САЙФЕР
Системы защиты информации
Интернет-банкинг

Сайфер БІС, ТОВ
04107, Київ, ул. Нагірна 25/27, 3-ій поверх

Тел.: +38 (044) 484-4612
Факс: +38 (044) 483-0322
E-mail: sales@cipher.kiev.ua
Web: www.cipher.kiev.ua

Дата модифікації: 28.10.2019

Персональний сервіс довірчих послуг

Настанова з установки та експлуатації

ЗМІСТ

Вступ

В цьому документі описано порядок дій користувача для установки програмного застосування «Персональний сервіс довірчих послуг», його функціональні можливості та необхідні відомості для роботи з ним.

Системні вимоги

Перед початком встановлення та роботи з програмним застосуванням необхідно переконатися, що апаратне забезпечення відповідає рекомендаціям розробника (відповідно до вимог Oracle, щодо інсталяції Java).

Вимоги Java 8 для MacOS X:

- Mac на базі процесора Intel під управлінням Mac OS X 10.7.3+, 10.8.3+, 10.9+;
- Повноваження адміністратора для установки;
- Браузер – 64-біт (наприклад Safari).

Вимоги Java 8 для ОС Ubuntu:

- Ubuntu Linux 12.04 LTS, 13.x;
- Ubuntu Linux 14.x (8u25 або більш нова версія);
- Ubuntu Linux 15.04 (8u45 або більш нова версія);
- Ubuntu Linux 15.10 (8u65 або більш нова версія);
- Браузери: Firefox.

Вимоги Java 8 для сімейства Windows:

- Windows 10 (8u51 або більш нова версія);
- Windows 8.x (настільна версія);
- Windows 7 з SP1;
- Windows Vista з SP2;
- Windows XP (версія не старша 8u111);
- Windows Server 2008 R2 з SP1 (64-розрядна версія);
- Windows Server 2012 та 2012 R2 (64-розрядна версія);
- RAM: 128 МБ;
- Дисковий простір: 124 МБ для JRE; 2 МБ для оновлення Java;
- Процесор: мінімальна вимога - Pentium II, тактова частота 266 МГц;

Браузери: Internet Explorer 9+, Firefox, Google Chrome.

Підготовка робочого місця для роботи з сервісом

Введення

Програмне застосування «Персональний сервіс довірчих послуг» реалізований мовою програмування Java, що дозволяє виконувати запуск на таких платформах:

- ОС Ubuntu.
- ОС Windows.
- ОС MacOS.

Основною умовою для користування «Персональним сервісом довірчих послуг» є встановлена Java машина. Для того щоб перевірити, чи середовище Java встановлено на комп'ютері і чи коректно працює, потрібно запустити тестовий аплет http://java.com/ru/download/installed.jsp?detect=jre.

За відсутності на комп'ютері користувача Java-машини – запуск програмного застосування неможливий, тому необхідно інсталювати її. Для початку потрібно завантажити дистрибутив відповідної компоненти (JDK) з офіційного сайту Java за посиланням java.com та слідувати відповідним інструкціям.

Якщо встановлена операційна система Windows XP, то з останніми версіями Java, «Персональний сервіс довірчих послуг» працює некоректно, тому слід завантажити за посиланням jre-8u111-windows-i586.exe (розрядність даної версії Java x32) та встановити саме цю версію.

Налаштування проксі-сервера

Вступ

У випадку, **якщо доступ до мережі Інтернет з робочого місця користувача здійснюється за допомогою проксі-сервера**, то «Персональний сервіс довірчих послуг» у вигляді Java Web Start Application використовує в своїй роботі проксі-сервер, який вказаний у налаштуваннях браузера, з якого був виконаний запуск програми. Якщо запуск програми проводиться за допомогою jnlp-файлу з файлової системи (локальної або мережевої), то буде використаний проксі-сервер, який вказаний в системних налаштуваннях.

Сучасні браузери підтримують три способи роботи з проксі:

- Автоматичне налаштування. За допомогою DNS- або DHCP-сервера вказується адреса скрипта (файлу) з налаштуваннями (детальніше - тут). **Цей спосіб є досить складним для пересічного користувача, тому слід звернутись до системного адміністратора або адміністратора мережі організації.**
- Задання скрипта з налаштуваннями проксі вручну аналогічне п.1, але адреса скрипта (файлу) вказується вручну.
- Задання параметрів роботи проксі-сервера вручну.

Для вибору зазначених вище способів роботи з налаштування проксі-сервера всі сучасні браузери (IE, Firefox, Chrome, Opera, Safari) мають відповідний призначений для користувача інтерфейс.

У разі використання проксі (незалежно від способу його налаштування) для коректної роботи «Персонального сервісу довірчих послуг» необхідно:

1. Додати в список адрес, для яких не слід використовувати проксі, адресу *local.cipher.kiev.ua*. Виконати можливо за допомогою відповідного призначеного для користувача інтерфейсу або через вказівку параметрів командного рядка при старті браузера. Відомості про доступні параметри командного рядка наведено в документації браузера.
2. Налаштування доступу через проксі в конфігурації середовища Java.

Якщо ж цей спосіб налаштування не вирішив проблему доступу через проксі, потрібно:

3. Додати в файл hosts ім’я local.cipher.kiev.ua в 127.0.0.1.

У разі, якщо використовується мережа з доменом Microsoft Windows Server (2008, 2012 2016), можливе налаштування проксі для робочих станцій користувача здійснюється через налаштування групової політики. Групові політики оперують тими ж самими параметрами, які доступні користувачеві локально через призначений для користувача інтерфейс (вибір способу або параметрів вручну). **В такому випадку потрібно звернутися до системного адміністратора або адміністратора мережі Вашої організації**.

Нижче послідовно розглянуто варіанти налаштувань.

Браузер Firefox

Для зміни налаштувань проксі потрібно в браузері Firefox обрати розділ «Настройки», Рис. 1.

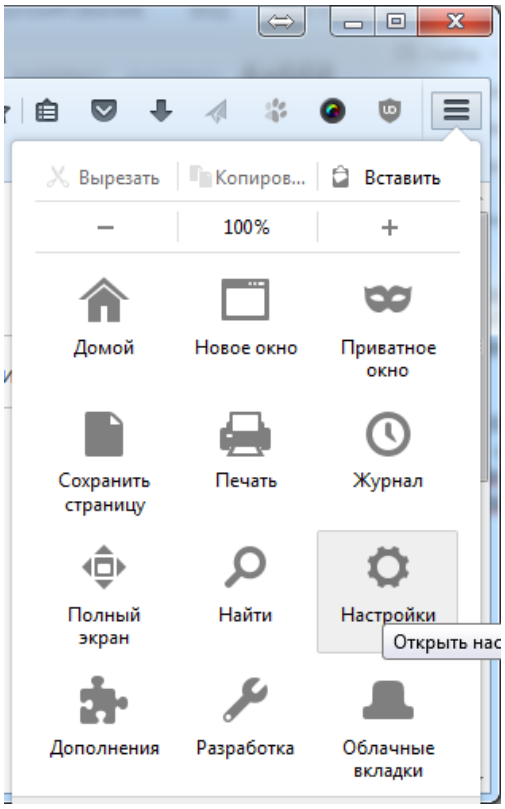

Рис. 1. Налаштування браузера Firefox

Далі послідовно обрати Налаштування: «Основные» -> «Проки-сервер», Рис. 2.

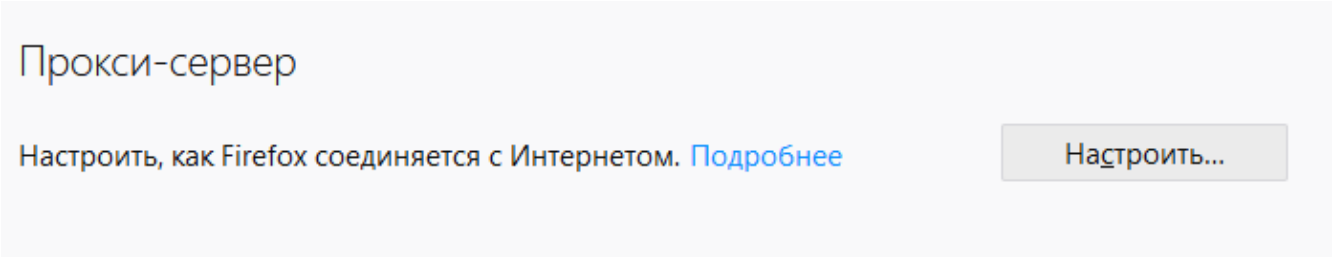

Рис. 2. Додаткові мережеві налаштування браузера

У вікні «Параметры соединения» в полі «Не использовать прокси для:» потрібно вказати адресу local.cipher.kiev.ua, Рис. 3.

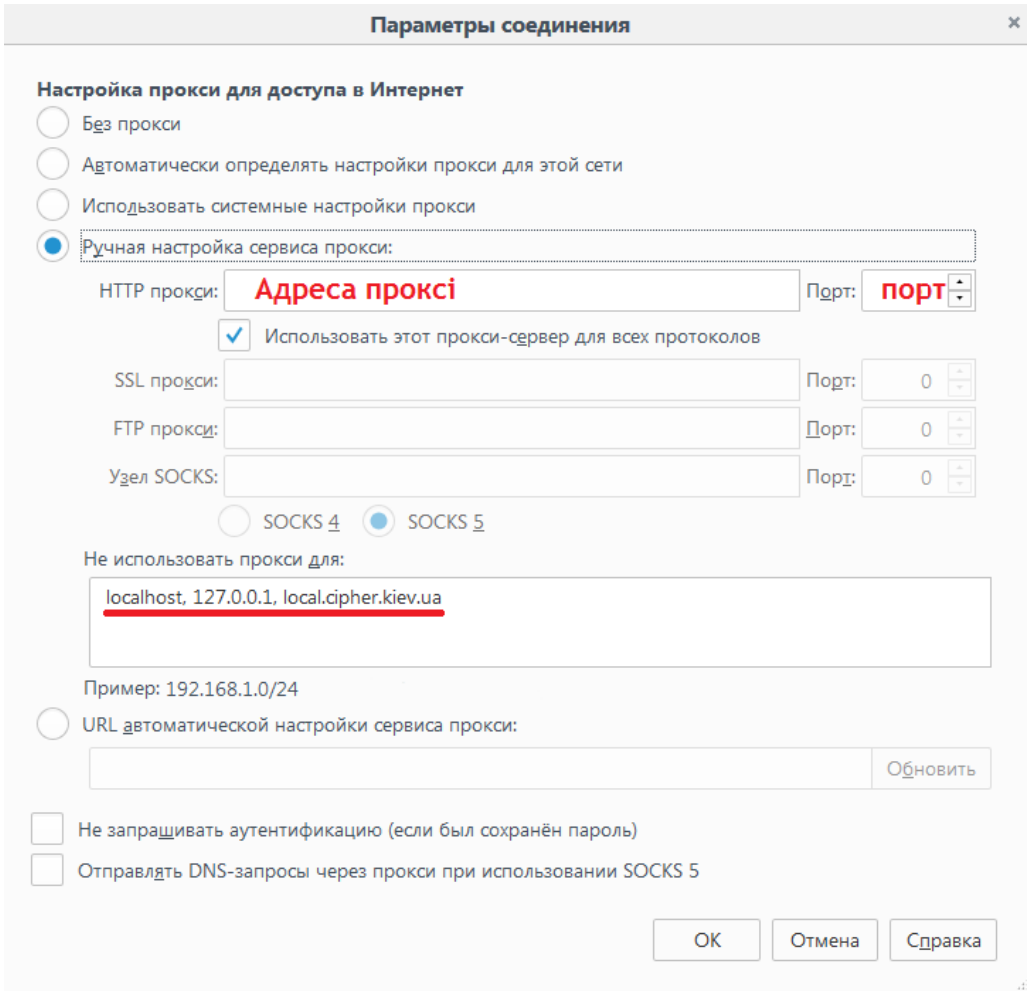

Рис. 3. Додаткові параметри з’єднання

Браузери Google Chrome та Internet Explorer

Для зміни налаштувань проксі-сервера потрібно в браузері Google Chrome обрати розділ «Настройки», пункт «Система» та натиснути «Настройки прокси-сервера», Рис. 4.

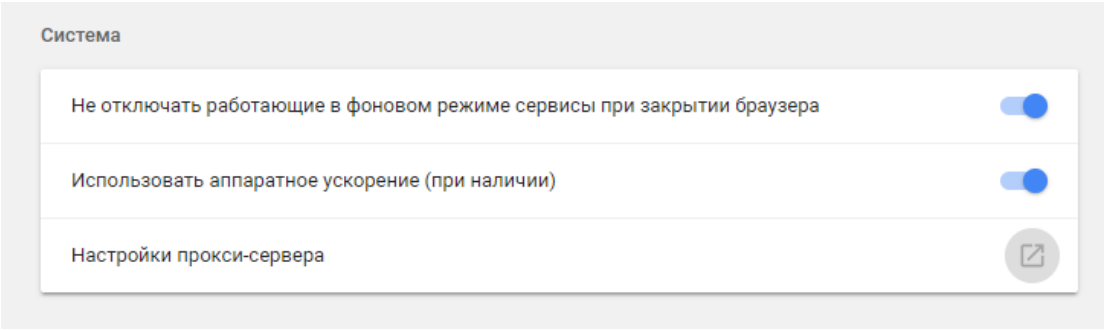

Рис. 4. Налаштування браузера Google Chrome

Для браузера Internet Explorer потрібно обрати «Свойства браузера», Рис. 5.

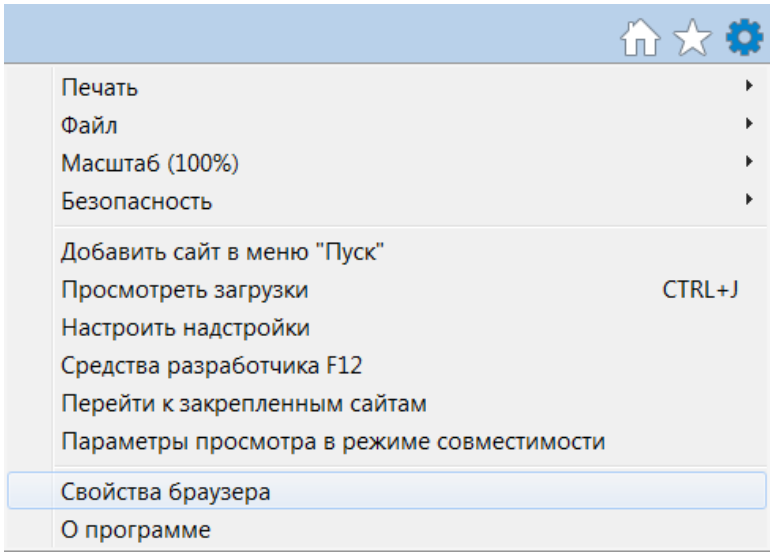

Рис. 5. Налаштування браузера Internet Explorer

Обрані налаштування для обох браузерів є системними. Тому подальший сценарій налаштувань мережі є стандартним для ОС Windows.

Системні налаштування проксі в мережі

У відкритому системному вікні «Свойства: Интернет» у вкладці «Подключение» потрібно натиснути «Настройка сети», Рис. 6.

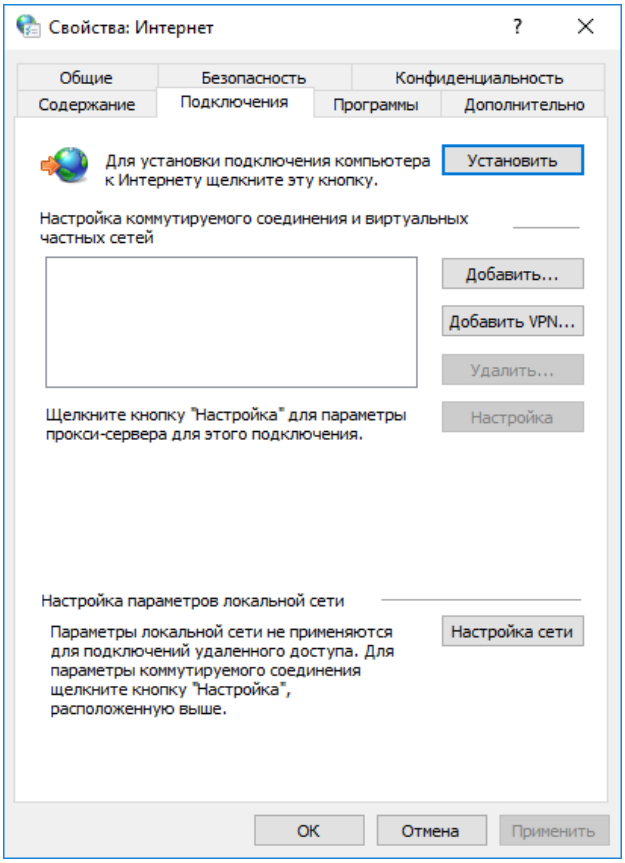

Рис. 6. Системні налаштування мережі

В налаштуваннях параметрів локальної мережі зазначені параметри проксі-сервера, що використовується, слід вказати опцію «Не использовать прокси-сервер для локальных адресов», Рис. 7.

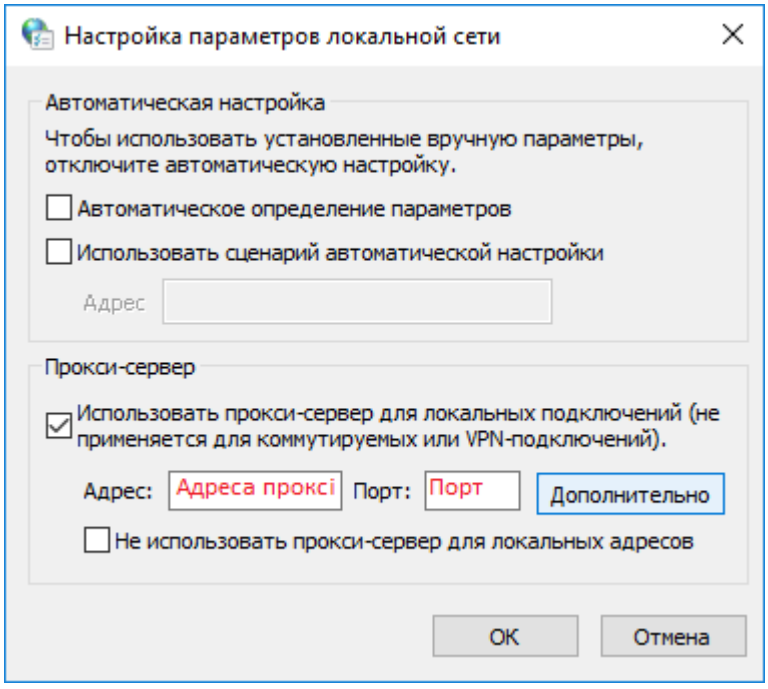

Рис. 7. Налаштування параметрів локальної мережі

Далі у наступному системному вікні потрібно натиснути в розділі «Проксі-сервер» опцію «Дополнительно» та вказати адреси – виключення у полі «Исключения», Рис. 8.

