МІНІСТЕРСТВО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ

ДЕРЖАВНЕ ПІДПРИЄМСТВО
"ДЕРЖАВНИЙ ЦЕНТР ІНФОРМАЦІЙНИХ РЕСУРСІВ УКРАЇНИ"

ІНСТРУКЦІЯ

Встановлення ПЗ «CryptoAutograph».

Використання ПЗ “CryptoAutograph ” для підписання файлів та перевірки кваліфікованого електронного підпису (КЕП).

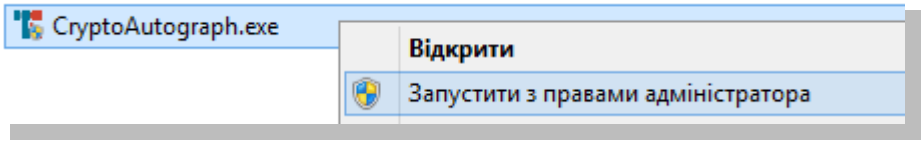
КИЇВ – 2021

ЗМІСТ:

1. Встановлення клієнтської компоненти «CryptoAutograph»

Перевірене та робоче програмне забезпечення розміщено на сайті Державного підприємства «Державний центр інформаційних ресурсів України» (https://dir.gov.ua/downloads/cryptoautograph). Необхідно завантажити архів інсталяційного пакету в локальну папку на комп'ютері та розпакувати архів.

Для встановлення програмного забезпечення треба запустити інсталяційний пакет з правами «Адміністратора» операційної системи.



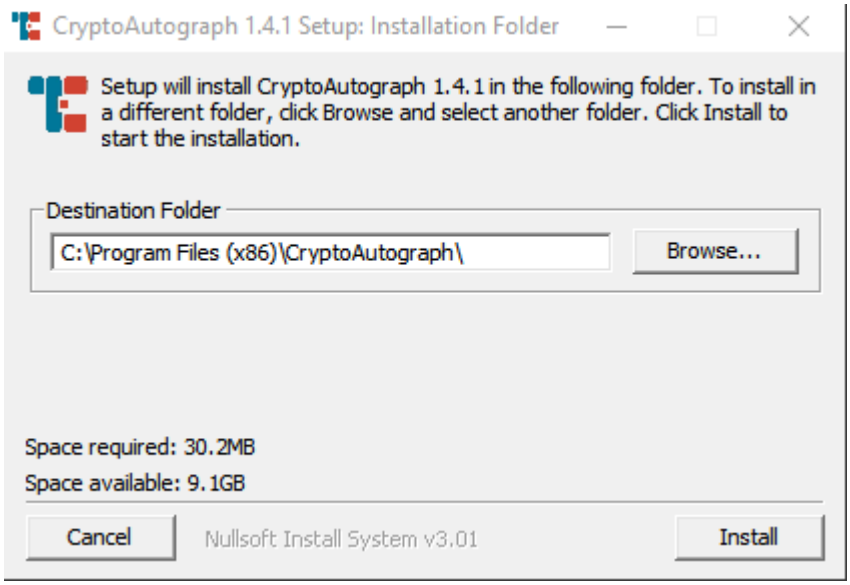
Запустити файл інсталяційного пакету «CryptoAutograph.exe» через файловий менеджер операційної системи за допомогою виділення його і натиснення клавіші «Enter», подвійного натискання лівої кнопки миші або через меню після натискання правої кнопки миші.

У вікні «CryptoAutograph 1.4.1 Setup…» необхідно обрати каталог для встановлення програмного забезпечення «Destination Folder» за допомогою кнопки «Browse…», але **рекомендується** залишити каталог для встановлення той, що пропонується «за замовчуванням»:

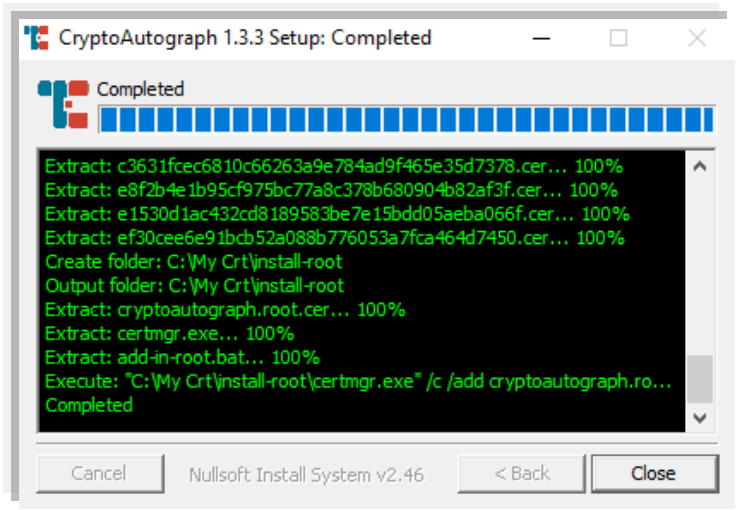
C:\Program Files (x86)\CryptoAutograph\

Для встановлення програмного забезпечення натисніть кнопку «Install».

Для відхилення процесу встановлення програмного забезпечення натисніть кнопку «Cancel».



Дочекайтеся завершення процесу встановлення програмного забезпечення.



Після завершення процесу встановлення програмного забезпечення необхідно натиснути кнопку «Close».

Програмне забезпечення «CryptoAutograph» готово до налаштування.

2. Встановлення файлу електронної ліцензії для роботи клієнтської компоненти «CryptoAutograph»

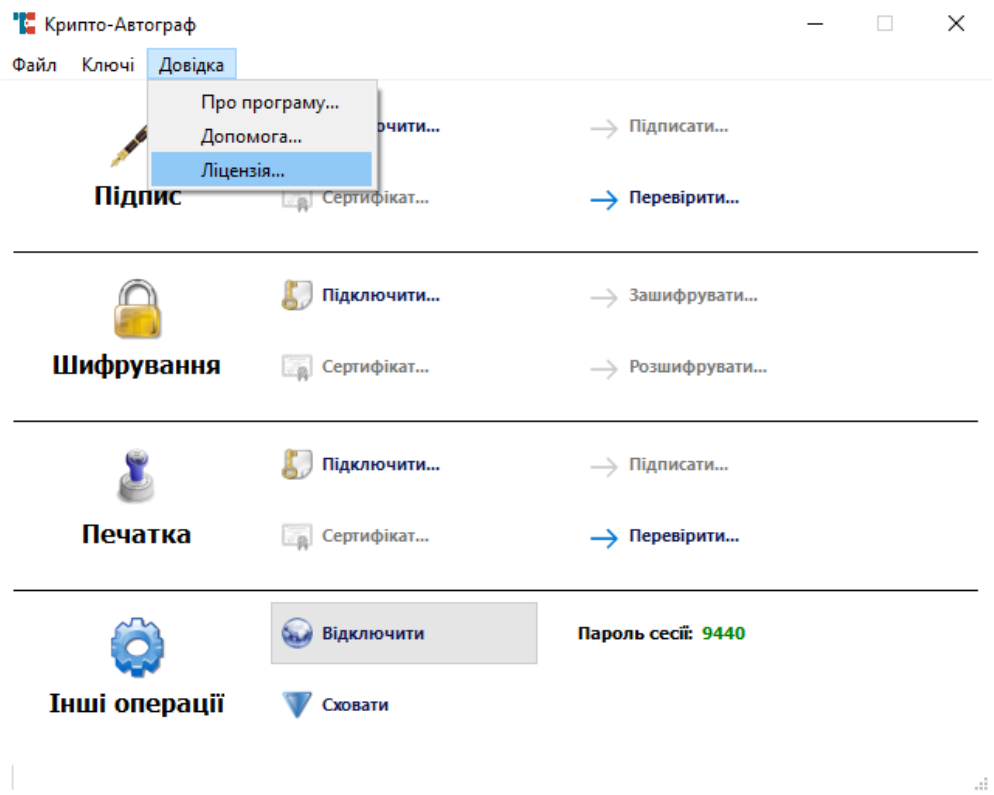
Отриманий електронний файл ліцензії «license.dat» (електронний файл ліцензії, який було надіслано поштою разом із новою версією «CryptoAutograph») скопіюйте до каталогу в який було встановлено програмне забезпечення «CryptoAutograph».

Примітка: Для копіювання фалу «license.dat» необхідно володіти правами «Адміністратора» операційної системи.

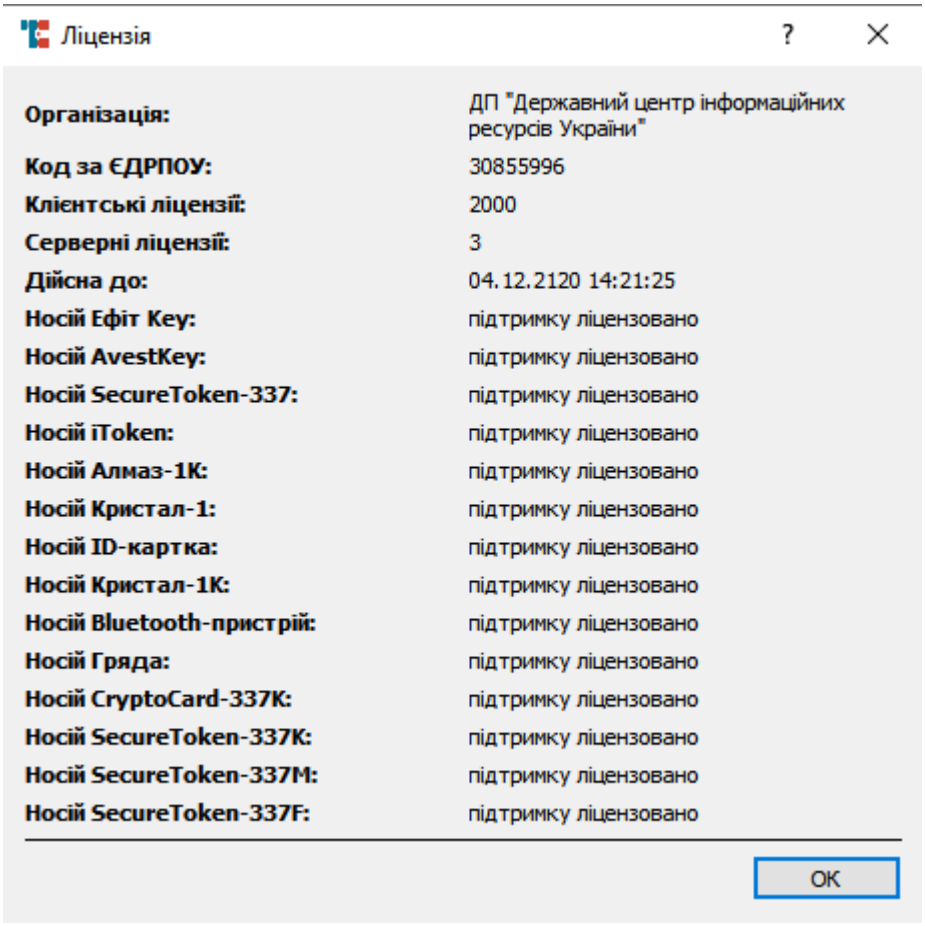
«За замовчуванням» це каталог: *C:\Program Files (x86)\CryptoAutograph*

В результаті копіювання електронний файл ліцензії повинен бути розміщений за посиланням: *C:\Program Files (x86)\CryptoAutograph\license.dat*

Для перевірки коректності встановлення ліцензії запустіть програмне забезпечення через ярлик «CryptoAutograph» на «Робочому столі» або меню «Пуск» та оберіть в графічному інтерфейсі програмного забезпечення «Довідка» → «Ліцензія…».



