійшов під іншим користувачем, створив підпапку, перевірив доступи, заборонив групі «Administrators» доступ.**

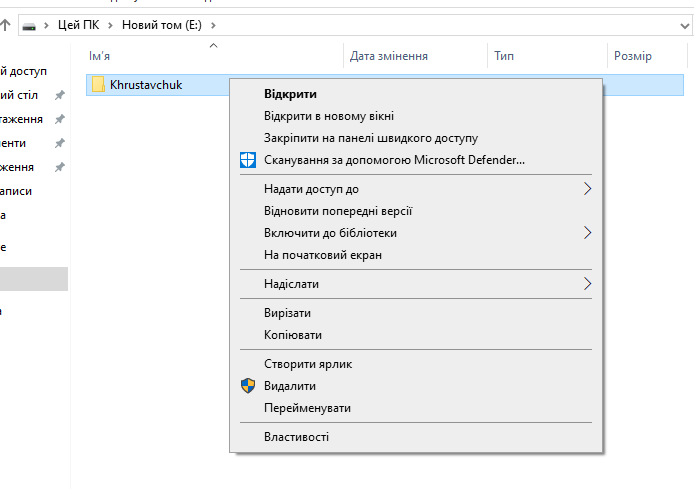


Рис. 3. Заборона видалення

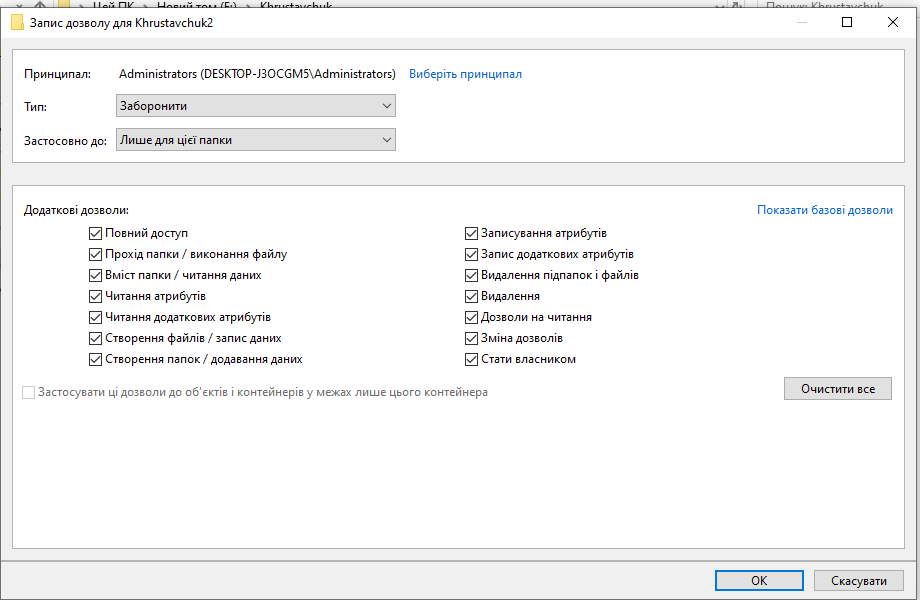


Рис. 4. Повна заборона доступу до підпапки

1. **Увійшов як адміністратор, перевірив доступ до підпапки, змінив власника та переглянув зміни в списку доступу.**

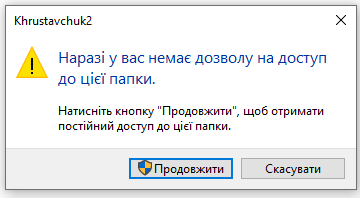


Рис. 5. Повідомлення системи про відмову в доступі на виконання операції

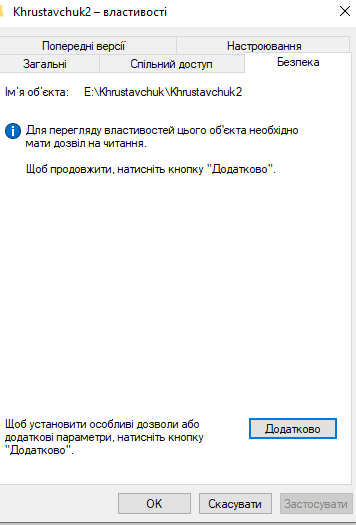


Рис. 6. Повідомлення системи безпеки

Це повідомлення означає, що поточний користувач не має дозволу на читання властивостей цього об’єкта (папки). Щоб переглянути чи змінити права доступу, потрібно натиснути «Додатково» і виконати дію з правами адміністратора або власника об’єкта.