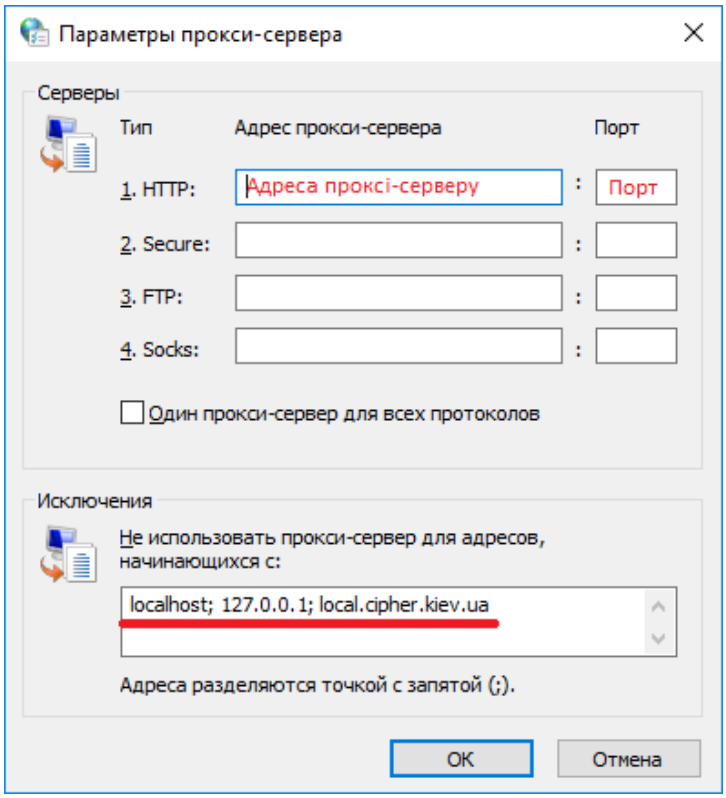

Рис. 8. Параметри проксі-сервера

Середовище Java

Для запуску Java Web Start Application застосувань з урахуванням проксі-сервера у мережі – потрібно внести зміни в налаштуваннях Java, Рис. 9.

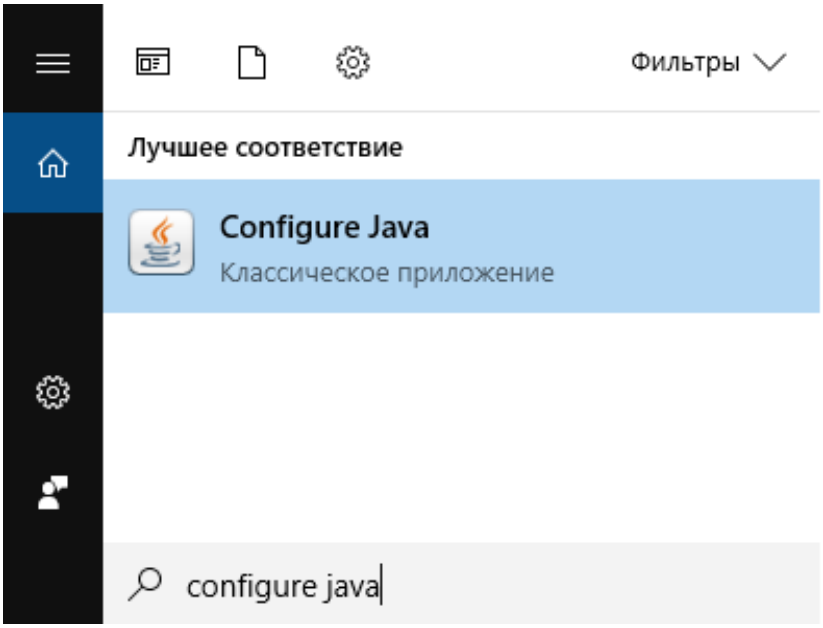

Рис. 9. Конфігурування java-середовища

У відкритій «Панелі управління Java» у вкладці «General» потрібно натиснути кнопку «Network Settings», Рис. 10.

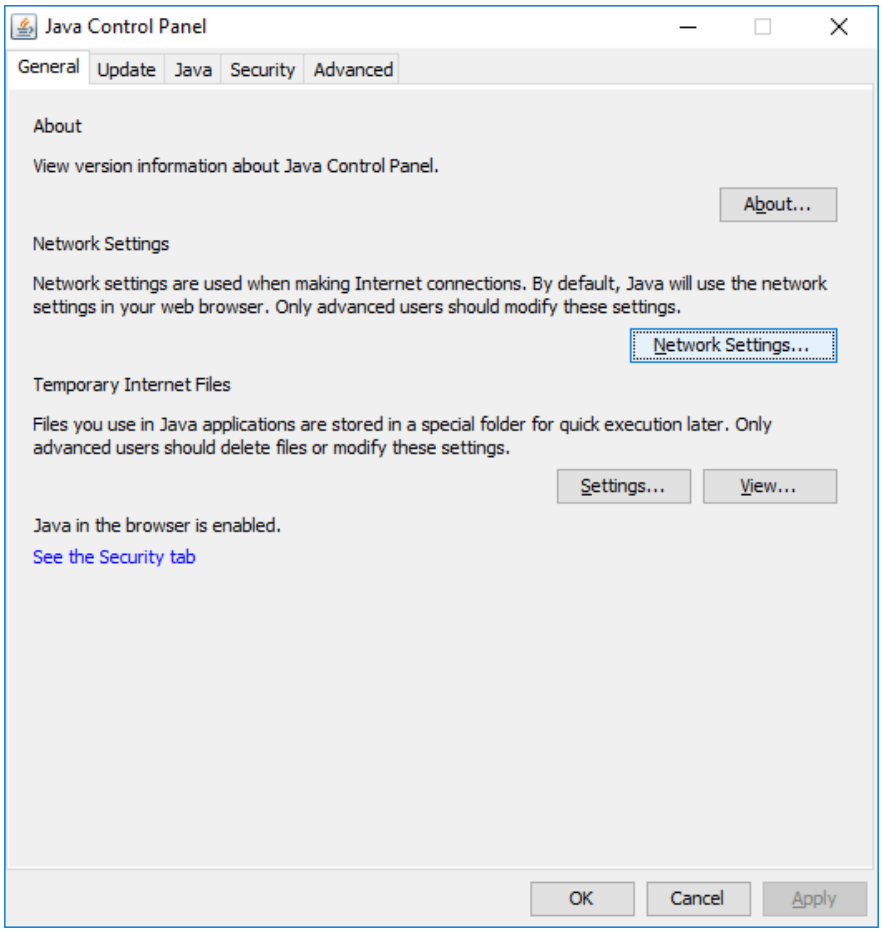

Рис. 10. Панель управління Java

Якщо в мережі використовується проксі-сервер – вказані на Рис. 11 поля будуть заповнені. Щоб додати певні ресурси у виключення – потрібно натиснути «Advanced».

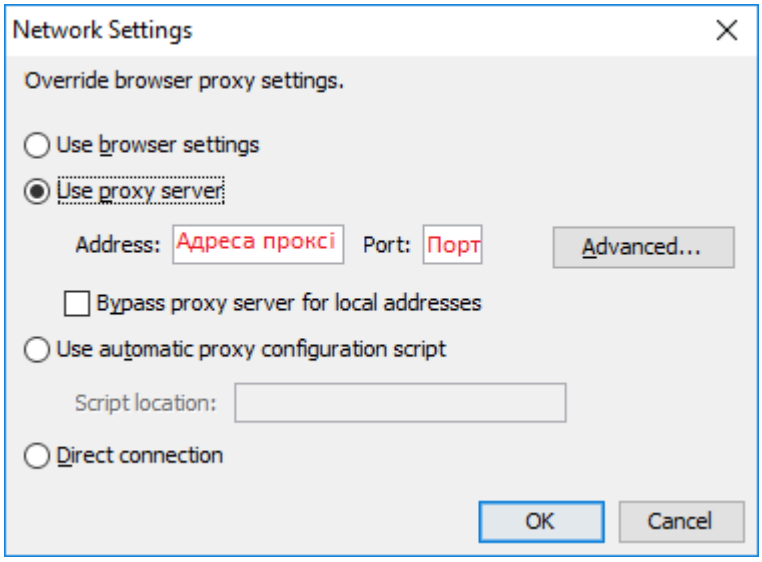

Рис. 11. Налаштування мережі

У розширених налаштуваннях проксі-серверів потрібно записати перелік адрес-виключень, тобто, доступ до яких буде здійснюватись без використання проксі, Рис. 12.

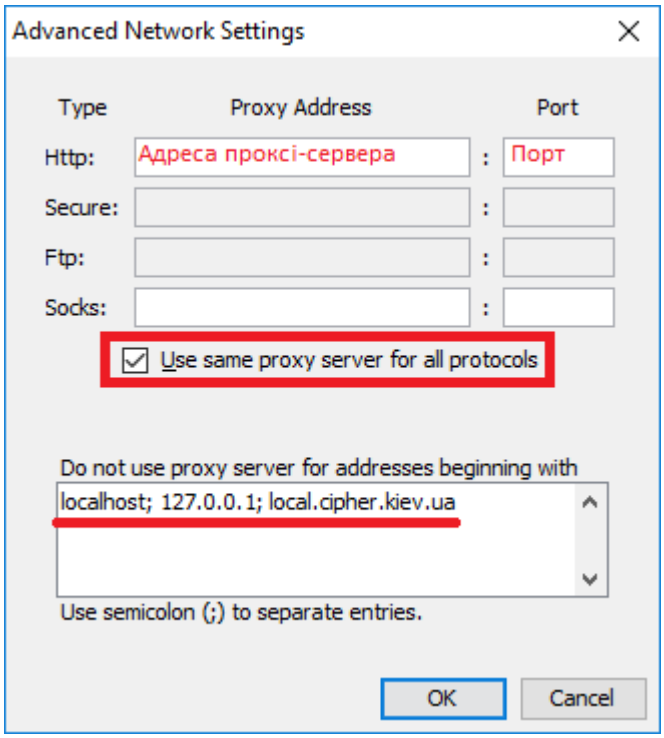

Рис. 12. Налаштування адрес-виключень

Системні налаштування hosts

Для остаточного результату потрібно відредагувати системний файл hosts, саме який відповідає у системі за взаємозв'язок між іменами хостів (сайтів, вузлів тощо) та визначення їх IP-адрес для забезпечення кінцевому користувачеві доступ до ресурсу.

Файл розташований в системі (для ОС Windows) :*C:\Windows\System32\drivers\etc\hosts*.

Для ОС Linux файл розташований в */etc/hosts*.

Для внесення змін – в файлі hosts додати рядок:

```
127.0.0.1 local.cipher.kiev.ua
```

Зберегти зміни в документі.

Застосування захищених носіїв у Персональному сервісі довірчих послуг

Вступ

Для роботи «Персонального сервісу довірчих послуг» із захищеними носіями обов'язковим є встановлення драйвера захищеного ключового носія або спеціального користувацького ПЗ.

«Персональний сервіс довірчих послуг» підтримує роботу з такими носіями у «активному» та «пасивному» режимі:

- Автор SecureToken-337 серії.

- Авест AvestKey.
- Ефіт EfitKey.
- ІІТ Алмаз.
- ІІТ Кристал.

Застосування захищеного носія Автор Secure Token - 337

Для наочної демонстрації роботи із захищеним носієм та встановлення додаткової бібліотеки, Ви можете переглянути поетапну відеоінструкцію за посиланням Налаштування захищеного носія Автор Secure Token 337.

Для роботи «Персонального сервісу довірчих послуг» із захищеними носіями Автор Secure Token-337, необхідні додаткові бібліотеки ***Av337CryptokiD.dll*** (x32/x64 у залежності від розрядності Вашої операційної системи та розрядності Java).

Додатковий .dll файл можна отримати у розробника захищеного носія, компанії Автор, або завантажити за посиланням, вказані нижче, та розмістити за шляхом:

- Для ОС Windows x86 та Java RE x32 Av337CryptokiD.dll. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: ***C:\Program Files (x86)\Java\jre1.8.0_181\bin***.
- Для ОС Windows x64 та для Java RE x64 Av337CryptokiD.dll. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: ***C:\Program Files\Java\jre1.8.0_181\bin***.

Для продовження роботи, необхідно повернутися до «Персонального сервісу довірчих послуг» та заповнити всі поля:

- З випадаючого списку обрати ***КНЕДП/АЦСК***, у якому було отримано захищений носій;
- Обрати ***Тип:***
  - [PKCS#11 пристрої] – активний режим;
  - [PKCS#11 пристрої] – пасивний режим.

У залежності від того, чи самостійно Ви записували ключ на носій (пасивний режим), чи вже отримали захищений носій з ключем (активний режим).

- ***Шлях до контейнера*** – необхідно натиснути кнопку ***«…»,*** Рис. 13;
- ***Пароль*** – вказати PIN до захищеного носія. Важливо звернути увагу на розкладку клавіатури.

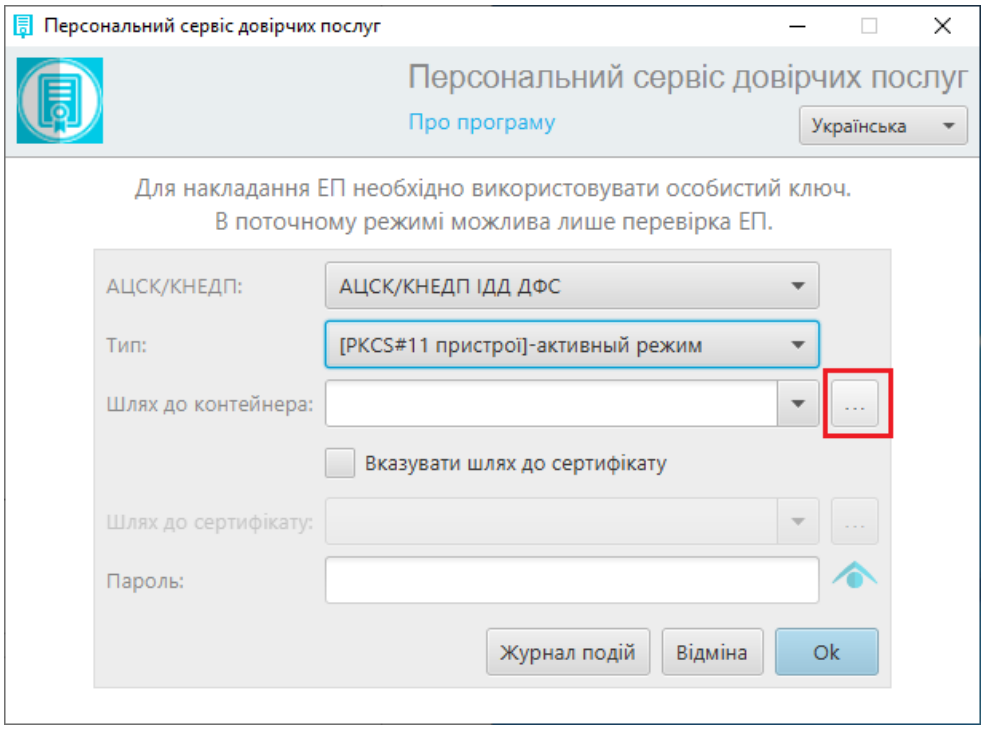

Рис. 13. Вказівка «Шлях до контейнера»

Після додаткового налаштування захищений носій буде відображатися у списку під'єднаних до комп'ютера носіїв, у вікні сервісу «Вибір носія», Рис. 14.

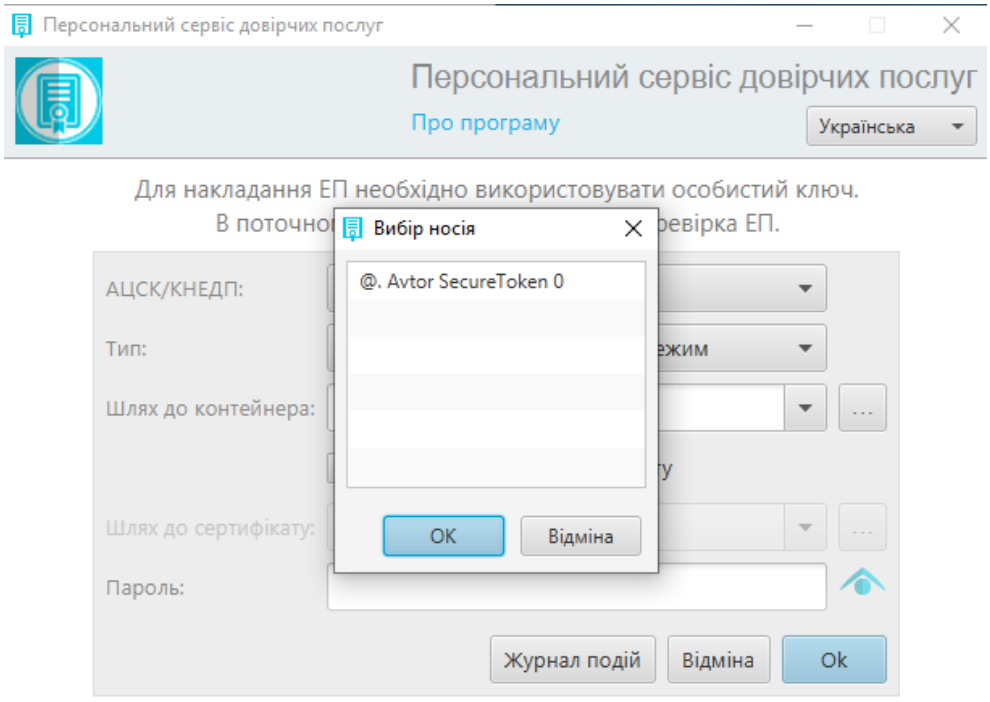

Рис. 14. Сервіс «Вибір носія»

Якщо захищений носій не виявлено, зверніться до:

- Постачальника захищених носіїв.

- Розробника захищених носіїв.
- Розробника «Персонального сервісу довірчих послуг».

Подальша робота «Персонального сервісу довірчих послуг» з PKCS#11 пристроями можлива тільки після повного усунення питань, пов'язаних з правильною роботою захищених носіїв.

Після встановлення програмного забезпечення для роботи із захищеними носіями, слід переконатися, що операційна система виявила їх та відображає в «Диспетчере устройств». Для перевірки необхідно перейти «Пуск» -> «Панель управления» -> «Диспетчер устройств» -> «SmartCard Reader».

Застосування захищеного носія "EFIT KEY"

Для наочної демонстрації можна переглянути поетапну відеоінструкцію за посиланням Установка та налаштування захищеного носія EFITKEY.

Необхідно завантажити за посиланням та встановити програмне забезпечення для роботи із захищеними носіями EFIT KEY.

Для продовження роботи, необхідно повернутися до «Персонального сервісу довірчих послуг» та заповнити всі поля:

- З випадаючого списку обрати ***КНЕДП/АЦСК***, у якому було отримано захищений носій;
- Обрати ***Тип:***
  - [PKCS#11 пристрої] – активний режим;
  - [PKCS#11 пристрої] – пасивний режим.
    У залежності від того, чи самостійно Ви записували ключ на носій (пасивний режим), чи вже отримали захищений носій з ключем (активний режим).
- ***Шлях до контейнера*** – необхідно натиснути кнопку «…», Рис. 15;
- ***Пароль*** – вказати PIN до захищеного носія. Важливо звернути увагу на розкладку клавіатури.

