****

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Рівненський фаховий коледж інформаційних технологій**

**Звіт**

**Про виконання лабораторної роботи №2**

**Цілісність і резервне копіювання даних.**

**Виконав**

**Студент 3 курсу групи КН-3/1**

**Валерій ФОРМАНЮК**

**13.09.2025 р.**

**м.Рівне**

**Лабораторна робота №2**

# **Тема: Цілісність і резервне копіювання даних**.

# **МЕТА РОБОТИ:**

Ознайомитися з методами забезпечення **цілісності даних**.

Навчитися використовувати **хеш-функції** для перевірки змін у файлах.

Освоїти базові підходи до **резервного копіювання** та **відновлення інформації**.

# **1. Обладнання та ПЗ:**

ПК з Windows.

Командний рядок Windows: certutil для обчислення хешів.

Програма для архівації: 7 - Zip.

Хмарний диск (Google Drive) або зовнішній USB.

# **2. Теоретичні відомості:**

## Цілісність даних - властивість, що гарантує відсутність

несанкціонованих змін.

Основний метод контролю цілісності: хешування.

## Популярні алгоритми:

SHA-256,

SHA-3 (актуальні),

MD5 (застарілий, використовується для демонстрацій).

## Резервне копіювання (backup):

повне (full),

інкрементальне (incremental),

диференціальне (differential).

## Засоби: вбудовані утиліти ОС, хмарні сервіси, зовнішні носії.

# **3. Хід роботи.**

## **Контроль цілісності файлів.**

Вибрати будь-який текстовий файл (наприклад, lab2.txt).

Обчислити його хеш у алгоритмах MD5 та ІРФ-256.

Windows:

certutil -hashfile lab2.txt MD5

certutil -hashfile lab2.txt SHA-256.

Внести зміни у файл і повторити обчислення хешів.

Порівняти результати та зробити висновок.

## **Резервне копіювання.**

Створити папку з кількома файлами (lab\_backup).

Виконати її архівацію у форматі ZIP.

Зберегти копію на зовнішньому носії або хмарному диску.

## **Відновлення даних.**

Видалити один із файлів у вихідній папці.

Розпакувати архів і відновити видалений файл.

# **4. Контрольні питання.**

## Чим відрізняється повне, інкрементальне і диференціальне резервне копіювання?

1. Чому MD5 вважається ненадійним для перевірки цілісності?
2. Наведіть приклади, коли порушення цілісності може призвести до критичних наслідків?
3. Як організувати регулярне резервне копіювання в ОС Windows?
4. Які недоліки у використанні лише резервних копій без хеш-контролю?

# **5. Форма звіту.**

1. Титульний аркуш.
2. Мета роботи.
3. Скріншоти/результати:

обчислення хешів,

архівування і відновлення даних.

1. Таблиця результатів:

| **Файл** | **Алгоритм** | **Хеш (до змін)** | **Хеш (після змін)** | **Висновок** |
| --- | --- | --- | --- | --- |

1. Висновки.

Шаблон таблиці для Лабораторної роботи №2

хешування

| № | Файл | Алгоритм хешування | Хеш (до змін) | Хеш (після змін) | Висновок(змінився/не змінився) |
| --- | --- | --- | --- | --- | --- |
| 1 | lab2.txt | MD5 |  |  |  |
| 2 | lab2.txt | SHA-256 |  |  |  |
| 3 |  |  |  |  |  |

резервне копіювання

| № | Операція | Засіб/Команда | Результат (скриншот/опис) | Висновок |
| --- | --- | --- | --- | --- |
| 1 | Архівація папки | 7-Zip |  |  |
| 2 | Збереження копії | Google Drive / USB |  |  |
| 3 |  |  |  |  |

