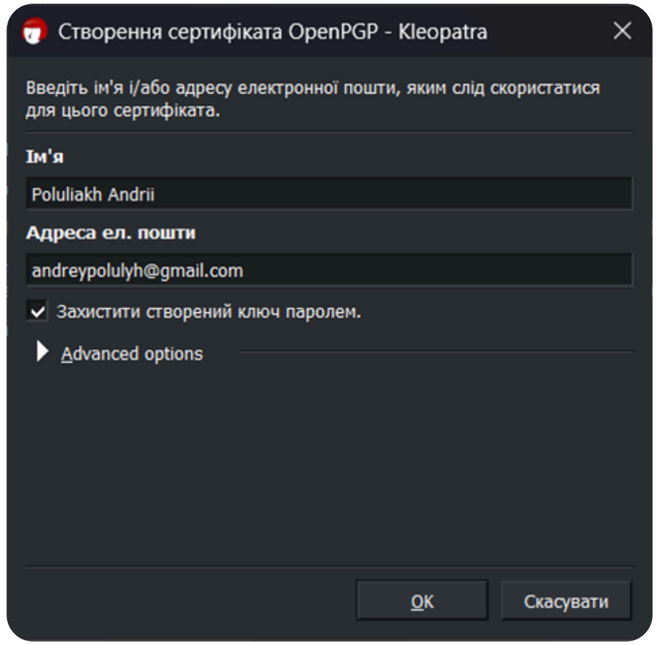
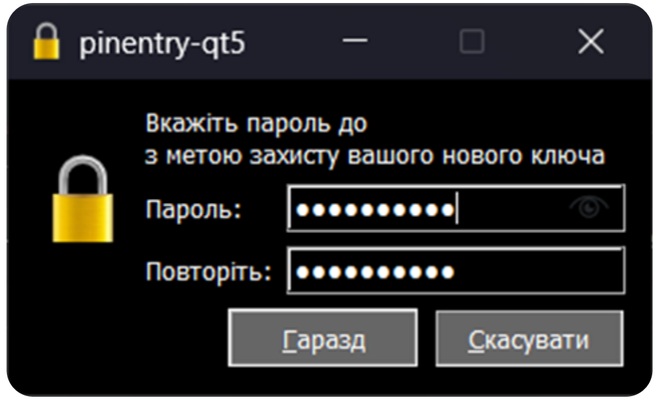
ЗАХИЩЕНА ЕЛЕКТРОННА ПОШТА

Виконав Полулях Андрій

КРОК 1. ДОСЛІДЖЕННЯ PGP-ШИФРУВАННЯ

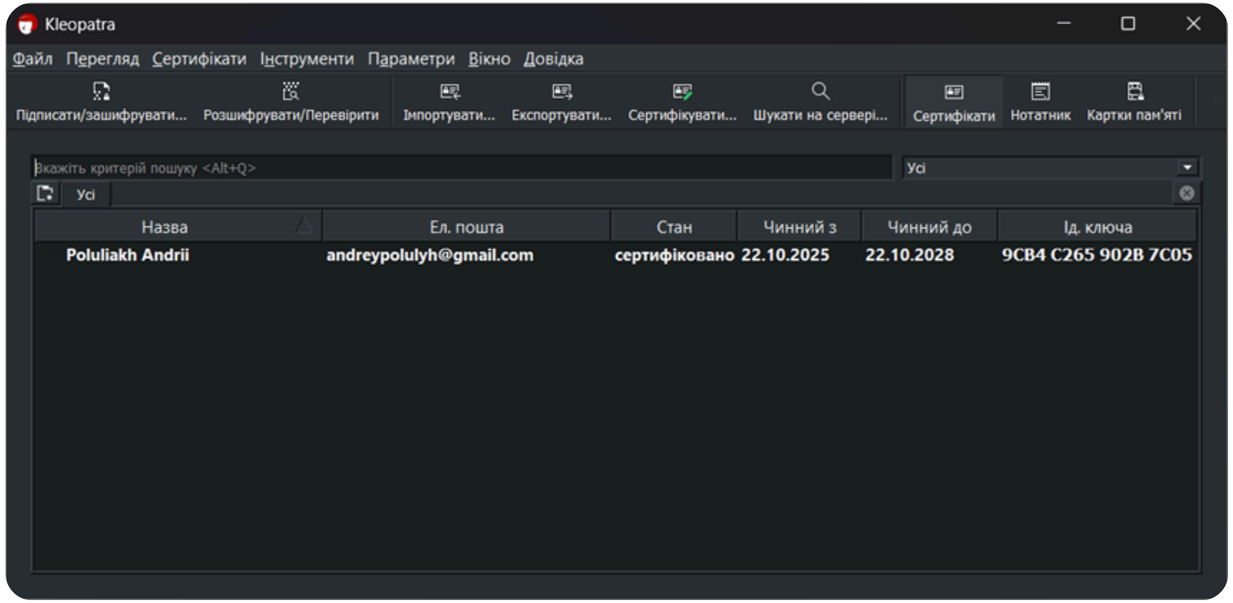
Для генерації пари ключів запускаємо програму Kleopatra.