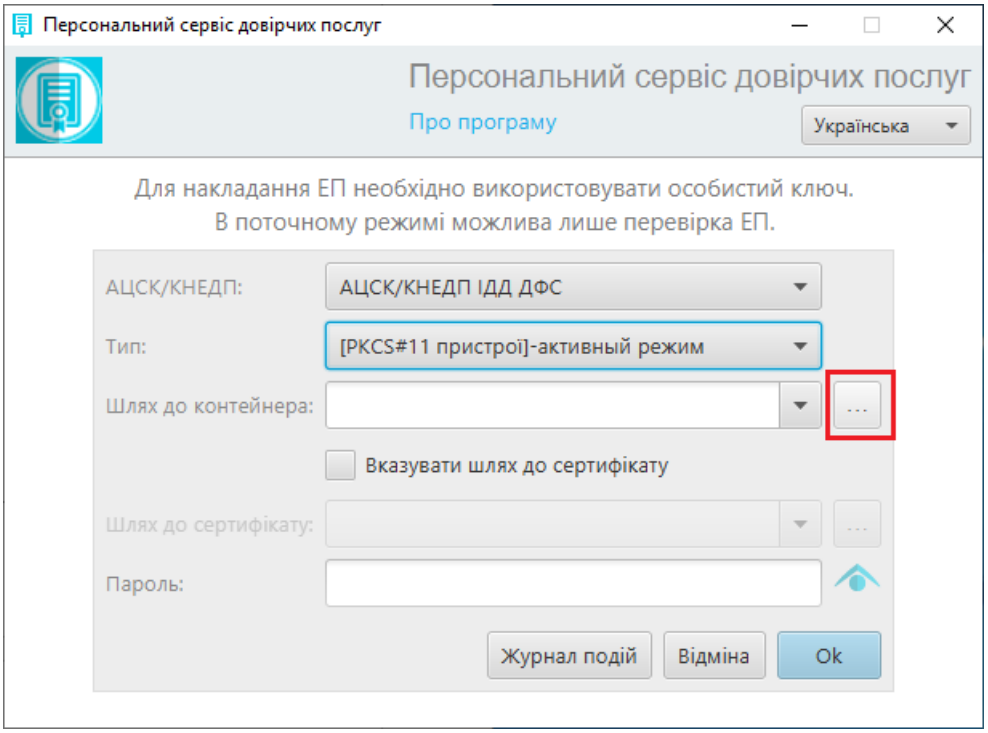

Рис. 15. Вказівка «Шлях до контейнера»

Після додаткового налаштування захищений носій буде відображатися у списку під'єднаних до комп'ютера носіїв у вікні сервісу «Вибір носія», Рис. 16.

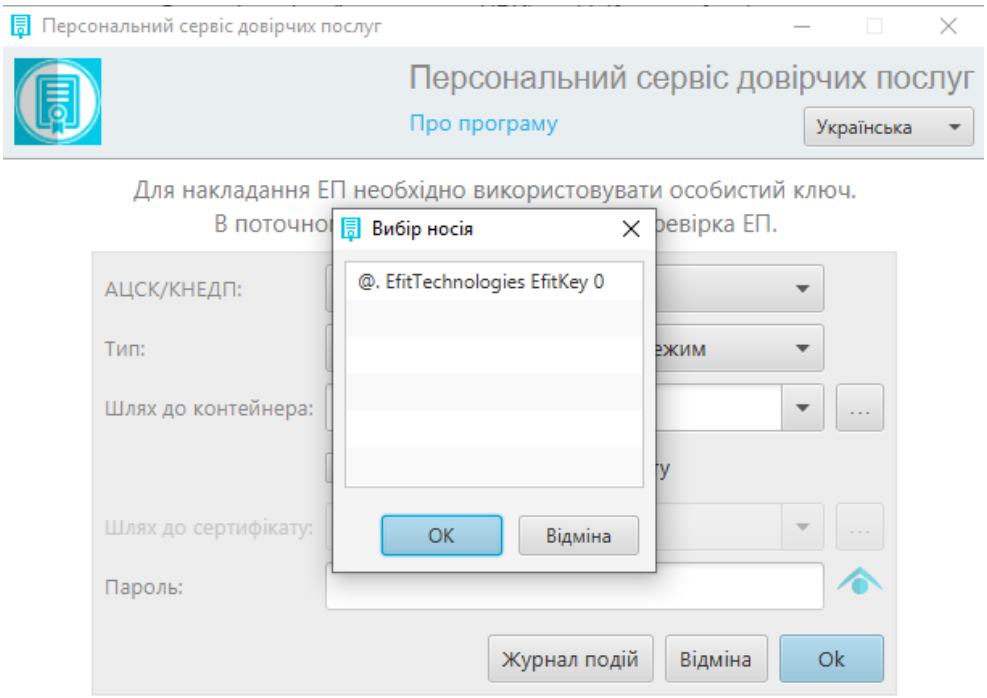

Рис. 16. Сервіс «Вибір носія»

Якщо захищений носій не виявлено, зверніться до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника «Персонального сервісу довірчих послуг».

Подальша робота «Персонального сервісу довірчих послуг» з PKCS#11 пристроями можлива тільки після повного усунення питань, пов'язаних з правильною роботою захищених носіїв.

Після встановлення програмного забезпечення для роботи із захищеними носіями, слід переконатися, що операційна система виявила їх та відображає в «Диспетчере устройств». Для перевірки необхідно перейти «Пуск» -> «Панель управления» -> «Диспетчер устройств» -> «SmartCard Reader».

Застосування електронного ключа "Алмаз-1К"

Для наочної демонстрації Ви можете переглянути поетапну відеоінструкцію за посиланням Налаштування та робота з електронним ключем "Алмаз-1К" у Персональному сервісі довірчих послуг.

Необхідно завантажити за посиланням та встановити програмне забезпечення для роботи з електронним ключем «Алмаз-1К», так як дане застосування допомагає керувати електронним ключем.

Для продовження роботи, необхідно закрити вищевказані застосування та повернутися до «Персонального сервісу довірчих послуг», де слід заповнити всі поля:

- З випадаючого списку обрати ***КНЕДП/АЦСК***, у якому було отримано захищений носій;
- Обрати ***Тип***:
  - [PKCS#11 пристрої] – активний режим;
  - [PKCS#11 пристрої] – пасивний режим.
    У залежності від того, чи самостійно Ви записували ключ на носій (пасивний режим), чи вже отримали захищений носій з ключем (активний режим).
- ***Шлях до контейнера*** – необхідно натиснути кнопку ***«...»,*** Рис. 17;
- ***Пароль*** – вказати PIN до захищеного носія. Важливо звернути увагу на розкладку клавіатури.

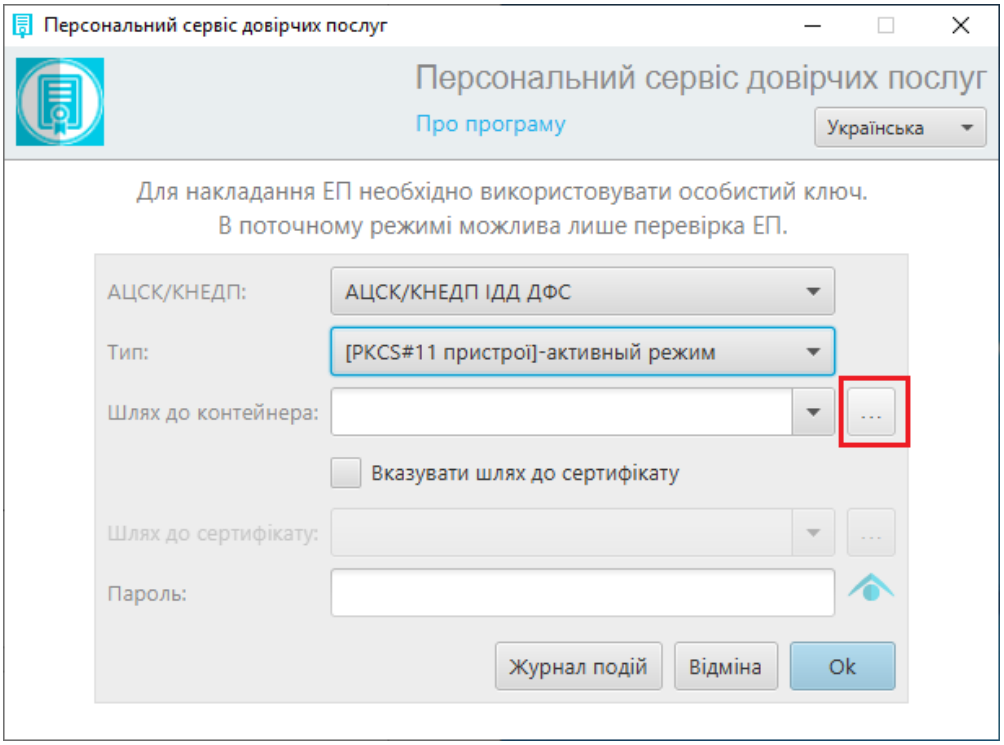

Рис. 17. Вказівка «Шлях до контейнера»

Після додаткового налаштування захищений носій буде відображатися у списку під'єднаних до комп'ютера носіїв у вікні сервісу «Вибір носія», Рис. 18.

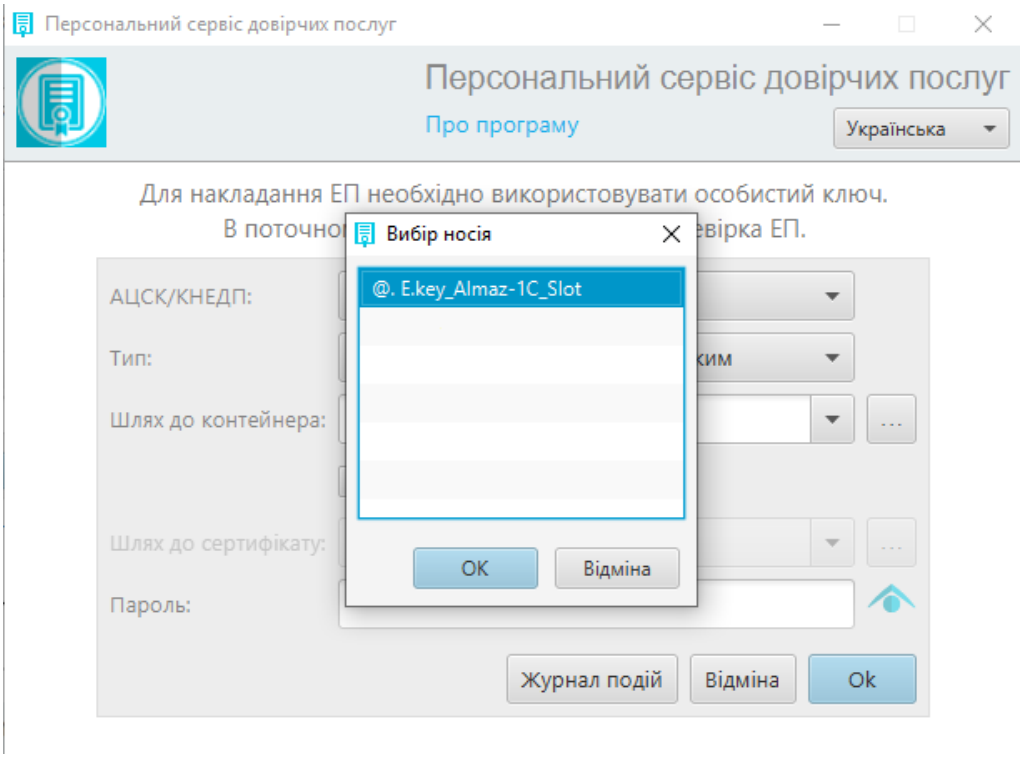

Рис. 18. Сервіс «Вибір носія»

Якщо захищений носій не виявлено, зверніться до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника «Персонального сервісу довірчих послуг».

Подальша робота «Персонального сервісу довірчих послуг» з PKCS#11 пристроями можлива тільки після повного усунення питань, пов'язаних з правильною роботою захищених носіїв.

Після встановлення програмного забезпечення для роботи із захищеними носіями, слід переконатися, що операційна система виявила їх та відображає в «Диспетчере устройств». Для перевірки необхідно перейти «Пуск» -> «Панель управления» -> «Диспетчер устройств» -> «SmartCard Reader».

Застосування електронного ключа "Кристал-1"

Для наочної демонстрації Ви можете переглянути поетапну відеоінструкцію за посиланням Налаштування та робота з електронним ключем "Кристал-1" у Персональному сервісі довірчих послуг.

Необхідно завантажити за посиланням та встановити програмне забезпечення для роботи з електронним ключем Кристал-1, так як дане застосування допомагає керувати електронним ключем.

Слід зауважити, що ключі на даному захищенному носії повинні бути згенеровані у режимі сумісності з PKCS#11. Це необхідно для роботи носія у Персональному сервісі довірчих послуг, якщо Ваш носій не відображається, слід звернутися до вашого КНЕДП/АЦСК та

здійснити перегенерацію ключа у режимі сумісності з PKCS#11 для роботи в активному режимі.

Для продовження роботи, необхідно закрити вищевказані застосування та повернутися до «Персонального сервісу довірчих послуг», де заповнити всі поля:

- З випадаючого списку обрати ***КНЕДП/АЦСК***, у якому було отримано захищений носій;
- Обрати ***Тип***:
  - [PKCS#11 пристрої] – активний режим;
  - [PKCS#11 пристрої] – пасивний режим.
    У залежності від того, чи самостійно Ви записували ключ на носій (пасивний режим), чи вже отримали захищений носій з ключем (активний режим).
- ***Шлях до контейнера*** – необхідно натиснути кнопку ***«...»,*** Рис. 19;
- ***Пароль*** – вказати PIN до захищеного носія. Важливо звернути увагу на розкладку клавіатури.

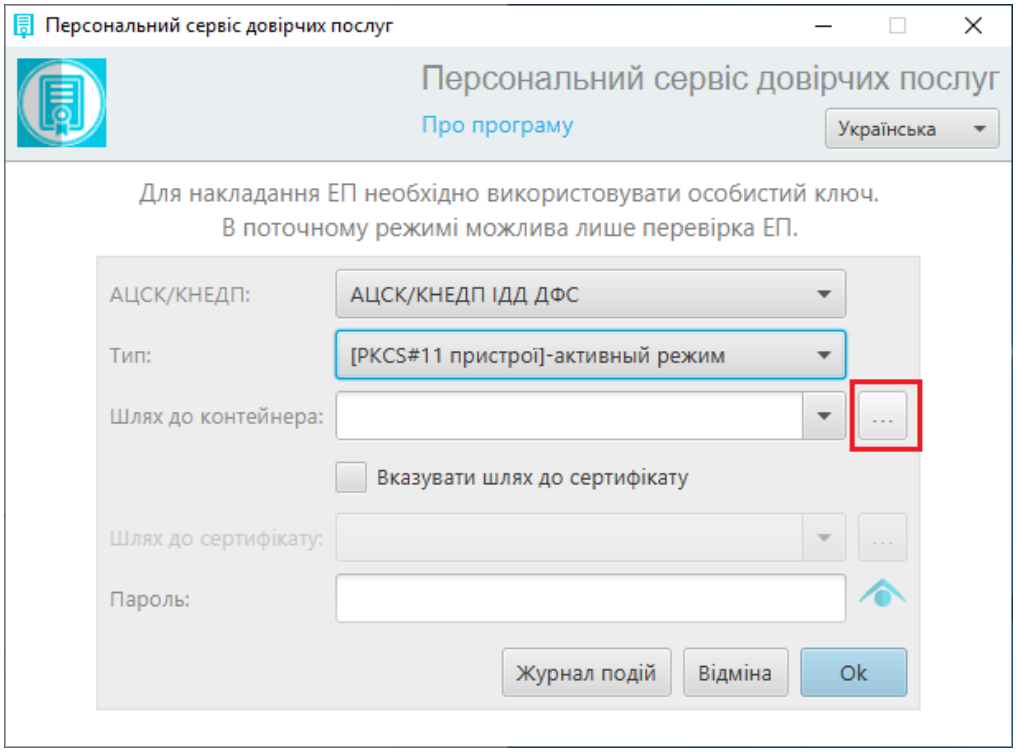

Рис. 19. Вказівка «Шлях до контейнера»

Після додаткового налаштування захищений носій буде відображатися у списку під'єднаних до комп'ютера носіїв у вікні сервісу «Вибір носія», Рис. 20.

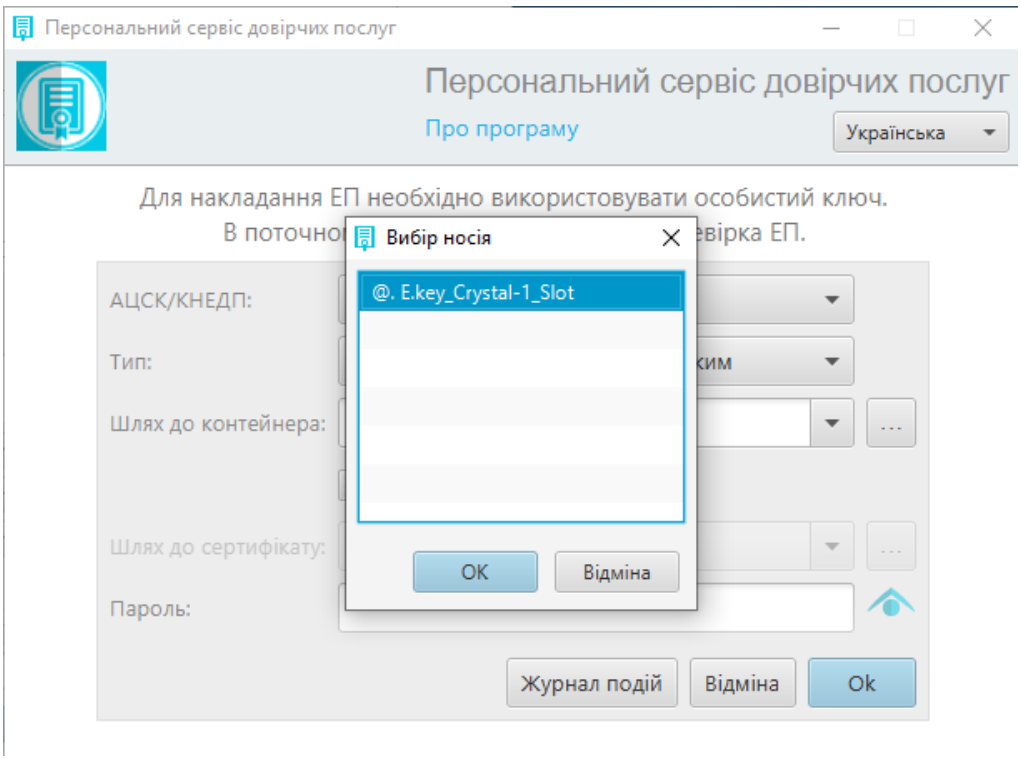

Рис. 20. Сервіс «Вибір носія»

Якщо захищений носій не виявлено, зверніться до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника «Персонального сервісу довірчих послуг».

Подальша робота «Персонального сервісу довірчих послуг» з PKCS#11 пристроями можлива тільки після повного усунення питань, пов'язаних з правильною роботою захищених носіїв.

Після встановлення програмного забезпечення для роботи із захищеними носіями, слід переконатися, що операційна система виявила їх та відображає в «Диспетчере устройств». Для перевірки необхідно перейти «Пуск» -> «Панель управления» -> «Диспетчер устройств» -> «SmartCard Reader».

Застосування смарт-карти у Персональному сервісі довірчих послуг

Для наочної демонстрації Ви можете переглянути поетапну відеоінструкцію за посиланням Налаштування та робота зі смарт-картою у Персональному сервісі довірчих послуг.

Необхідно завантажити та розмістити бібліотеку для роботи зі смарт-картою, так як даний перелік програмного забезпечення дозволяє працювати зі смарт-картою.

Додатковий .dll файл можна отримати у розробника смарт-карти, або завантажити за посиланням, вказані нижче, та розмістити за шляхом:

- Для ОС Windows x86 та Java RE x32 plcpkcs11-x86.dll. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: ***C:\Program Files (x86)\Java\jre1.8.0_181\bin***.

- Для ОС Windows x64 та для Java RE x64 plcpkcs11.dll. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: ***C:\Program Files\Java\jre1.8.0_181\bin***.