Відображення інформації про вміст «електронного файлу ліцензії» свідчить про успішне встановлення Вами ліцензії на програмне забезпечення «CryptoAutograph».

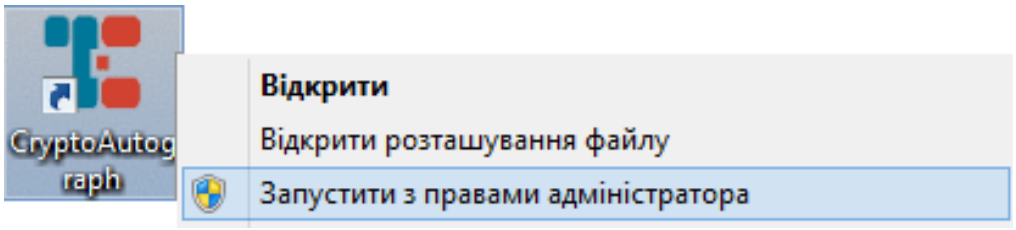

Ліцензія
?
Організація:
ДП "Державний центр інформаційних ресурсів України"
Код за ЄДРПОУ:
30855996
Клієнтські ліцензії:
2000
Серверні ліцензії:
3
Дійсна до:
04.12.2120 14:21:25
Носій Ефіт Key:
підтримку ліцензовано
Носій AvestKey:
підтримку ліцензовано
Носій SecureToken-337:
підтримку ліцензовано
Носій iToken:
підтримку ліцензовано
Носій Алмаз-1К:
підтримку ліцензовано
Носій Кристал-1:
підтримку ліцензовано
Носій ID-картка:
підтримку ліцензовано
Носій Кристал-1К:
підтримку ліцензовано
Носій Bluetooth-пристрій:
підтримку ліцензовано
Носій Гряда:
підтримку ліцензовано
Носій CryptoCard-337K:
підтримку ліцензовано
Носій SecureToken-337K:
підтримку ліцензовано
Носій SecureToken-337M:
підтримку ліцензовано
Носій SecureToken-337F:
підтримку ліцензовано
OK

3. Налаштування клієнтської компоненти «CryptoAutograph»

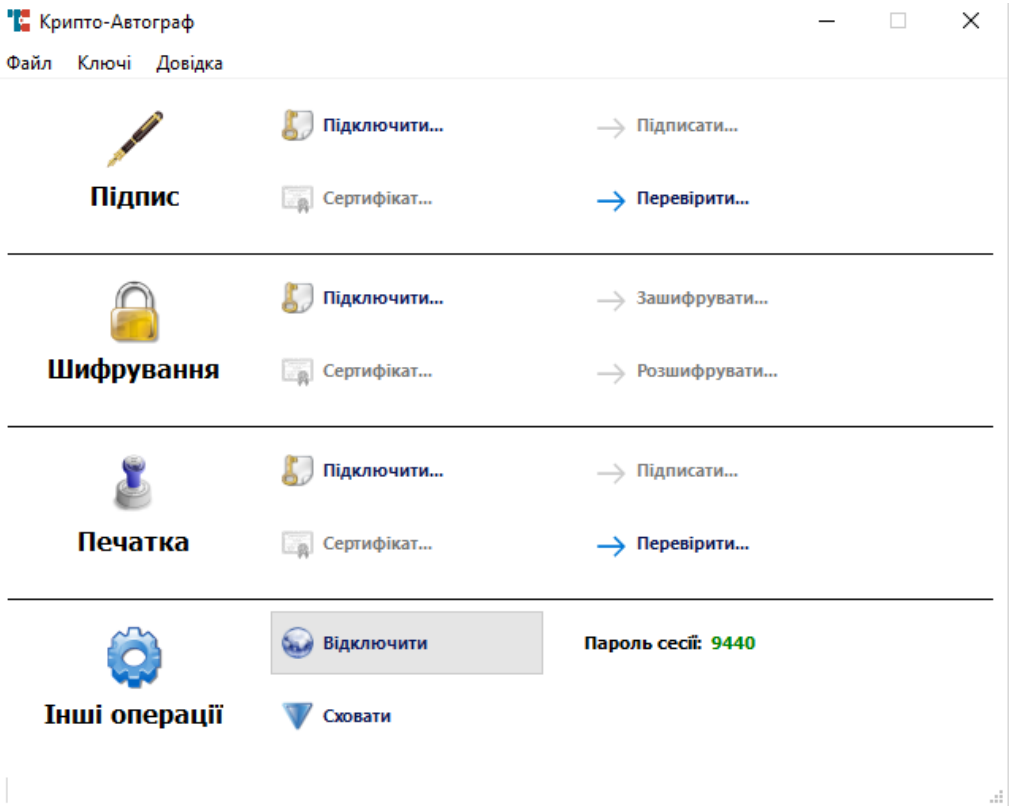
Для здійснення та збереження налаштувань необхідно володіти правами «Адміністратора» операційної системи та відповідно запустити «CryptoAutograph» з правами «Адміністратора» операційної системи.

На «Робочому столі» операційної системи та в меню «Пуск» доступний ярлик «CryptoAutograph» для запуску встановленого програмного забезпечення та здійснення подальшого налаштування.

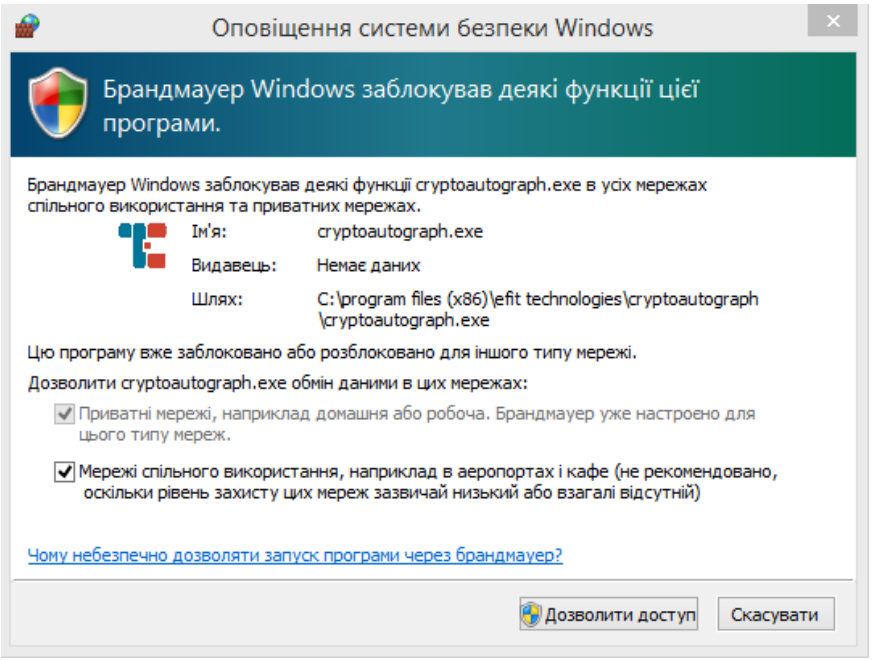
Запустіть програмне забезпечення використовуючи ярлик «CryptoAutograph» з правами «Адміністратора» операційної системи або виділіть ярлик «CryptoAutograph» натисканням правої кнопки миші та оберіть пункт меню «Запустити з правами адміністратора».



Відкриється вікно, що наведено нижче.

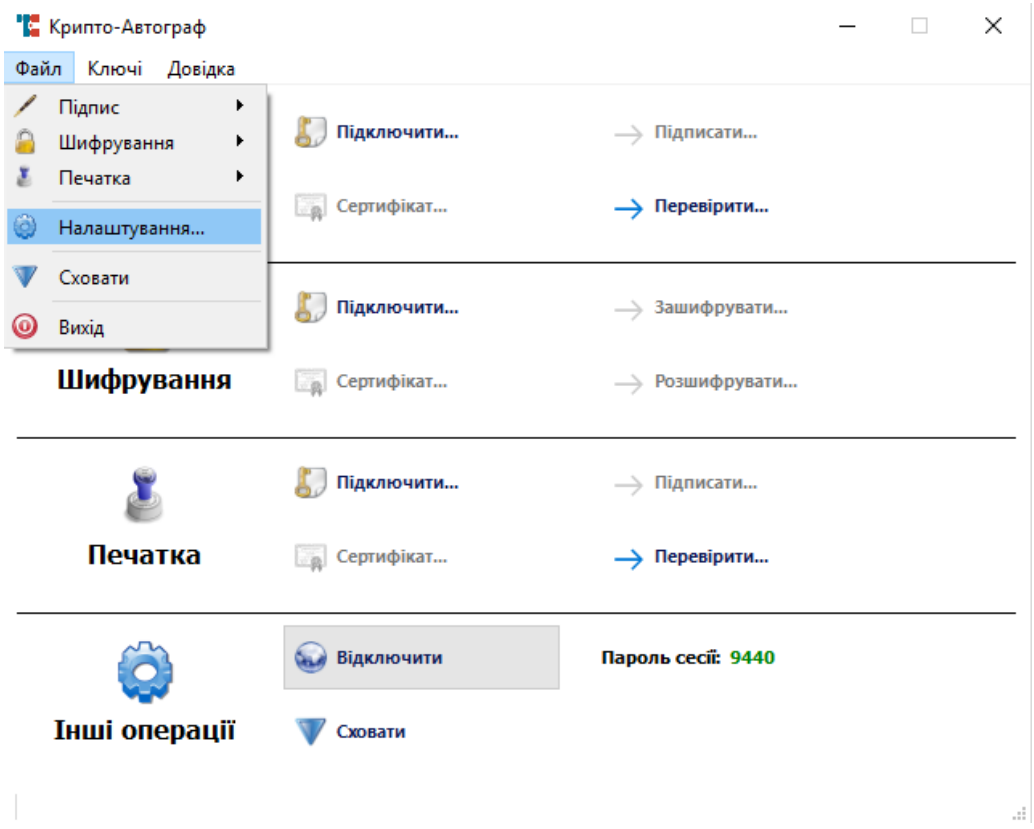


У вікні брандмауера операційної системи необхідно обрати мережі та натиснути кнопку «Дозволити доступ».



