

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ  
УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №4  
з курсу «Безпека банківських систем»

ДОСЛІДЖЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ У СПРОЩЕНИХ  
EDI-СИСТЕМАХ

Харків 2023



**Мета:** ознайомитися з системою EDI (Electronic Data Interchange) та методами захисту інформації в даній системі. Отримати практичні навички з роботи із системою GNU Privacy Guard із використанням оболонки Kleopatra

## 1 ТЕОРЕТИЧНІ ВІДОМОСТІ

### 1.1 Технологія EDI

EDI (Electronic Data Interchange) – це процес передачі структурованої цифрової інформації, що дозволяє організаціям передавати одна одній комерційні дані – торгові, фінансові, транспортні та інші.

Структурований документ – документ у форматі XML/JSON, тобто такий, який передається у попередньо налаштованій та стандартизованій структурі даних.

Неструктурований документ – це документ з довільною структурою даних; до таких документів належать PDF, PNG, JPG, DOCX, XLSX та інші формати.

EDI існує по крайній мірі з початку 70-х років, і існує безліч стандартів EDI (включаючи X12, EDIFACT, ODETTE і т. д.), деякі з яких відповідають потребностям конкретних галузей або регіонів. Це також відноситься до конкретного сімейства стандартів. У 1996 році Національний інститут стандартів і технологій визначив електронний обмін даними як «обмін між комп'ютерами строго відформатованими повідомленнями, які представляють документи, відмінні від грошових інструментів». EDI передбачає послідовність повідомлень між двома сторонами, будь-яка з яких може виступати в якості відправника або отримувача. Відформатовані дані, що представляють документи, можуть бути передані відправнику для одержання по телекомунікаціям або фізично перенесені на електронних носіях. В EDI звичайна обробка отриманих повідомлень здійснюється тільки комп'ютером. Втручання людини в обробку отриманого повідомлення зазвичай призначене



лише для виправлення помилок, для перевірки якості та для виконання спеціальних дій. Коротко кажучи, EDI можна визначити як передачу структурованих даних у відповідності з узгодженими стандартами повідомлень з однієї комп'ютерної системи в іншу без втручання людини.

Переваги використання EDI-технологій:

- спрощує передачу електронних даних, оскільки є підготовлені форми структурованих документів, які дають можливість буквально за кілька кліків «миші» обмінюватися даними зі своїми контрагентами;
- пришвидшення обробки даних – скорочення на 80% часу на опрацювання кожного документа у цілому ланцюгу;
- зводяться до мінімуму вплив людського фактора та ризик виникнення помилок – система EDI автоматично виявляє та усуває їх;
- значно прискорюється і спрощується пошук необхідної інформації у базі даних;
- можливість в секунду запускати бізнес-процеси і заощаджувати на витратах, пов'язаних з паперовим документообігом: людино-години, витратні матеріали та ін.

Приклад використання EDI у банківській сфері – «Товариство всесвітніх міжбанківських фінансових каналів зв'язку», – *SWIFT* – міжнародна міжбанківська система передачі інформації та здійснення платежів. Сама система не є платіжною – вона не виконує функцій розрахунку та взаємного клірингу між учасниками.

## 1.2 Стандарти передачі даних у EDI

Інформація в рамках EDI передається не в довільному порядку – для цього розробили та застосовують низку стандартів та правил, що дозволяють відправникам та одержувачам даних «розмовляти однією мовою».

Найпоширеніші типи стандартних EDI-документів:

- Замовлення. При необхідності оформити замовлення у постачальника використовують документ ORDERS. Документ містить вичерпну інформацію



про перелік замовлених товарів (послуг), їх кількість, ціни, дати і адреси доставки.

– Відповідь на замовлення. Постачальник може підтвердити або не підтвердити замовлення. Для цього він використовує EDI-документ ORDRSP. Постачальник має право розширити стандартну інформацію в ньому та доповнити її пропозиціями альтернативних товарів, іншими відомостями.

– Каталог товарів. Виробники та постачальники зацікавлені в інформуванні своїх клієнтів про асортимент наявної продукції. Вони роблять це за допомогою ще одного стандартного EDI-документа – PRICAT. Це електронне повідомлення, що містить повний або ж частковий перелік товарів, а саме: детальний опис товарів, включаючи цінові дані, логістичні характеристики, технічні і функціональні дані товарів.