Слід зауважити, що ключі на даній смарт-карті повинні бути згенеровані у режимі сумісності з PKCS#11. Це необхідно для роботи носія у Персональному сервісі довірчих послуг, якщо Ваш носій не відображається, слід звернутися до вашого КНЕДП/АЦСК та здійснити перегенерацію ключа у режимі сумісності з PKCS#11 для роботи в активному режимі.

Для продовження роботи, необхідно закрити вищевказані застосування та повернутися до «Персонального сервісу довірчих послуг», де заповнити всі поля:

- З випадаючого списку обрати ***КНЕДП/АЦСК***, у якому було отримано захищений носій;
- Обрати ***Тип***:
  - [PKCS#11 пристрої] – активний режим;
- ***Шлях до контейнера*** – необхідно натиснути кнопку ***«...»,*** Рис. 23;
- ***Пароль*** – вказати PIN до захищеного носія. Важливо звернути увагу на розкладку клавіатури.

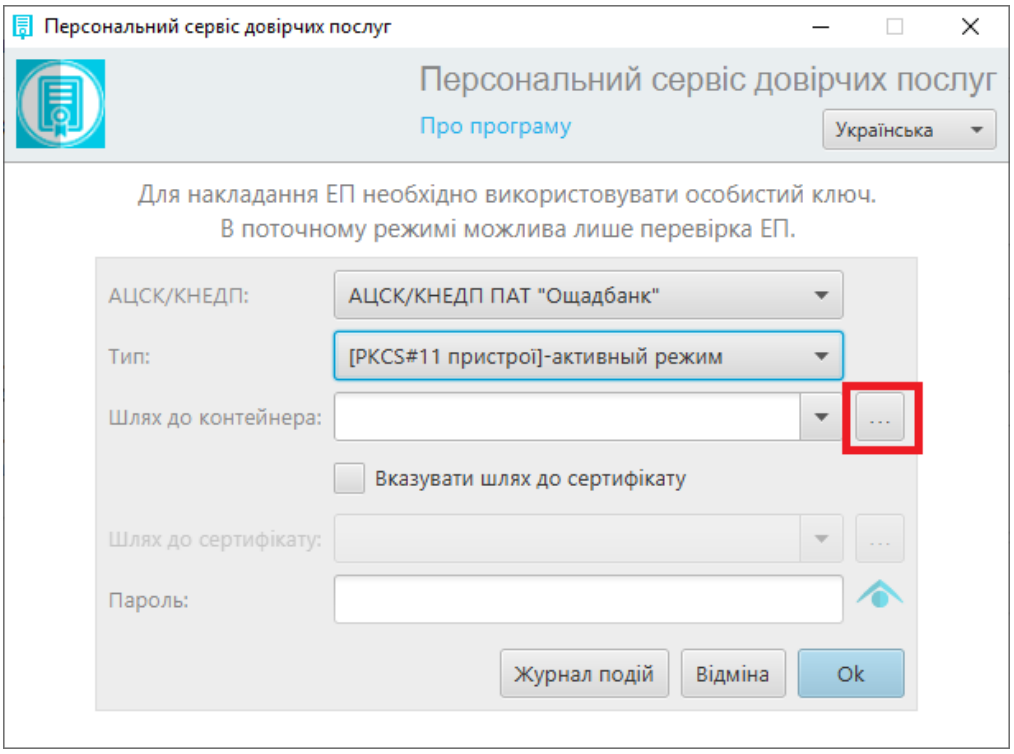

Рис. 21. Вказівка «Шлях до контейнера»

Після додаткового налаштування захищений носій буде відображатися у списку під'єднаних до комп'ютера носіїв у вікні сервісу «Вибір носія», Рис. 24.

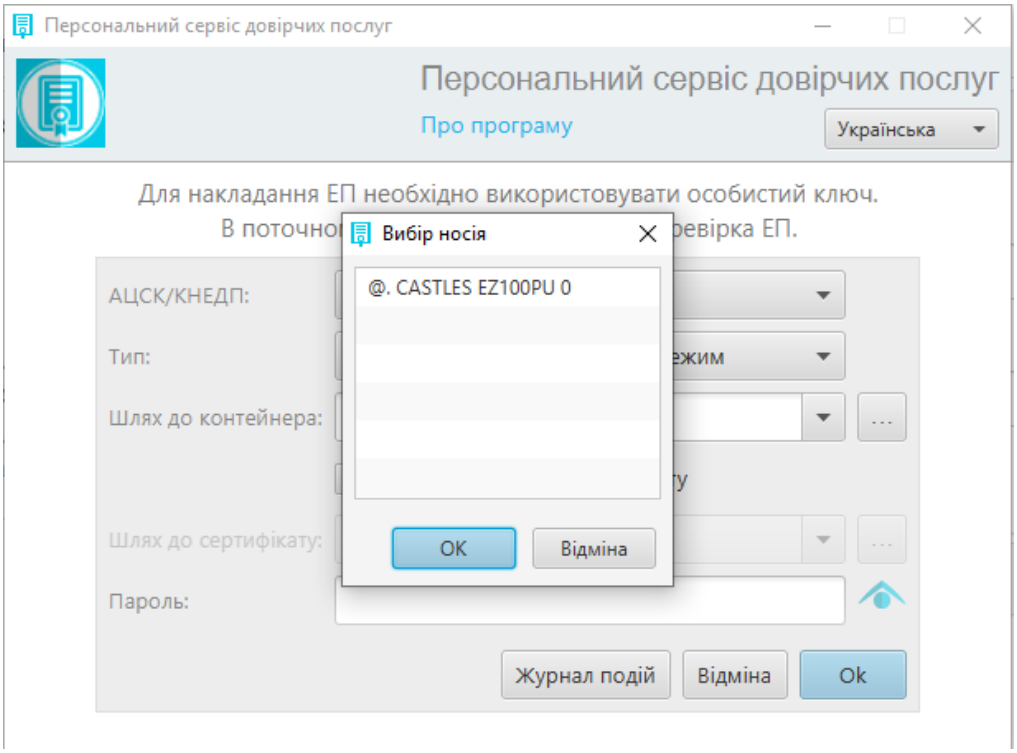

Рис. 22. Сервіс «Вибір носія»

Якщо захищений носій не виявлено, зверніться до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника «Персонального сервісу довірчих послуг».

Подальша робота «Персонального сервісу довірчих послуг» з PKCS#11 пристроями можлива тільки після повного усунення питань, пов'язаних з правильною роботою захищених носіїв.

Після встановлення програмного забезпечення для роботи зі смарт-картами, слід переконатися, що операційна система виявила їх та відображає в «Диспетчере устройств». Для перевірки необхідно перейти «Пуск» -> «Панель управления» -> «Диспетчер устройств» -> «SmartCard Reader».

Робота з Персональним сервісом довірчих послуг

Запуск

1. Стартове вікно Персонального сервісу довірчих послуг у веб-браузері виглядає так, Рис. 23.

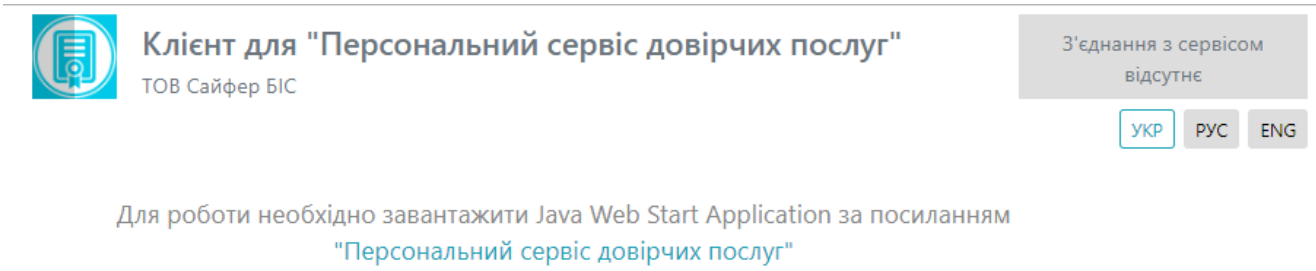

Рис. 23. Стартове вікно Персонального сервісу довірчих послуг

2. При першому запуску потрібно обрати пункт «Открыть в Java (TM) Web Start Launcher», Рис. 24.

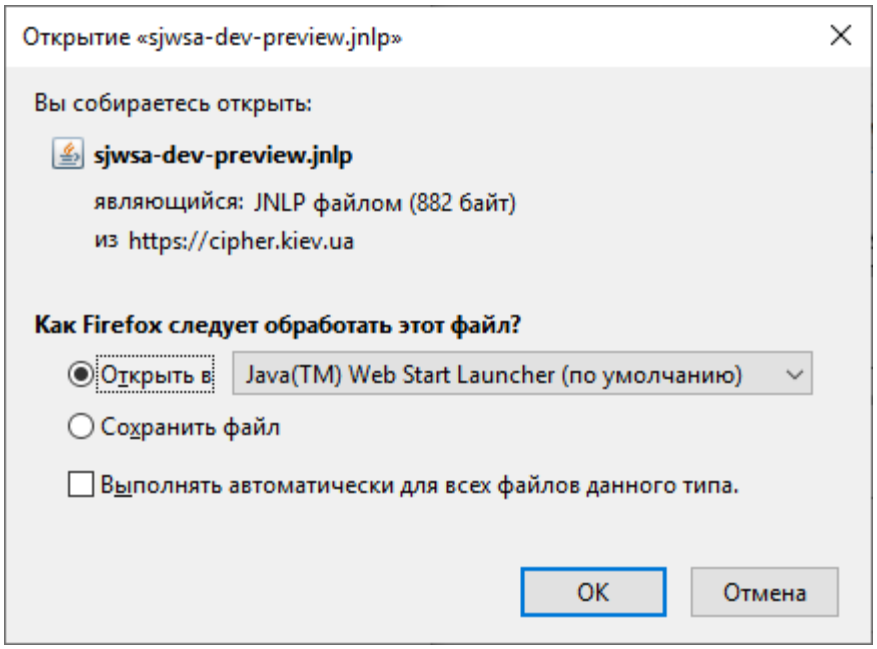

Рис. 24. Запуск jnlp-файлу

Для запобігання появи такого діалогового вікна при подальших запусках «Персонального сервісу довірчих послуг», слід встановити позначку «Выполнять автоматически для всех файлов данного типа». Натискаємо «ОК».

3. Можна натиснути «Сохранить файл», тоді файл буде збережно, його слід відкрити засобами Java-машини, яка попередньо була встановлена на комп'ютері. Для коректної роботи, необхідно попередньо встановити Java 8 версії, та оновлювати її.

Виникає помилка при завантаженні jnlp-файлу з веб-сторінки «Персонального сервісу довірчих послуг» у браузері Google Chrome, але необхідно натиснути «Сохранить» та відкрити завантажений файл, Рис. 25.

Рис. 25. Повідомлення при завантажені jnlp-файлу у браузері Google Chrome

Якщо встановлена операційна система Windows XP, то з останніми версіями Java, «Персональний сервіс довірчих послуг» працює некоректно, тому слід завантажити за посиланням [jre-8u111-windows-i586.exe] та встановити саме цю версію.

4. При старті «Персонального сервісу довірчих послуг» виникає попередження з яким необхідно ознайомитися та підтвердити запуск програми. Правильними значеннями таких параметрів як, *Name*, *Publisher* та *Location* повинні бути, як вказано на Рис. 26.

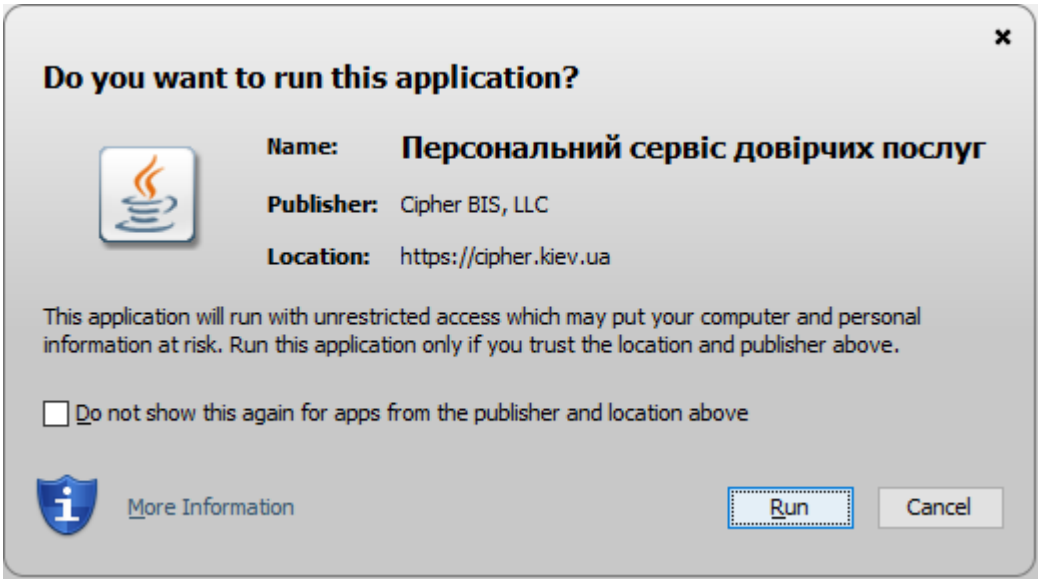

Рис. 26. Інформація від Java про видавця «Персонального сервісу довірчих послуг»

Після ознайомлення з інформацією про видавця Java-застосування «Персональний сервіс довірчих послуг» - успішно запускається.

5. Наступним кроком є відкриття «Персонального сервісу довірчих послуг», Рис. 27.

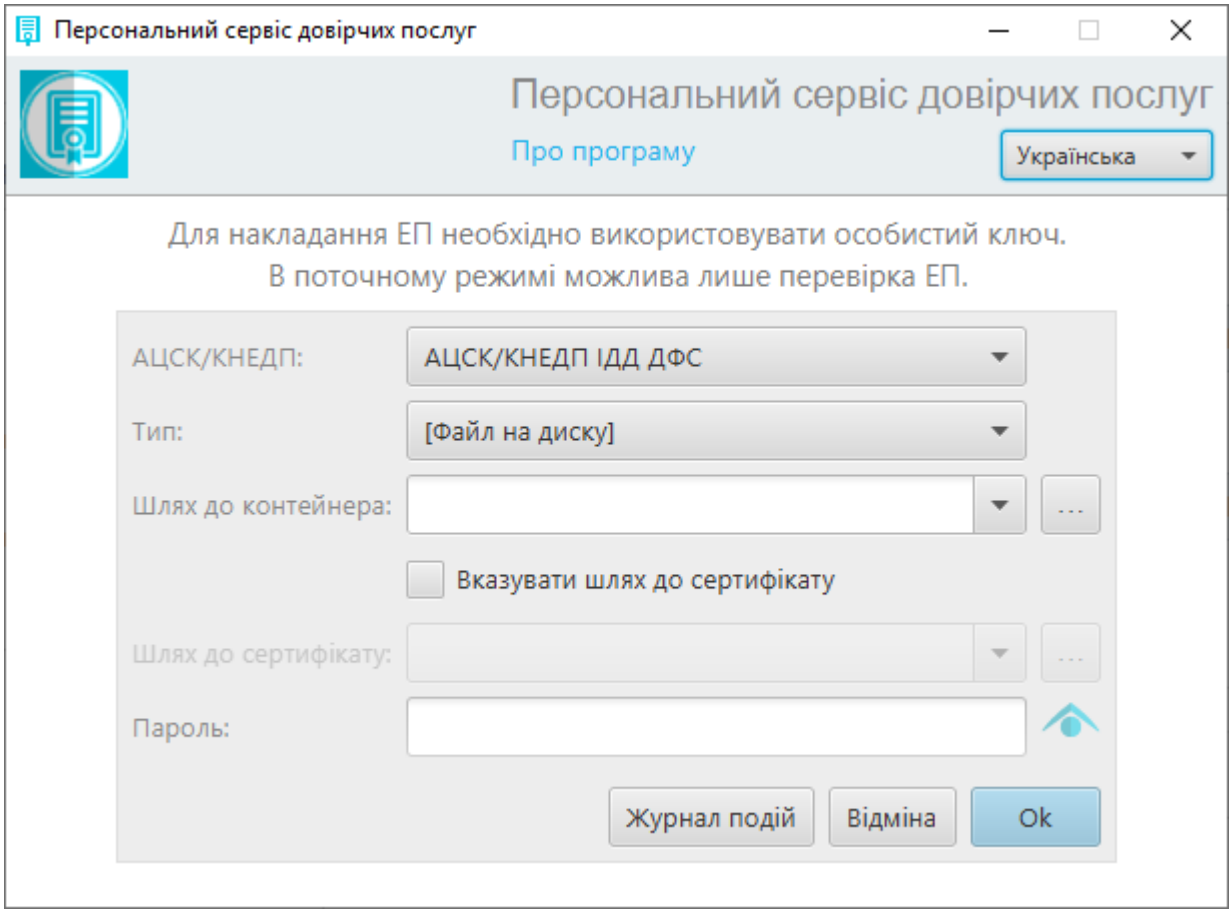

Рис. 27. Форма завантаження особистого ключа

Для подальшої роботи необхідно правильно ввести дані, а саме:

- Обрати з переліку ***КНЕДП/АЦСК (Центр сертифікації ключів),*** у якому було отримано захищений носій чи ключ, Рис. 28;

Перелік КНЕДП/АЦСК, які підтримуються «Персональним сервісом довірчих послуг»:

- КНЕДП/АЦСК ІДД ДФС;
- Тестовий ЦСК ІІТ;
- Тестовий ЦСК Сайфер;
- Тестовий ЦСК Сайфер (проксі);
- КНЕДП/АЦСК ПАТ «Комерційний банк «Приватбанк»;
- КНЕДП/АЦСК ПАТ «Ощадбанк»;
- КНЕДП/АЦСК ТОВ «Центр сертифікації ключів «Україна».