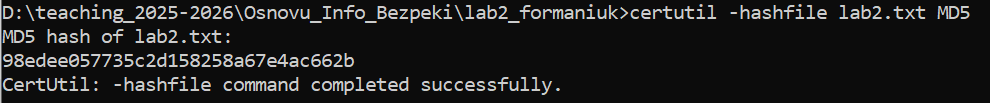
# **1. Хід Роботи**

## **1.1. Контроль цілісності файлів.**

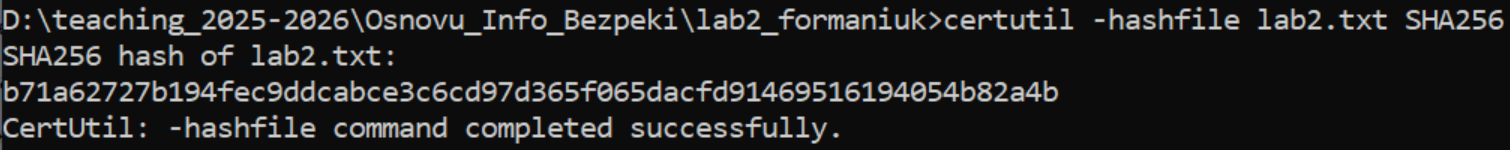
Створив файл (lab2.txt) у папці D:\teaching\_2025-2026\Osnovu\_Info\_Bezpeki\lab2\_formaniuk.

У командному рядку Windows виконав обчислення хешів за допомогою утиліти **certutil**:

certutil -hashfile lab2.txt MD5 (хеш до змін)

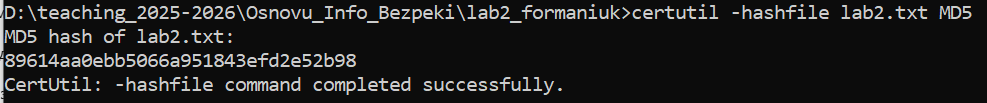


certutil -hashfile lab2.txt SHA256 (хеш до змін)

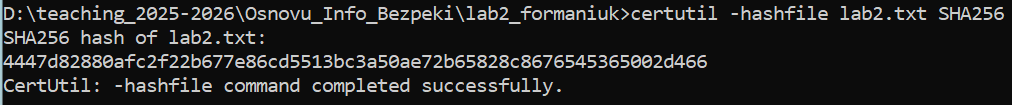


Вніс зміни до файлу та повторно виконав обчислення хешів.

хеш після змін MD5



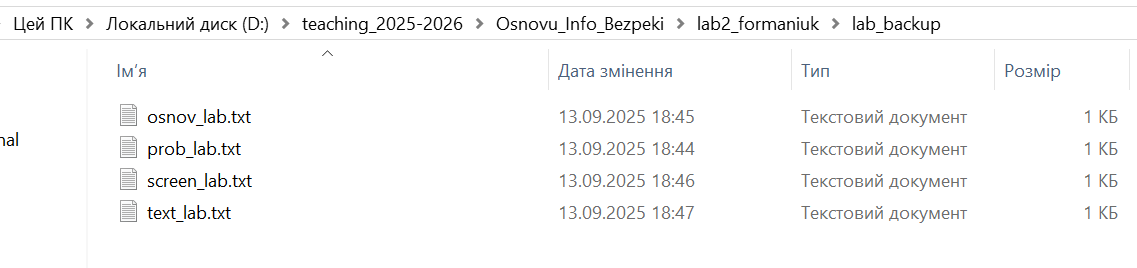
хеш після змін SHA256



Висновок: отримані результати не співпадають що свідчить: при зміні символів значення хешів змінюється повністю.

## **1.2. Резервне копіювання.**

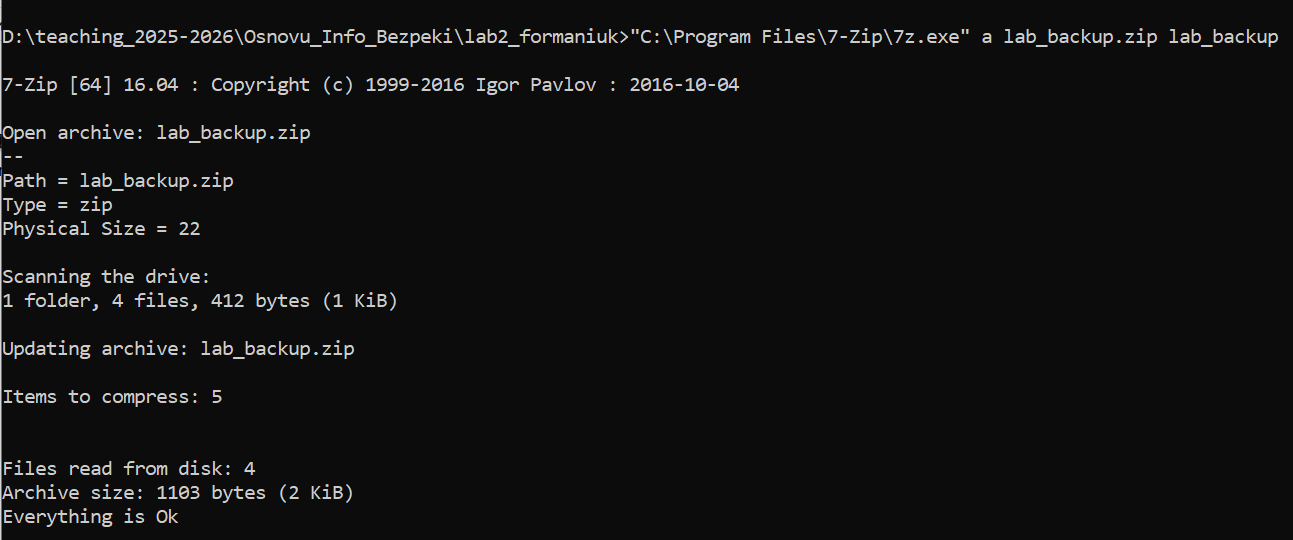
1. Створив папку lab\_backup з кількома текстовими файлами (в які вніс кілька рядків тексту для прикладу)