– Рахунок-фактура. Щоб автоматично сформувати рахунок-фактуру для оплати поставлених товарів, використовують документ INVOIC. З його допомогою можна не лише оплачувати продукцію, а й звітувати перед податковою інспекцією (в останньому випадку знадобиться електронний цифровий підпис).

– Повідомлення про відвантаження. Існує EDI-аналог паперового товаросупровідного документа – DESADV. Це електронне повідомлення про успішне відвантаження товарів зі складу, яке містить докладну інформацію про поставлену продукцію.

– Повідомлення про прийом. Покупець повинен проінформувати постачальника про прийняту продукцію. Для цього є таке повідомлення EDI, як RECADV.

– Повідомлення про повернення. Покупець із тих чи інших причин може відмовитися від отримання товару та повернути його постачальнику. Для цього він використовує такий документ, як RETANN, що містить відомості про товари, що повертаються, і причини відмови в їх прийманні.



### 1.3 EDI – автономний об'єкт захисту

Електронний документ (спільно з його метаданими), будучи самостійним юридичним об'єктом, з погляду інформаційної безпеки також є самостійним, якщо точніше – автономним об'єктом захисту, для якого мають бути забезпечені наступні пріоритети безпеки та вимоги безпеки:

- має бути забезпечена цілісність (ідентичність, автентичність документа). Пріоритет є абсолютним і має бути забезпечений на всіх етапах життєвого циклу документа;
- має бути забезпечено доступність документа на всіх етапах життєвого циклу документа. Правила надання доступу до документа з часом можуть змінюватись залежно від його статусу;
- має бути забезпечена конфіденційність документа. Вимоги до віднесення документа до категорії конфіденційних можуть змінюватися з часом;
- має бути забезпечено збереження документа на всьому життєвому циклі та захищеність від неконтрольованого знищення.

Основний фактор, що дозволяє використовувати електронний документ у системі правовідносин – це можливість надання йому у разі необхідності юридичної сили протягом усього життєвого циклу, або з точки зору права забезпечити необхідний рівень довіри.

Довіра до документа виникає лише тому випадку, коли забезпечується його автентичність, що передбачає забезпечення ідентичності (ідентифікації) і цілісності електронного документа, природно також протягом усього його життєвого циклу.



## 2 ХІД РОБОТИ

**2.1 GNU Privacy Guard, GnuPG** – вільно поширюване програмне забезпечення, що використовує криптографію з відкритим ключем. Перша версія проекту, створена Вернером Кохом (Werner Koch) та профінансована німецьким урядом, вийшла в світ у 1999 році під ліцензією GNU General Public. Функції GnuPG дозволяють шифрувати та підписувати повідомлення за допомогою цифрового підпису, а також керувати списками відкритих ключів респондентів.

Звичним інтерфейсом для GnuPG є командний рядок, проте на сьогоднішній день існують різні зовнішні оболонки, які роблять доступною функціональність цієї програми через графічний інтерфейс користувача, наприклад *Kleopatra* для Windows (<https://www.gpg4win.org/download.html>) або *GNU Privacy Assistant* (GPA) для Linux.

В GnuPG використовуються різні криптографічні алгоритми: симетричні шифри, шифрування з відкритим ключем і змішані (гібридні) алгоритми.

### 2.2 Гібридна (змішана, комбінована) криптосистема

Гібридна (змішана, комбінована) криптосистема – це криптосистема, в якій розподіл ключів здійснюється за допомогою асиметричних криптоалгоритмів, а процес шифрування даних – за допомогою симетричних. Тобто симетричний ключ використовується для шифрування даних, а асиметричний для шифрування самого симетричного ключа. Гібридні криптосистеми поєднують в собі зручність розподілу секретних ключів та високу швидкість шифрування.


Як правило, при гібридному шифруванні створюється *одноразовий секретний сеансовий ключ* – це псевдовипадкове число, яке генерується на основі випадкових рухів миші, натискань клавіш клавіатури тощо. Такий ключ використовується лише один раз для шифрування повідомлення з використанням деякого надійного та швидкого симетричного алгоритму.