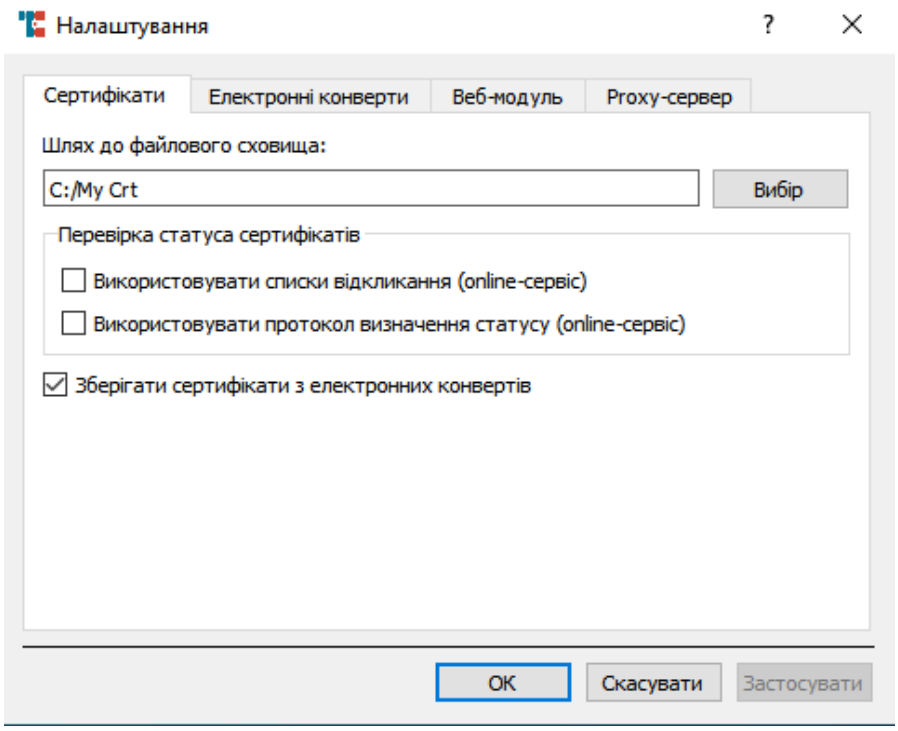
<u>Примітка: У разі використання міжмережевих екранів необхідно в політиках безпеки міжмережевого екрану дозволити використання програмою порту «4434» та «443».</u>

Для здійснення первинних налаштувань необхідно у графічному меню програмного забезпечення обрати «Параметри» → «Налаштування».

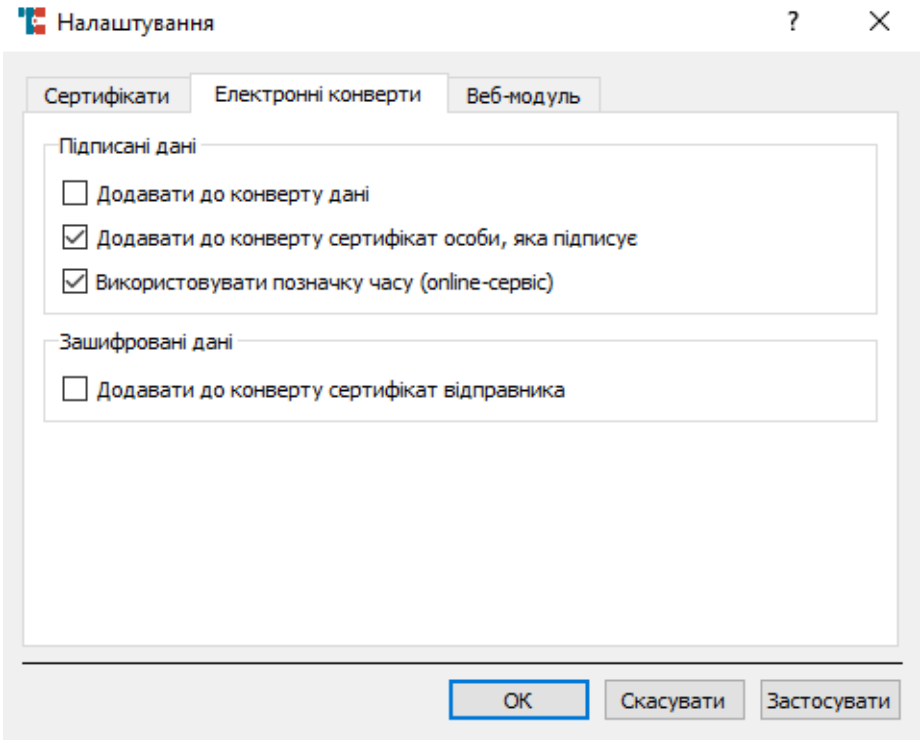


На вкладці налаштувань «Сертифікати» необхідно перевірити «Шлях до файлового сховища» Повинен бути обраний каталог «C:\My Crt». За допомогою чек-боксів («галочки») оберіть відповідні опції як показано у прикладі:

Приклад:



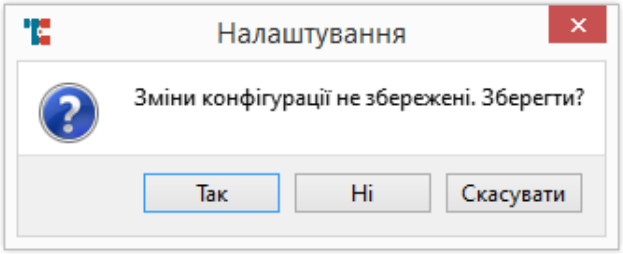
На вкладці налаштувань «Електронні конверти» відключити опції «Додавати до конверту дані» та включити опції «Додавати до конверту сертифікат» та «Використовувати позначку часу (online-сервіс)».



На вкладці налаштувань «Веб-модуль» необхідно перевірити наявність включеної опції «Включати під час запуску програми»

Усі необхідні налаштування виконані / перевірені! Необхідно натиснути кнопку «Застосувати», далі - «Ок».

У вікні «Налаштування» необхідно натиснути кнопку «Так» для збереження здійснених налаштувань (вікно «Налаштування» може не відображатися).



Усі необхідні налаштування виконані успішно.

У подальшому програмне забезпечення рекомендовано запускати з правами «Користувача» операційної системи.

Необхідно перевірити каталог «My Crt» системного диску «C:\» на наявність сертифікатів відкритого ключа. Каталог повинен містити файли «*.cer» або «*.crt».

Приклад:

C:\My Crt\Іванова П.А.cer → сертифікат користувача

C:\My Crt\CZOROOT.cer → сертифікат ЦЗО

C:\My Crt\CZOOCSP.cer → сертифікат ЦЗО сервісу OCSP

C:\My Crt\CA-TSP-ACSKInformjust-080415.cer → сертифікат АЦСК TSA

C:\My Crt\CA-ACSKInformjust-080415.cer → сертифікат АЦСК

У разі відсутності сертифікатів відкритого ключа їх необхідно скопіювати до каталогу «My Crt» системного диску «C:\» та перезапустити програмне забезпечення «CryptoAutograph» (з метою перечитування каталогу).

У разі відсутності сертифікатів ЦЗО їх можна завантажити з офіційного сайту за посиланням: https://czo.gov.ua/ca-registry.

Кваліфіковані надавачі електронних довірчих послуг

	Назва юридичної особи	Назва кваліфікованого надавача електронних довірчих послуг
1	АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК "ПРИВАТБАНК"	Кваліфікований надавач електронних довірчих послуг АЦСК АТ КБ "ПРИВАТБАНК"
2	Військова частина 2428	Кваліфікований надавач електронних довірчих послуг "Військова частина 2428" Державної прикордонної служби України
3	Генеральний штаб Збройних Сил України	Кваліфікований надавач електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України"
4	Офіс Генерального прокурора	Кваліфікований надавач електронних довірчих послуг органів прокуратури України
5	Державна казначейська служба України	Кваліфікований надавач електронних довірчих послуг Державної казначейської служби України
6	Державне підприємство "Оператор ринку"	Кваліфікований надавач електронних довірчих послуг "АЦСК ринку електричної енергії"
7	Державне підприємство "ДІЯ"	Кваліфікований надавач електроних довірчих послуг "ДІЯ"
8	Державне підприємство "Українські спеціальні системи"	Кваліфікований надавач електронних довірчих послуг Державного підприємства "Українські спеціальні системи"

На сторінці конкретного електронного реєстру суб'єктів, які надають послуги пов'язані з КЕП є можливість перейти на офіційний сайт АЦСК чи завантажити Сертифікати Центру.

Електронний реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів

Реєстр – електронна база даних, в якій містяться відомості про самопідписані сертифікати електронної печатки ЦЗО, сертифікати ЦЗО для додавання електронної печатки до Довірчого списку та до даних у протоколі визначення статусу сертифіката у режимі реального часу, сертифікати кваліфікованих надавачів електронних довірчих послуг (далі – надавачі), сформовані з використанням самопідписаного сертифіката електронної печатки ЦЗО, статус та обмеження у використанні таких сертифікатів, а також списки відкликаних сертифікатів ЦЗО.

Наказ Міністерства цифрової трансформації України від 28 липня 2020 року № 112 "Про затвердження Порядку ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів", зареєстрований в Міністерстві юстиції України 18.08.2020 за № 798/35081

Кваліфіковані надавачі електронних довірчих послуг, які внесені до Довірчого списку на підставі рішення засвідчувального центру, можуть надавати електронні довірчі послуги лише у банківській системі України та при здійсненні переказу коштів.

Найменування юридичної особи: Державне підприємство "ДІЯ"
Код ЄДРПОУ: 43395033
Електронна пошта: ca@informjust.ua
Веб-сайт: https://ca.diia.gov.ua
Контакти: місцезнаходження надавача: 03150, м. Київ, вул. Ділова, будинок 24

тел.: +38 (096) 111-59-11; +38 (050) 011-59-11

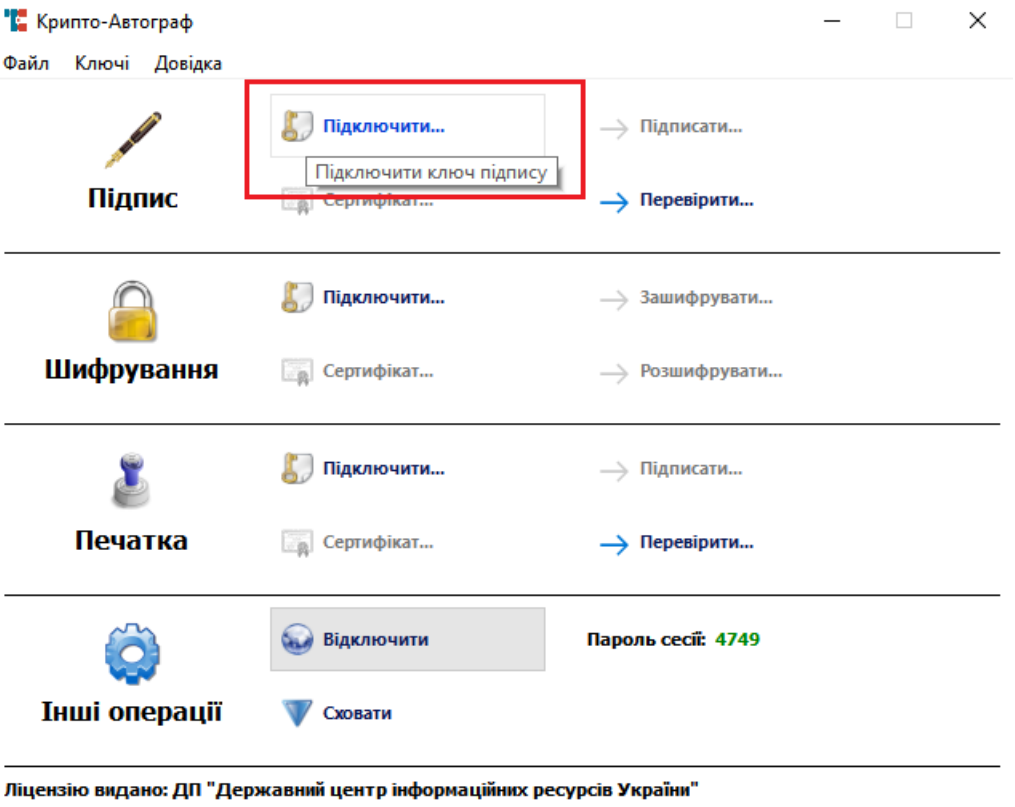
Сертифікати Надавача:

Найменування послуги	Строки дії сертифіката	Статус сертифіката	Завантажити
Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки	08.04.2015 - 08.04.2020	Скасований	
Кваліфікована електронна довірча послуга формування,			

4. Робота користувача з клієнтською компонентою «CryptoAutograph»

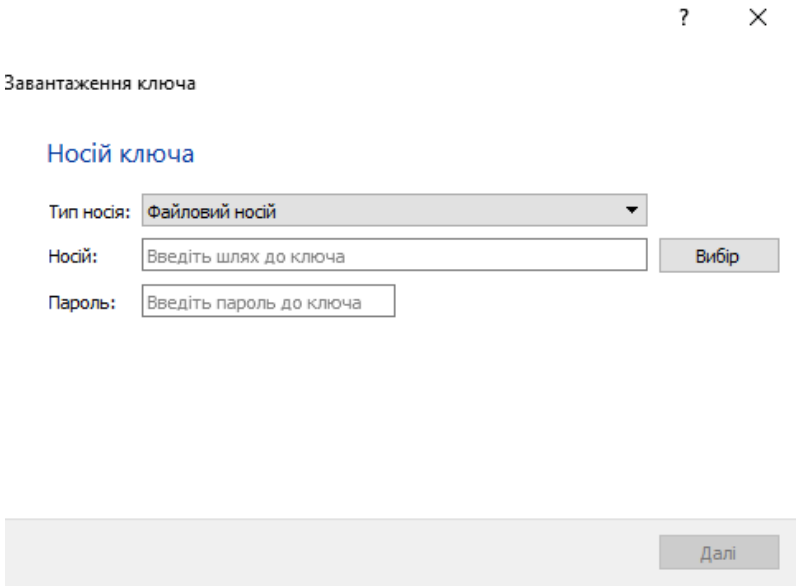
На «Робочому столі» операційної системи та в меню «Пуск» доступний ярлик «CryptoAutograph» для запуску встановленого програмного забезпечення.

У графічному інтерфейсі програмного забезпечення біля пера з написом «Підпис» необхідно натиснути «Підключити» (для підключення особистого ключа електронного цифрового підпису користувача, який вже є у наявності в даного користувача та отриманий від акредитованого центру сертифікації ключів).



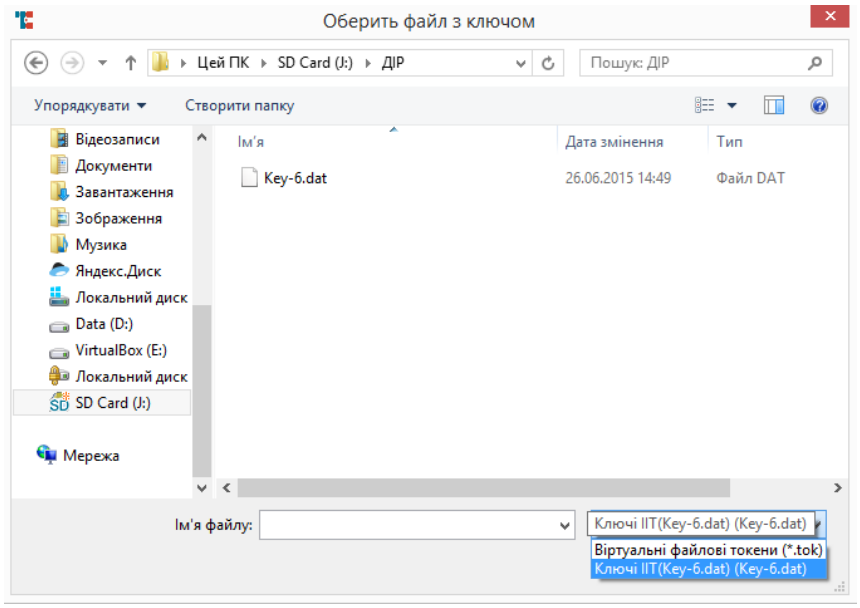
У вікні «Завантаження ключа» оберіть «Тип носія» - «Файловий носій».

В полі «Носій» оберіть шлях до файлу з ключом, де той розміщено. Для цього натисніть кнопку «Вибір».

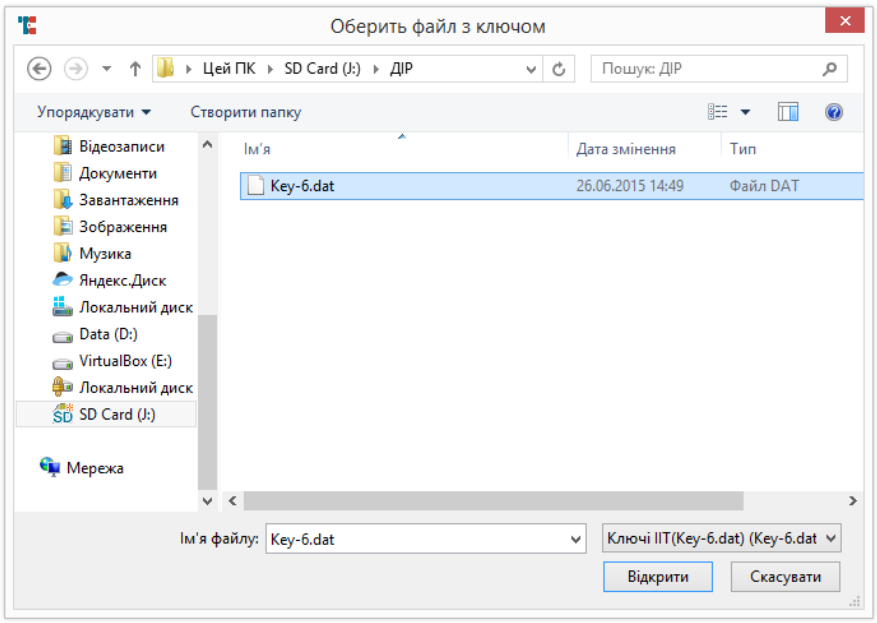


Оберіть носій інформації та каталог (теку), де розміщено особистий ключ (зазвичай це файл “key-6.dat”) електронного цифрового підпису (локально на комп’ютері, на флешці, на CD диску, дискеті тощо) де користувач зберігає свій особистий ключ електронного цифрового підпису).

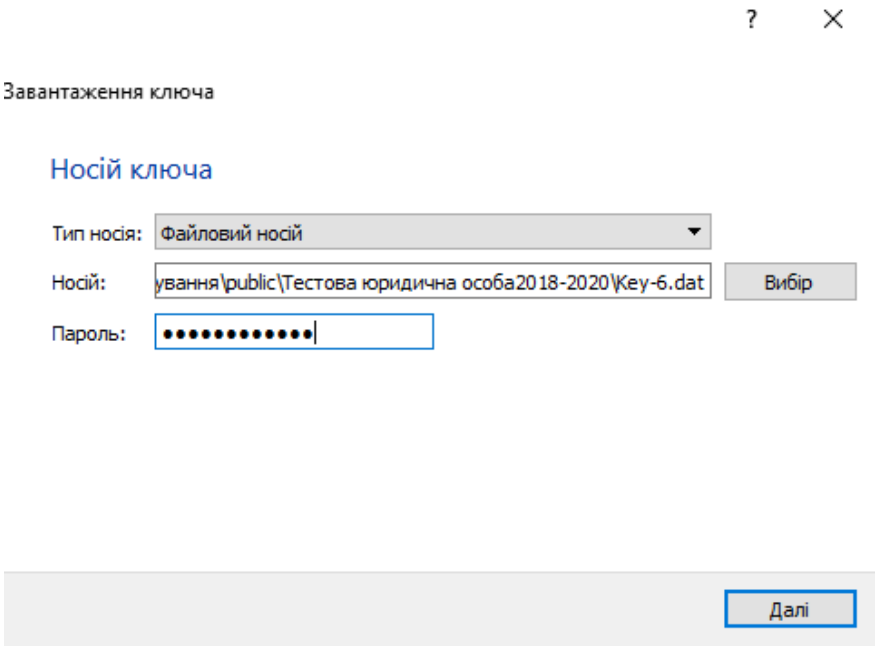
У фільтрі оберіть *«Ключ IIT (Key-6.dat) (Key-6.dat)»* для полегшення пошуку файлу особистого ключа.



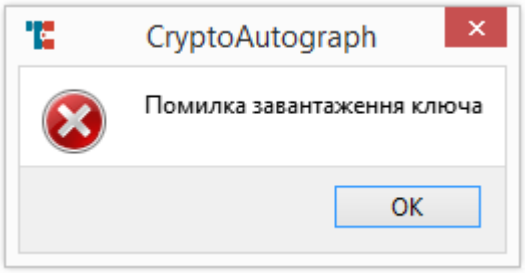
Оберіть особистий ключ електронного цифрового підпису користувача «Key-6.dat» та натисніть кнопку «Відкрити».



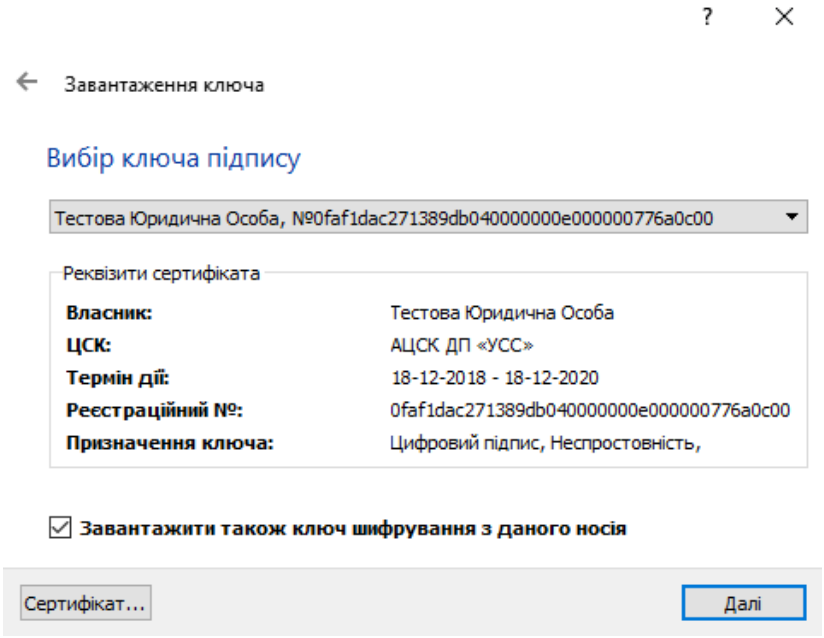
Після обрання файлу, що містить особистий ключ електронного цифрового підпису користувача «Key-6.dat» необхідно у позиції «Пароль:» ввести пароль доступу до особистого ключа КЕП користувача та натиснути кнопку «Далі».