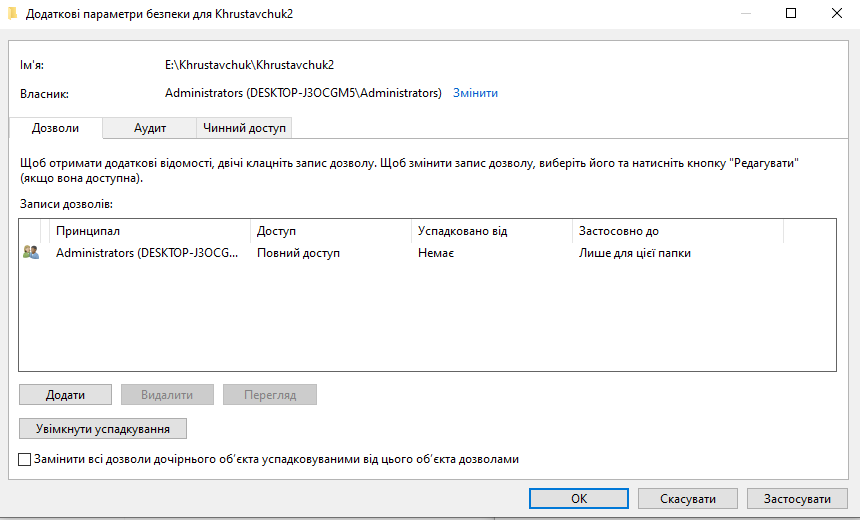


Рис. 7. Надання доступу

1. **Використав "Замінити всі дозволи дочірнього…" для синхронізації дозволів із батьківською папкою.**

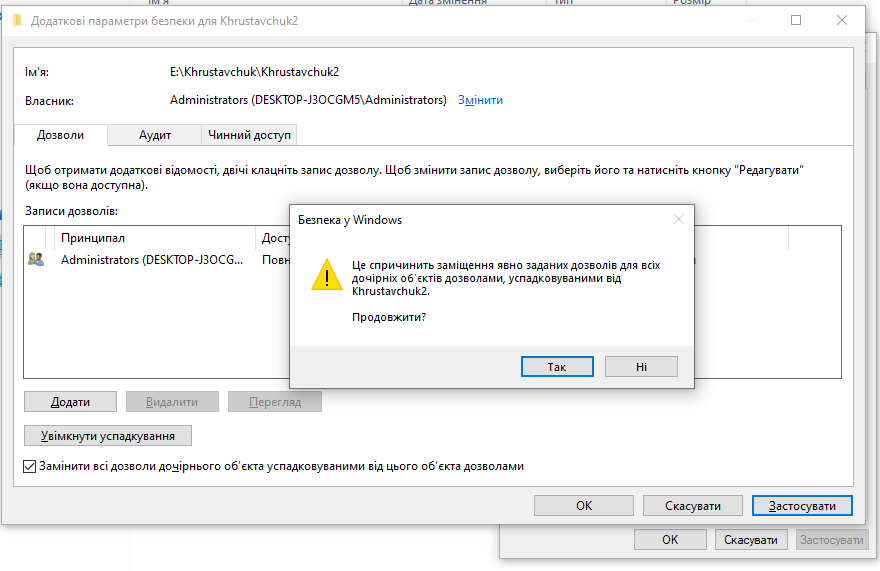


Рис. 8. Заміна дозволів

1. **Включив квоти на тому NTFS і створив індивідуальний запис квоти для користувача.**

