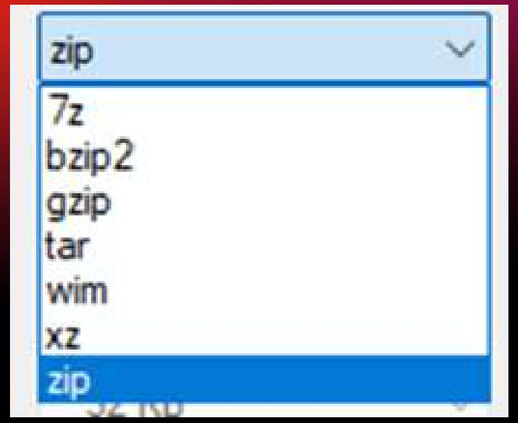
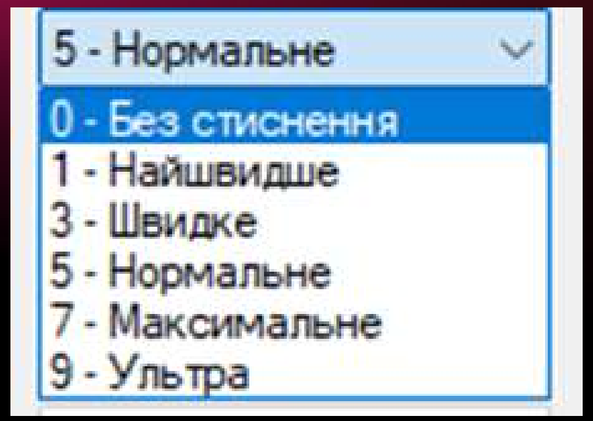
ЛАБОРАТОРНА РОБОТА 7