Примітка: У разі відображення повідомлення «Помилка завантаження ключа» необхідно перевірити каталог «My Crt» системного диску «C:\» на наявність в ньому сертифіката Центрального засвідчувального органу, сертифіката акредитованого центру сертифікації ключів, сертифіката електронного цифрового підпису користувача. Також дана помилка може виникати у разі введення невірного пароль (ПІН-коду) до особистого ключа електронного цифрового підпису користувача.



Зверніть увагу, що у реквізиті сертифіката «Призначення ключа:» повинно бути відображено **«Цифровий підпис, Неспростовність»**. У разі відображення «Узгодження ключа» необхідно обрати інший сертифікат шляхом «Перегляду сертифікату». Для застосування сертифіката натисніть кнопку «Завершити».



Особистий ключ підключено та програмне забезпечення готове для роботи з документами.

5. Підписання файлу локально на ПК користувача

При завантаженому особистому ключі користувача необхідно натиснути на кнопку **«Підписати»** (рис. 1).

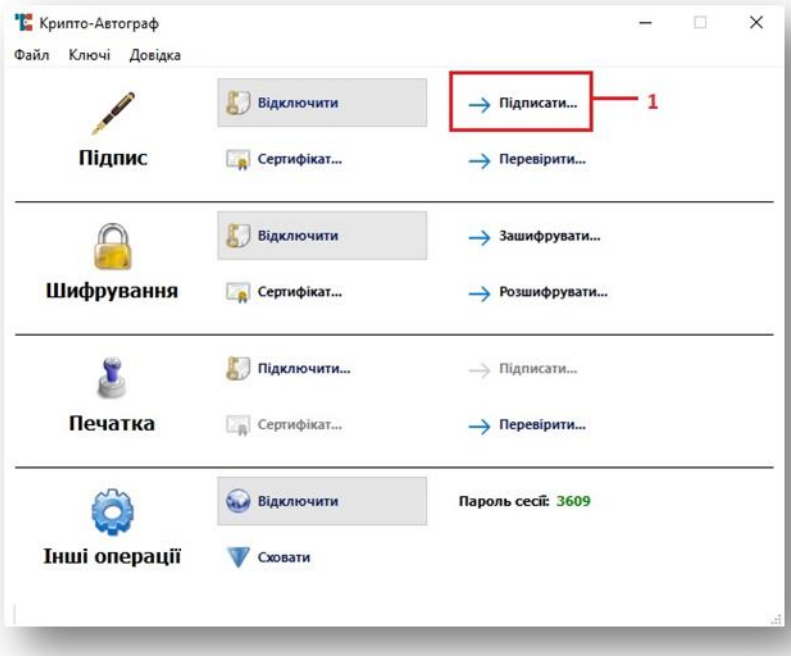


Рис.1 Початок підписання.

1 – *кнопка «Підписати»*

У вікні завантаження файлу на підписання заповнити **«Налаштування»**, виставивши необхідні чек-бокси(«галочки»)(рис.2). Для того, щоб завантажити файл на підписання необхідно натиснути на кнопку **«Вибір»**.

Обрати необхідний файл для підпису та натиснути кнопку **«Открыть»** (рис.3).

Після того, як відбулося завантаження файлу до ПЗ «КриптоАвтограф», необхідно натиснути кнопку **«Далі»** (рис. 4).

Після успішного виконання операції створюється файл КЕП **невеликого (не більше ніж сам документ!)** розміру з розширенням ***.p7s з тою ж назвою та по тому ж шляху (в тому ж каталозі), що і підписуваний документ!** Натискаємо кнопку **«Завершити»** (рис. 5).

Відображення підписуваного файлу та його КЕП в каталозі зображено на рис. 6.

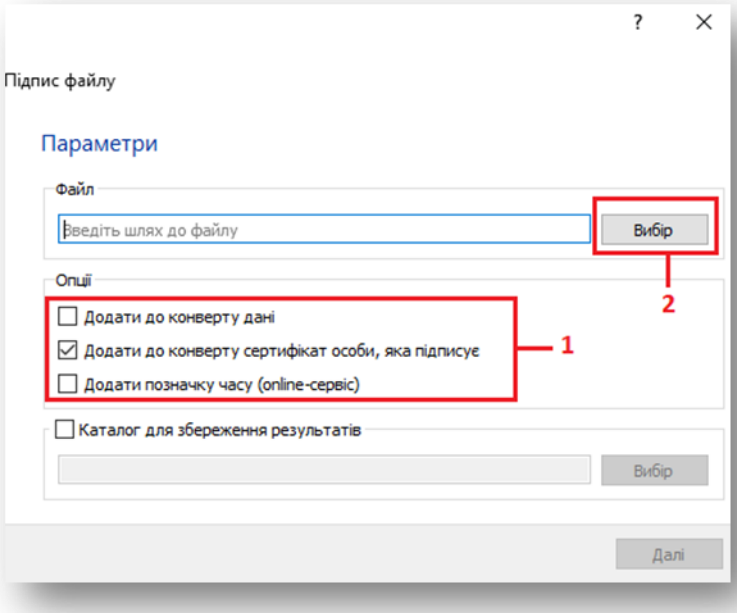


Рис. 2. Завантаження файлу на підписання.

1 – *«Опції» підписання,* **2** – *кнопка «Вибір»*

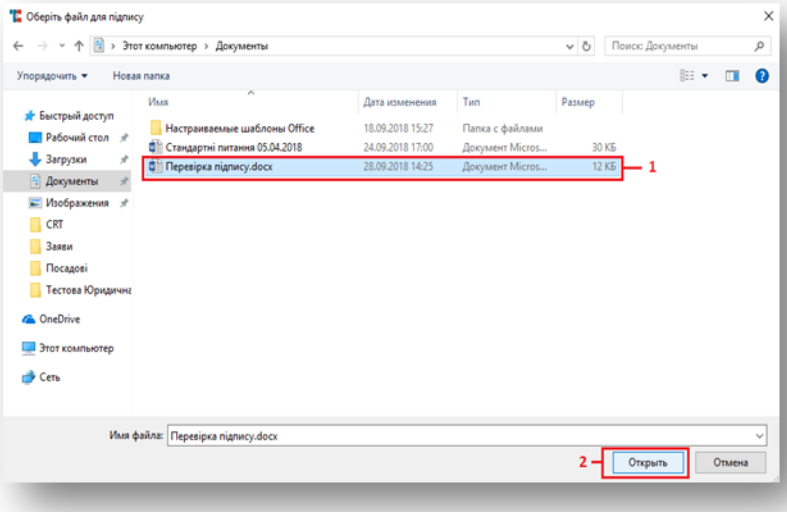


Рис.3. Вибір файлу для підписання.

1 – *необхідний файл,* **2** – *кнопка «Открыть»*

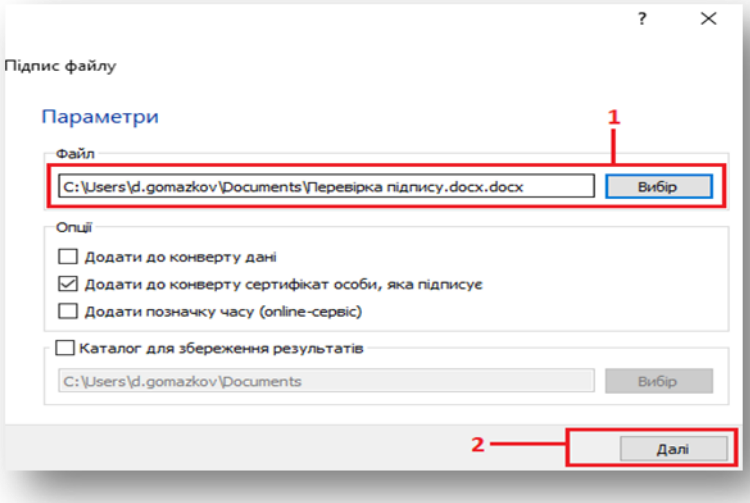


Рис.4. Завершення завантаження файлу для підписання.

1 – *шлях до файлу,* **2** – *кнопка «Далі»*

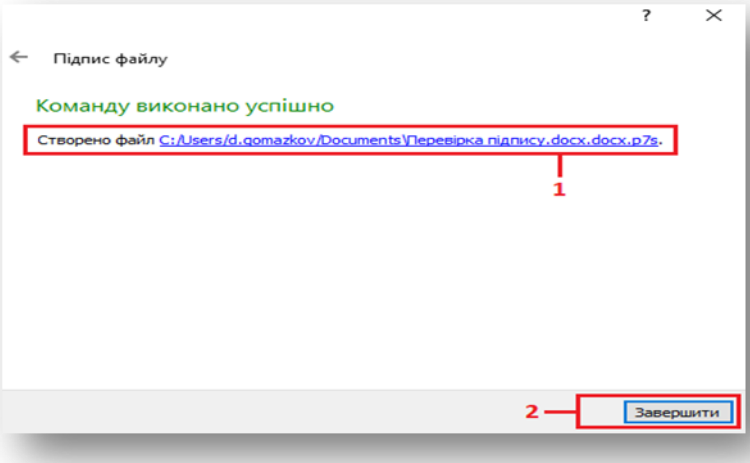


Рис. 5. Завершення підписання файлу.

1 – *шлях до створеного КЕП,* **2** – *кнопка «Завершити»*

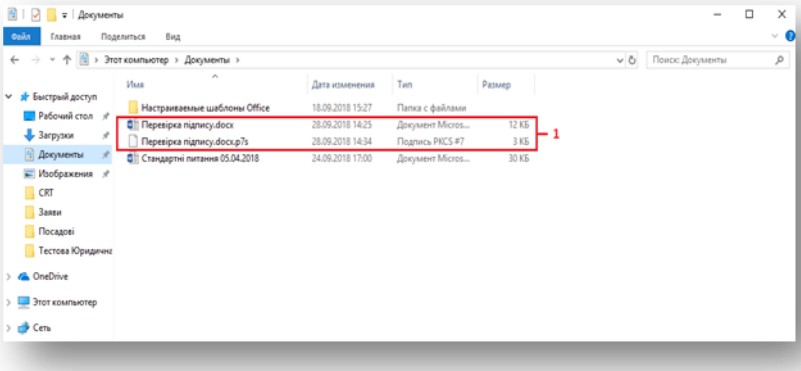


Рис.6. Відображення в каталозі

1 – *пара «документ-КЕП»*

6. Завантаження локально підписаного файлу до РКК

Для створення нового документу в СЕВ ОВВ необхідно натиснути: «Вихідні» - «Нові» - «Створити» та заповнити належним чином перші дві вкладки РКК. Третя вкладка («Прикріплені файли») використовується для завантаження файлів документів та підписів до них.