Примітка. Повну інформацію можна переглянути за посиланням:
https://docs.cipher.kiev.ua/pages/viewpage.action?pageId=8618204

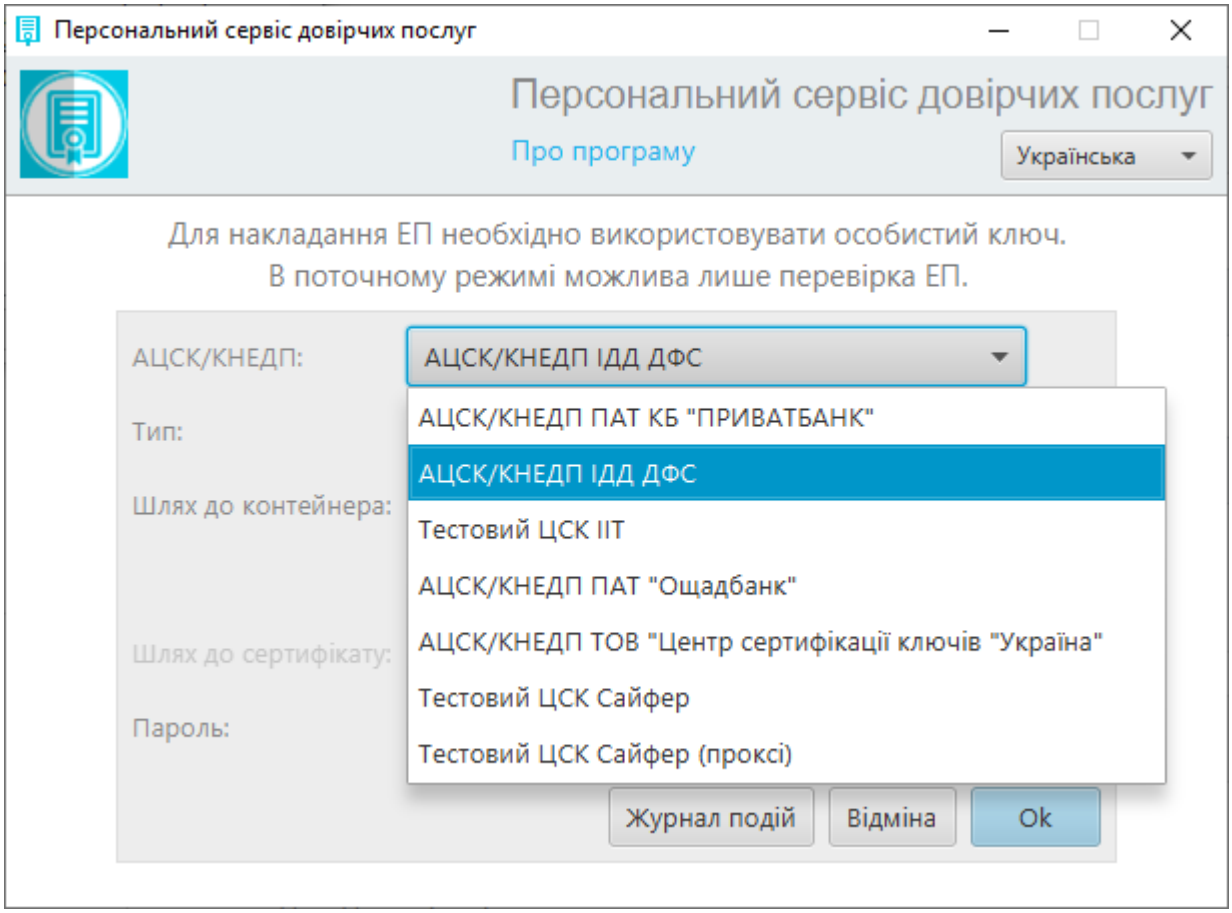

Рис. 28. Вибір КНЕДП/АЦСК

- Обрати ***Тип***:
  - [Файл на диску] – для ключового контейнера, Рис. 29;
  - [PKCS#11 пристрої] – активний режим;
  - [PKCS#11 пристрої] – пасивний режим.
    У залежності від того, чи самостійно Ви записували ключ на носій (пасивний режим), чи вже отримали захищений носій з ключем (активний режим), Рис. 30.

Перелік захищених носіїв:

- Авест AvestKey.
- Ефіт EfitKey, відеоінструкція.
- Autor SecureToken-337, відеоінструкція.
- ІІТ Алмаз відеоінструкція;
- ІІТ Кристал, відеоінструкція.

Захищений носій, який **не підтримується** «Персональним сервісом довірчих послуг»:

- Plasticard TEllipse;

Примітка. Повну інформацію про застосування захищений носіїв у «Персональному сервісі довірчих послуг», можна переглянути за посиланням:
https://docs.cipher.kiev.ua/pages/viewpage.action?pageId=8618414

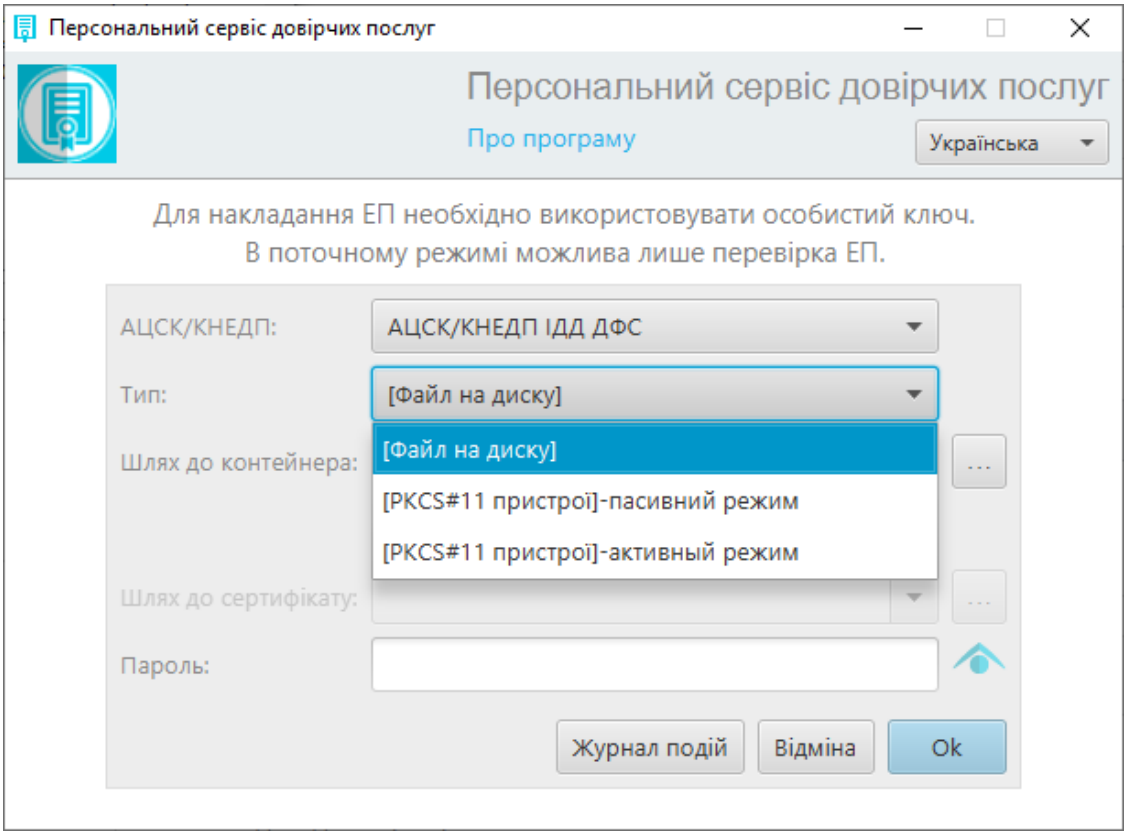

Рис. 29. Вибір Типу для ключового контейнеру

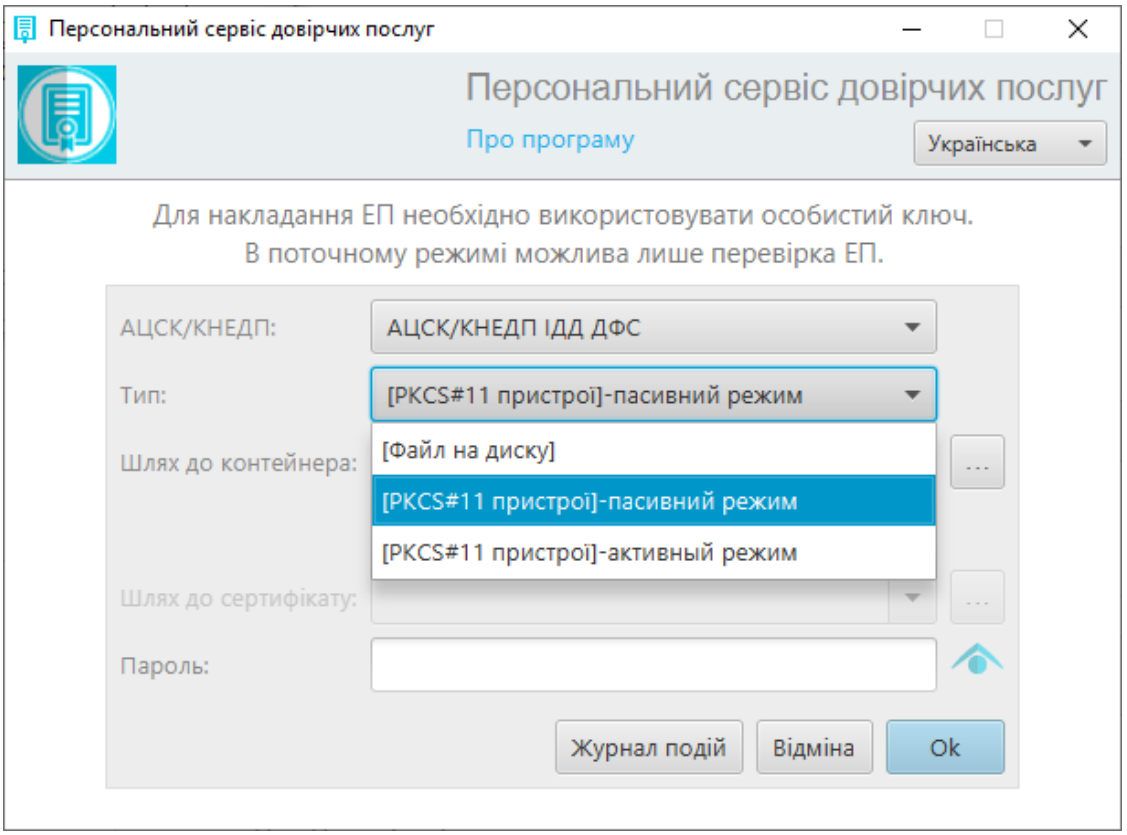

Рис. 30. Вибір Типу для захищеного носія

- Вказати ***Шлях до контейнера*** – необхідно натиснути кнопку «**...**» та вказати місцезнаходження для файлу:
  - Якщо це файл – відкривається «Відкрити контейнер», у якому необхідно вказати місцезнаходження ключового контейнера, Рис. 31. Слід зауважити, що файл необхідно розмістити у корені диску, чи у папці, яка містить цифри чи латинські літери;
  - Якщо це захищений носій – відкривається вікно «Вибір носія», у якому необхідно обрати під'єднаний захищений носій, Рис. 32.

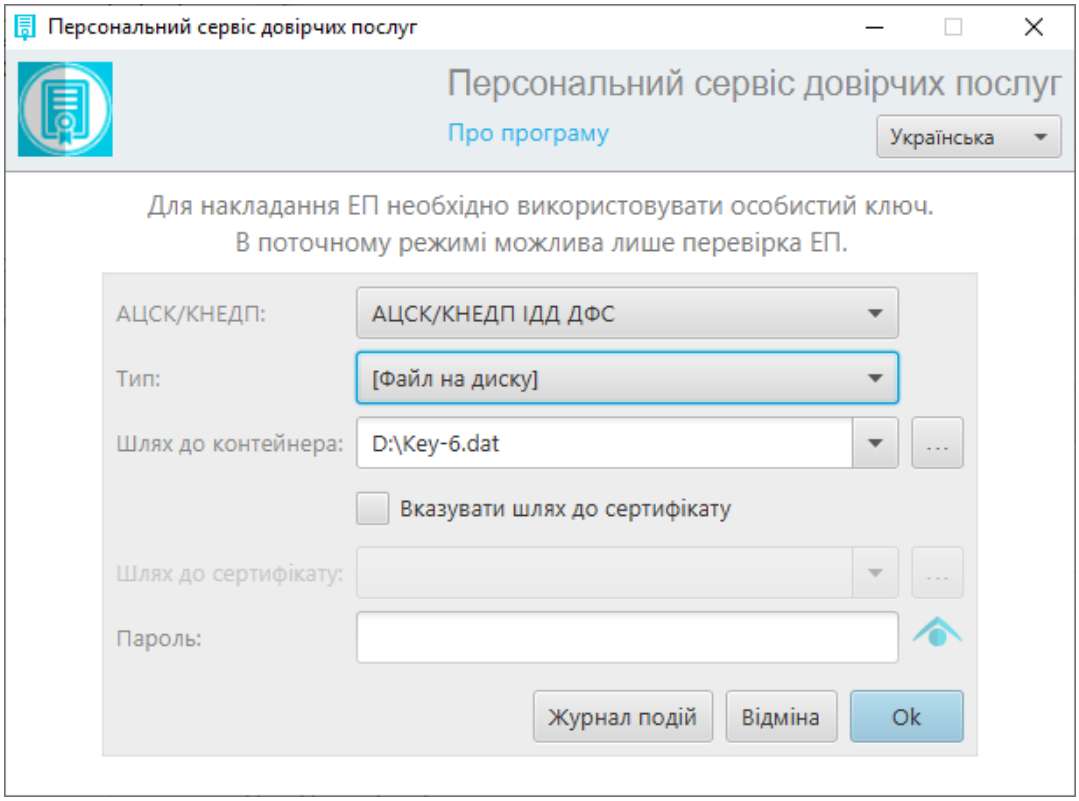

Рис. 31. Поле Шлях до контейнера для файлу

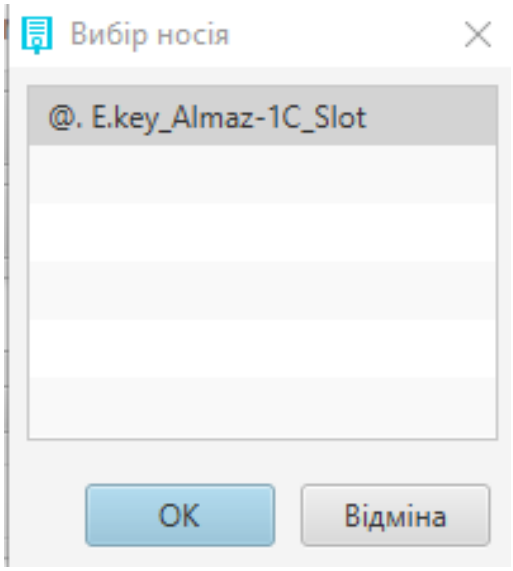

Рис. 32. Поле Шлях до контейнера для захищеного носія

- ***Вказувати шлях до сертифікату*** – позначка, яка дає змогу активувати поле «Шлях до сертифікату» та його вказати, Рис. 33. Передбачено для деяких з КНЕДП/АЦСК, що не забезпечують сервіс СМР (наприклад КНЕДП/АЦСК ТОВ «Центр сертифікації ключів «Україна»), тому необхідно самостійно вказувати файл сертифікату відкритого ключа. Сертифікат потрібен для отримання інформації про власника ЕП при підписанні документів.

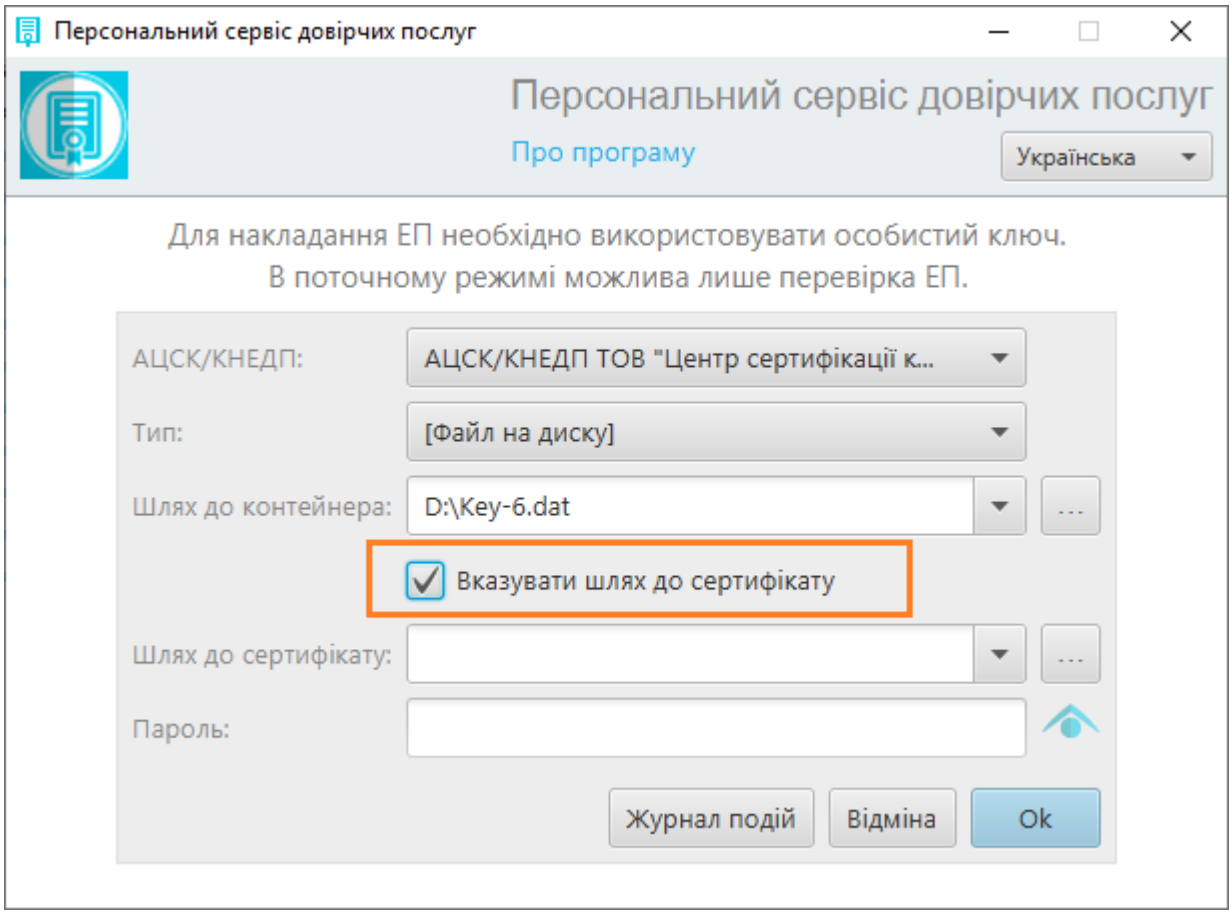

Рис. 33. Позначка Вказувати шлях до сертифікату

- Вказати ***Шлях до сертифікату*** – вказується за необхідності, лише для файлу (за умови якщо попередньо встановлено позначку «Вказувати шлях до сертифікату»). Необхідно натиснути кнопку «**...**», відкривається вікно «Вказати сертифікат», далі вказується місцезнаходження сертифікату, Рис. 34.

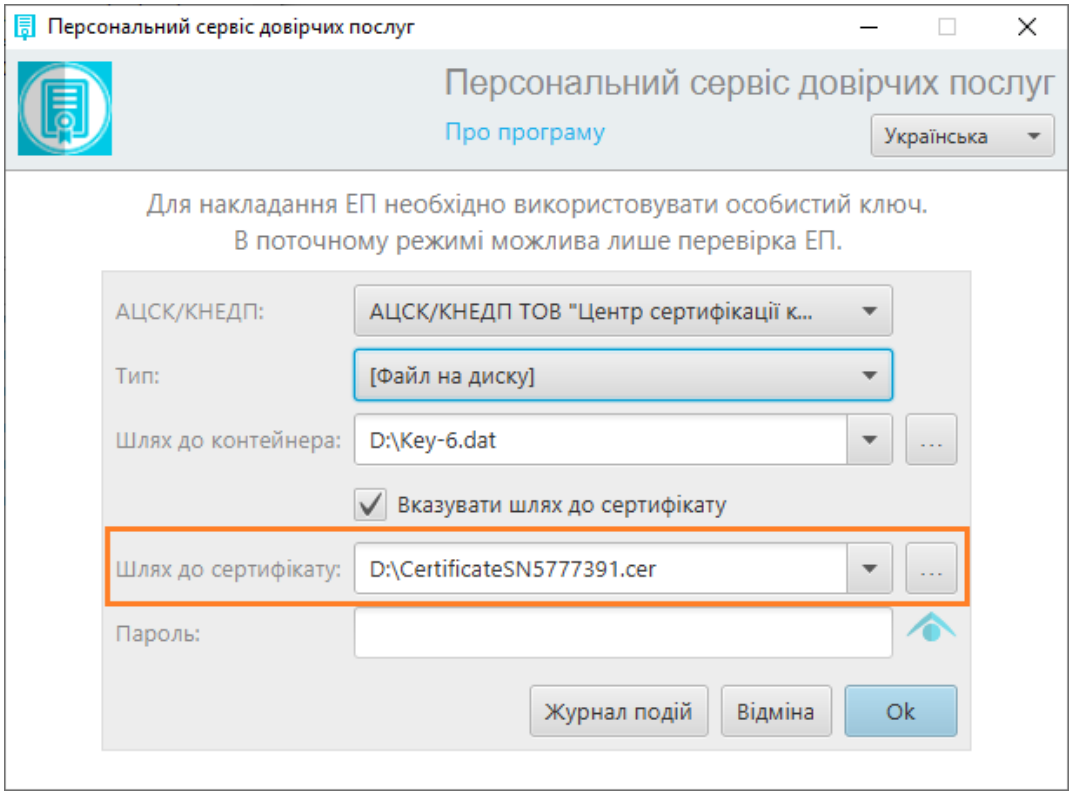

Рис. 34. Поле Шлях до сертифікату

- Ввести ***Пароль*** – ввести пароль до файлу чи захищеного носія. Важливо звернути увагу на розкладку клавіатури, Рис. 35.

