МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНИ СЕМЕНА КУЗНЕЦЯ

ЗВІТ
о виконанні лабораторної роботи №7
з дисципліни «Захист інформації»
за темою «Комплексний захист особистого проекту»

Виконав:
Студент 4 курсу
групи 6.04.122.010.22.1
факультету ІТ
Холоша Сергій

Перевірив:
Професор кафедри
кібербезпеки та ІТ
Тютюнник В. В.

Харків – 2025

Мета роботи: створити комплексну систему захисту інформації, що поєднує декілька методів з попередніх лабораторних робіт, провести порівняльний аналіз різних комбінацій захисту та оцінити їх ефективність.

Порядок виконання практичної частини

Крок 1. Дослідження готових рішень комплексного захисту

1) Завантажити та протестувати архіватор 7-Zip, WinRAR, AxCrypt, VeraCrypt, або будь-який інший аналог, з паролем та різними рівнями шифрування;

2) Встановити VeraCrypt та створити зашифрований контейнер з каскадним шифруванням;

3) Протестувати комбінований підхід: створити зашифрований архів та приховати його у зображення;

4) Зафіксувати час виконання операцій та розміри файлів для кожного методу.

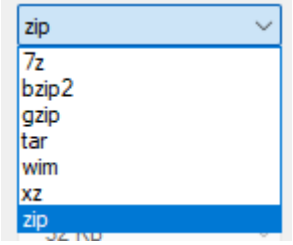

Рис. 1 Варіанти архівування в 7zip

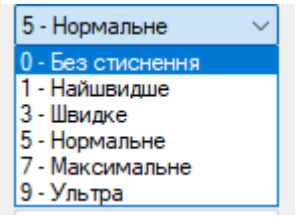

Рис. 2 Варіанти стиснення в 7zip

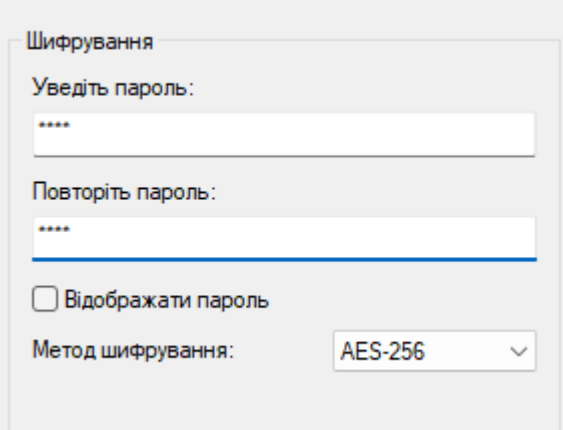

Рис. 3 Шифрування в 7zip

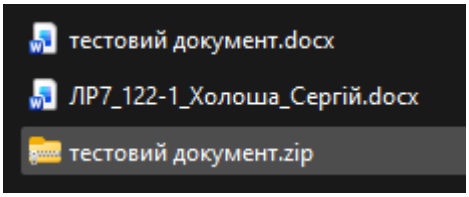

Рис. 4 Документ зашифрований за допомогою 7zip

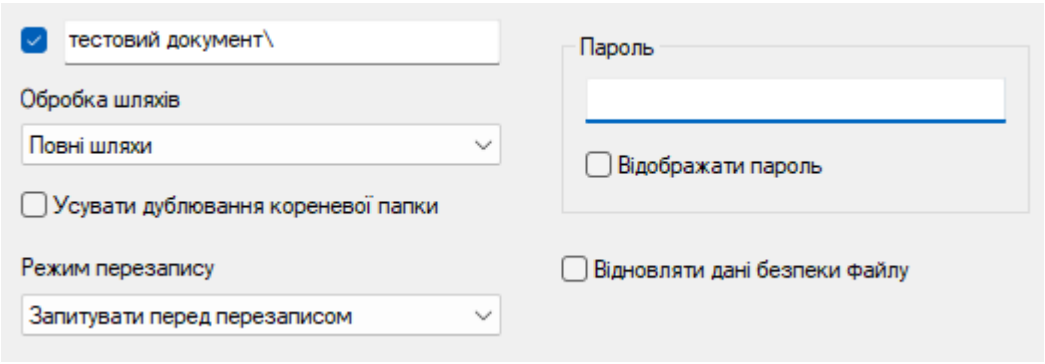

Рис. 5 Запит паролю при спробі відкрити архів

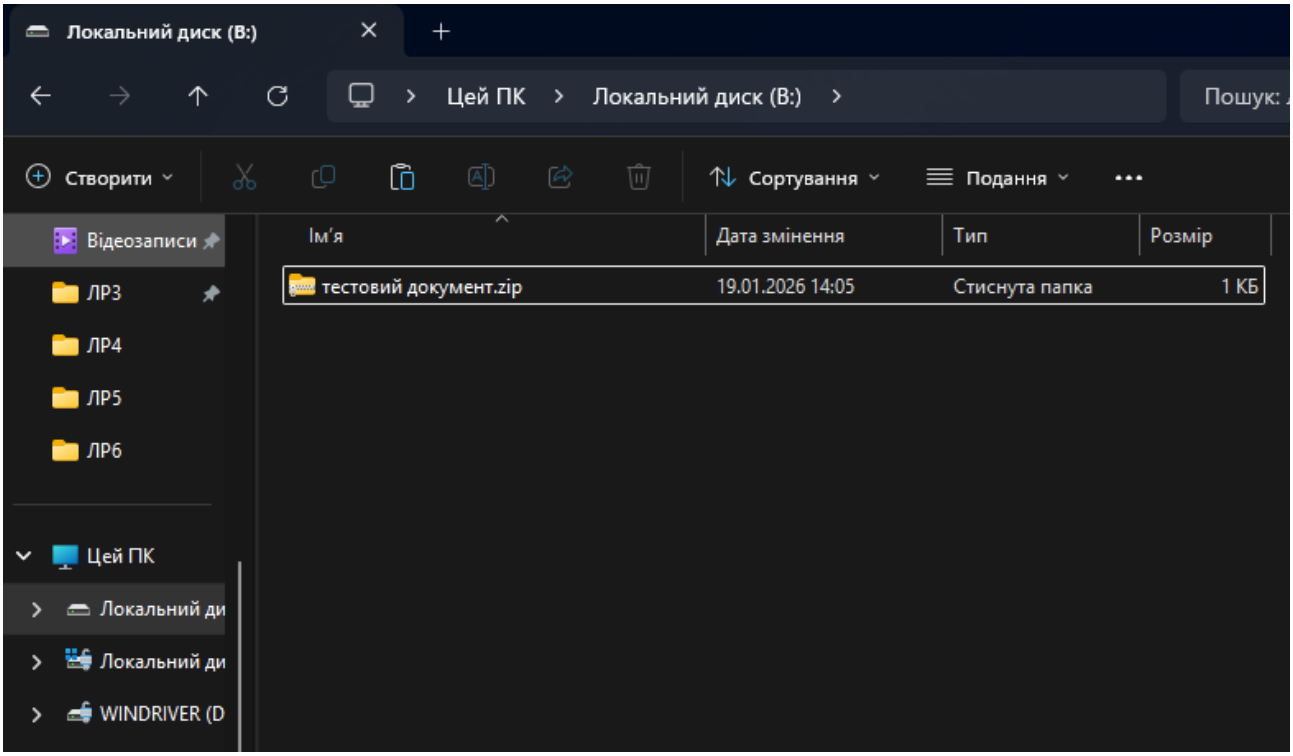

Рис. 6 Створений та змонтований контейнер VeraCrypt

Рис. 7 Зображення з прихованим архівом

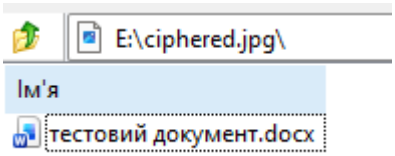

Рис. 8 Файл прихований в зображенні

Крок 2. Порівняльний аналіз різних комбінацій методів захисту

Обрати три різні комбінації з попередніх лабораторних робіт:

– Комбінація А: шифрування + стеганографія;

– Комбінація Б: цифровий підпис + шифрування;

– Комбінація В: стеганографія + цифровий підпис.