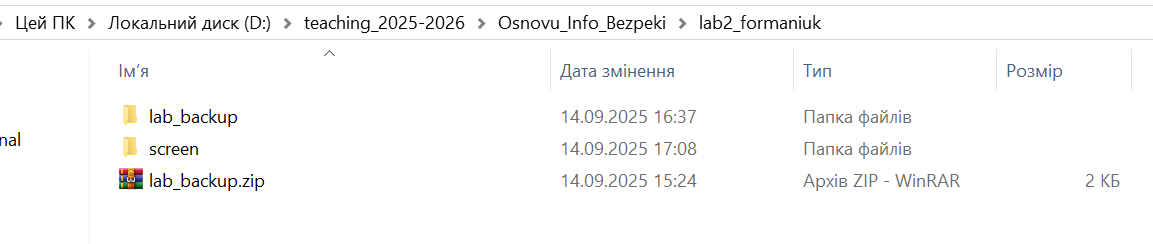


1. Виконав архівацію використавши програму 7-Zip для архівації папки у форматі ZIP.

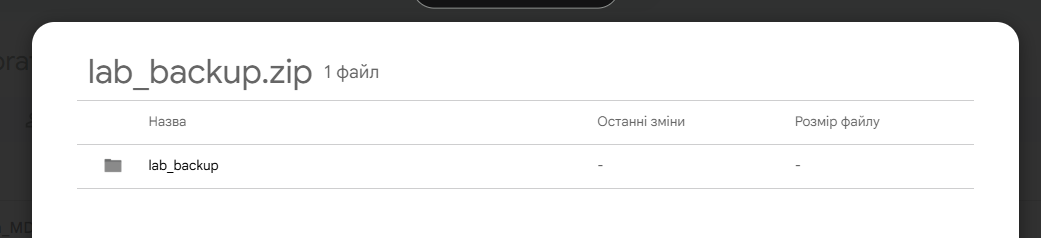
Ввівши команду в командний рядок:

“C:\Program Files\7-Zip\7z.exe” a lab\_backup.zip lab\_backup\



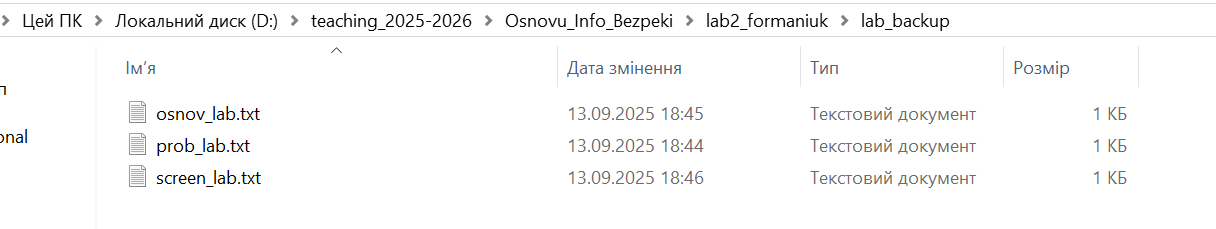


1. Зберіг копію папки lab\_backup.zip на (Google Drive)