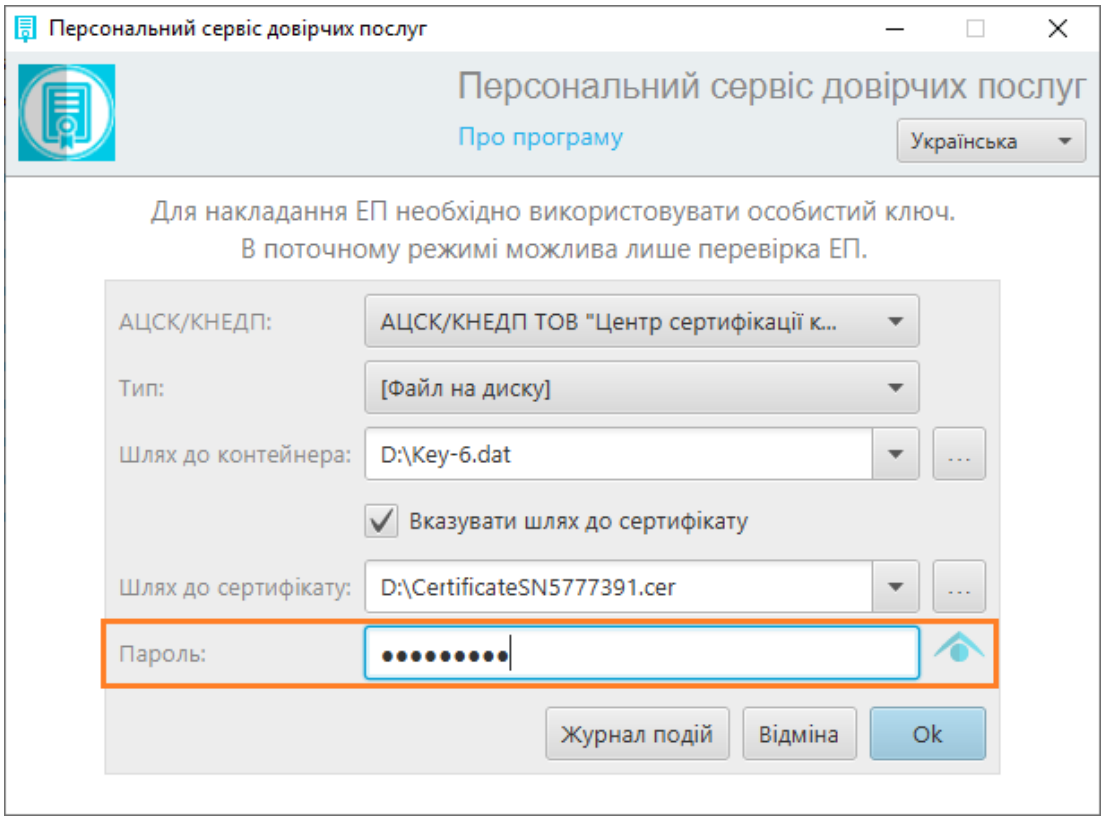

Рис. 35. Поле для введення паролю для файлу чи захищеного носія

Вибір ключа ЕП – файлу

Для накладання ЕП необхідно використовувати особисті ключі. Без ключа ЕП, можна лише перевірити файл з підписом.

Стартове вікно «Персонального сервісу довірчих послуг» містить форму вибору КНЕДП/АЦСК та особистого ключа ЕП, Рис. 36.

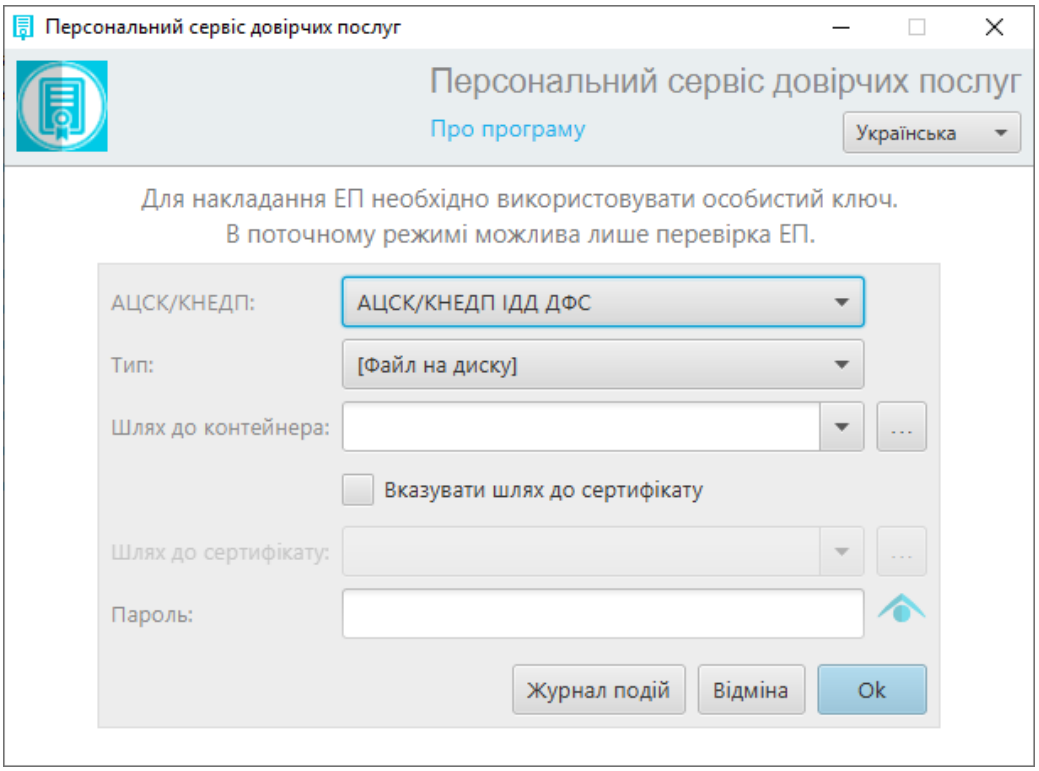

Рис. 36. Стартова форма «Персонального сервісу довірчих послуг»

- ***КНЕДП/АЦСК*** – слід обрати з випадаючого списку центр сертифікації ключів, що видавав ключ ЕП користувачу, Рис. 37.

Перелік КНЕДП/АЦСК, які підтримуються «Персональним сервісом довірчих послуг»:

- КНЕДП/АЦСК ІДД ДФС;
- Тестовий ЦСК ІІТ;
- Тестовий ЦСК Сайфер;
- Тестовий ЦСК Сайфер (проксі);
- КНЕДП/АЦСК ПАТ «Комерційний банк «Приватбанк»;
- КНЕДП/АЦСК ПАТ «Ощадбанк»;
- КНЕДП/АЦСК ТОВ «Центр сертифікації ключів «Україна».

Примітка. Повну інформацію можна переглянути за посиланням:
https://docs.cipher.kiev.ua/pages/viewpage.action?pageId=8618204

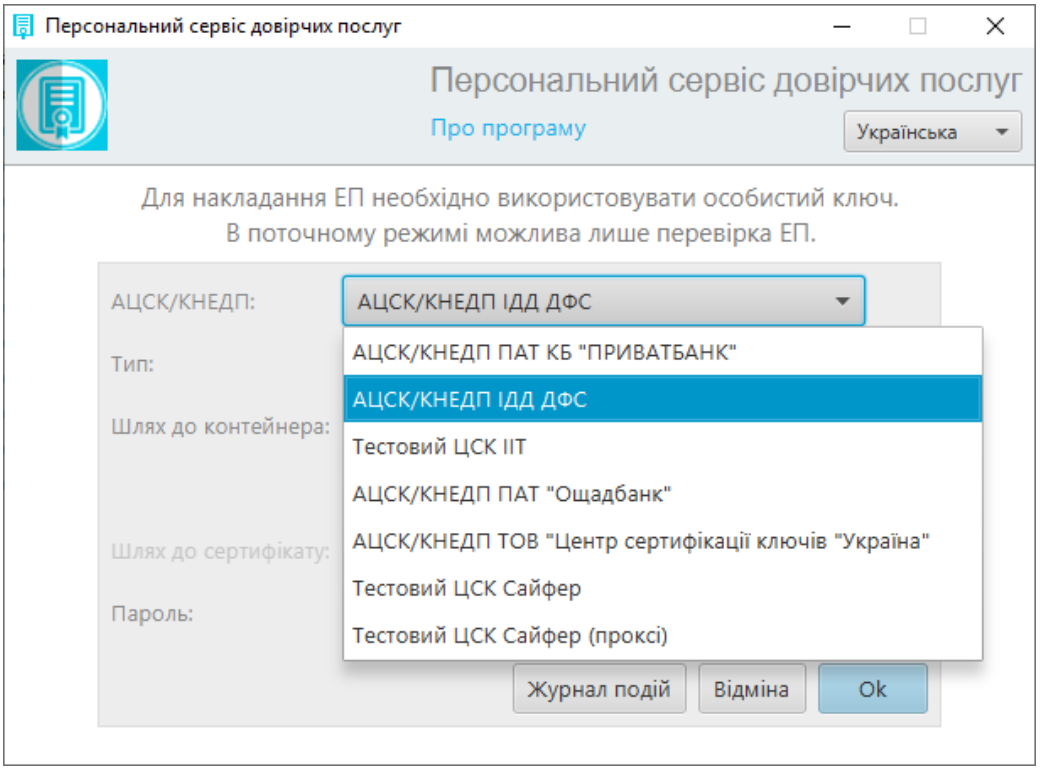

Рис. 37. Вибір Центра сертифікації ключів

- ***Тип*** — обрати із випадаючого переліку тип ключового носія, який використовується для зберігання особистого ключа ЕП.

Файл на диску – особистий ключ зберігається у вигляді файлу з розширенням ***.dat, *.pfx, ZS2** або ***.p12**, Рис. 38.

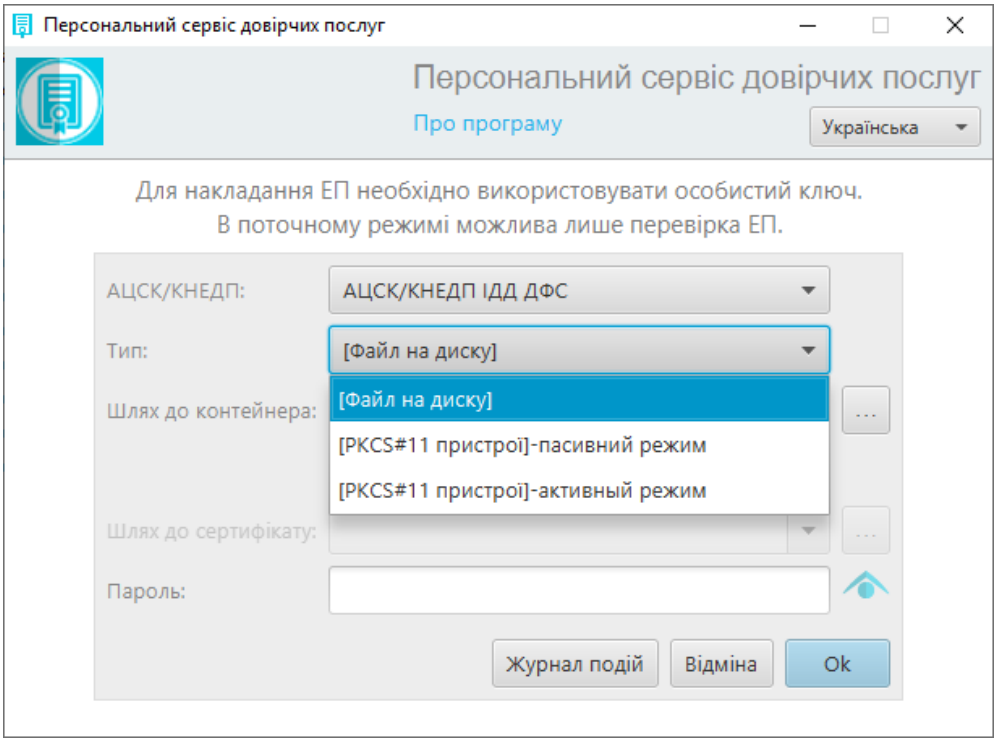

Рис. 38. Обрання типу файлу

- ***Шлях до контейнера*** — обрати з випадаючого переліку раніше обрані файли з ключовим контейнером або вказати шлях до нього, натиснувши на кнопку «…», Рис. 39.

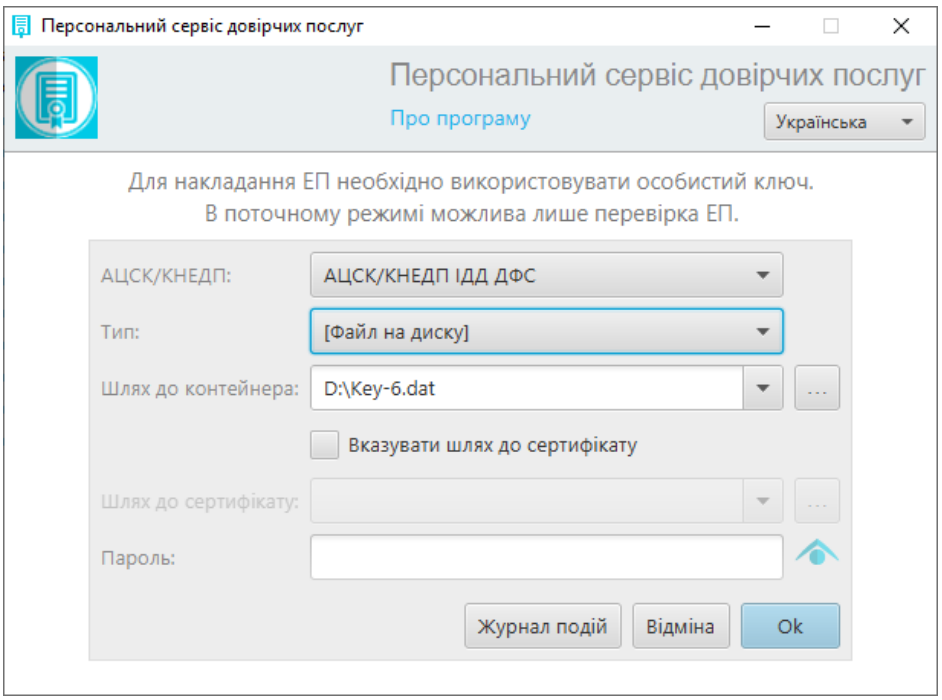

Рис. 39. Поле Шлях до контейнера

- ***Вказувати шлях до сертифікату*** — опцію передбачено для деяких з КНЕДП/АЦСК, що не забезпечують сервіс СМР (наприклад КНЕДП/АЦСК ТОВ «Центр сертифікації ключів «Україна»), тому необхідно самостійно вказувати файл сертифікату відкритого ключа. Сертифікат потрібен для отримання інформації про власника ЕП при підписанні документів, Рис. 40.

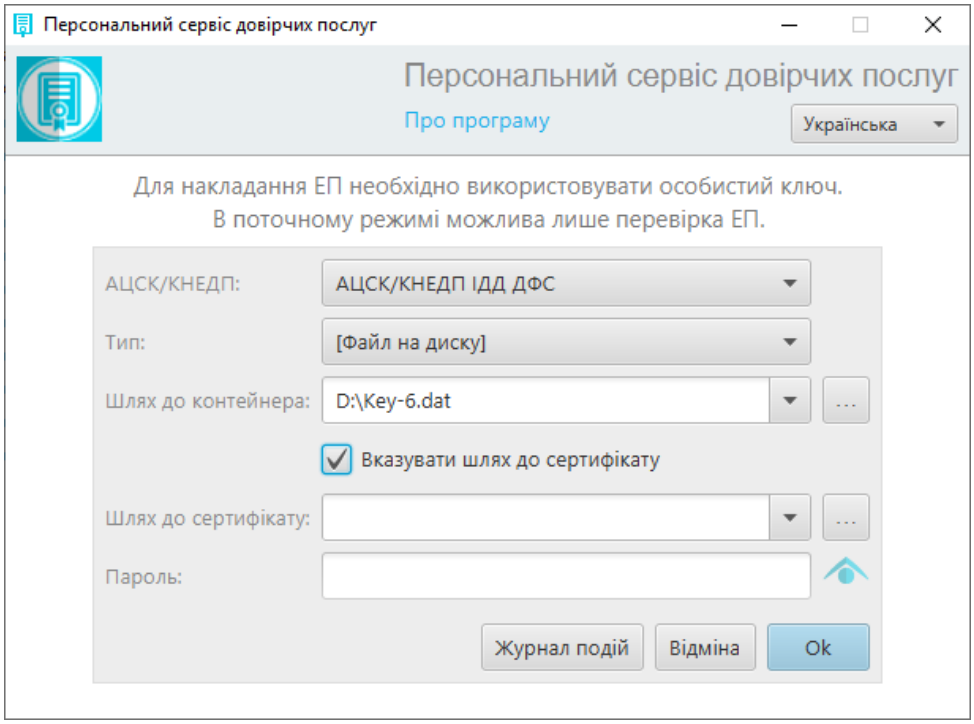

Рис. 40. Позначка Вказувати шлях до сертифікату

- ***Шлях до сертифікату*** – обрати з випадаючого списку раніше обрані файли сертифікатів або вказати шлях до нього натиснувши на кнопку «…», Рис. 41;

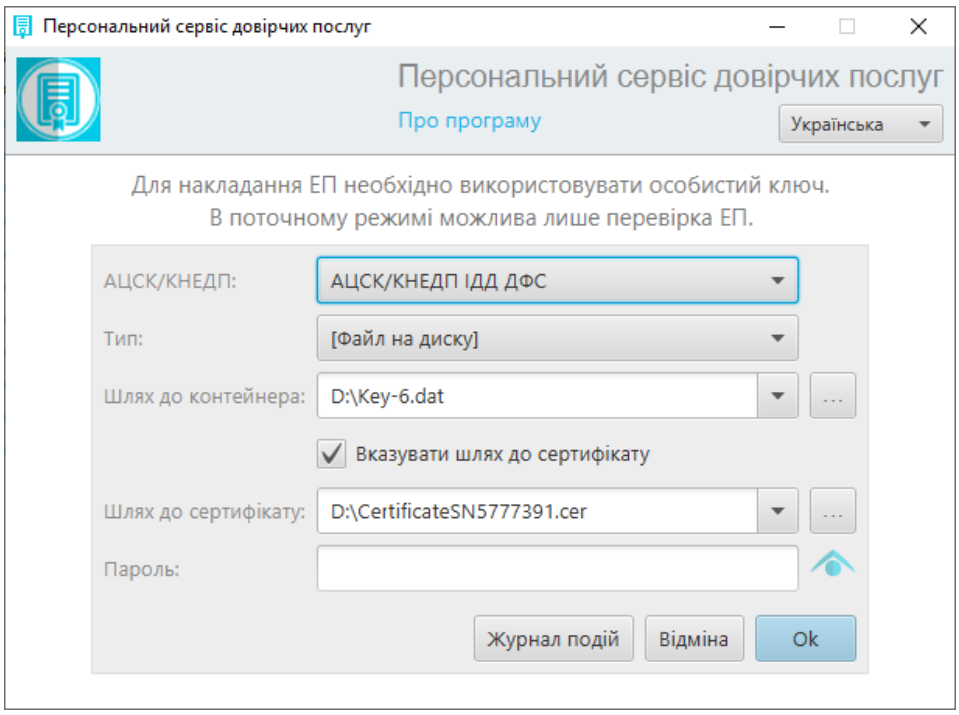

Рис. 41. Поле Шлях до сертифікату

- ***Пароль*** — ввести пароль до файлового ключового контейнеру, Рис. 42.