Крок 2.1. Застосувати кожну комбінацію до одного й того ж тестового файлу (наприклад, власне резюме).

Крок 2.2. Заповнити порівняльну таблицю:

Критерій	**Комбінація А**	**Комбінація Б**	**Комбінація В**
Час обробки			
Розмір результату			
Складність налаштування			
Рівень приховування			
Забезпечення цілісності			

Комбінація А

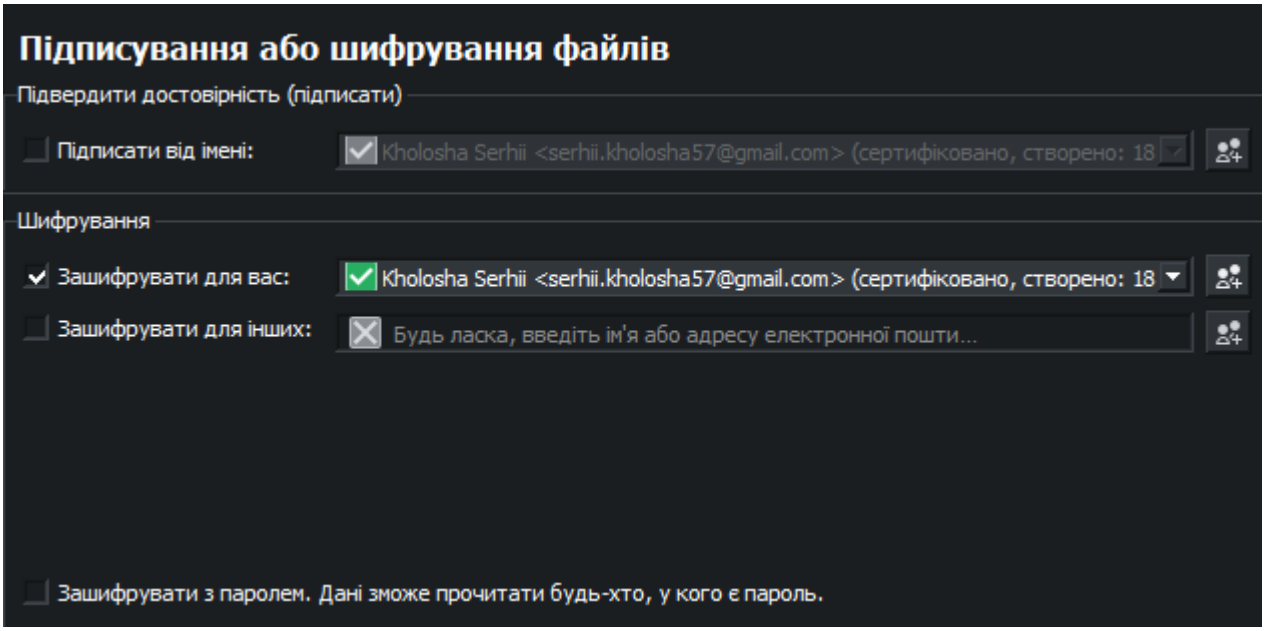

Рис. 9 Налаштування шифрування

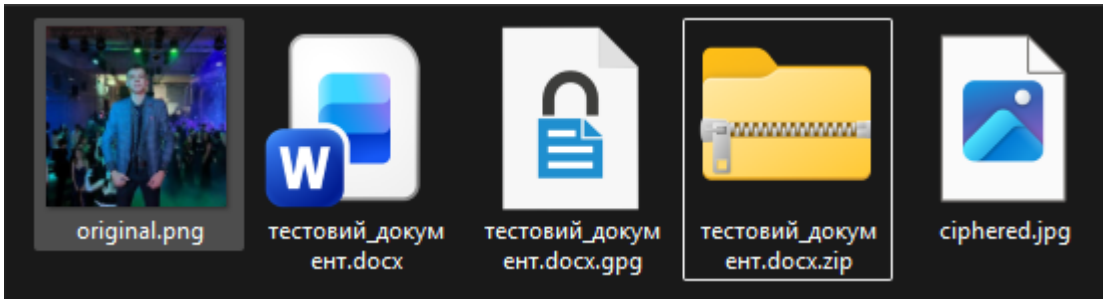

Рис. 10 Створене зображення з архівом

Рис. 11 Вигляд архіву

Оцінка комбінації

Час обробки: швидкий

