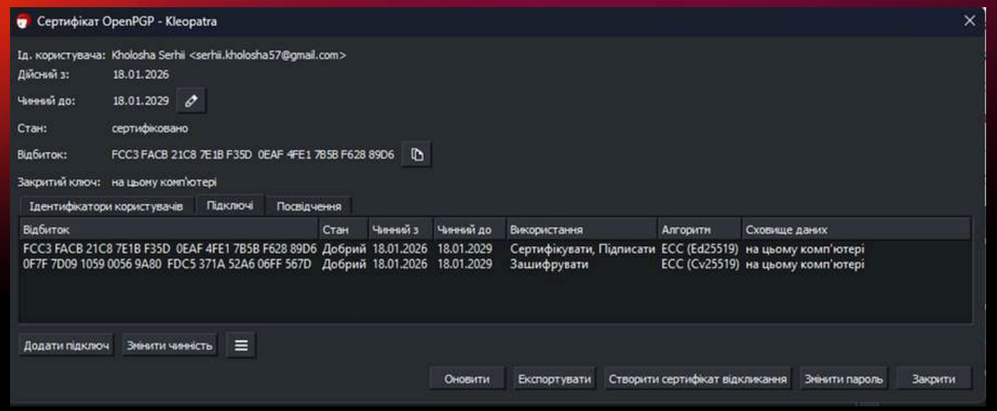
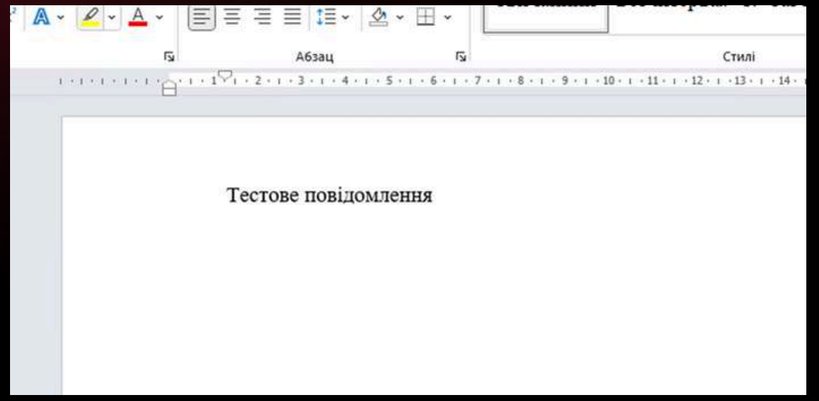
ЛАБОРАТОРНА РОБОТА 5