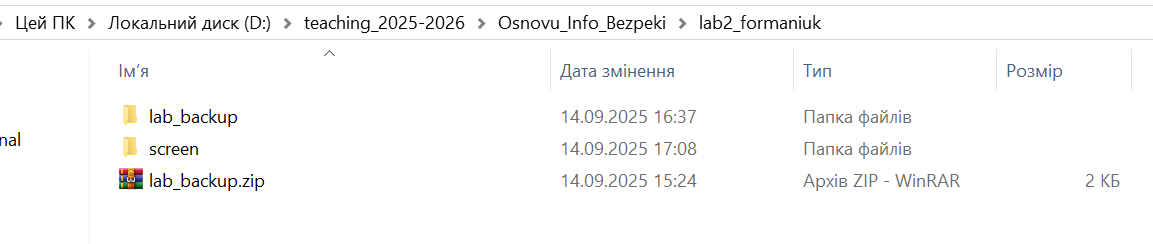
## **1.3. Відновлення даних.**

1. Видалив один із файлів у папці lab\_backup



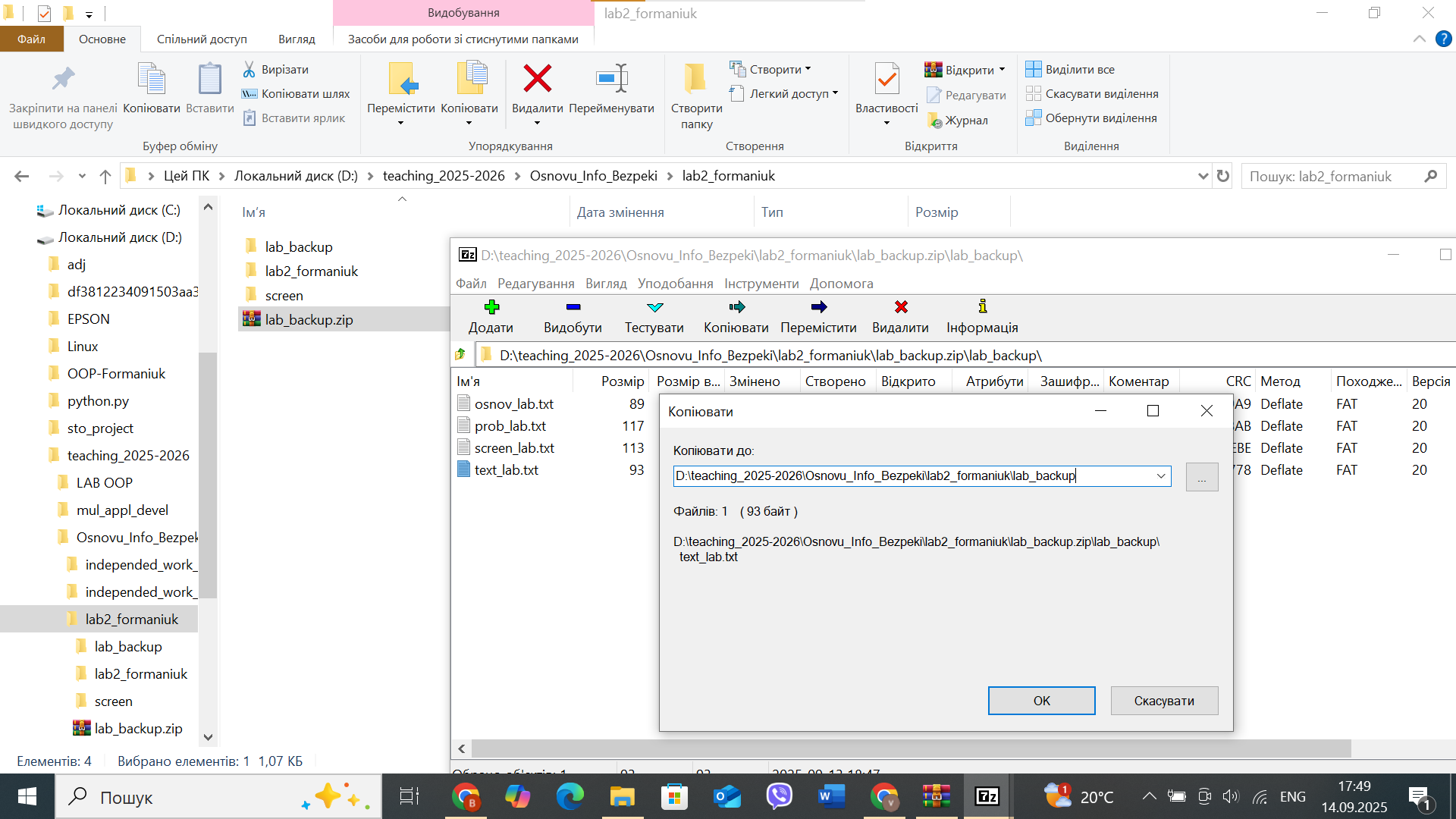
1. Відновлення даних (файлу).