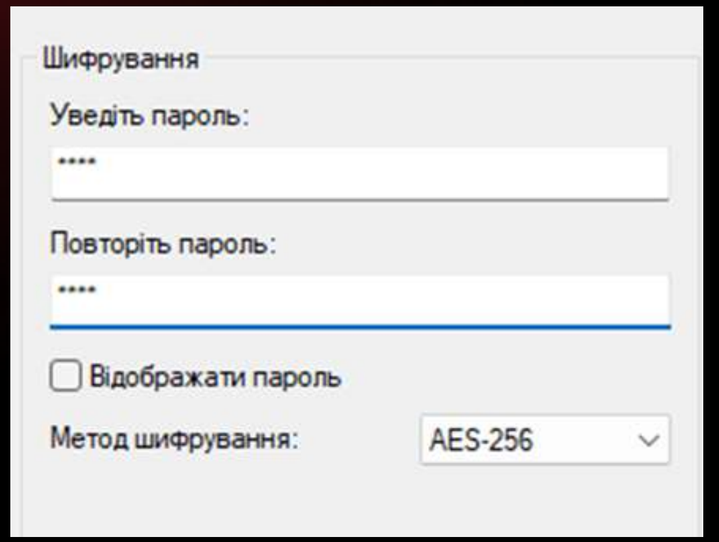
Комплексний захист особистого проекту

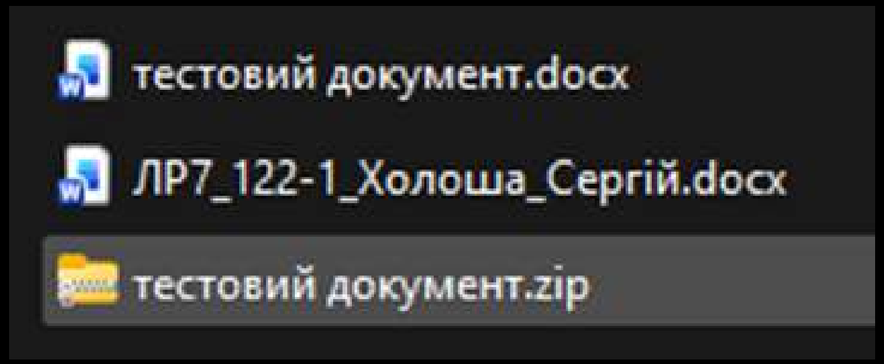
Виконав Холоша Сергій

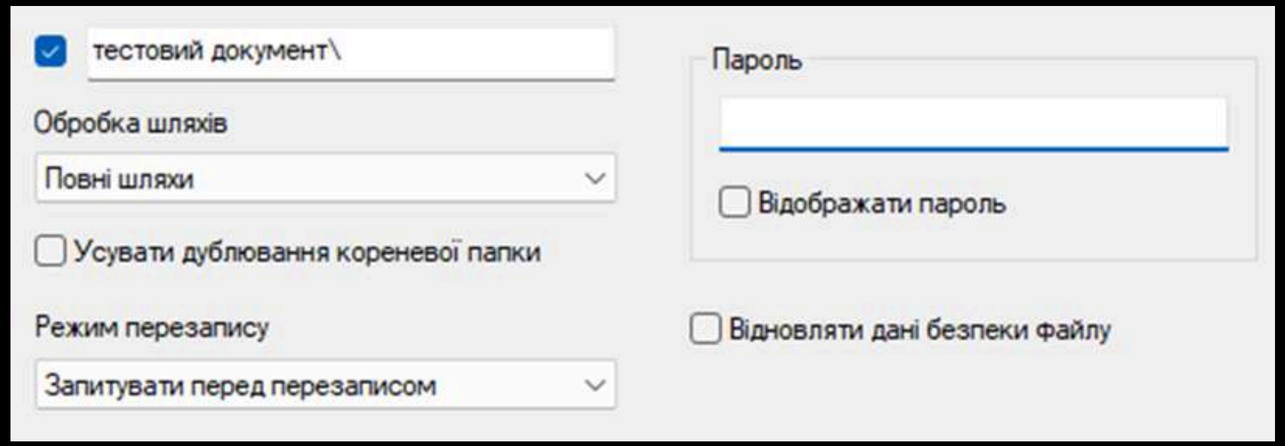
Дослідження готових рішень комплексного захисту