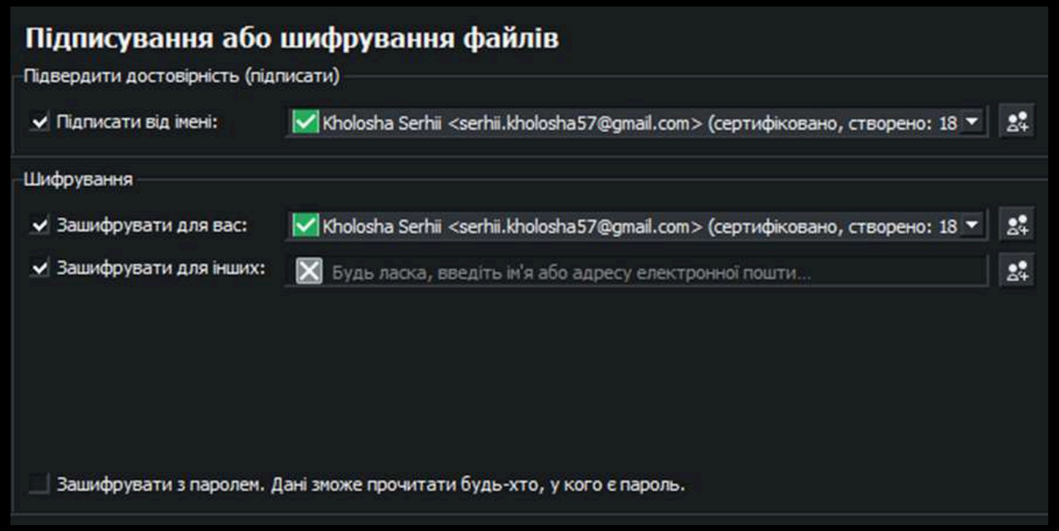
# Захищена електронна пошта

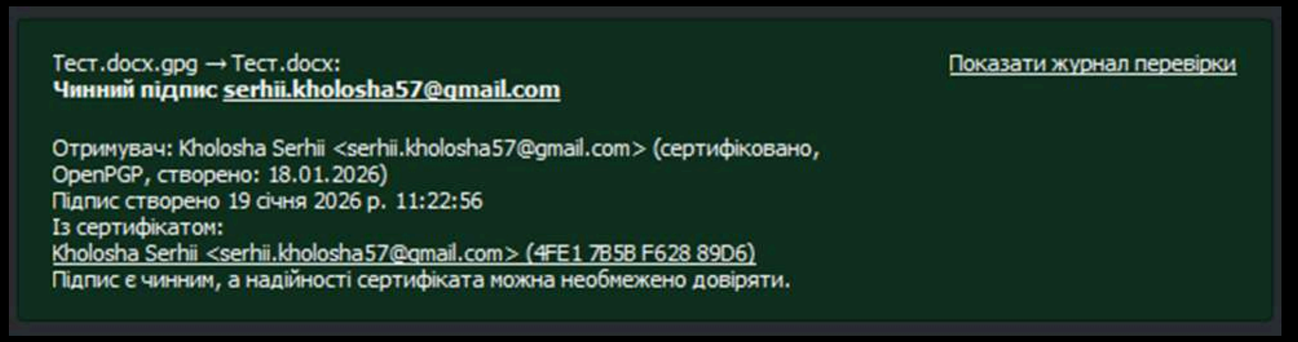
Виконав Холоша Сергій

# Дослідження PGP-шифрування


Сертифікат OpenPGP - Kleopatra
Ід. користувача: Kholosha Serhii <serhii.kholosha57@gmail.com>
Дійсний з: 18.01.2026
Чинний до: 18.01.2029
Стан: сертифіковано
Відбиток: FCC3 FACB 21C8 7E1B F35D 0EAF 4FE1 7B5B F628 89D6
Закритий ключ: на цьому комп'ютері
Ідентифікатори користувачів
Підключі
Посвідчення
Відбиток Стан Чинний з Чинний до Використання Алгоритм Сховище даних
FCC3 FACB 21C8 7E1B F35D 0EAF 4FE1 7B5B F628 89D6 Добрий 18.01.2026 18.01.2029 Сертифікувати, Підписати ECC (Ed25519) на цьому комп'ютері
0F7F 7D09 1059 0056 9A80 FDC5 371A 52A6 06FF 567D Добрий 18.01.2026 18.01.2029 Зашифрувати ECC (Cv25519) на цьому комп'ютері
Додати підключ
Змінити чинність
Оновити
Експортувати
Створити сертифікат відкликання
Змінити пароль
Закрити