Розмір результату: розмір файлу (стиснений в архів) + розмір зображення

Складність налаштування: середній

Рівень приховування: високий

Забезпечення цілісності: відсутнє, адже містить лише шифрування

Комбінація Б

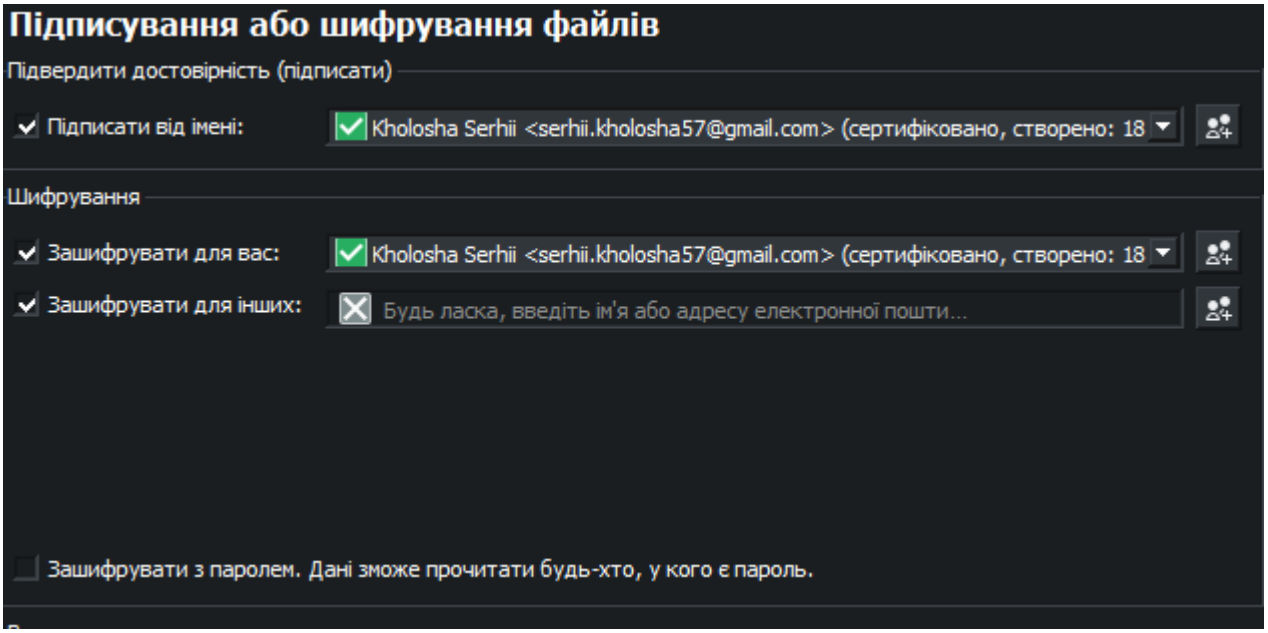

Рис. 12 Параметри шифрування та підпису

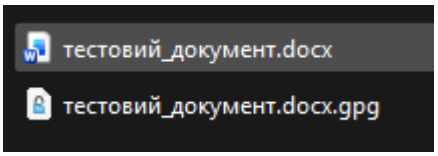

Рис. 13 Отриманий результат

Час обробки: швидкий
Розмір результату: розмір файлу
Складність налаштування: низький
Рівень приховування: приховування відсутнє
Забезпечення цілісності: високе, містить цифровий підпис