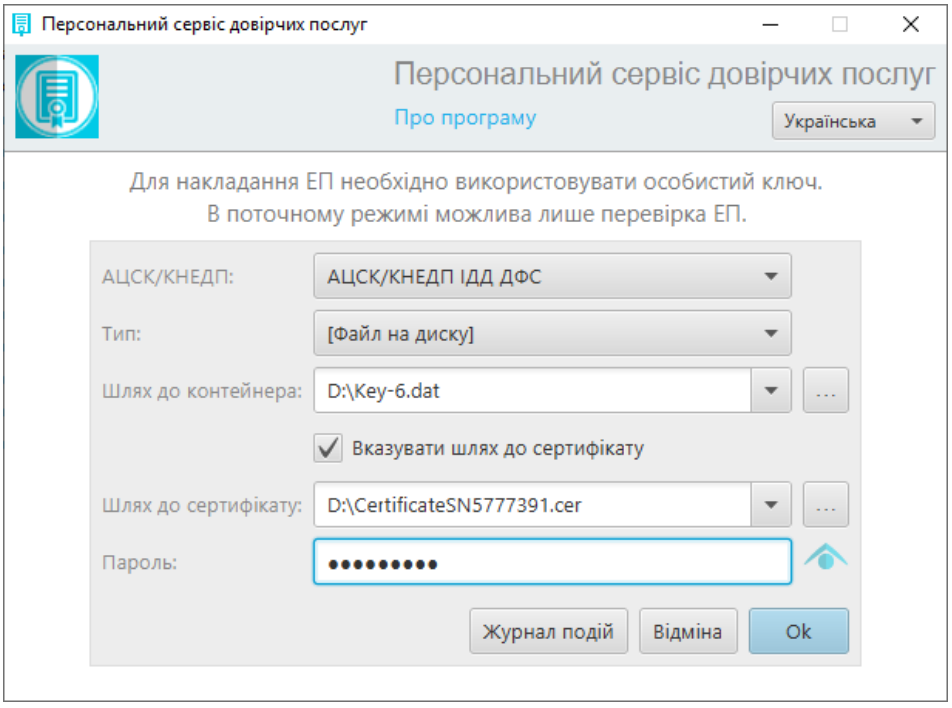

Рис. 42. Поле для введення паролю для файлу

Після введення всіх коректних параметрів, необхідно натиснути кнопку *«ОК»*, щоб підтвердити його використання. У разі необхідності переглянути послідовність дій і подій по завантаженню персонального ключа ЕП - натисніть на кнопку «Журнал подій».

Далі у вікні «Персонального сервісу довірчих послуг» у полі «Стан» з’явиться інформація про завантажений ключ і його власника, Рис. 43.

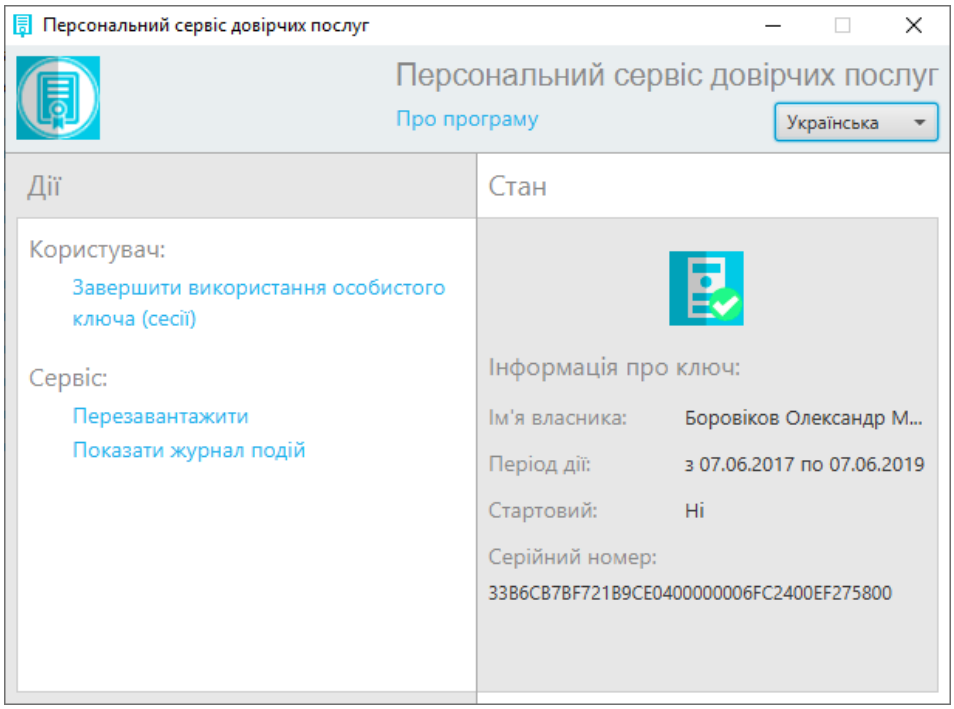

Рис. 43. Стан сервісу – інформація про ключ користувача

Вибір ключа ЕП – захищеного носія

Для накладання ЕП необхідно використовувати особисті ключі . Без ключа ЕП, можна лише перевірити раніше накладений ЕП.

Стартове вікно «Персонального сервісу довірчих послуг» містить форму вибору КНЕДП/АЦСК та особистого ключа ЕП, Рис. 44.

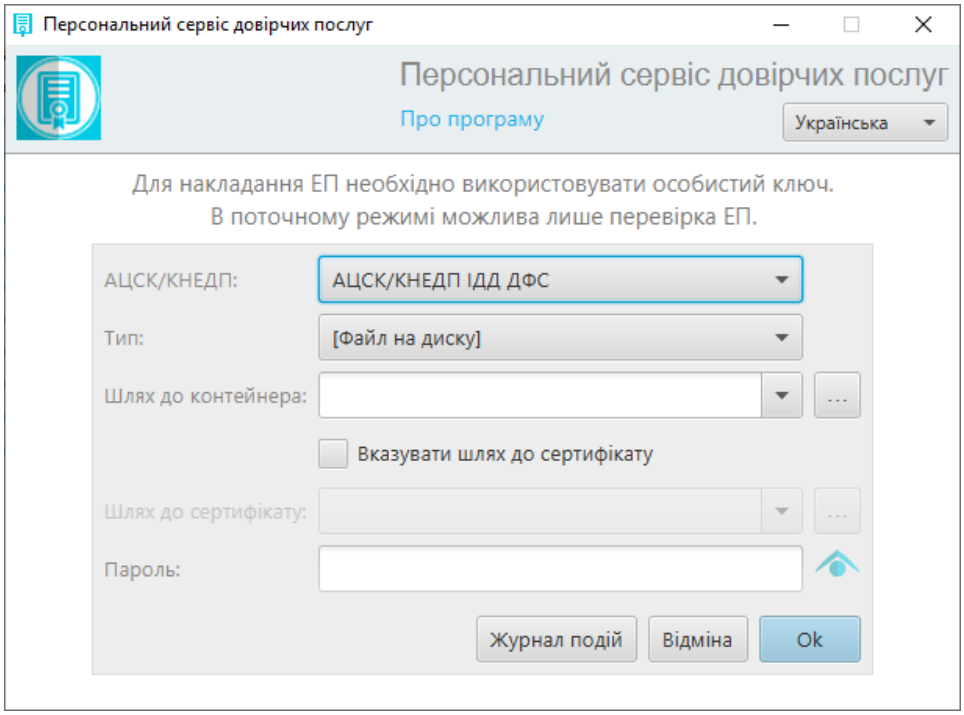

Рис. 44. Стартова форма «Персонального сервісу довірчих послуг»

- ***КНЕДП/АЦСК*** – слід обрати з випадаючого списку центр сертифікації ключів, який видав захищений носій користувачу, Рис. 45.

Перелік КНЕДП/АЦСК, які підтримуються «Персональним сервісом довірчих послуг»:

- КНЕДП/АЦСК ІДД ДФС;
- Тестовий ЦСК ІІТ;
- Тестовий ЦСК Сайфер;
- Тестовий ЦСК Сайфер (проксі);
- КНЕДП/АЦСК ПАТ «Комерційний банк «Приватбанк»;
- КНЕДП/АЦСК ПАТ «Ощадбанк»;
- КНЕДП/АЦСК ТОВ «Центр сертифікації ключів «Україна».

Примітка. Повну інформацію можна переглянути за посиланням:
https://docs.cipher.kiev.ua/pages/viewpage.action?pageId=8618204

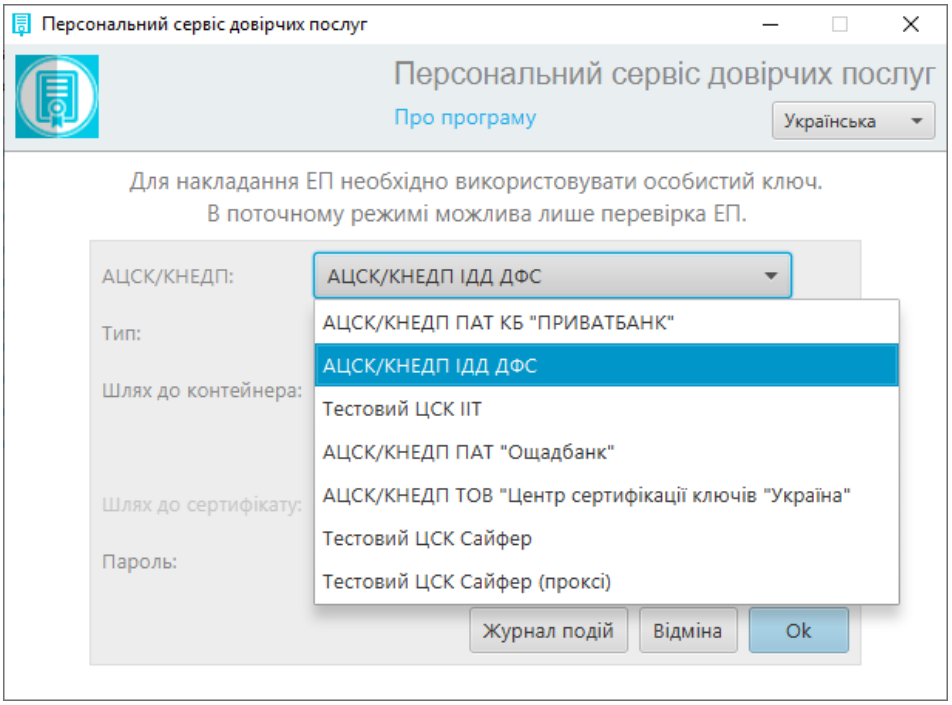

Рис. 45. Вибір Центра сертифікації ключів

- ***Тип*** — обрати із випадаючого переліку тип ключового носія, який використовується для зберігання особистого ключа ЕП, Рис. 46.
  - [PKCS#11 пристрої] – активний режим – для захищеного носія. Захищений апаратний носій у активному режимі. Виконання операцій з ЕП відбувається за інтерфейсом PKCS#11.
  - [PKCS#11 пристрої] – пасивний режим – для захищеного носія. Захищений апаратний носій у пасивному режимі. Виконання операцій з ЕП відбувається за інтерфейсом PKCS#11.

Перелік захищених носіїв:

- Авест AvestKey.
- Ефіт EfitKey, відеоінструкція.
- Autor SecureToken-337, відеоінструкція.
- ІІТ Алмаз, відеоінструкція;
- ІІТ Кристал, відеоінструкція.

Захищені носії, які **не підтримуються** «Персональним сервісом довірчих послуг»:

- Plasticard TEllipse.

Примітка. Повну інформацію про застосування захищений носіїв у «Персональному сервісі довірчих послуг», можна переглянути за посиланням:

https://docs.cipher.kiev.ua/pages/viewpage.action?pageId=8618414

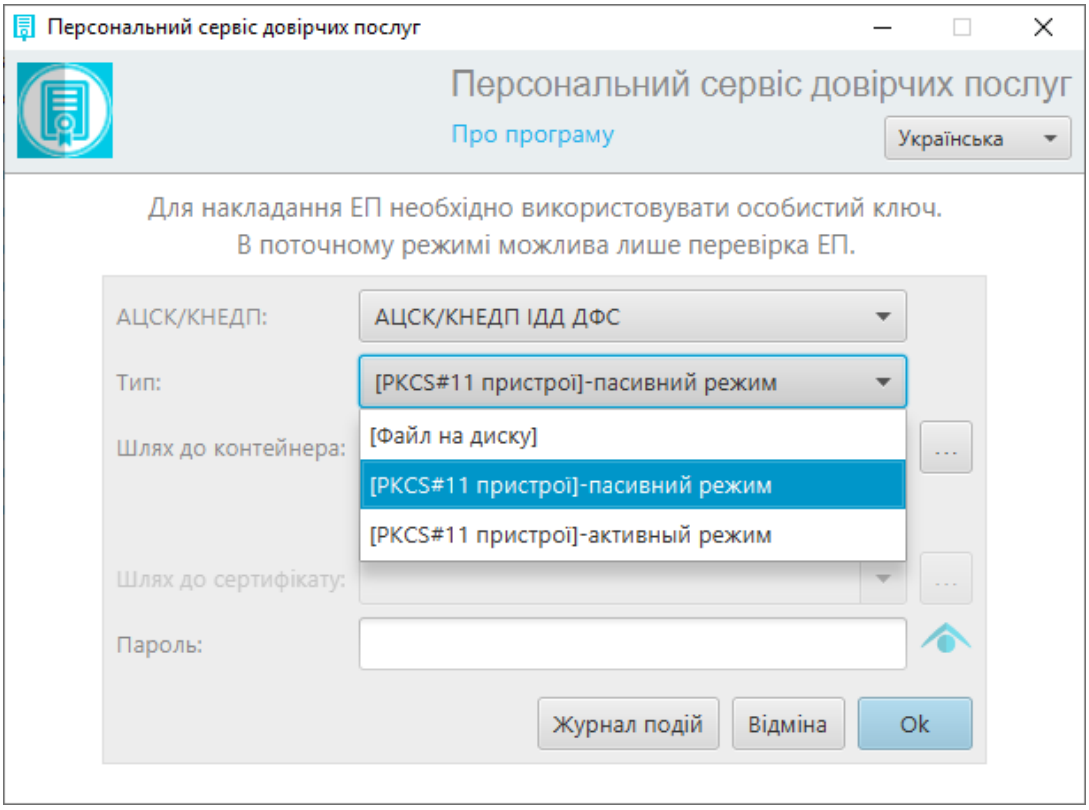

Рис. 46. Обрання типу файлу

- ***Шлях до контейнера*** —натиснути на кнопку ***«...»*** та обрати під'єднаний носій з вікна «Вибір носія», Рис. 47.

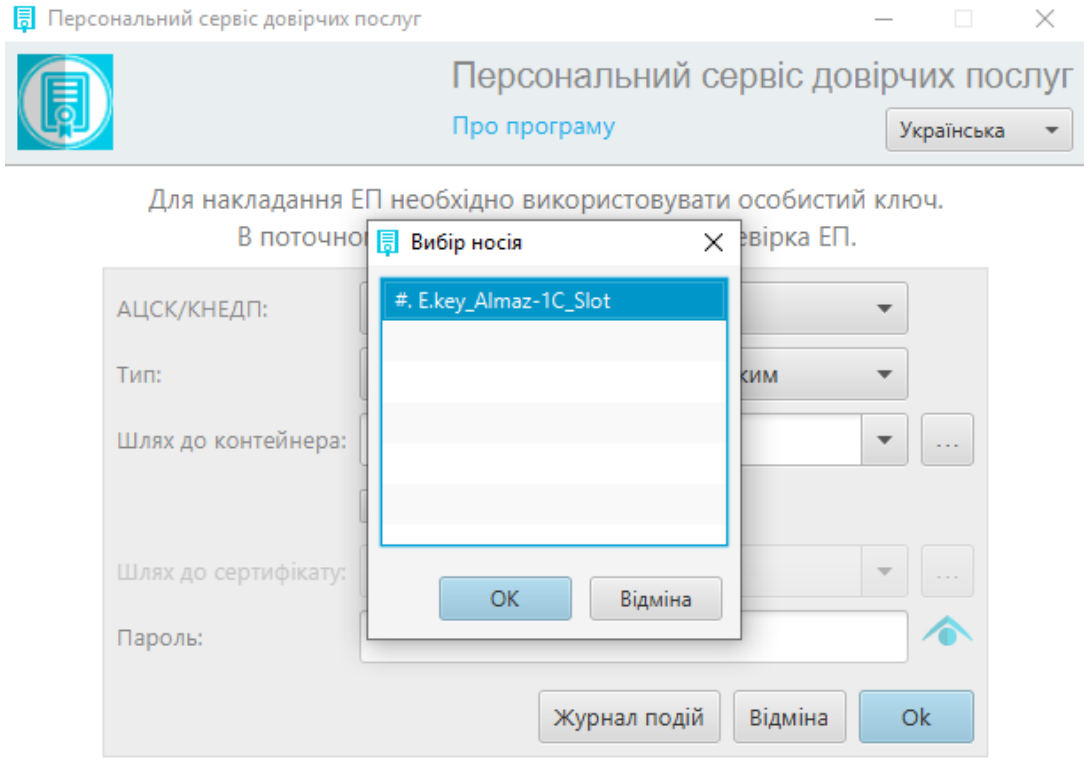

Рис. 47. Поле Шлях до контейнера

- ***Пароль*** – ввести PIN до захищеного носія.

Після введення всіх коректних параметрів необхідно натиснути кнопку *«ОК»*, щоб підтвердити використання. У разі необхідності переглянути послідовність дій і подій по завантаженню персонального ключа ЕП - натисніть на кнопку «Журнал подій».

Далі у вікні «Персонального сервісу довірчих послуг» у полі «Стан» з’явиться інформація про завантажений ключ і його власника, Рис. 48.