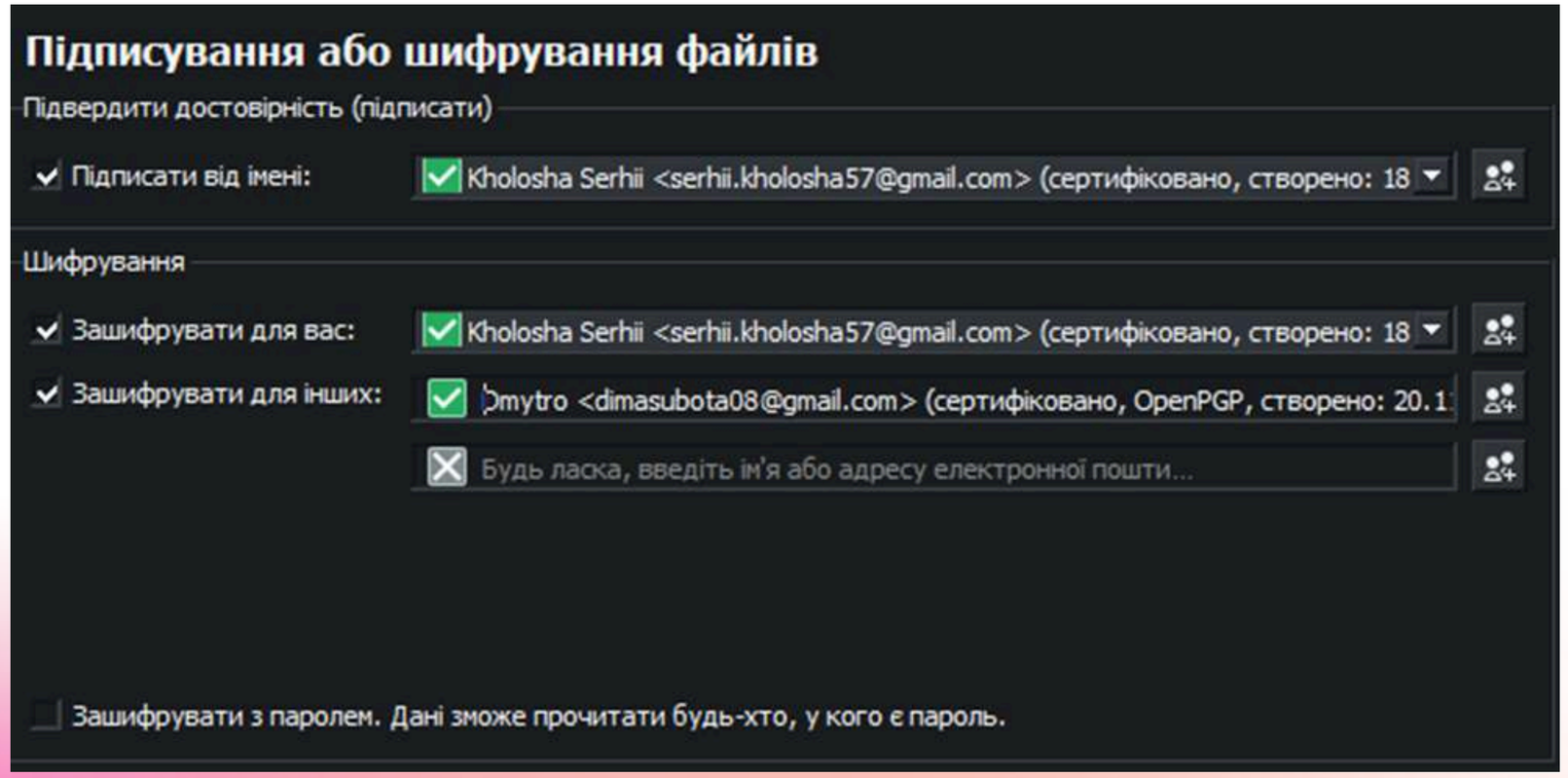

Абзац
Стилі
Тестове повідомлення

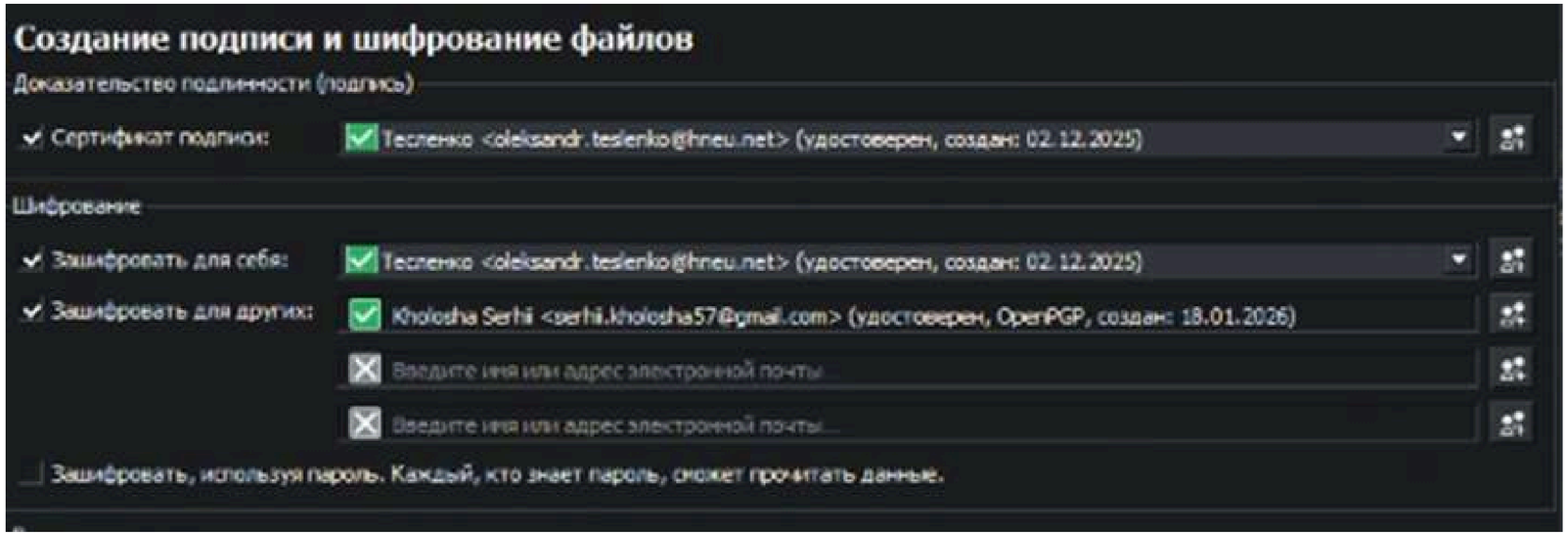

Підписування або шифрування файлів
Підвердити достовірність (підписати)
Підписати від імені:
Kholosha Serhii <serhii.kholosha57@gmail.com> (сертифіковано, створено: 18
Шифрування
Зашифрувати для вас:
Kholosha Serhii <serhii.kholosha57@gmail.com> (сертифіковано, створено: 18
Зашифрувати для інших:
Будь ласка, введіть ім'я або адресу електронної пошти...