Комбінація Б

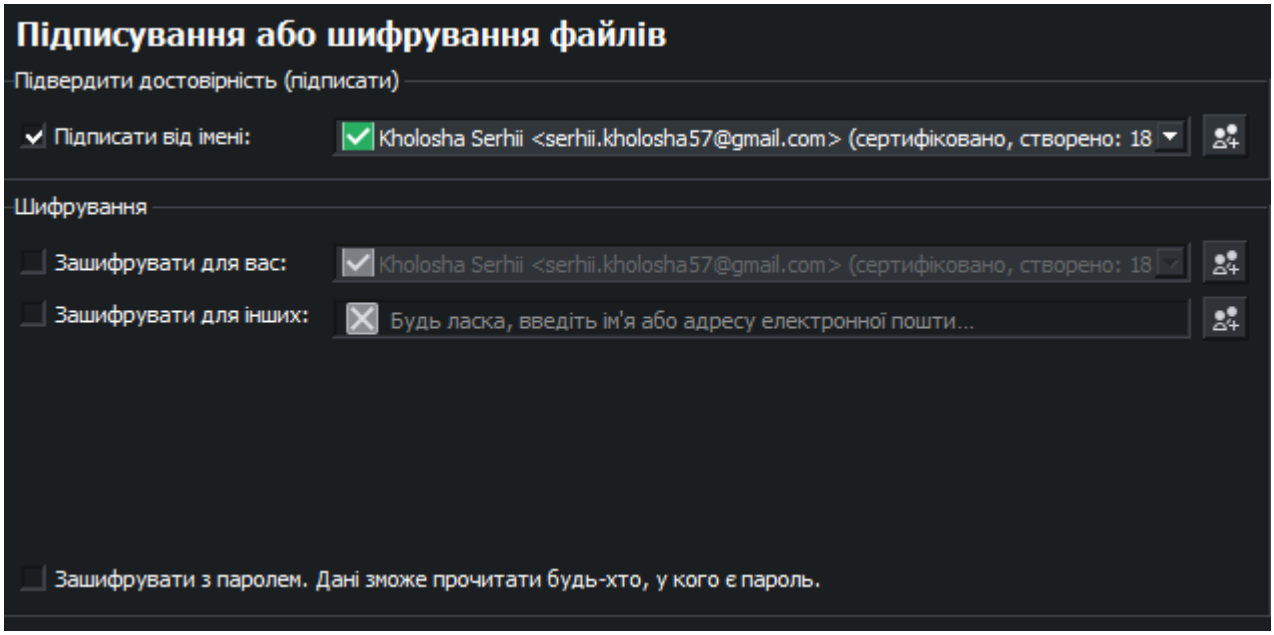

Рис. 14 Налаштування підпису

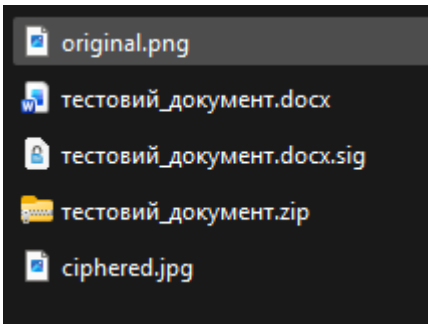

Рис. 15 Отриманий результат

Рис. 16 Вигляд архіву

Час обробки: швидкий

Розмір результату: розмір файлу + розмір підпису (стиснені в архів) + розмір зображення

Складність налаштування: середній

Рівень приховування: високий

Забезпечення цілісності: високе, містить цифровий підпис

Крок 2.3. Обрати найкращу комбінацію та обґрунтувати свій вибір.

На мою думку найкращою комбінацією є варіант Б – цифровий підпис та шифрування достатньою мірою захистять цілісність та недоступність файлу. Якщо необхідно приховати факт передачі то варіант Б можна модифікувати методом архівації підписаного та зашифрованого документа для подальшого приховання в зображенні.

Крок 3. Тестування стійкості обраної системи захисту

1) Спробувати “зламати” власну систему захисту без знання ключів:
   - Чи можна виявити, що файл містить приховану інформацію?
   - Чи можна обійти захист, знаючи лише принцип роботи?
2) Попросити одногрупника спробувати отримати доступ до захищеного файлу;
3) Протестувати поведінку системи при спробах підробки:
   - Що відбувається при зміні одного байта у файлі?
   - Чи виявляє система спроби несанкціонованого доступу?
4) Задокументувати всі спроби атак та їх результати.