Сеансовий ключ зашифровується відкритим ключем одержувача та додається до шифротексту. Під час дешифрування процедури виконуються у зворотному порядку.

### 2.3 Створення пари ключів

При першому запуску *Kleopatra* (рис. 2.1) потрібно створити власну зв'язку ключів. Для цього необхідно виконати наступні дії:

1) натиснути кнопку  або скористатися меню *Файл*→*Створити пару ключів*;

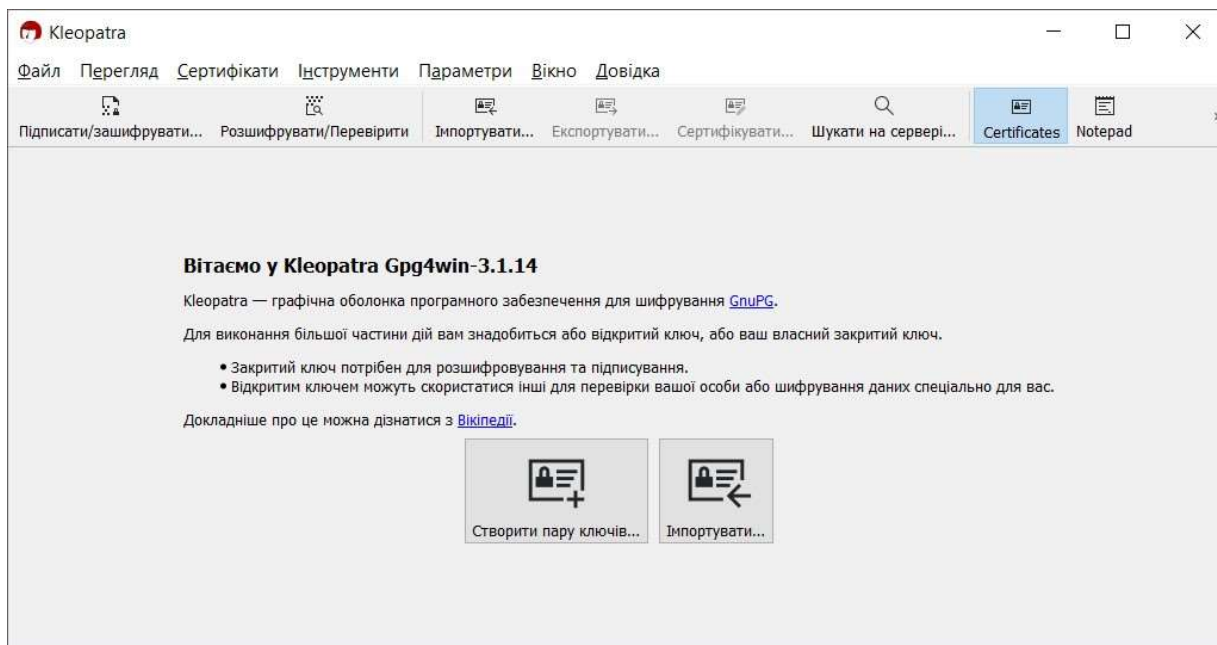
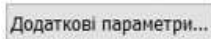


Рис. 2.1 – Стартове вікно оболонки Kleopatra

2) у вікні *Майстра створення ключів* (рис. 2.2) потрібно ввести відомості про себе у відповідні поля (ім'я, електронну адресу); кнопка  дозволяє вибрати тип ключа його довжину, строк дії тощо.

Основною особливістю GnuPG є система ключів. В GnuPG користувач створює декілька ключів, причому кожен служить для окремої дії (і використовує різні алгоритми). Один із ключів, що створюється першим, є *головним ключем*, решта ключів йому підпорядковані – це *підключі* (субключі).