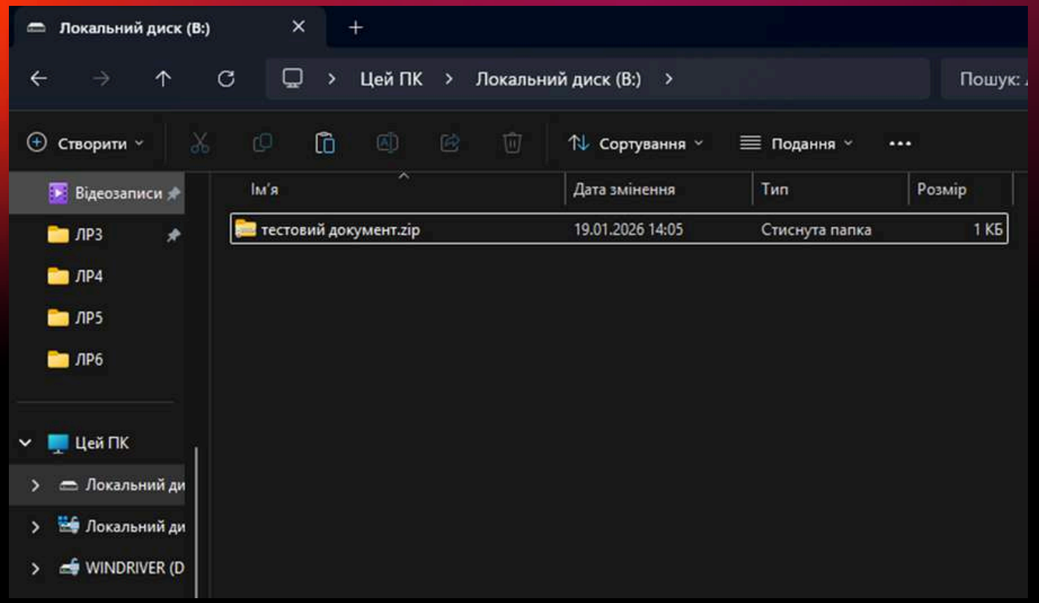

zip
7z
bzip2
gzip
tar
wim
xz
zip

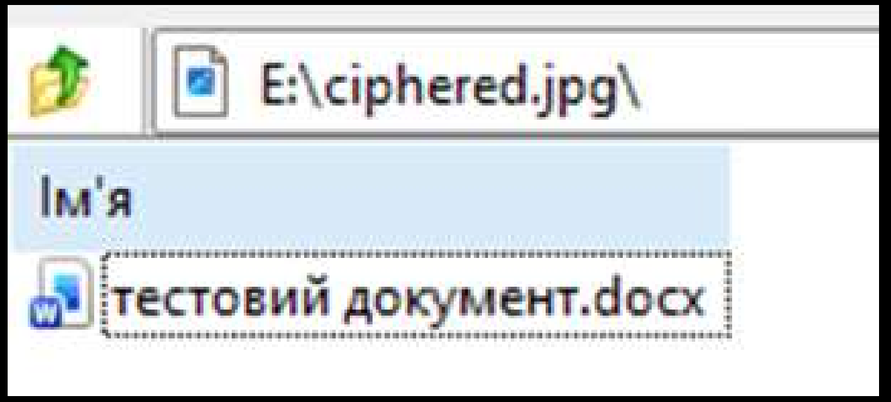

5 - Нормальне
0 - Без стиснення
1 - Найшвидше
3 - Швидке
5 - Нормальне
7 - Максимальне
9 - Ультра


Шифрування
Уведіть пароль:
Повторіть пароль:
Відображати пароль
Метод шифрування:
AES-256

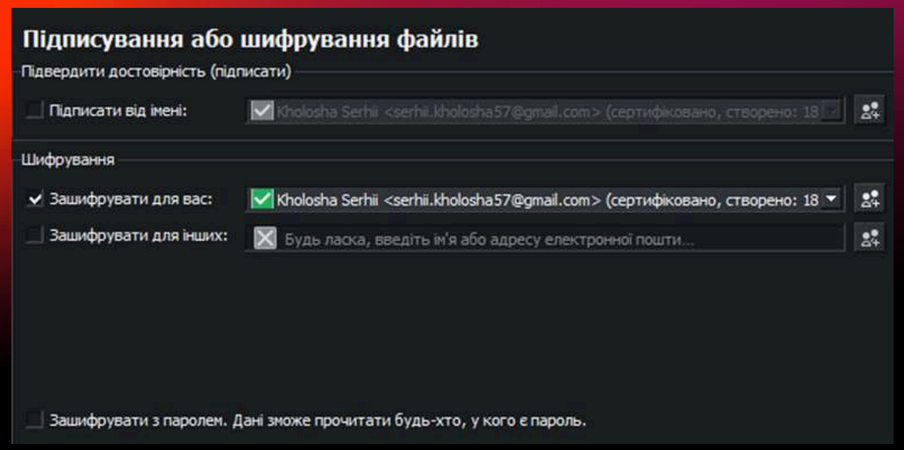

тестовий документ.docx
ЛР7_122-1_Холоша_Сергій.docx
тестовий документ.zip

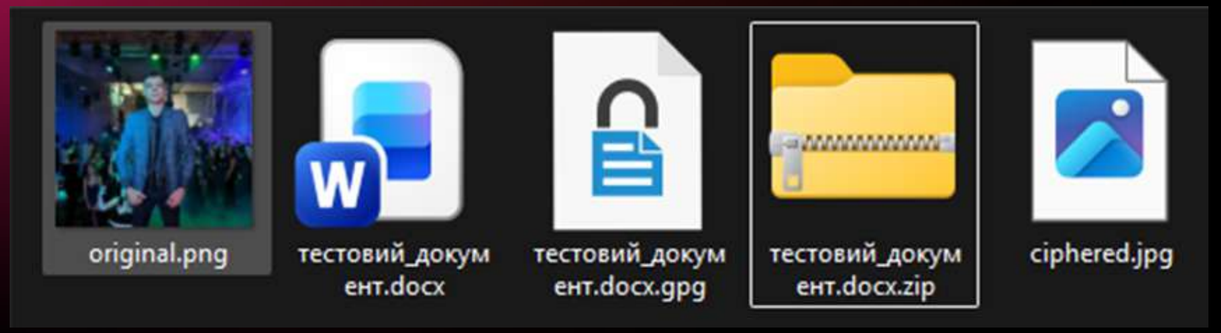

тестовий документ\
Обробка шляхів
Повні шляхи
Усувати дублювання кореневої папки
Режим перезапису
Запитувати перед перезаписом
Пароль
Відображати пароль
Відновляти дані безпеки файлу