1) В варіантах А та В виявити наявність прихованого файлу буде досить важко, адже зображення виглядають нормальними на перший погляд. Втім, чим більше файл, тим більш незвичний вигляд буде мати файл. Знаючи принцип роботи файли отримати можна
3) При спробі зміни файлу варіанти Б та В, що мають цифровий підпис, дадуть кінцевому отримувачу знати що файл скомпрометовано, варіант А є відкритим до внесення змін за умови що до неї було отримано доступ. Система не виявляє спроби несанкціонованого доступу, якщо пароль введено неправильно вона дозволяє спробувати знову безліч разів.

Крок 4. Оцінка практичності та зручності використання

1) Оцінити, наскільки складно звичайному користувачу працювати з системою;

2) Визначити слабкі місця у вашій реалізації (що можна покращити);

3) Запропонувати сценарії реального використання для створеної системи.

Звичайному користувачу після ознайомлення буде не складно користуватися системою Kleopatra, інтерфейс є доволі зрозумілим та інтуітивним.

Кожна з комбінацій містить свій недолік:

А – відсутність цифрового підпису

Б – хоча це й важко назвати недоліком, відсутність приховання факту передачі

В – відсутність шифрування

В реальному світі варіанти зі стеганографією можуть бути використані всюди де необхідно приховати факт передачі даних – передача інформації з окупованої території України, приховання цифрового підпису в зображенні з міркувань інтелектуальної власності і т.д. Варіант Б є стандартом передачі даних на корпоративному рівні, наприклад в банківській сфері.

Технічне завдання

Завдання: Створити комплексну систему захисту, що поєднує два, або більше методи з попередніх лабораторних робіт та включає аналітичну компоненту для оцінки ефективності.

Обов'язкові функціональні вимоги:

– реалізація двох методів захисту з попередніх лабораторних робіт у вигляді єдиної системи;

– автоматичне послідовне застосування обох методів до файлу;

– функція повного відновлення оригінального файлу;

– аналітичний модуль для збору метрик: час обробки, розмір файлів, статистика операцій;

– демонстрація того, що обидва етапи захисту необхідні для доступу до даних.

```
============================================================
ЗВІТ ПРО ЕФЕКТИВНІСТЬ ДВОЕТАПНОЇ СИСТЕМИ ЗАХИСТУ
============================================================
Дата: 2026-01-19 12:44:32

ЕТАП 1: ШИФРУВАННЯ AES
------------------------------------------------------------
Розмір оригінального файлу: 343 байт
Розмір зашифрованих даних: 384 байт
Накладні витрати: 41 байт (11.95%)
Час виконання: 0.0426 сек

ЕТАП 2: LSB-СТЕГАНОГРАФІЯ
------------------------------------------------------------
Розмір зашифрованих даних: 384 байт
Розмір зображення-контейнера: 481076 байт
Розмір стего-зображення: 481076 байт
Час виконання: 0.0589 сек

ВІДНОВЛЕННЯ: ЕКСТРАКЦІЯ
------------------------------------------------------------
Розмір витягнутих даних: 384 байт
Час виконання: 0.0064 сек

ВІДНОВЛЕННЯ: ДЕШИФРУВАННЯ
------------------------------------------------------------
Розмір розшифрованих даних: 343 байт
Час виконання: 0.0177 сек

ЗАГАЛЬНА СТАТИСТИКА
------------------------------------------------------------
Загальний час захисту: 0.1020 сек
Загальний час відновлення: 0.0246 сек
Загальний час операцій: 0.1266 сек

АНАЛІЗ ТА РЕКОМЕНДАЦІЇ
------------------------------------------------------------
✓ Час шифрування прийнятний
Використання ємності зображення: 0.21%
✓ Низьке використання ємності - висока непомітність

ВИСНОВОК
------------------------------------------------------------
Система успішно реалізує двоетапний захист:
1. AES-256 шифрування забезпечує конфіденційність даних
2. LSB-стеганографія приховує факт наявності зашифрованих даних
Обидва етапи необхідні для повного відновлення даних
============================================================
```

Рис. 17 Результат виконання програми

Посилання на GitHub: zahist-informaciji/lab7 at main · serhiikholosha57/zahist-informaciji

Висновок: в ході лабораторної роботи було створено комплексну систему захисту інформації, що поєднує декілька методів з попередніх лабораторних робіт, проведено порівняльний аналіз різних комбінацій захисту та оцінено їх ефективність