Після завершення операції підписання в ПЗ «Cryptoautograph» в поле вкладених файлів необхідно долучити **по черзі обидва файли**, шляхом натискання на кнопку «Додати файл», **обов'язково прибравши «галочку» «Використовувати Cryptoautograph для підписання файлів».** Це виконується через те, що документ уже підписаний локально і ще раз підпису **не потребує** (рис. 7).

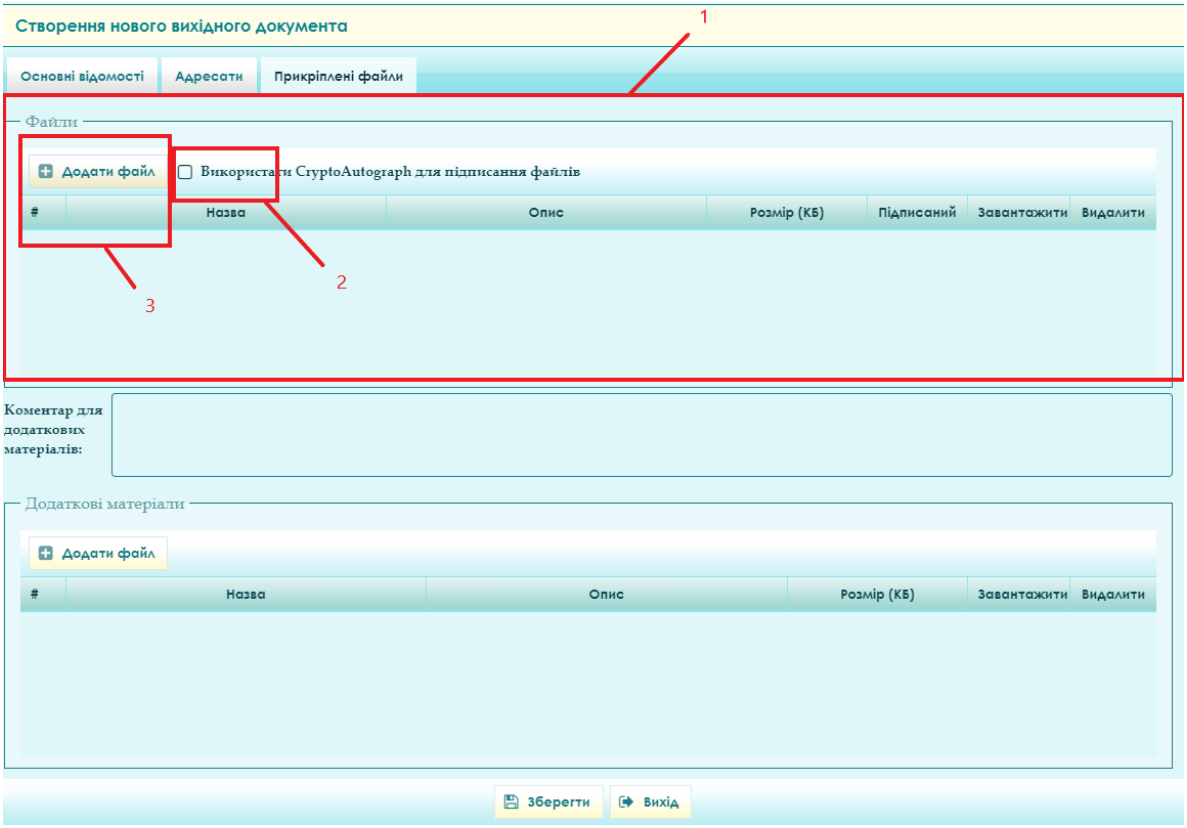


Рис. 7. Процес завантаження підписаних локально файлів до РКК

1 – *поле основних вкладених файлів,* **2** - *«галочка» «Використовувати Cryptoautograph для підписання файлів», яку необхідно зняти (як на рис.),* **3** – *кнопка «Додати файл»*

На картці завантаження файлів натиснути на кнопку **«Виберіть файл»** (рис. 8).

Після того, як файл було завантажено до Картки завантаження файлів необхідно натиснути на кнопку **«Завантажити»** (рис.9) та виконати аналогічні дії для файлу КЕП.

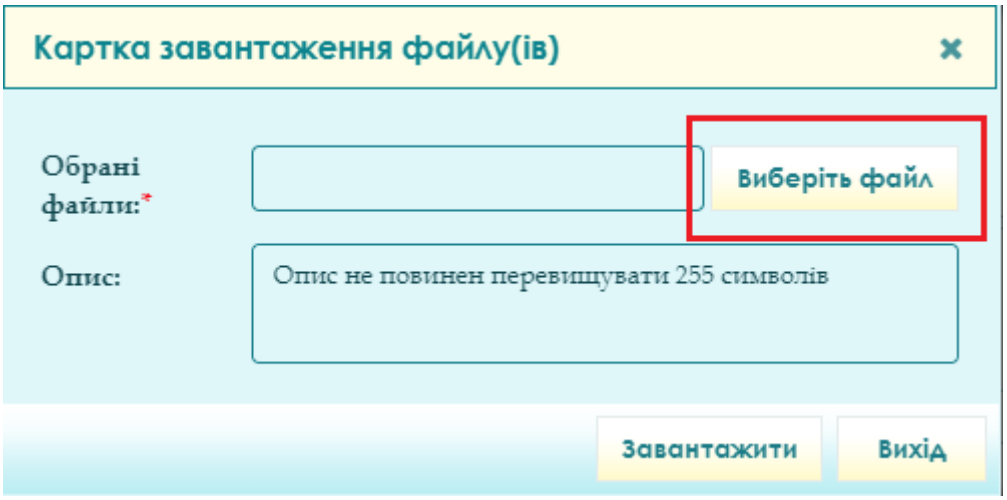


Рис.8. Початок завантаження файлу

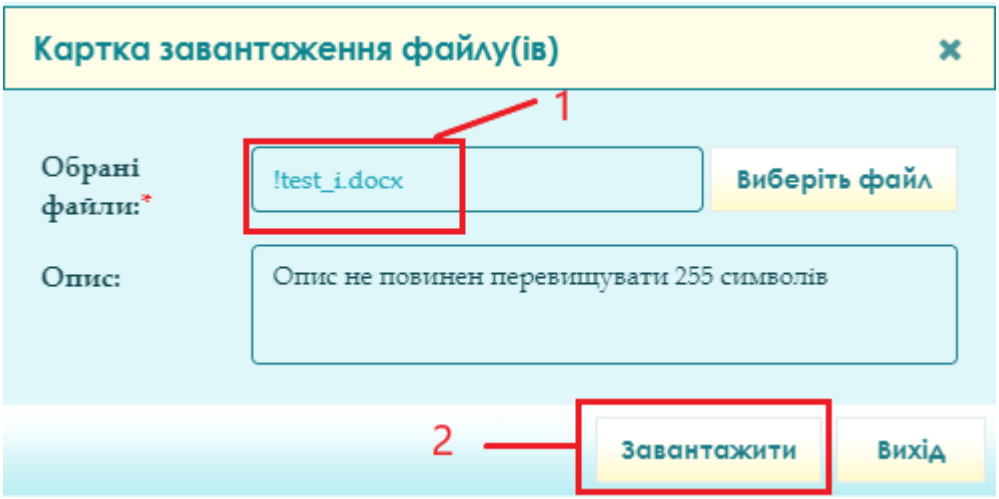


Рис. 9. Завершення завантаження файлу

1 – *завантажений підписуваний файл,* **2** – *кнопка «Завантажити»*

Результатом виконання операції завантаження пари файлів (документ та КЕП на цей документ) до РКК є два файли **без помітки** «Підписаний», що можна побачити на рис. 10.

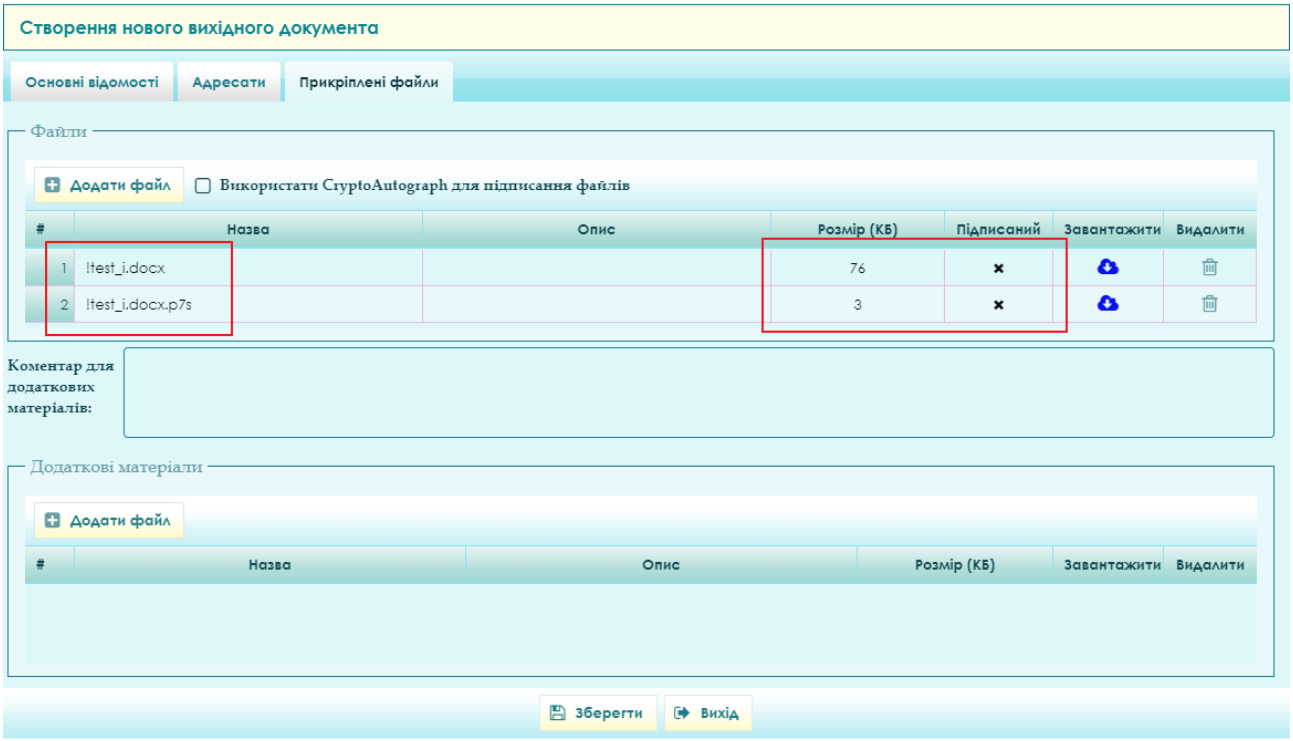


Рис. 10. Завантажені до РКК файли

1 - *пара «документ-КЕП»*

Наступним кроком, перевіривши всі необхідні та обов’язкові поля на вкладках «Основні відомості» та «Адресати», можна зберігати та надсилати створену РКК.

7. Підписання файлу при заповненні РКК

(Підписання «на льоту»)

Після запуску програмного забезпечення «CryptoAutograph» та завантаження особистого ключа користувача завжди створюється новий **пароль сесії** (рис. 11).