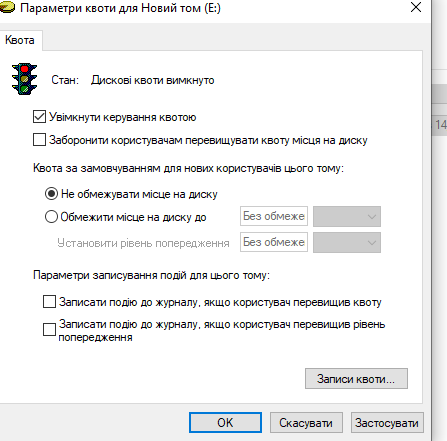


Рис. 9. Вкладка квот у властивостях дискового тому

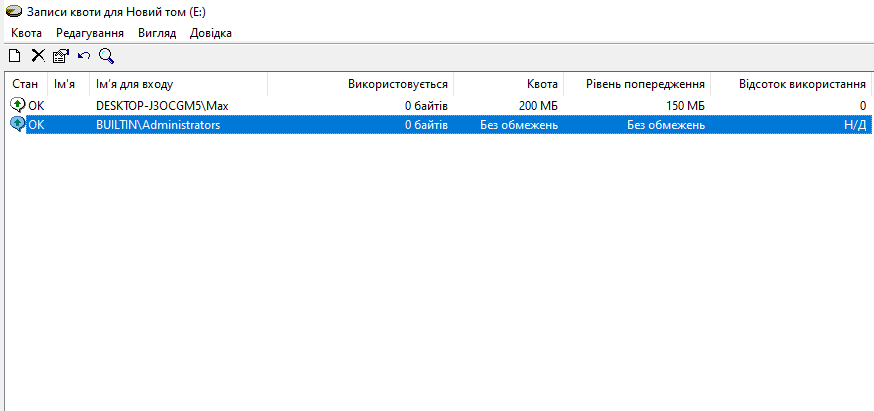


Рис. 10. Вікно записів квот для дискового тому

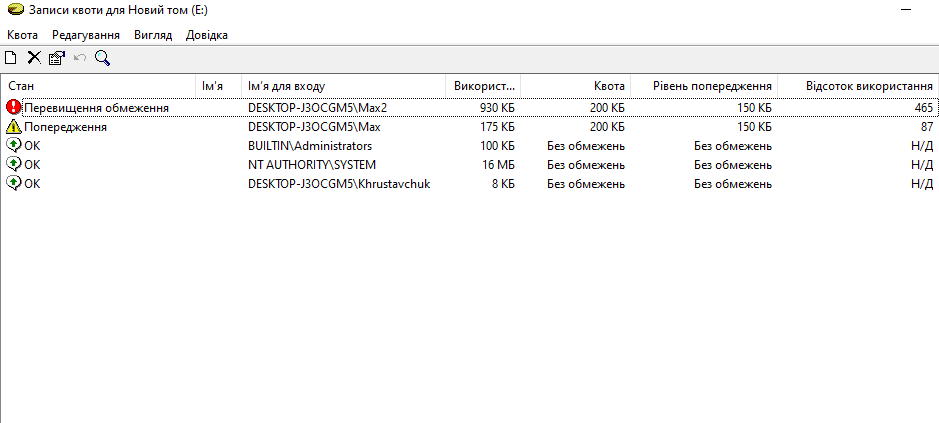


Рис. 11. Вікно записів квот для дискового тому (один користувач перевищив поріг квоти, а один – поріг попереджень)