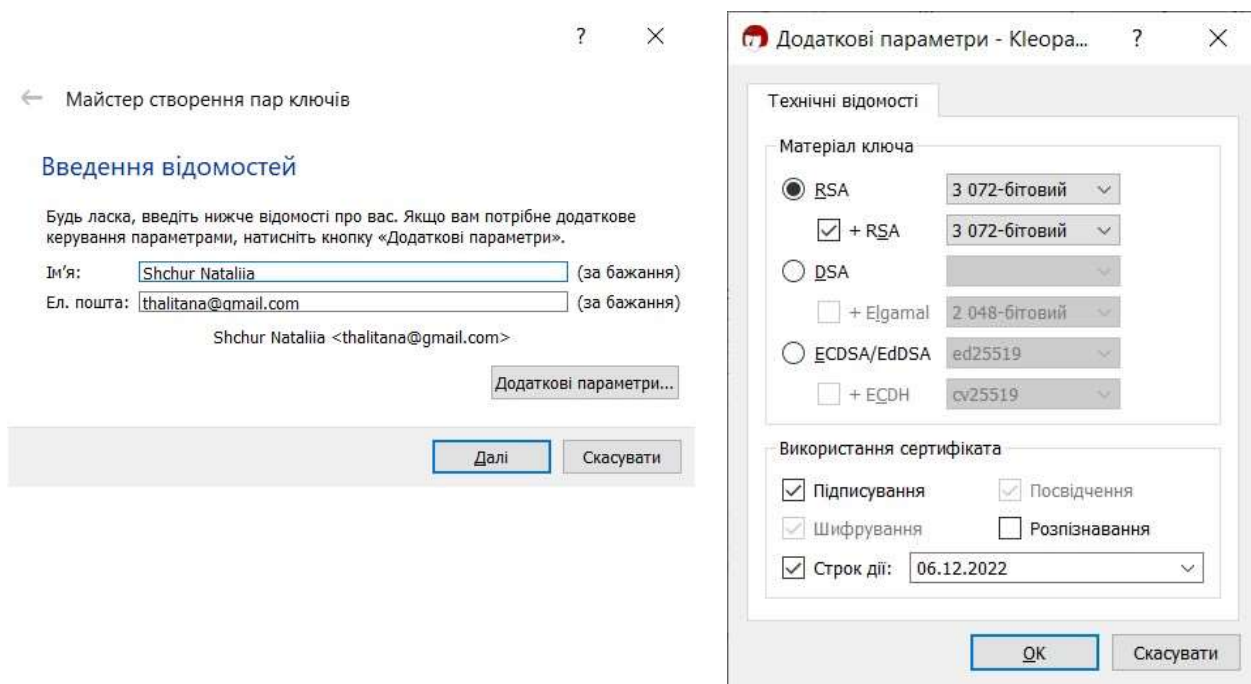


Рис. 2.2 – Створення пари ключів за допомогою майстра

3) у наступному вікні необхідно натиснути Створити та ввести пароль для захисту нового ключа (рис. 2.3);

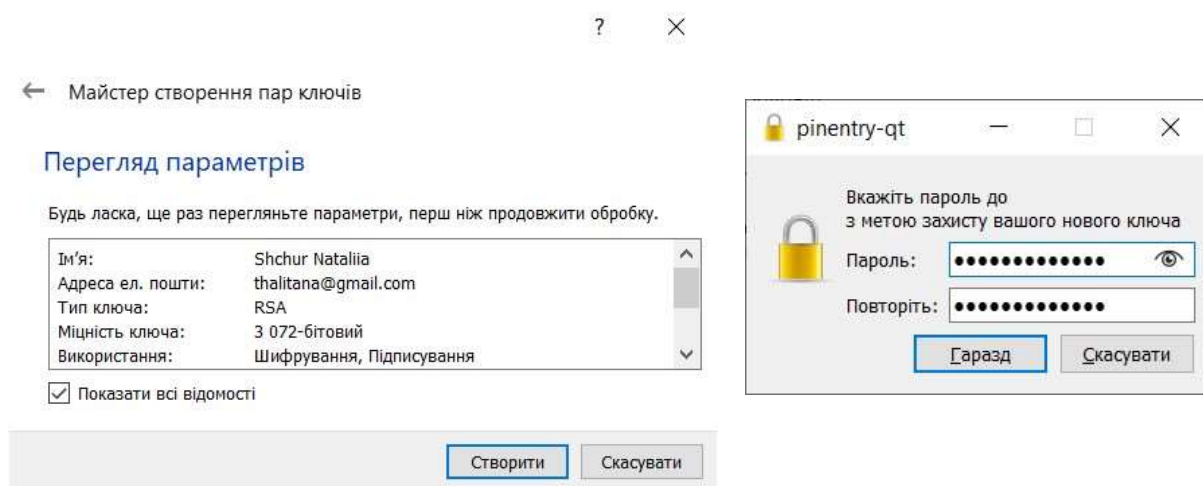


Рис. 2.3 – Введення паролю для захисту нового ключа

4) у наступному вікні майстер має повідомити про успішне створення ключів (рис. 2.4), після чого потрібно натиснути кнопку Завершити.