Локальний диск (B:)
Цей ПК
Локальний диск (B:)
Створити
Сортування
Подання
Відеозаписи
ЛР3
ЛР4
ЛР5
ЛР6
Цей ПК
Локальний ди
Локальний ди
WINDRIVER (D
Ім'я
Дата змінення
Тип
Розмір
тестовий документ.zip
19.01.2026 14:05
Стиснута папка
1 КБ


E:\ciphered.jpg\
Ім'я
тестовий документ.docx

Порівняльний аналіз різних комбінацій методів захисту





Комбінація А

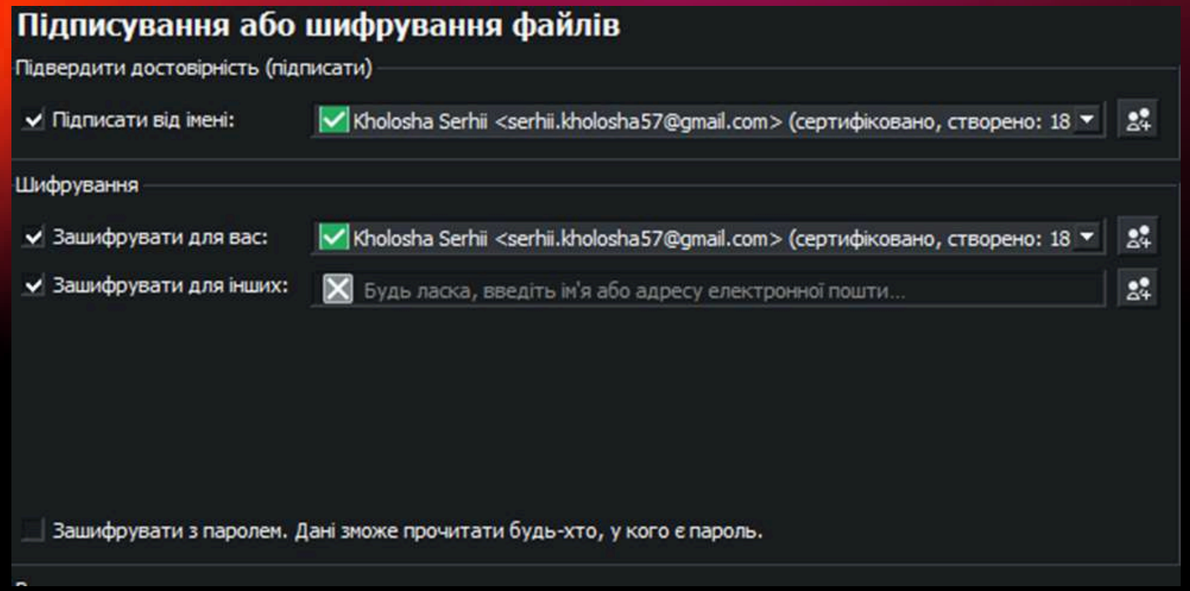
Час обробки: швидкий

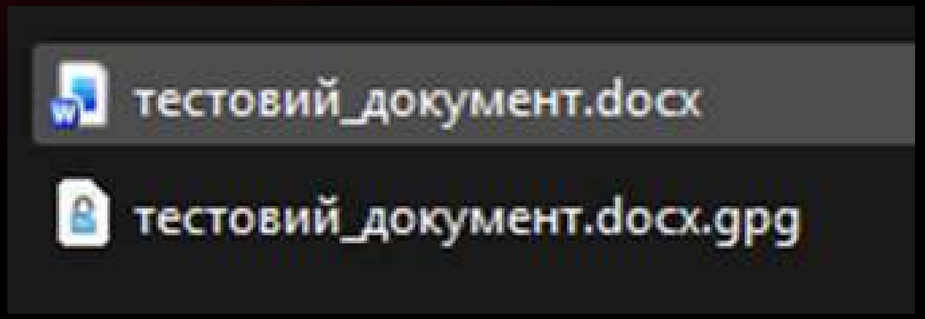
Розмір результату: розмір файлу (стиснений в архів) + розмір зображення