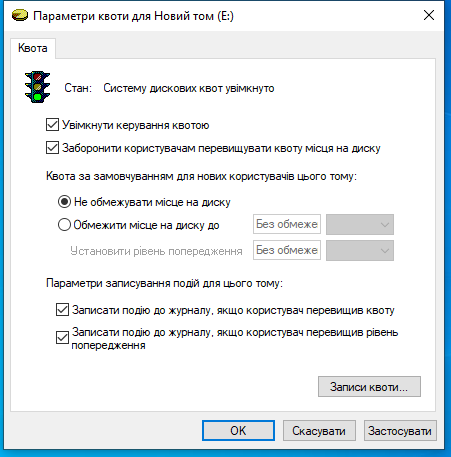


Рис. 12. Заборона перевищення квоти місця

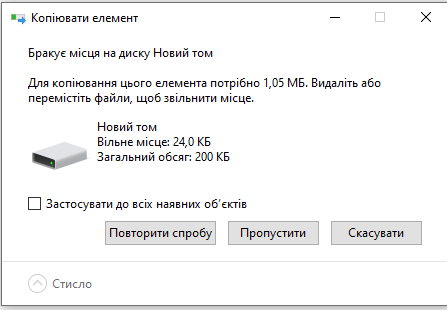


Рис. 13. Заборона операції

1. **Створив агента відновлення шифрованих даних**

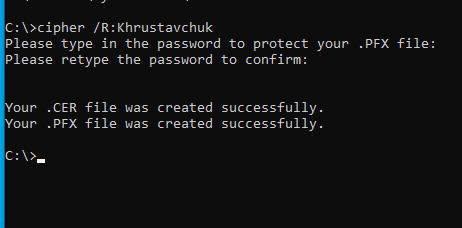


Рис. 14. Створення сертифікату агента відновлення

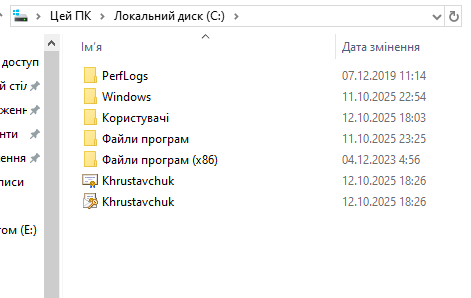


Рис. 15. Створені файли

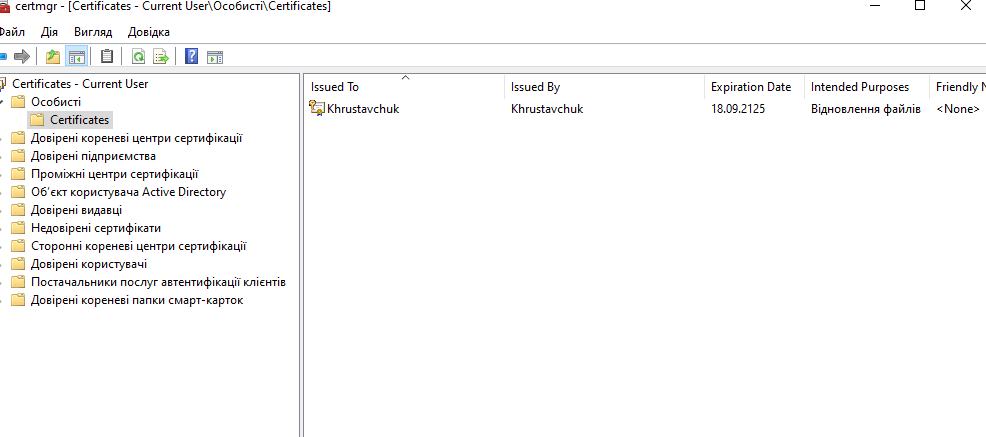


Рис. 16. Імпортований сертифікат

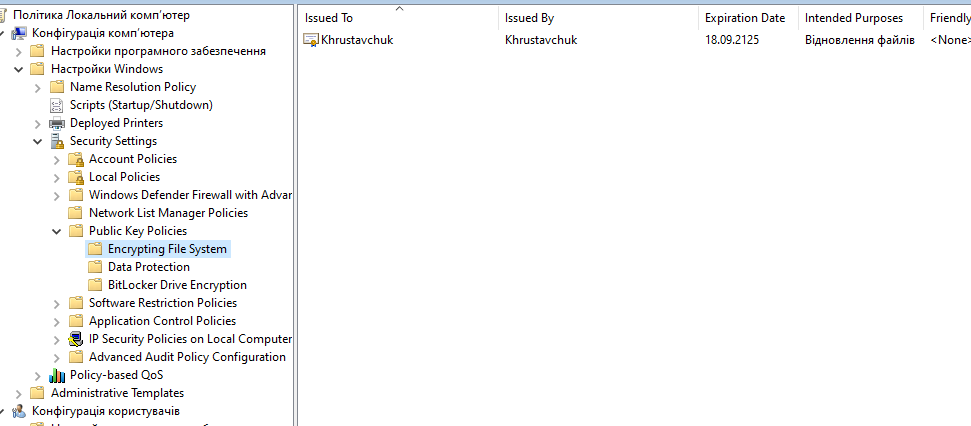


Рис. 17. Сертифікат

1. **Зашифрував файли для кількох користувачів, перевірив доступ до шифрованих файлів і створення сертифіката EFS**