Зашифрувати з паролем. Дані зможе прочитати будь-хто, у кого є пароль.

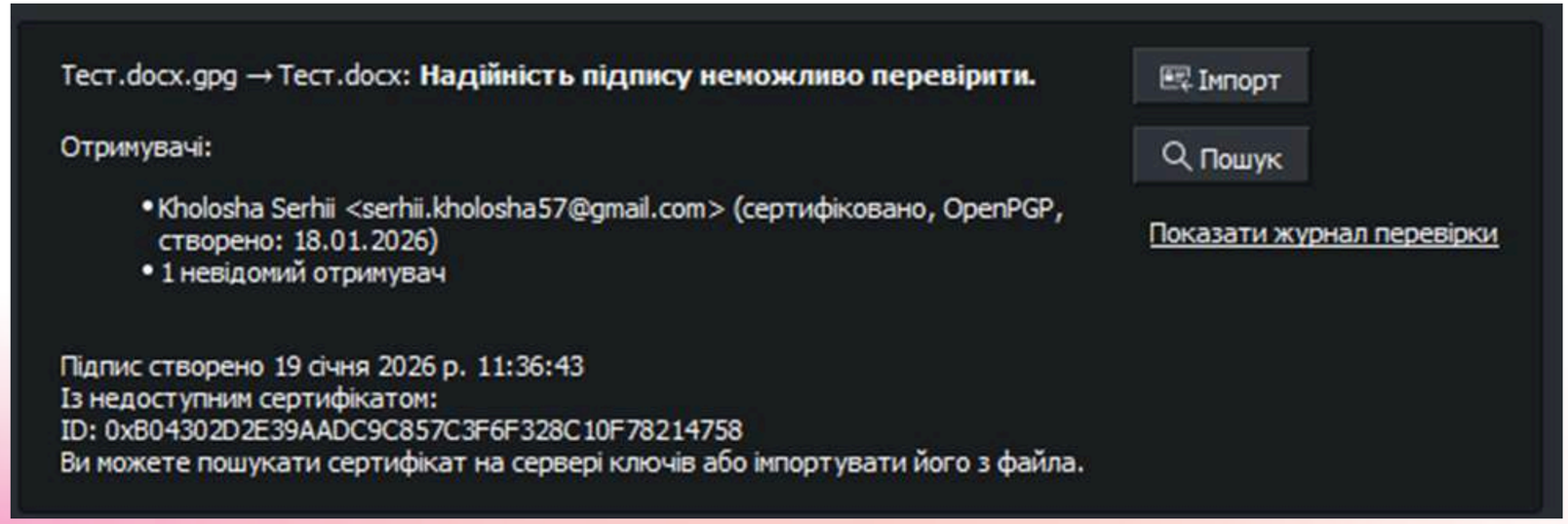

Тест.docx.gpg → Тест.docx:
Показати журнал перевірки
Чинний підпис serhii.kholosha57@gmail.com
Отримувач: Kholosha Serhii <serhii.kholosha57@gmail.com> (сертифіковано, OpenPGP, створено: 18.01.2026)
Підпис створено 19 січня 2026 р. 11:22:56
Із сертифікатом:
Kholosha Serhii <serhii.kholosha57@gmail.com> (4FE1 7B5B F628 89D6)
Підпис є чинним, а надійності сертифіката можна необмежено довіряти.