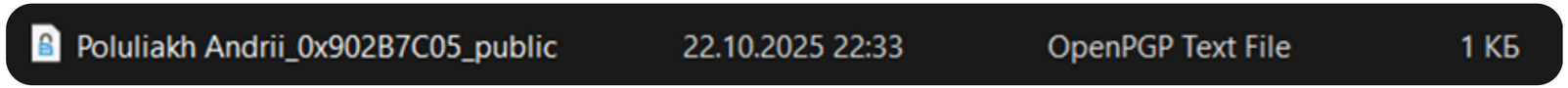
КРОК 1. ДОСЛІДЖЕННЯ PGP-ШИФРУВАННЯ

На головній сторінці відобразився створений ключ



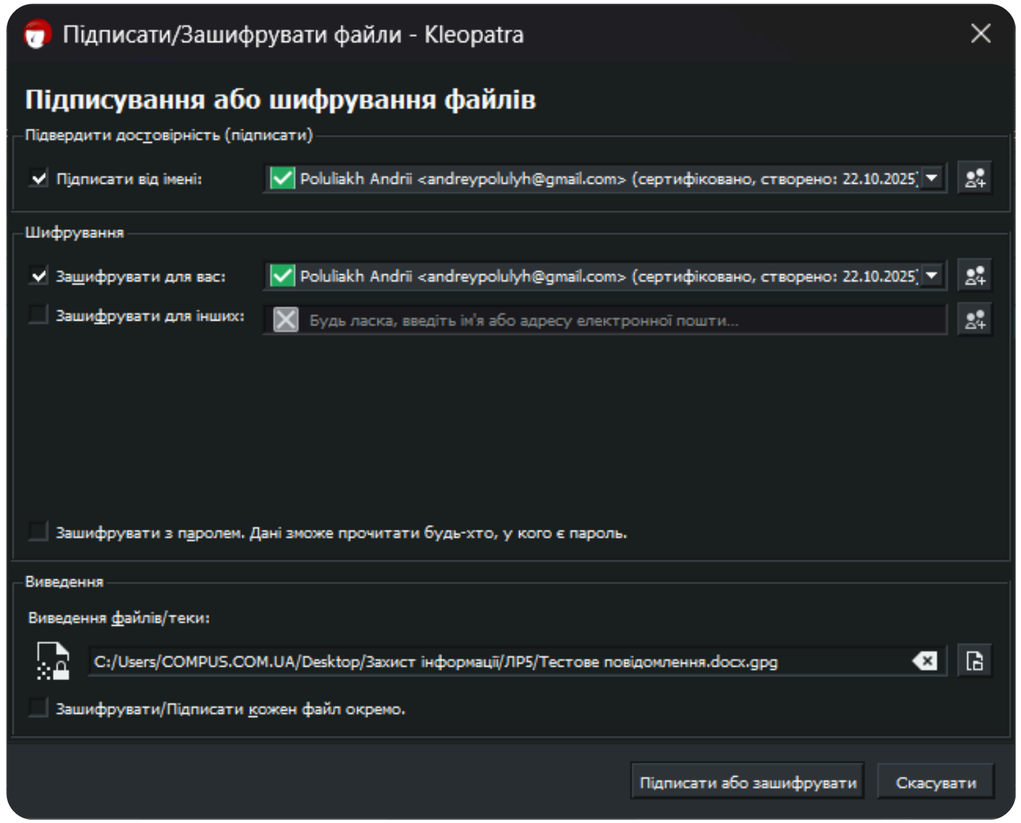
КРОК 1. ДОСЛІДЖЕННЯ PGP-ШИФРУВАННЯ

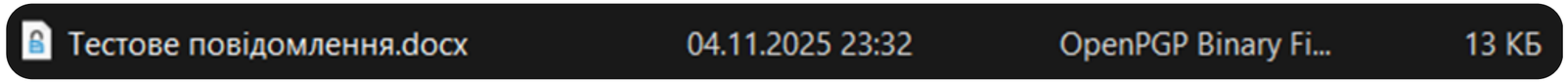
Для створення публічного ключа обираємо щойно створений приватний ключ та на панелі інструментів обираємо функцію «Експортувати позначений сертифікат»