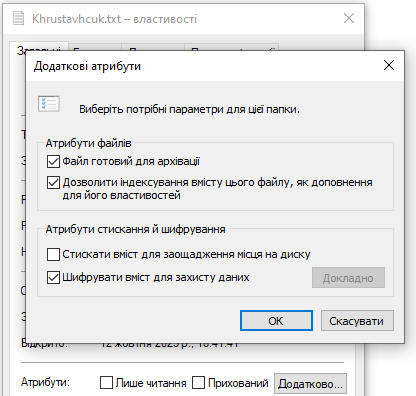


Рис. 18. Встановлення додаткових атрибутів файлу

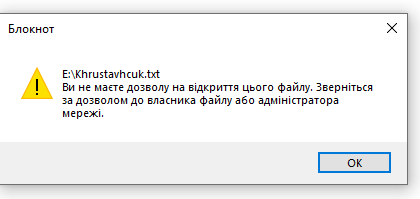


Рис. 19. Заборона дозволу до зашифрованого файлу іншому користувачу

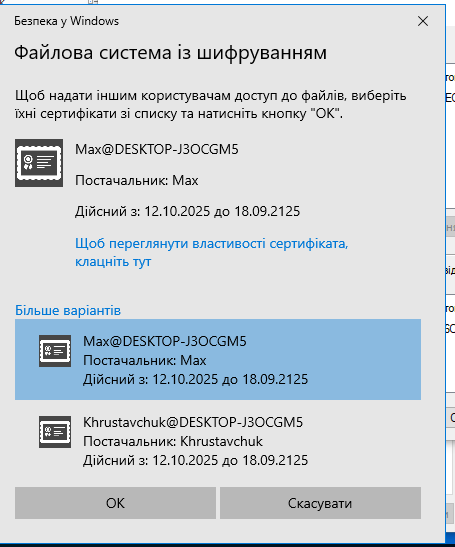


Рис. 20. Доступ на спільне розшифрування

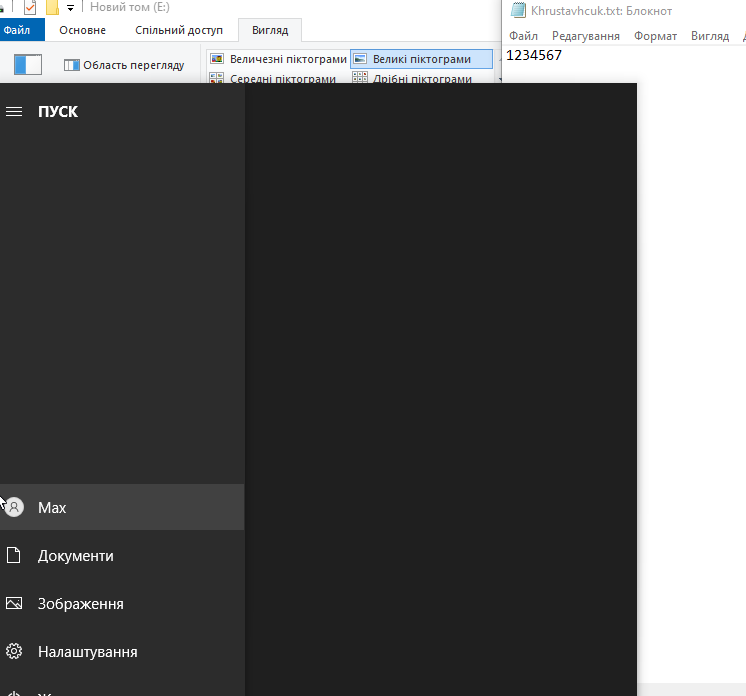


Рис. 21. Перевірка спільного розшифрування

**ВИСНОВКИ**

У результаті виконання лабораторної роботи було досліджено механізм керування доступом і квотами у файловій системі NTFS, а також застосування шифрування EFS для захисту даних. Було налаштовано права доступу до папок, створено облікові записи користувачів із різними рівнями дозволів та перевірено дію обмежень. Також реалізовано шифрування файлів і роботу агента відновлення даних. Отримані навички дозволяють ефективно забезпечувати контроль безпеки та захист інформації у середовищі Windows 10.