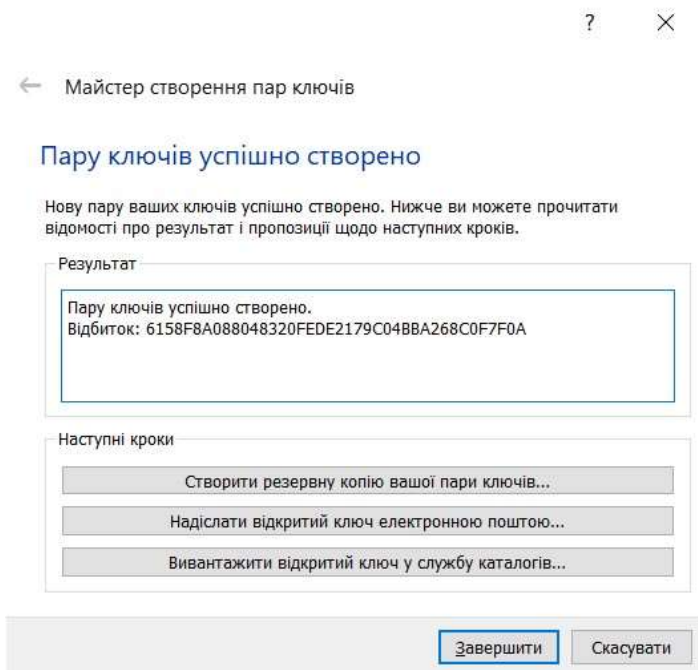


Рис. 2.4 – Повідомлення про успішне створення ключів

Усі функції управління ключами здійснюються у вікні Kleopatra (рис. 2.5), в якому висвітлюються всі ключі, створені користувачем для власного користування, а також усі імпортовані публічні ключі його кореспондентів.

Ключі зберігаються у зашифрованій формі у вигляді двох файлів, які називаються зв'язками ключів (keyrings). Ці файли записуються у папках на диску відповідно до поточних налаштувань.

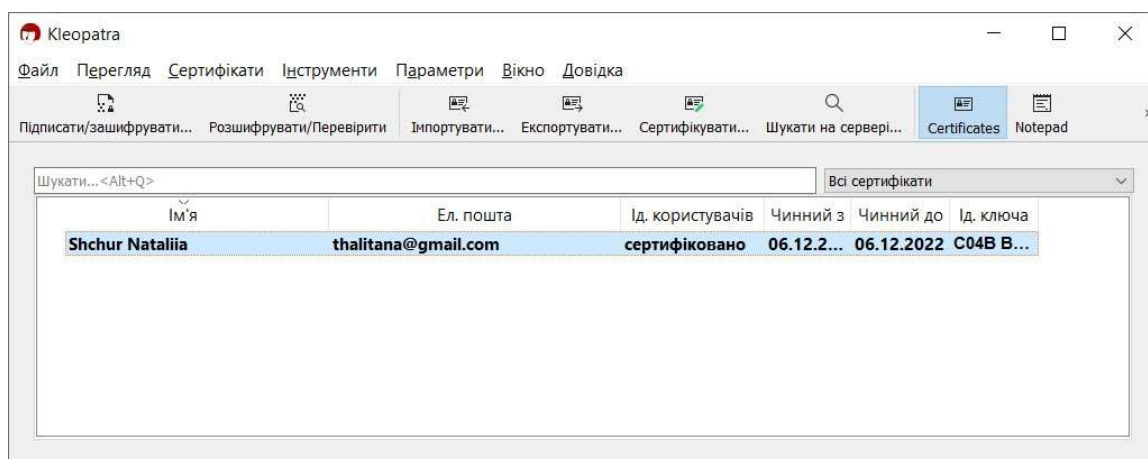


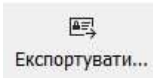
Рис. 2.5 – Список наявних ключів у вікні оболонки Kleopatra

## 2.4 Експорт ключів

До початку обміну повідомленнями з іншими користувачами GPG варто обмінятися з ними публічними ключами.