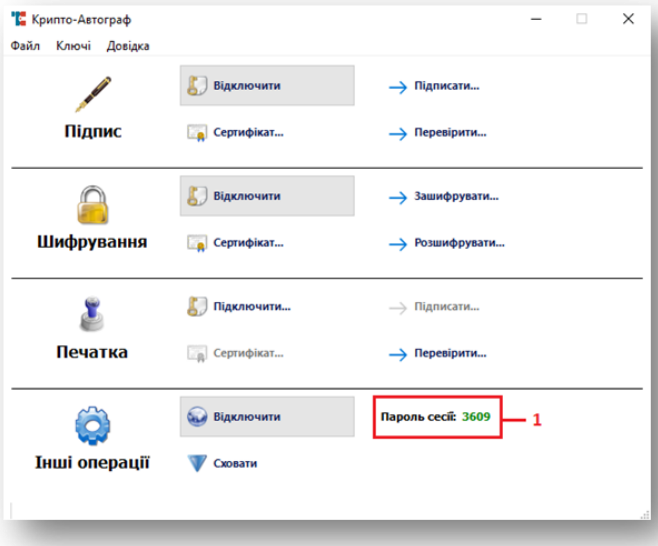


Рис. 11. *Запуск КриптоАвтографа.* **1 -** *Пароль сесії.*

Не вимикаючи Криптоавтограф, переходимо до створеної РКК в СЕВ ОВВ з вже заповненими вкладками «Основні відомості» та «Адресати».

У третій вкладці «Прикріплені файли» check-box **«Використовувати Cryptoautograph для підписання файлів»** **залишаємо!** Долучаємо не підписаний документ в поле вкладених файлів, натиснути кнопку **«Додати файл»** (рис.12).

На картці завантаження файлів натиснути на кнопку «Виберіть файл», **обрати файл документу** та ввести **Пароль криптосесії**, заповнивши відповідне поле чотиризначним числом, яке було згенеровано в КриптоАвтографі (рис. 11).

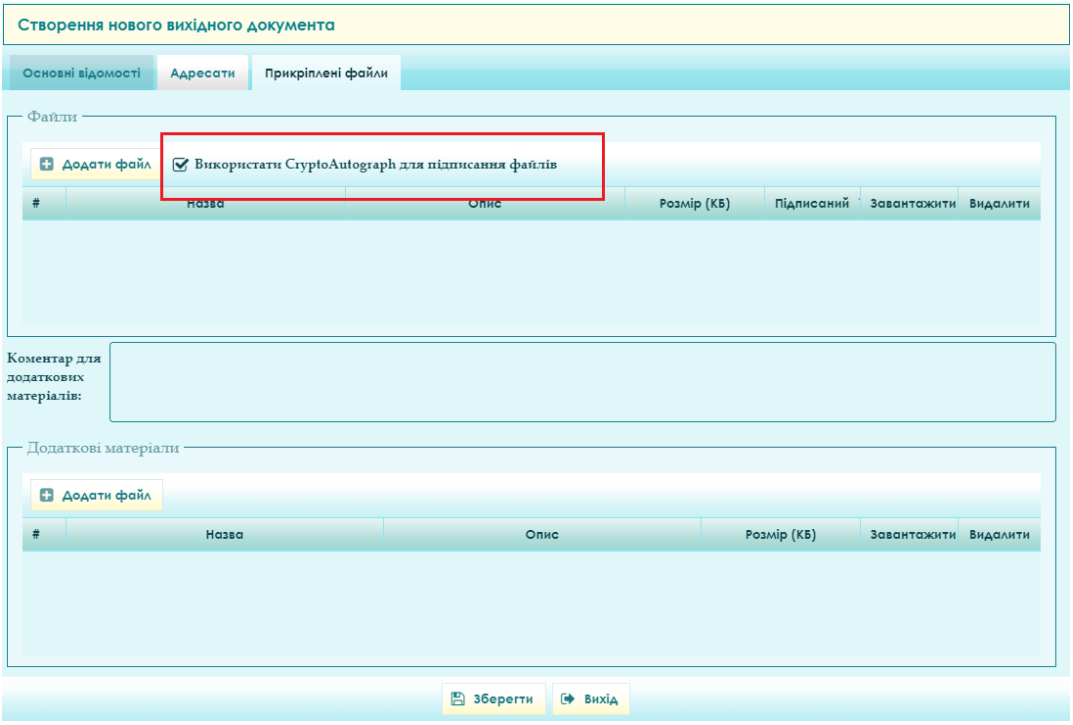


Рис. 12. Процес завантаження файлів до РКК,

check-box «Використовувати Cryptoautograph для підписання файлів», необхідно ***залишити!***

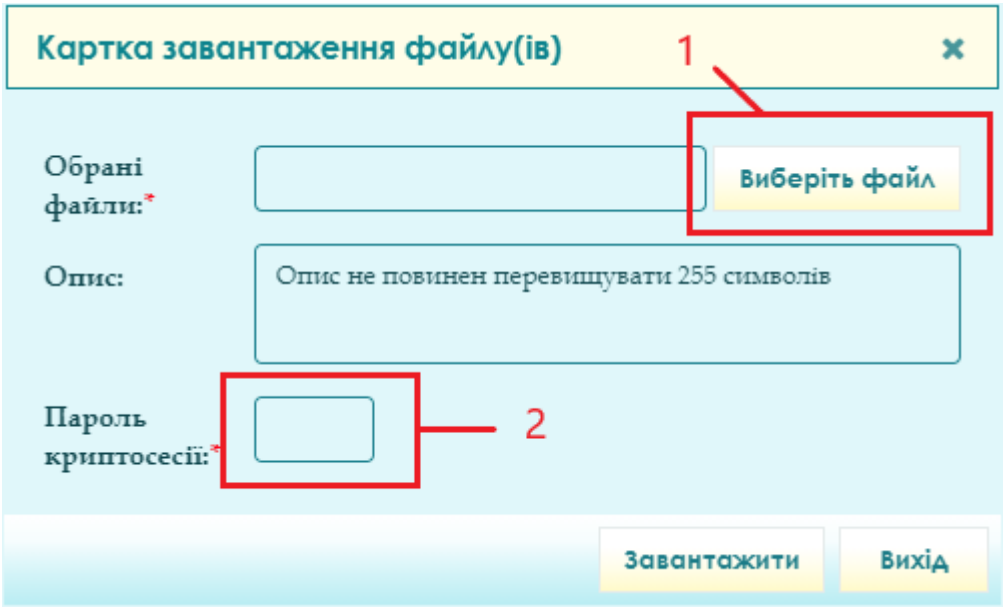


Рис. 13. Початок завантаження файлу

1 *– кнопка «Виберіть файл»,* **2** *– поле для введення паролю сесії*

Після того, як файл було завантажено до системи та введено пароль криптосесії, необхідно натиснути на кнопку **«Завантажити»** (рис.14).

Рис. 14. Завершення завантаження файлу

1 – *завантажений підписуваний файл,* **2** – *заповнене поле «Пароль криптосесії»*, **3** – *кнопка «Завантажити»*

Результатом виконання операції підписання файлу при завантаженні до РКК є один файл **з поміткою «Підписаний»**, що можна побачити на рис. 15.

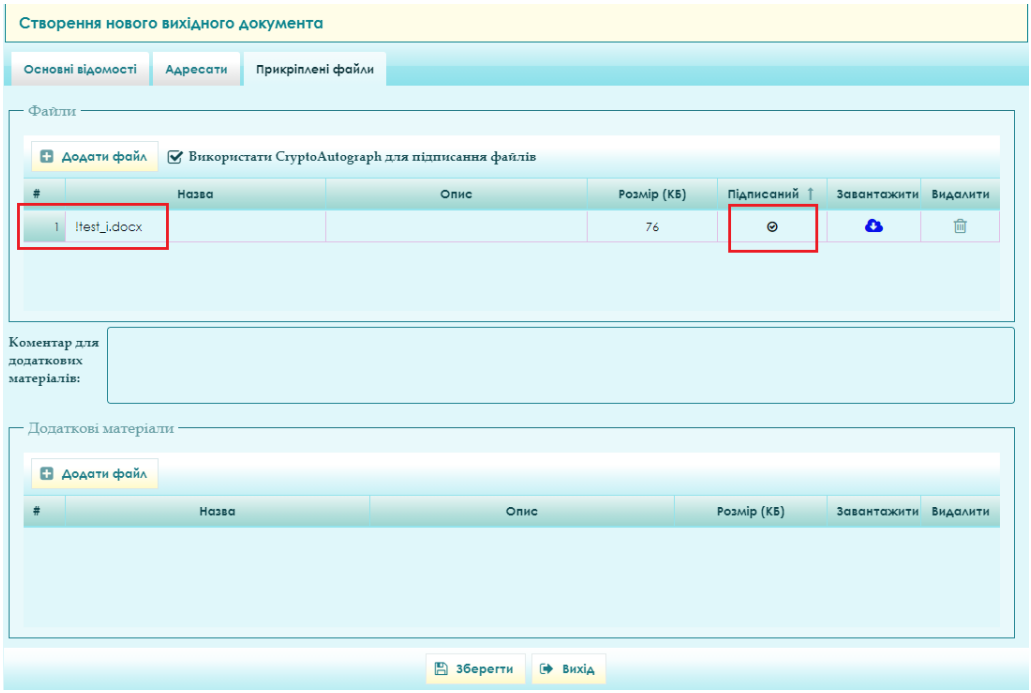


Рис. 15. Завантажений та підписаний РКК файл

1 – *підписаний файл*

8. Перевірка підпису

Для перевірки підпису за допомогою CryptoAutograph необхідно з картки вхідного/вихідного документу (РКК) завантажити обидва файли – файл підпису та документ – в одну папку, натискаючи кнопку «Завантажити» (Рис. 16).

Файли обов’язково повинні опинитися в одному каталозі (теці).