КРОК 1. ДОСЛІДЖЕННЯ PGP-ШИФРУВАННЯ

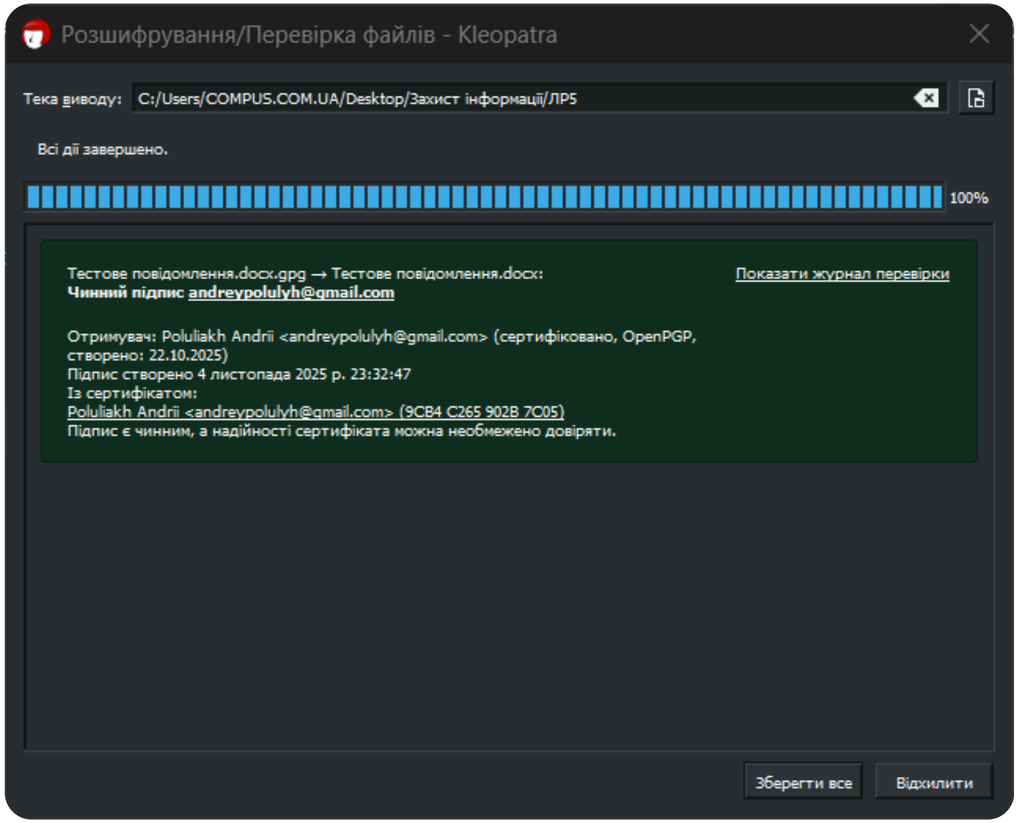
Щоб зашифрувати тестовий файл, на панелі інструментів обираю функцію «Підписати/зашифрувати» та обираю файл для шифрування