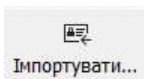


Для експорту ключа потрібно:

- 1) у вікні *Kleopatra* натиснути кнопку  або у контекстному меню електронного ключа вибрати пункт *Експортувати*, або використати меню *Файл* → *Експортувати*;
- 2) обрати папку для збереження ключа, ввести його ім'я та натиснути *Зберегти*.

## 2.5 Імпорт ключів

Імпортувати відкриті ключі інших користувачів можна, виконавши такі дії:

- 1) у вікні *Kleopatra* натиснути кнопку  або у контекстному меню електронного ключа вибрати пункт *Імпортувати*, або використати меню *Файл* → *Імпортувати*;
- 2) обрати ключ на диску, ввести його ім'я та натиснути *Відкрити*;
- 3) також варто погодитися із перевіркою сертифіката ключа (рис. 2.5).

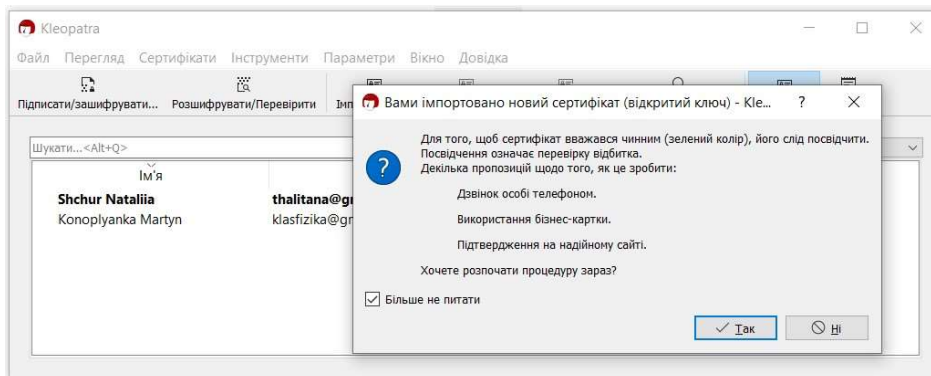


Рис. 2.5 – Перевірка сертифіката ключа, що імпортується

## 2.6 Шифрування та (або) підписування файлів

Для шифрування та (або) підписування файлу необхідно натиснути

кнопку  або використати меню *Файл* → *Підписати/зашифрувати*. Відкриється діалогове вікно

Підписати/зашифрувати файли (рис. 2.6), у якому потрібно обрати необхідну дію та обрати відкриті ключі одержувача(-ів)