Виконав відновлення з архіву: відкрив провідник, знайшов lab\_backup.zip



у папці D:\teaching\_2025-2026\Osnovu\_Info\_Bezpeki\lab2\_formaniuk

відкрив архів за допомогою 7-Zip та розархівував у папку lab\_backup видалений файл (text\_lab.txt)



Видалений файл був успішно відновлений.

# **2. Контрольні питання.**

## **2.1. Чим відрізняється повне, інкрементальне і диференціальне резервне копіювання?**

Повне резервне копіювання - копіюються всі файли кожного разу. Найнадійніше, але займає багато місця.

Інкрементальне резервне копіювання - копіюються тільки ті файли, які були змінені або додані після останнього копіювання. Економить місце, але для відновлення потрібно всі попередні копії.

Диференціальне - копіюються всі зміни після останнього повного копіювання. Займає більше місця ніж інкрементальне, але відновлювати легше.

## **2.2. Чому MD5 вважається ненадійним для перевірки цілісності?**

MD5 вважається ненадійним, тому що для нього існують колізії - різні файли можуть мати однакове хеш-значення. Це дозволяє зловмисникам підмінювати дані без виявлення.

## **2.3. Наведіть приклади, коли порушення цілісності може призвести до критичних наслідків?**

Пошкодження системних файлів Windows - OC не завантажується.

Зміна файлів бази даних - втрата або спотворення інформації.

Модифікація файлів програм - запуск шкідливого коду.

Підробка фінансових документів чи звітів - матеріальні збитки.

## **2.4. Як організувати регулярне резервне копіювання в ОС Windows?**

Використати вбудований засіб (Резервне копіювання та відновлення (Windows backup)).

Налаштувати розклад через Планувальник завдань, щоб автоматично запускати backup.

Для хмарного зберігання - налаштувати OneDrive / Google Drive

## **2.5. Які недоліки у використанні лише резервних копій без хеш-контролю?**

Можна зберегти вже пошкоджені або змінені файли.

Неможливо відрізнити оригінал від модифікованої версії.

Втрачається гарантія цілісності: відновлені дані можуть бути некоректними.

# **3. Висновок.**

У ході лабораторної роботи я ознайомився з методами забезпечення **цілісності даних** та з базовими підходами до **резервного копіювання і відновлення інформації**.

Для перевірки цілісності файлів було використано вбудовану утиліту Windows certutil.

Я створив файл lab2.txt.

Оголосив його хеші за алгоритмами MD5 та SHA-256.

Після внесення змін у файл повторно обчислив хеші та порівняв результати.

Висновок: при зміні навіть одного символу у файлі значення хешу повністю змінюється, що підтверджує придатність хеш-функцій для контролю цілісності.

Для резервного копіювання я створив папку lab\_backup з кількома файлами (osnov\_lab.txt, prob\_lab.txt, screen\_lab.txt, text\_lab.txt).

За допомогою утиліти 7-Zip (команда у терміналі “C:\Program Files\7-Zip\7z.exe” a lab\_backup.zip lab\_backup\) я створив архів lab\_backup.zip

Для перевірки відновлення даних я видалив один з файлів із папки lab\_backup.

Далі виконав відновлення з архіву розпакувавши файл lab\_backup.zip за допомогою утиліти 7-Zip та відновив видалений файл.

Файл успішно відновився.

[Папка з скріншотами до lab2](https://drive.google.com/drive/u/0/folders/1fJcckGGFtYGt3uvAWaeeSr2dp1tj-28M)

https://drive.google.com/drive/u/0/folders/1fJcckGGFtYGt3uvAWaeeSr2dp1tj-28M