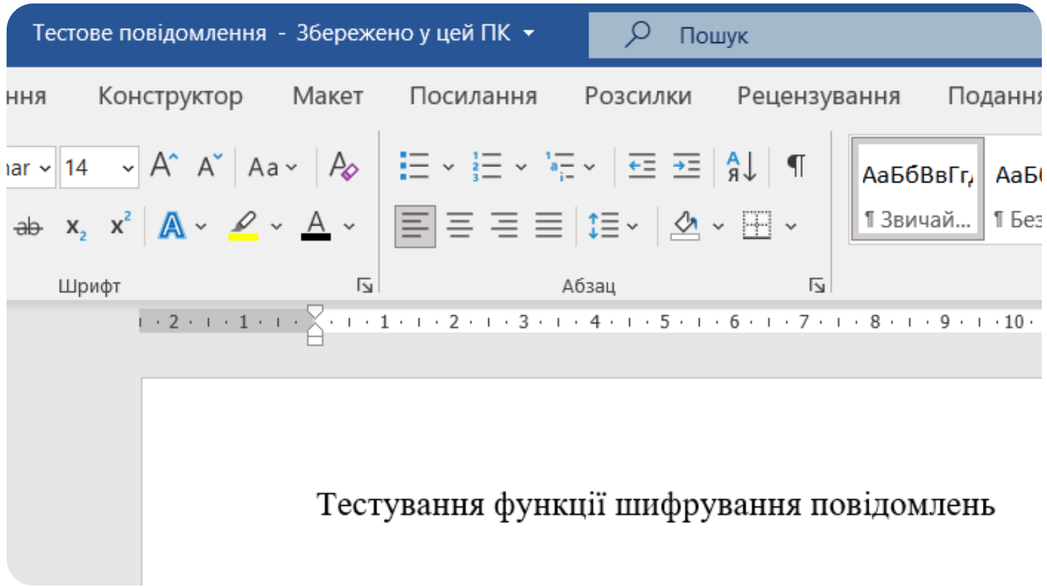


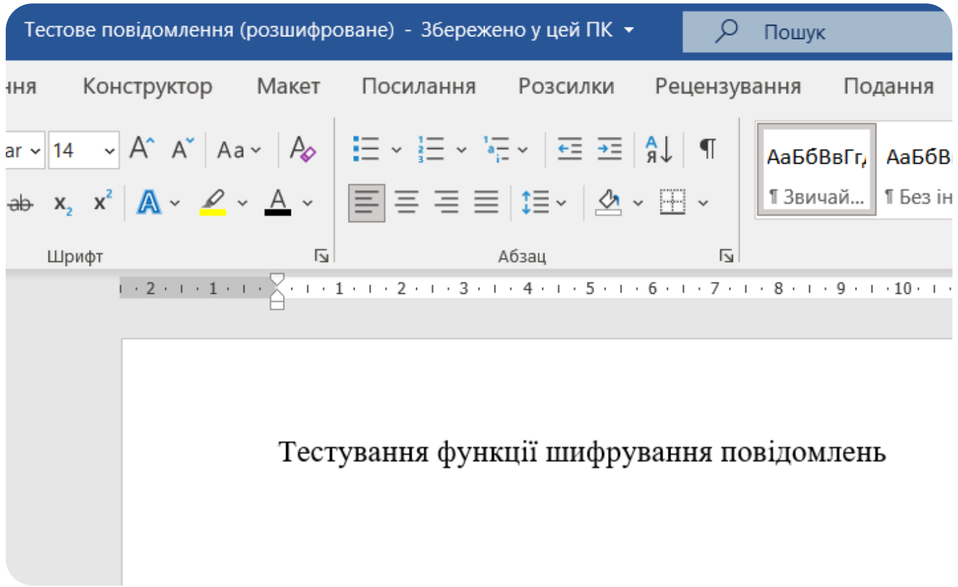
КРОК 1. ДОСЛІДЖЕННЯ PGP-ШИФРУВАННЯ

Для розшифрування натискаємо двічі ЛКМ по файлу, вводимо пароль та зберігаємо. Після чого з’являється розшифрований файл