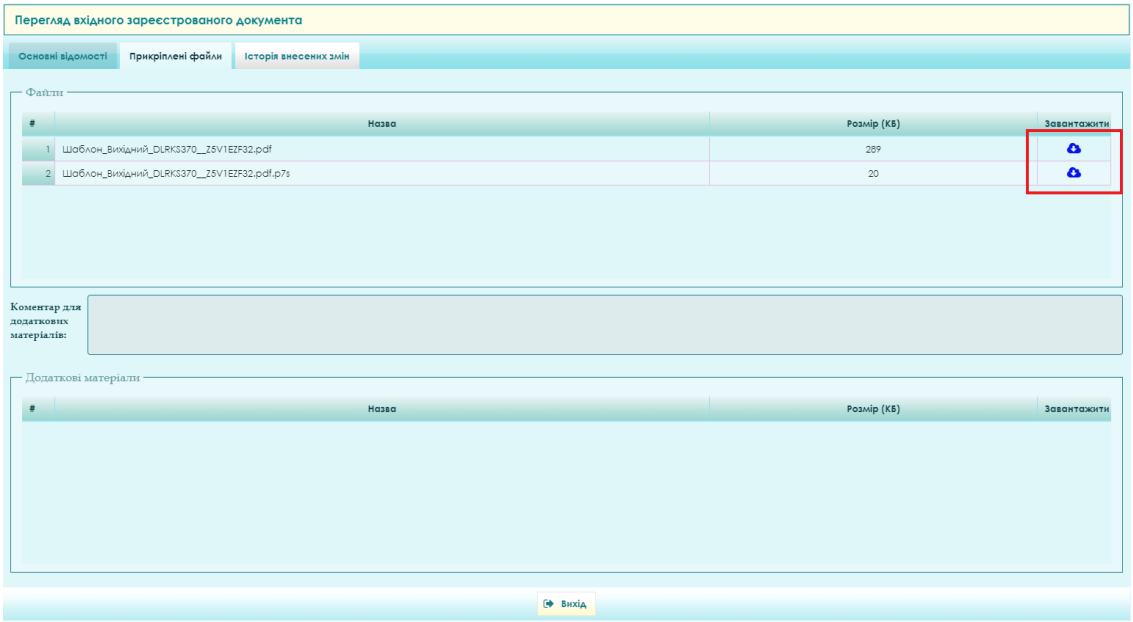


Рис. 16. Кнопка «Завантажити»

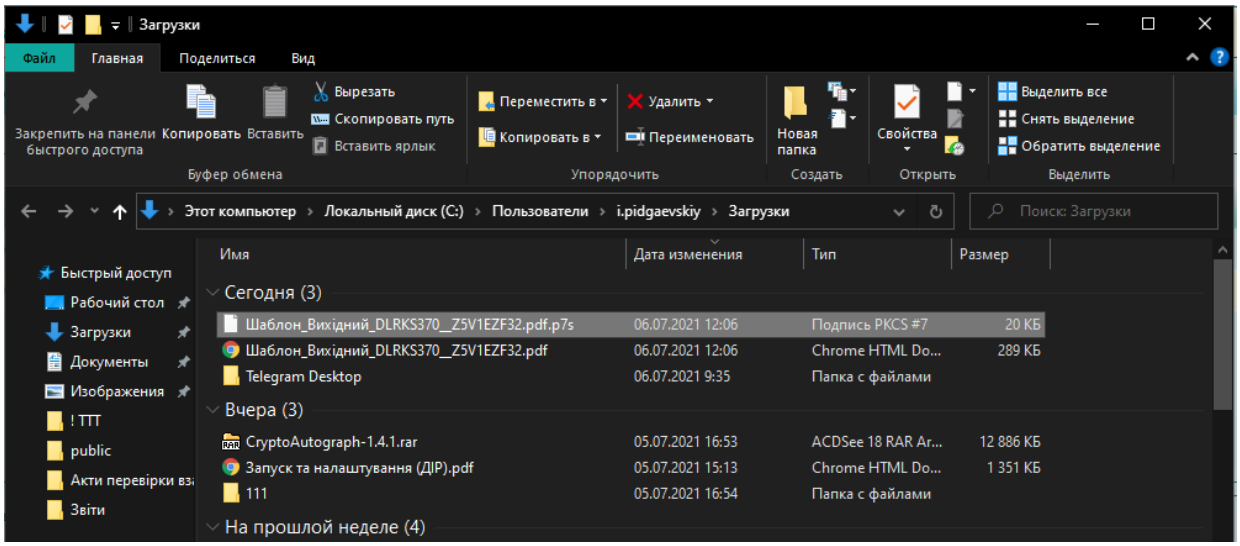


Рис. 17. Документ та файл підпису, що знаходяться в одному каталозі

Для перевірки КЕП документу за допомогою CryptoAutograph потрібно діяти наступним чином:

Запустити CryptoAutograph та натиснути на кнопку «Перевірити»

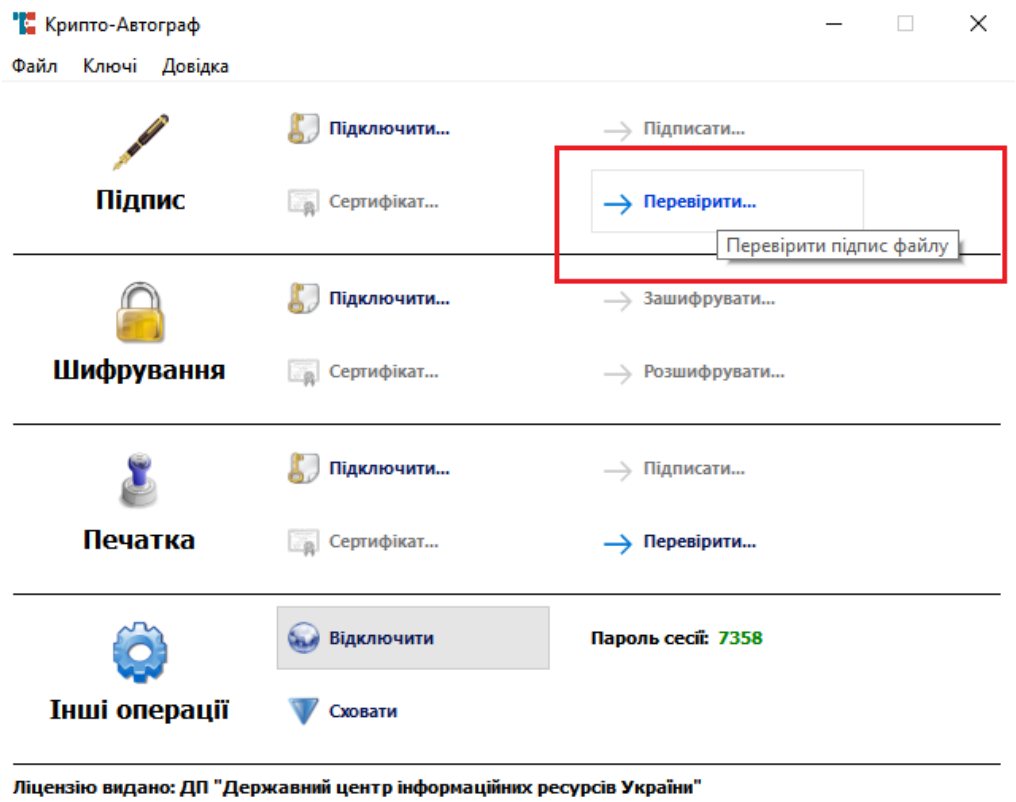


Рис. 18. Кнопка «Перевірити»

У вікні перевірки КЕП, завантажити файл підпису (*.p7s), що знаходиться поруч із файлом документа (в одній теці) та натиснути кнопку «Вибір». Для уникнення плутанини з документами необхідно зняти відмітку «зберігати данні з конверту». Натиснути кнопку «Далі» для початку перевірки (Рис. 19).

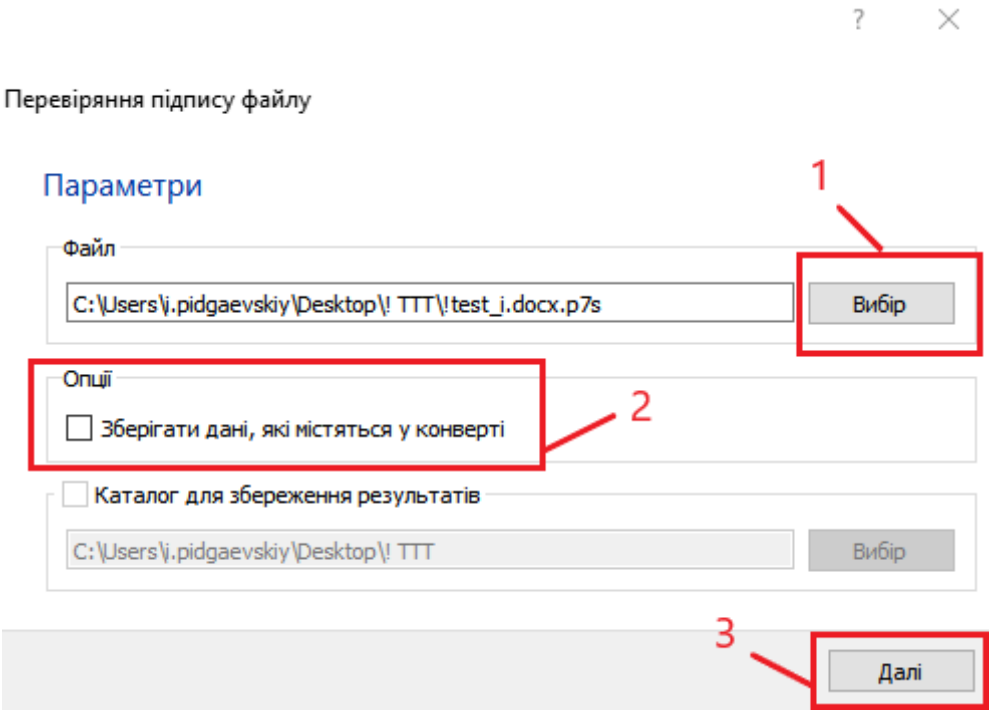


Рис. 19 Перевірка підпису файлу.

1 – *кнопка «Вибір»*, **2** – *знята «галочка» «Зберігати дані, що містяться в конверті»*, **3** – *кнопка «Далі»*

Отримуємо звіт перевірки файлу підпису на документ. Підпис вірний, позначка часу присутня.

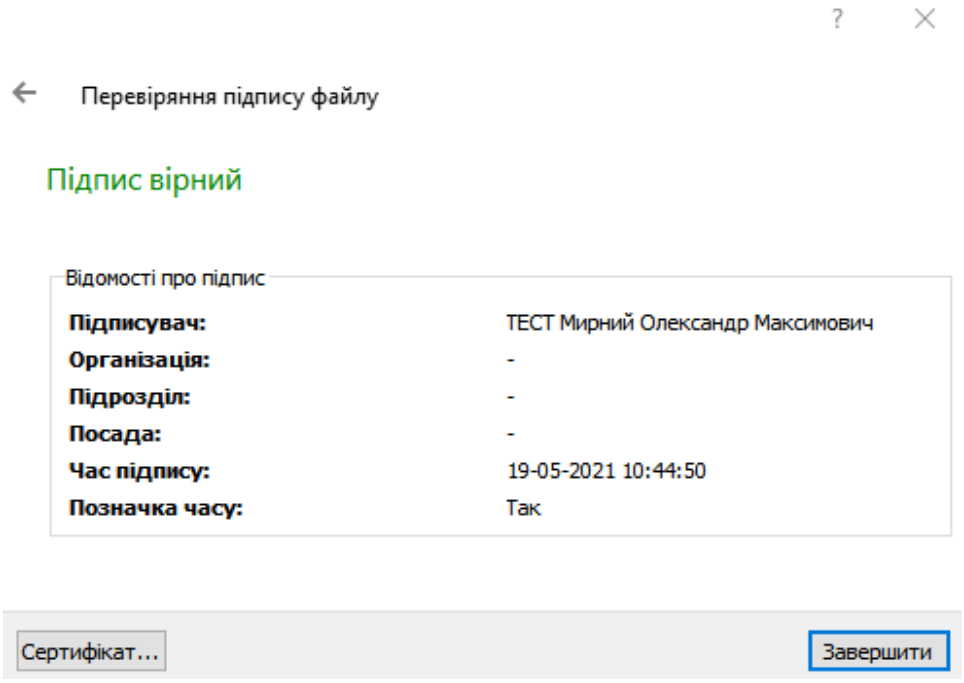


Рис. 20 Результат перевірки підпису файлу.