повідомлення, натиснувши по піктограмі

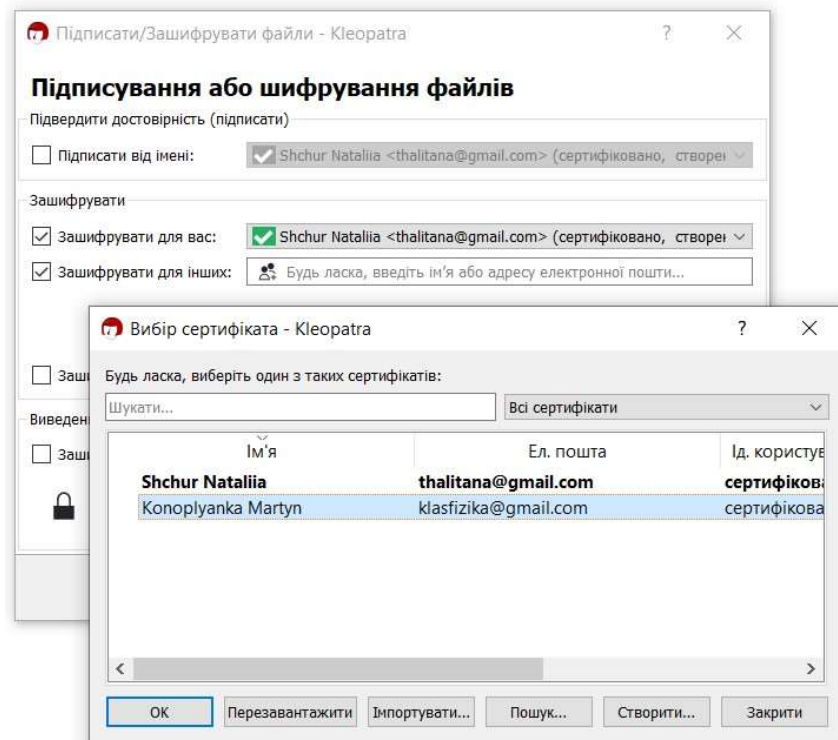



Рис. 2.6 – Діалогове вікно Підписати/зашифрувати файли

Підписати файл за допомогою свого відкритого ключа дозволяє опція:



Також існує можливість виконати дві описані вище операції одночасно.

## 2.7 Розшифрування та (або) перевірка підпису файлів

Для розшифрування/перевірки цифрових підписів файлів використовуються кнопка  Розшифрувати/Перевірити та пункт меню *Файл* → *Розшифрувати/Перевірити*.

Під час розшифрування на екрані з'явиться вікно перевірки пароля. Файл буде розшифрований після введення правильного пароля за умови, що його було зашифровано з використанням відкритого ключа отримувача (рис. 2.7). Очевидно також, що розшифрування файлу можливе тільки за умов наявності

у середовищі вікна *Kleopatra* закритого ключа отримувача. Розшифрованому файлу автоматично присвоюється назва файлу-оригіналу (файлу, який було зашифровано).

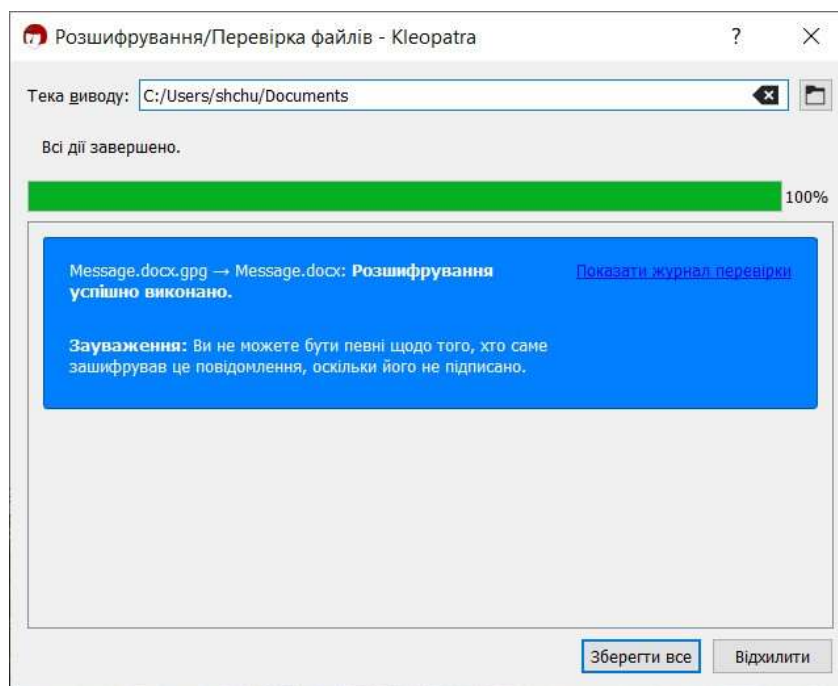


Рис. 2.7 – Вікно розшифрування файлу

Якщо файл має підпис, на екрані з'являється вікно з повідомленням, яке містить назву файлу, відомості про особу, яка підписала файл, дату і час накладання підпису та позначку, чи залишається підпис дійсним (рис. 2.8).