КРОК 1. ДОСЛІДЖЕННЯ PGP-ШИФРУВАННЯ





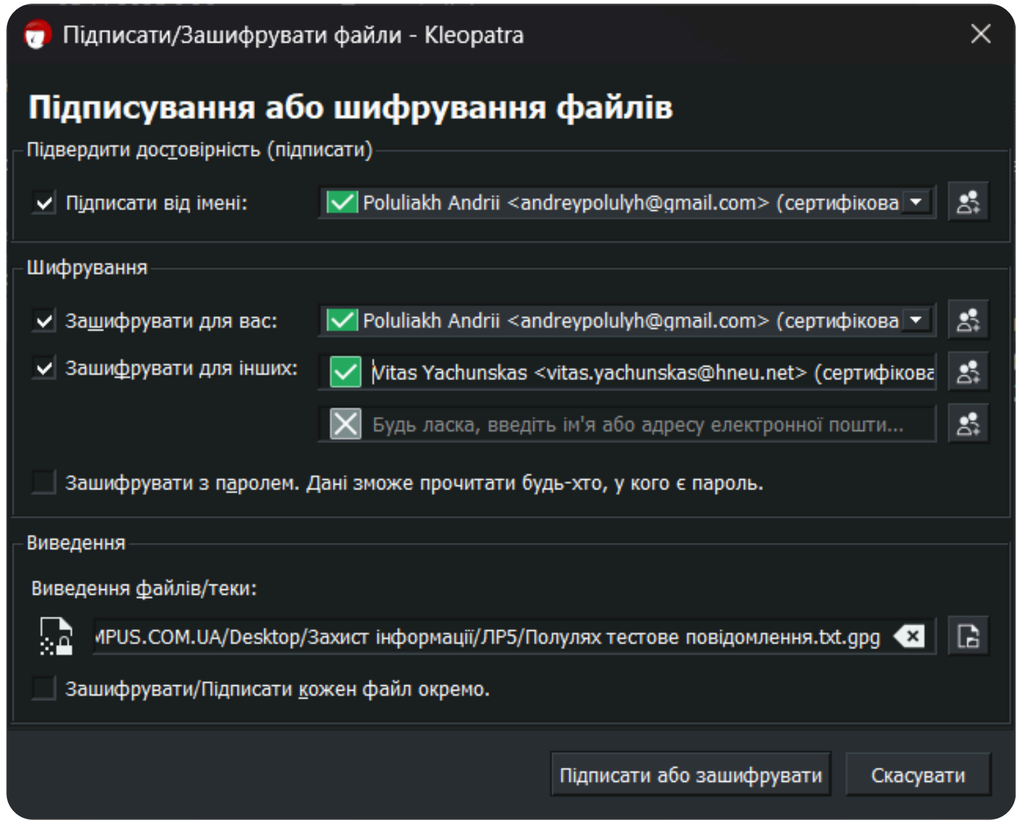
КРОК 2. ЗАШИФРОВАНА КОРЕСПОНДЕНЦІЯ

Отримую публічний ключ від Вітаса

Ячунскаса та надсилаю свій

КРОК 2. ЗАШИФРОВАНА КОРЕСПОНДЕНЦІЯ

Шифрую повідомлення для Вітаса з використанням його публічного ключа

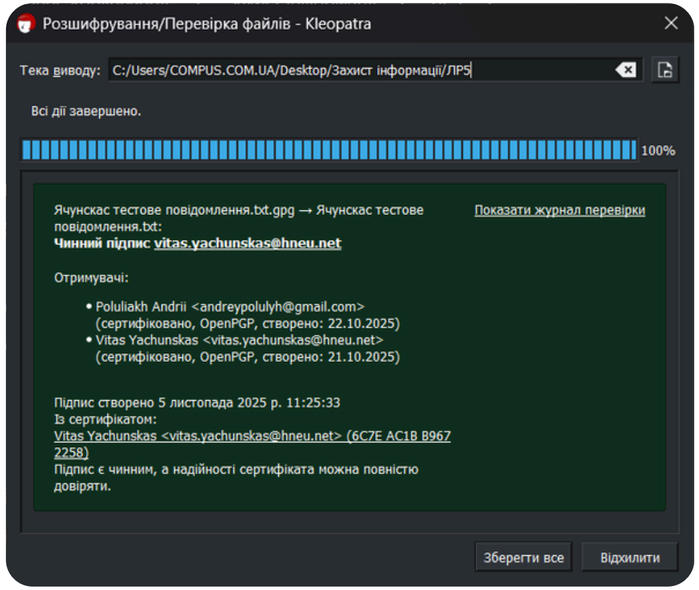


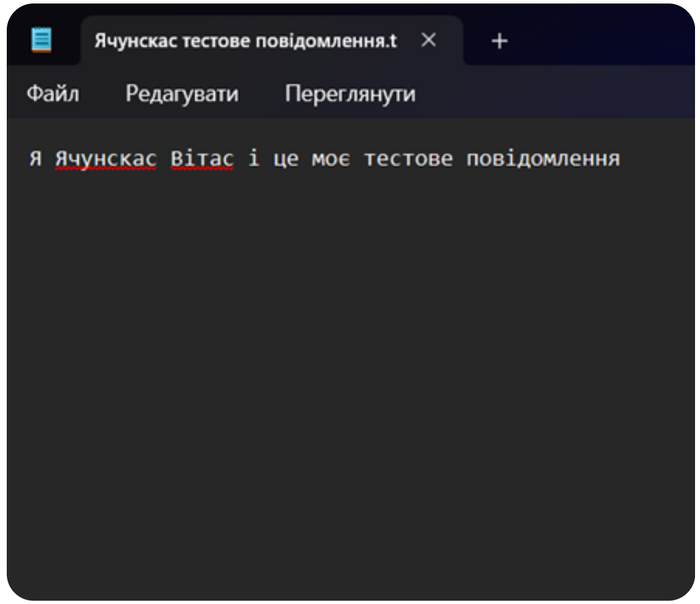
КРОК 2. ЗАШИФРОВАНА КОРЕСПОНДЕНЦІЯ

У той же час отримую зашифроване моїм публічним ключем повідомлення від Вітаса

КРОК 2. ЗАШИФРОВАНА КОРЕСПОНДЕНЦІЯ