# Зашифрована кореспонденція

| Назва | Ел. пошта | Стан | Чинний з | Чинний до | Ід. ключа |
|---|---|---|---|---|---|
| Dmytro | dimasubota08@gmail.com | сертифіковано | 20.11.2025 | 20.11.2028 | D3AC CE86 4BC3 8B6D |
| **Kholosha Serhii** | **serhii.kholosha57@gmail.com** | **сертифіковано** | **18.01.2026** | **18.01.2029** | **4FE1 7B5B F628 89D6** |






На зображенні бачимо напис «надійність підпису неможливо перевірити», він виникає з тої причини що в моєму клієнті Kleopatra не імпортований ключ одногрупника який шифрував повідомлення для мене

# Аналіз безпеки електронної пошти

```
MIME-Version: 1.0
Date: Mon, 19 Jan 2026 11:42:15 +0200
Message-ID: <CAOd_q1H7jZdVXEY5_B7k4wNe--9h4KhD5G5JcMsJkuv-=4VhqQ@mail.gmail.com>
Subject: Файл без шифрування
From: "Сергій Холоша" <serhii.kholosha57@gmail.com>
To: "Сергій Холоша" <serhii.kholosha57@gmail.com>
Content-Type: multipart/mixed; boundary="00000000000096cc310648ba8135"

--00000000000096cc310648ba8135
Content-Type: multipart/alternative; boundary="00000000000096cc2f0648ba8133"

--00000000000096cc2f0648ba8133
Content-Type: text/plain; charset="UTF-8"



--00000000000096cc2f0648ba8133
Content-Type: text/html; charset="UTF-8"

<div dir="ltr"><br></div>

--00000000000096cc2f0648ba8133--
--00000000000096cc310648ba8135
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document; name="Тест.docx"
Content-Disposition: attachment; filename="Тест.docx"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_mkkz7u7a0
Content-ID: <f_mkkz7u7a0>


--00000000000096cc310648ba8135--
```

```
MIME-Version: 1.0
Date: Mon, 19 Jan 2026 11:42:28 +0200
Message-ID: <CAOd_q1HydYYbLKQ9T-DbAOeDuibmFDJaxZ9U+8e5mv88VBx9ww@mail.gmail.com>
Subject: Файл з шифруванням
From: "Сергій Холоша" <serhii.kholosha57@gmail.com>
To: "Сергій Холоша" <serhii.kholosha57@gmail.com>
Content-Type: multipart/mixed; boundary="0000000000006a34420648ba821e"

--0000000000006a34420648ba821e
Content-Type: multipart/alternative; boundary="0000000000006a34410648ba821c"

--0000000000006a34410648ba821c
Content-Type: text/plain; charset="UTF-8"



--0000000000006a34410648ba821c
Content-Type: text/html; charset="UTF-8"

<div dir="ltr"><br></div>

--0000000000006a34410648ba821c--
--0000000000006a34420648ba821e
Content-Type: application/octet-stream; name="Тест.docx.gpg"
Content-Disposition: attachment; filename="Тест.docx.gpg"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_mkkz85gj0
Content-ID: <f_mkkz85gj0>


--0000000000006a34420648ba821e--
```

Оригінали листів є ідентичними за змістом, відрізняються лише надісланим файлом

# Технічне завдання

```
=== Демонстрація захищеної комунікації ===

Відправник: ivan.petrenko@gmail.com
Персональні дані для ключа: IvanPetrenko1995
Вихідне повідомлення: Секретні дані про місцеположення ворога

Зашифроване повідомлення:
gAAAAABpbf1PBaIP_ZEKi7mLe2BKLB1lIg2t7gLYQSAbP_XSDJD7_ooFVPV8sEvy7cE2W0Agn3EYJJKkkfwGwtkkoxwTSnd4i_ZI_iZUvpttwZrSiLQe6TmTQ6zwQqCq9ThNcV4mf13QweB86TKaJ2A7rlxbXwTGDeyjXyc9VRRBSCrWoM4vcTiY=

--- Передача зашифрованого повідомлення ---

Розшифроване повідомлення: Секретні дані про місцеположення ворога
```

# Дякую за увагу!

Висновок: в ході лабораторної роботи було налаштовано шифрування для захисту особистої електронної кореспонденції та реалізовано власний алгоритм шифрування повідомлень