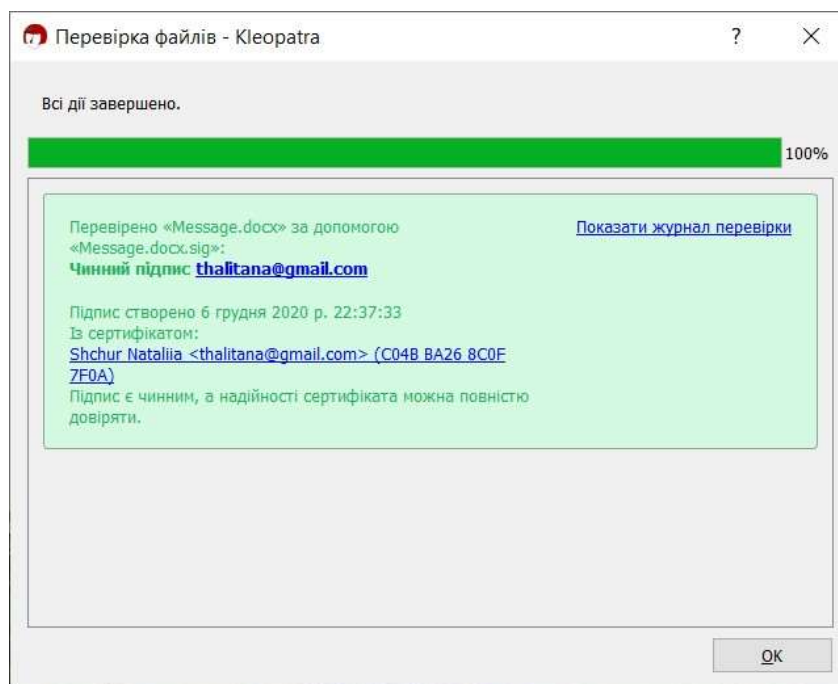


Рис. 2.8 – Вікно перевірки підпису

## 2.8 Доступ до функцій GPG

Для забезпечення зручного виконання операцій шифрування, підписування, дешифрування, перевірки підпису тощо, у контекстному меню файлу (рис. 2.8) можна обрати *Sign and encrypt* або *More GpgEX option*.

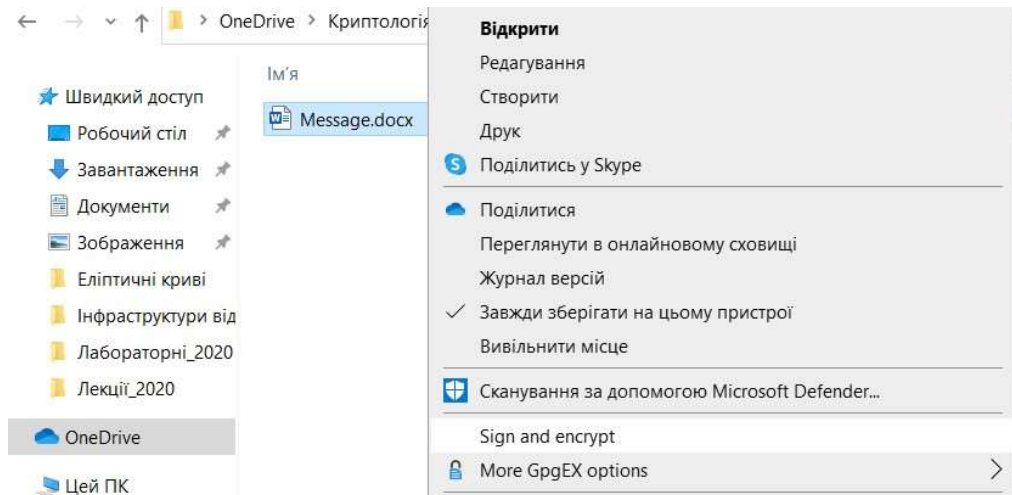


Рис. 2.9 – Вибір у контекстному меню документа команд GPG

### 3 ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

1. Завантажити та встановити програмне забезпечення GNU Privacy Guard із використанням оболонки Kleopatra.
2. Повторити приклади з Розділу 2.
3. Протестувати програму на роботу з помилковими ключами.
4. Перевірити можливість прочитати файл без використання системи дешифрування.

#### Контрольні питання:

1. Що являє собою система EDI?
2. Які типи стандартних EDI-документів ви знаєте?
3. Як використовується система EDI в банківській сфері?
4. Яке призначення програми GNU Privacy Guard?
5. Яким чином GNU Privacy Guard захищає документи?