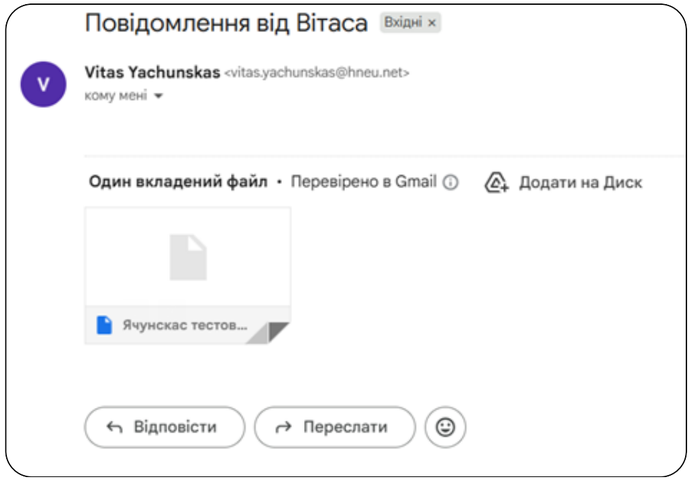
Для розшифрування відкриваю файл подвійним натисканням ЛКМ та вводжу пароль власного ключа, після чого з’являється вікно «Розшифрування/Перевірка файлів», де натискаю «Зберегти все». Розшифроване повідомлення з’являється у новому файлі

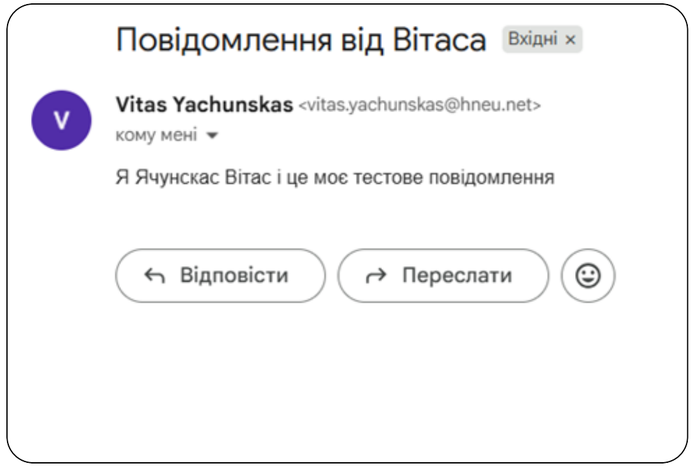




КРОК 3. АНАЛІЗ БЕЗПЕКИ ЕЛЕКТРОННОЇ ПОШТИ

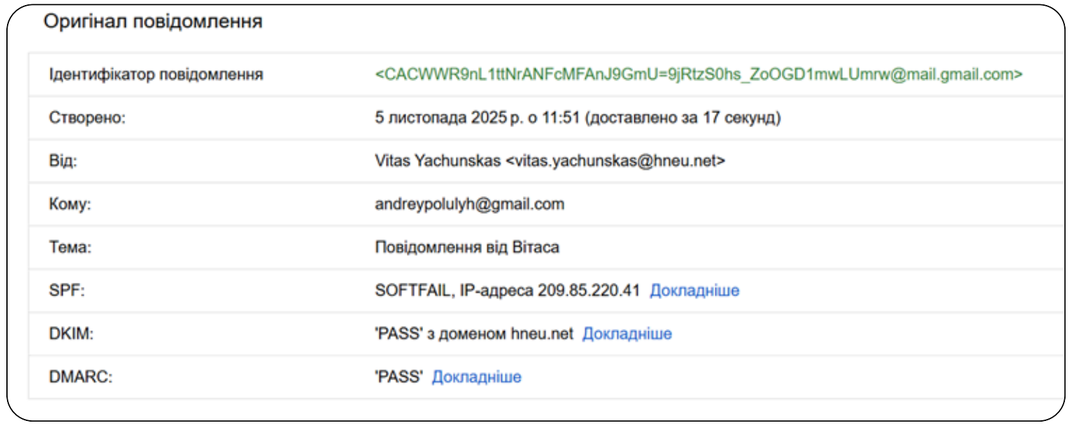
Оскільки сам лист зашифрувати неможливо, будемо відправляти файл з зашифрованим повідомленням