Складність налаштування: середній

Рівень приховування: високий

Забезпечення цілісності: відсутнє, адже містить лише шифрування





Комбінація Б

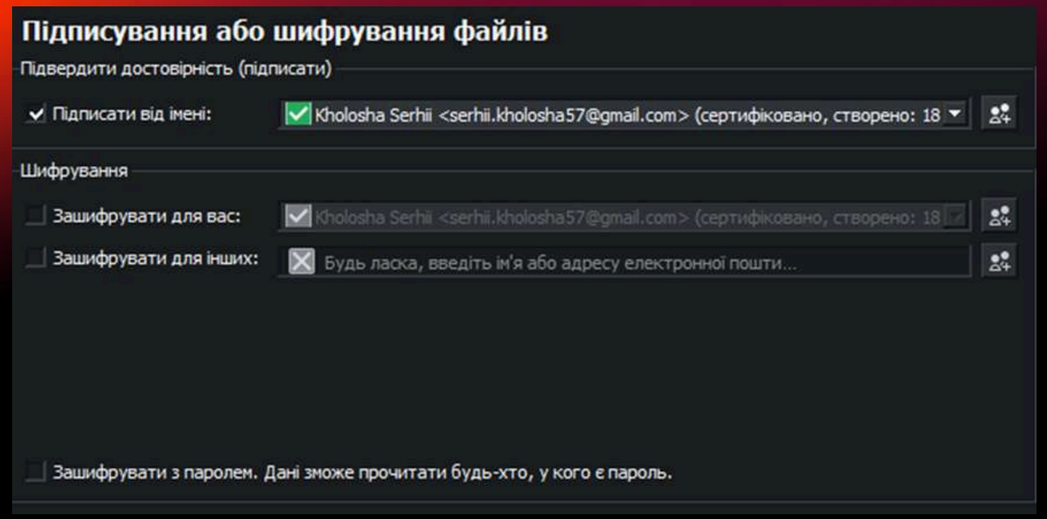
Час обробки: швидкий

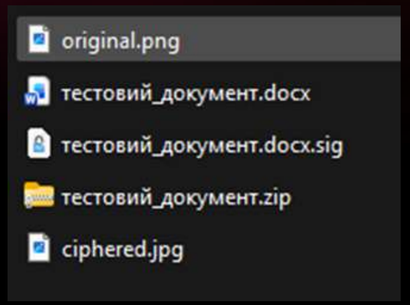
Розмір результату: розмір файлу

Складність налаштування: низький

Рівень приховування: приховування відсутнє

Забезпечення цілісності: високе, містить цифровий підпис





Комбінація B

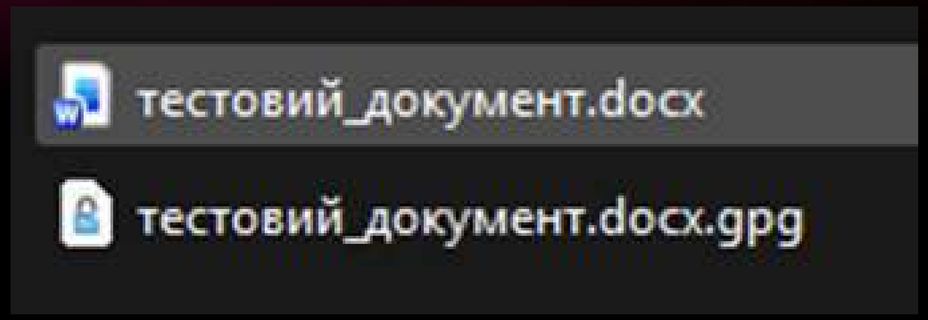
Час обробки: швидкий

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

Складність налаштування: середній

Рівень приховування: високий

Забезпечення цілісності: високе, містить цифровий підпис



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.

Тестування стійкості обраної системи захисту

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.

Оцінка практичності та зручності використання

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

```
============================================================
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
============================================================
```

Дякую за увагу!

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