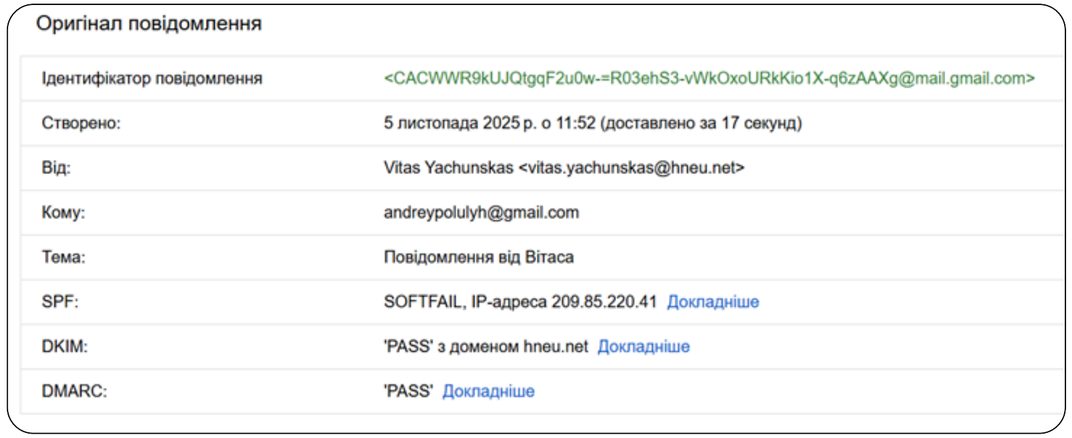
КРОК 3. АНАЛІЗ БЕЗПЕКИ ЕЛЕКТРОННОЇ ПОШТИ

Порівнюючи метадані листів, не спостерігаємо ніяких відмінностей



Оригінал повідомлення

Ідентифікатор повідомлення	<CACWWR9nL1ttNrANFcMFAnJ9GmU=9jRtzS0hs_ZoOGD1mwLUmrw@mail.gmail.com>
Створено:	5 листопада 2025 р. о 11:51 (доставлено за 17 секунд)
Від:	Vitas Yachunskas <vitas.yachunskas@hneu.net>
Кому:	andreypolulyh@gmail.com
Тема:	Повідомлення від Вітаса
SPF:	SOFTFAIL, IP-адреса 209.85.220.41 Докладніше
DKIM:	'PASS' з доменом hneu.net Докладніше
DMARC:	'PASS' Докладніше



Оригінал повідомлення

Ідентифікатор повідомлення	<CACWWR9kUJQtgqF2u0w-=R03ehS3-vWkOxoURkKio1X-q6zAAXg@mail.gmail.com>
Створено:	5 листопада 2025 р. о 11:52 (доставлено за 17 секунд)
Від:	Vitas Yachunskas <vitas.yachunskas@hneu.net>
Кому:	andreypolulyh@gmail.com
Тема:	Повідомлення від Вітаса
SPF:	SOFTFAIL, IP-адреса 209.85.220.41 Докладніше
DKIM:	'PASS' з доменом hneu.net Докладніше
DMARC:	'PASS' Докладніше

КРОК 3. АНАЛІЗ БЕЗПЕКИ ЕЛЕКТРОННОЇ ПОШТИ

Роблячи висновок, можна сказати, що рівень приватності на високому рівні, якщо брати до уваги лише захищеність повідомлень. Метадані листів у будь-якому випадку задані явно, оскільки сам лист не шифрується. Це зменшує приватність, але не критично.

ДЯКУЮ ЗА УВАГУ