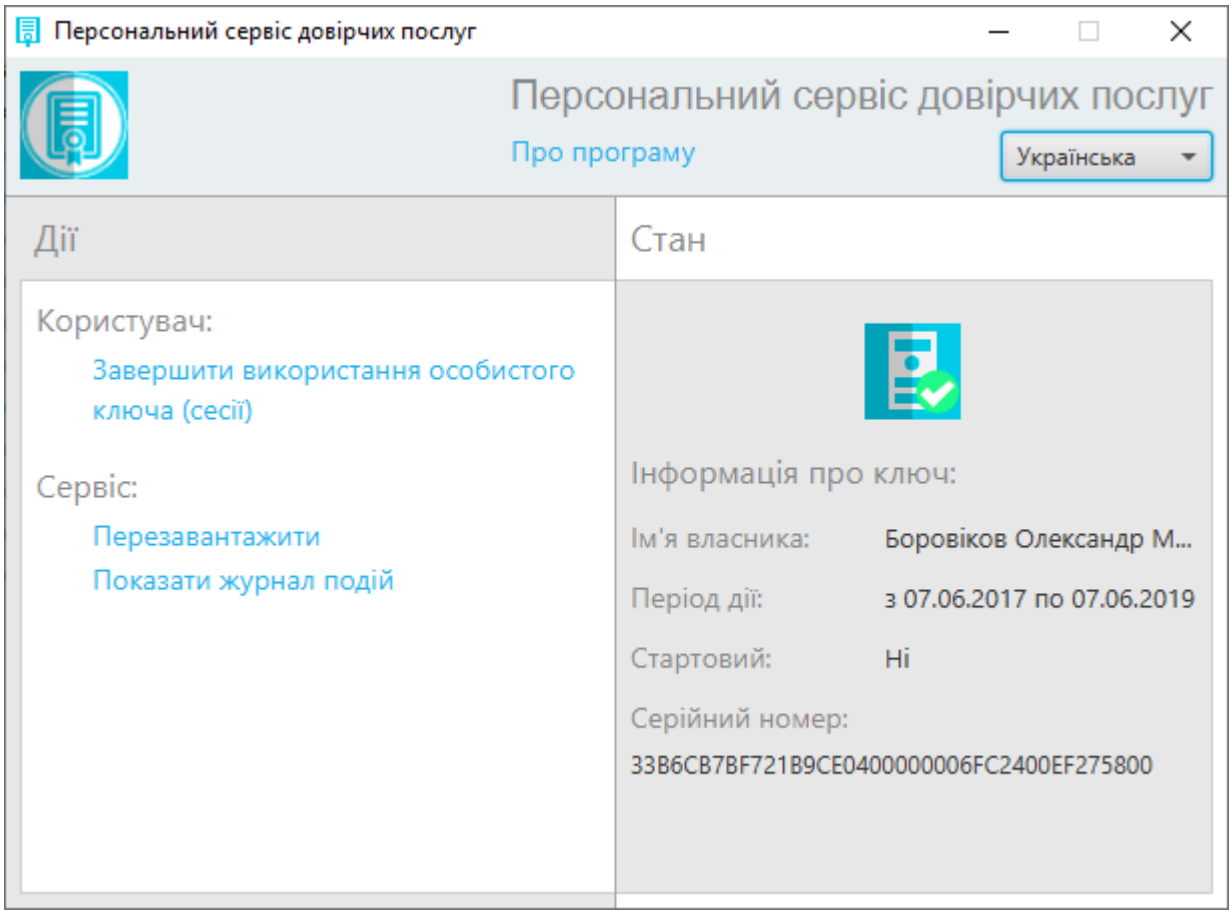

Рис. 48. Стан сервісу – інформація про ключ користувача

Службові функції та опції Персонального сервісу довірчих послуг

Основна форма «Персонального сервісу довірчих послуг» містить такі поля та відповідні опції, Рис. 49:

1. «Основні дані про «Персональний сервіс довірчих послуг»:
   - перегляд інформації про програму;
   - вибір мови інтерфейсу.
2. «Стан» - моніторинг поточного стану сервісу (інформація про ключ).
3. «Дії користувача» - завершити використання особистого ключа.
4. «Дії сервісу»:
   - перезавантаження сервісу;
   - перегляд журналу подій.

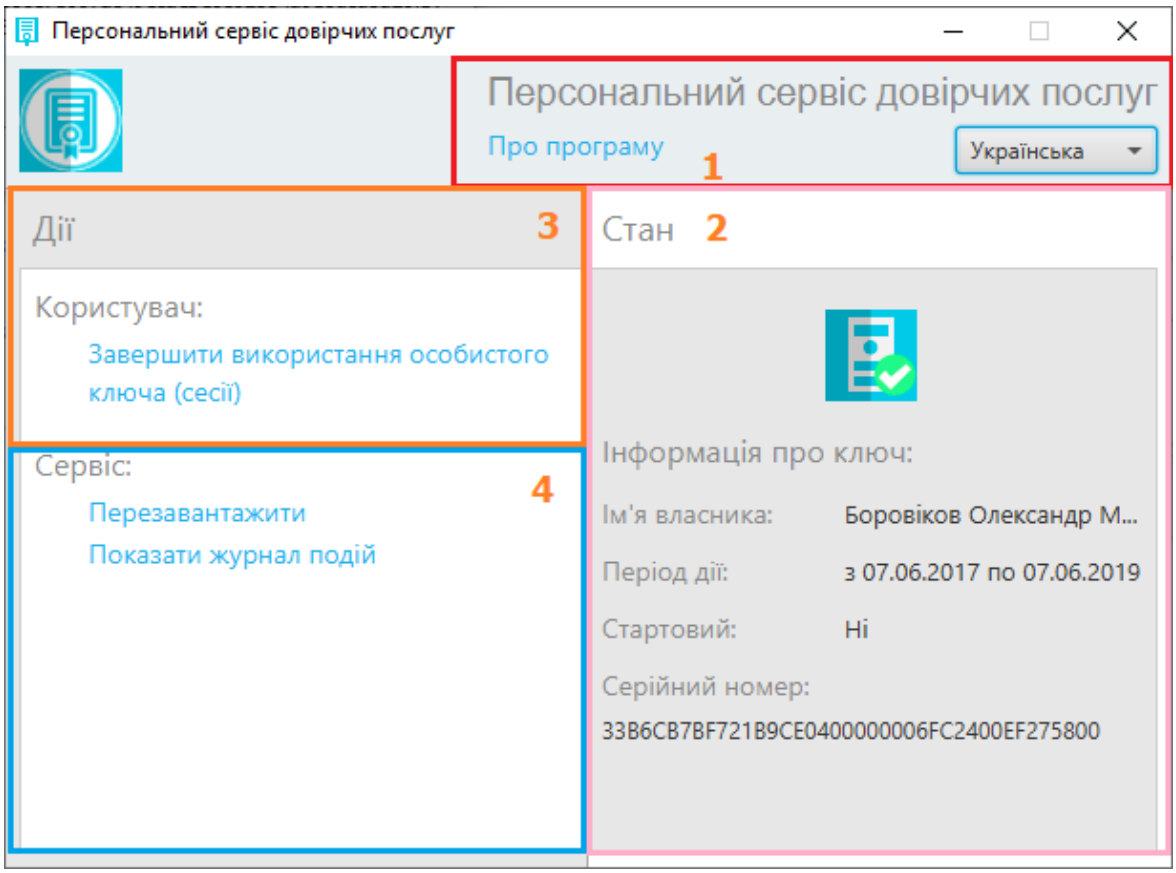

Рис. 49. Форма «Персональний сервіс довірчих послуг»

Функціональні можливості сервісу реалізовані у вигляді кнопок, випадаючих списків та гіперпосилань.

Основні опції:.

- ***Про програму*** - при натисканні на даному посиланні у окремому вікні відкривається інформація про розробника сервісу, версії даного програмного забезпечення та системи криптографічного захисту інформації, до якої він належить, Рис. 50.

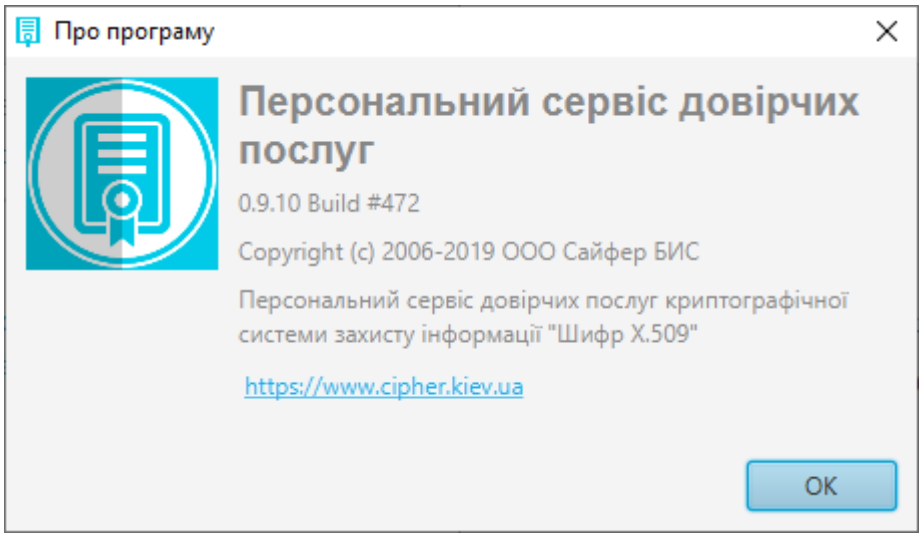

Рис. 50. Інформація про програму

- У полі випадаючого списку можна обрати одну з трьох мов інтерфейсу ЕП: Українську, Російську чи Англійську, Рис. 51.

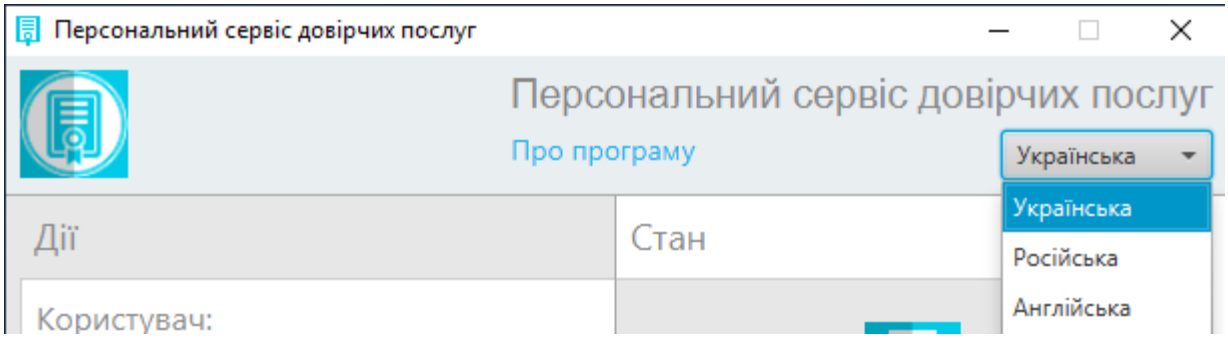

Рис. 51. Вибір мови інтерфейсу

У полі ***Дії*** вікна «Персонального сервісу довірчих послуг» у розділі ***Сервіс*** розташовані функції:

- ***Перезавантажити сервіс*** – перезавантаження сервісу ЕП без необхідності перезавантажувати програму в цілому;
- ***Показати журнал подій*** – текстовий журнал (лог) подій, що відбулися у «Персональному сервісі довірчих послуг» з моменту його запуску. Журнал подій можна передивитися та за потреби очистити, Рис. 52.

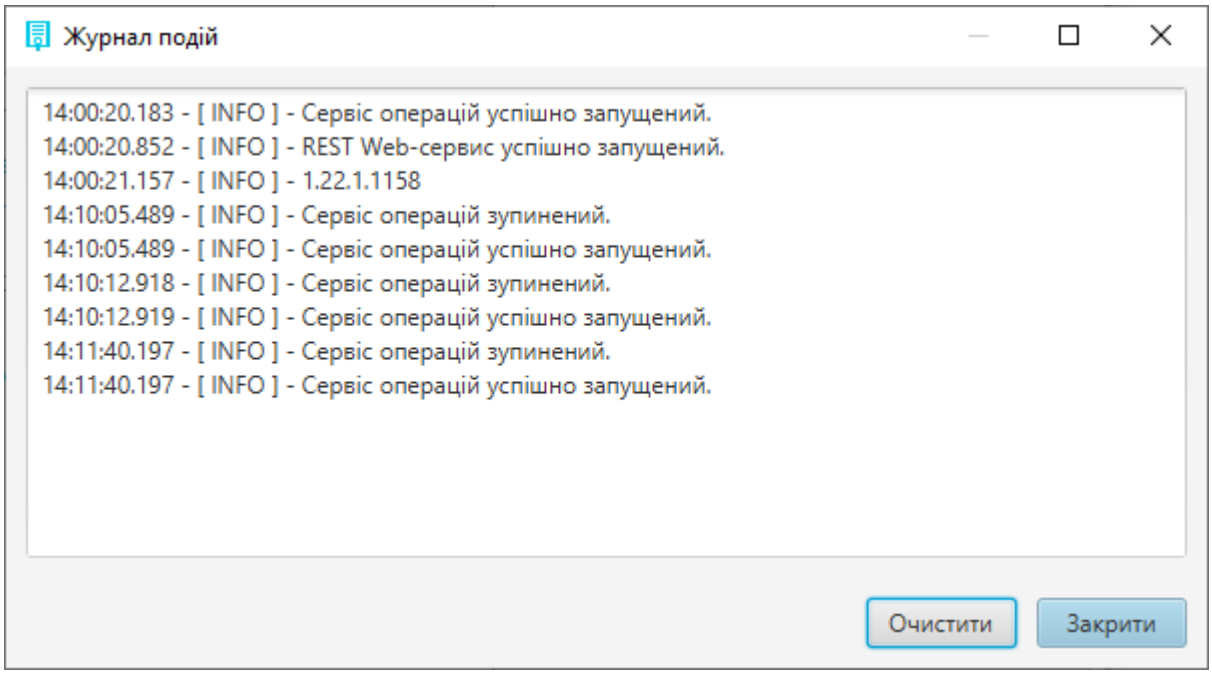

Рис. 52. Журнал подій сервісу

Створення ЕП

Вкладка «Створити ЕП» містить розділи: Параметри створення ЕП, Файл та Текстові дані, Рис. 53.

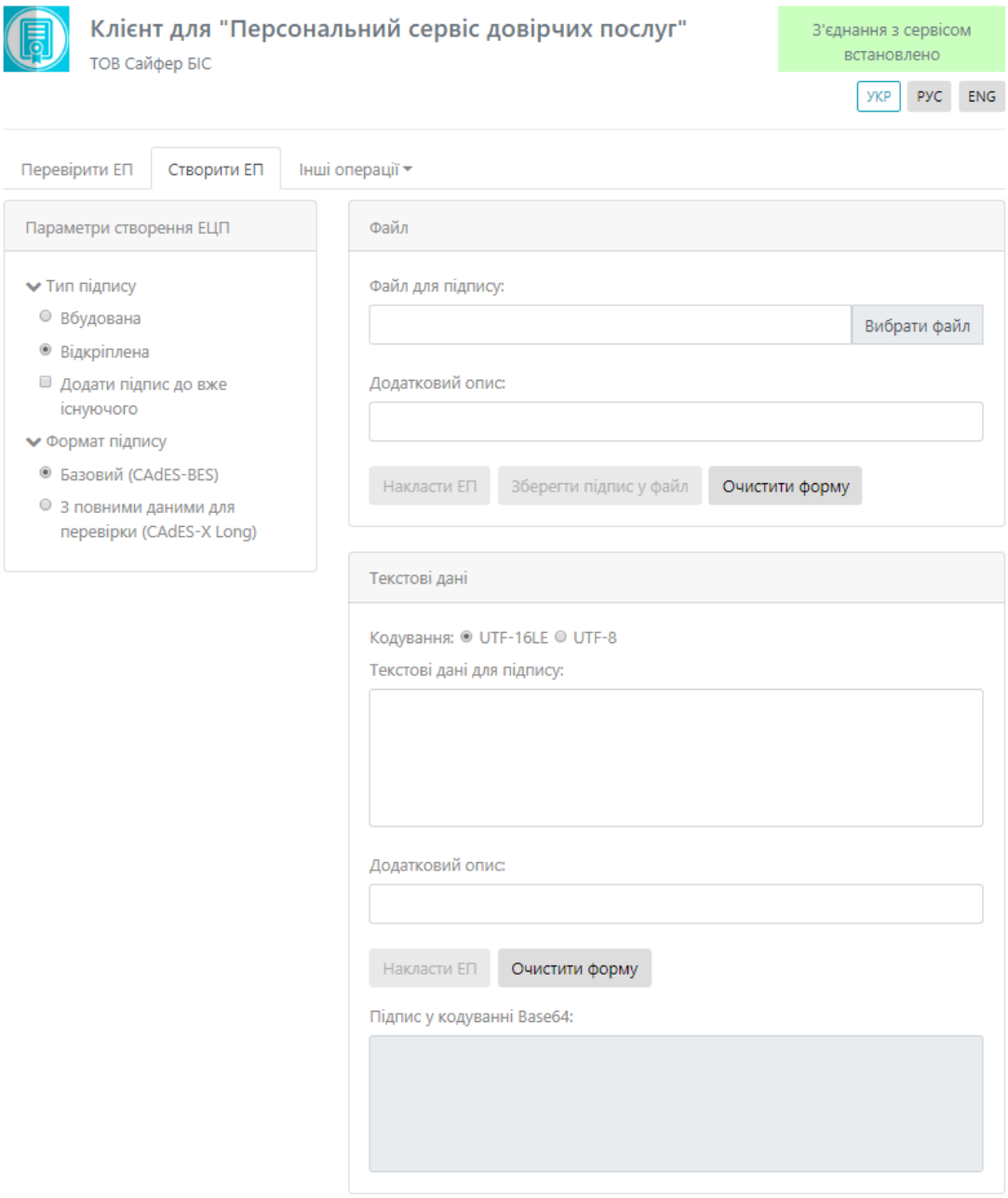

Рис. 53. Вкладка «Створити ЕП»

Розділ «Параметри створення ЕП», який у свою чергу включає:

1. Поле «Тип ЕП», яке містить:
   - Вбудована (переглянути відеоінструкцію можливо за посиланням);
   - Відкріплена (переглянути відеоінструкцію можливо за посиланням);
   - Додати підпис до вже існуючого (накладається підпис на файл, на який вже попередньо накладено ЕП).
2. Поле «Формат ЕП», яке містить:

- Базовий (CAdES-BES) (використовується для автентифікації підписанта та перевірки цілісності електронного документа в період чинності сертифіката відкритого ключа (сертифікат). Формат «Базовий» не надає можливості встановити дійсність підпису у випадку, якщо ЕП перевіряється після закінчення строку чинності сертифіката або скасування сертифіката після формування ЕП).
- З повними даними для перевірки (CAdES-X Long) (можливість встановлення дійсності ЕП у довгостроковому періоді (після закінчення строку чинності сертифікату)).

Розділ «Файл», який у свою чергу включає:

- Файл для підпису (натискаємо кнопку «Вибрати файл» та обираємо необхідний файл для підпису);
- Додатковий опис (назва файлу з яким буде зберігатися файл з підписом, заповнюється автоматично, але можна змінити назву);
- Кнопка «Створити ЕП» (здійснює накладання ЕП на файл, який завантажено);
- Кнопка «Зберегти підпис у файл» (здійснює збереження файлу, на який накладено підпис);
- Кнопка «Очистити форму» (здійснює очищення всієї форми).

Розділ «Текстові дані», який у свою чергу включає:

- Кодування (обираємо стандарт кодування тексту): UTF-16LE чи UTF-8;
- Поле «Текстові дані для підпису» (введення тексту, на який необхідно створити ЕП);
- Поле «Додатковий опис» (для введення необхідного додаткового опису для текстових даних);
- Кнопка «Створити ЕП» (здійснює накладання ЕП на текстові дані);
- Кнопка «Очистити форму» (здійснює очищення всієї форми);
- Поле «Підпис в кодуванні Base64» (зашифровані дані).

Процес Створення ЕП починається з того, що обираються «Параметри для створення ЕП», обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 54. За необхідності можна змінити файл.

Принцип створення ЕП за типом «Відкріплена» та «Вбудована» є аналогічними.

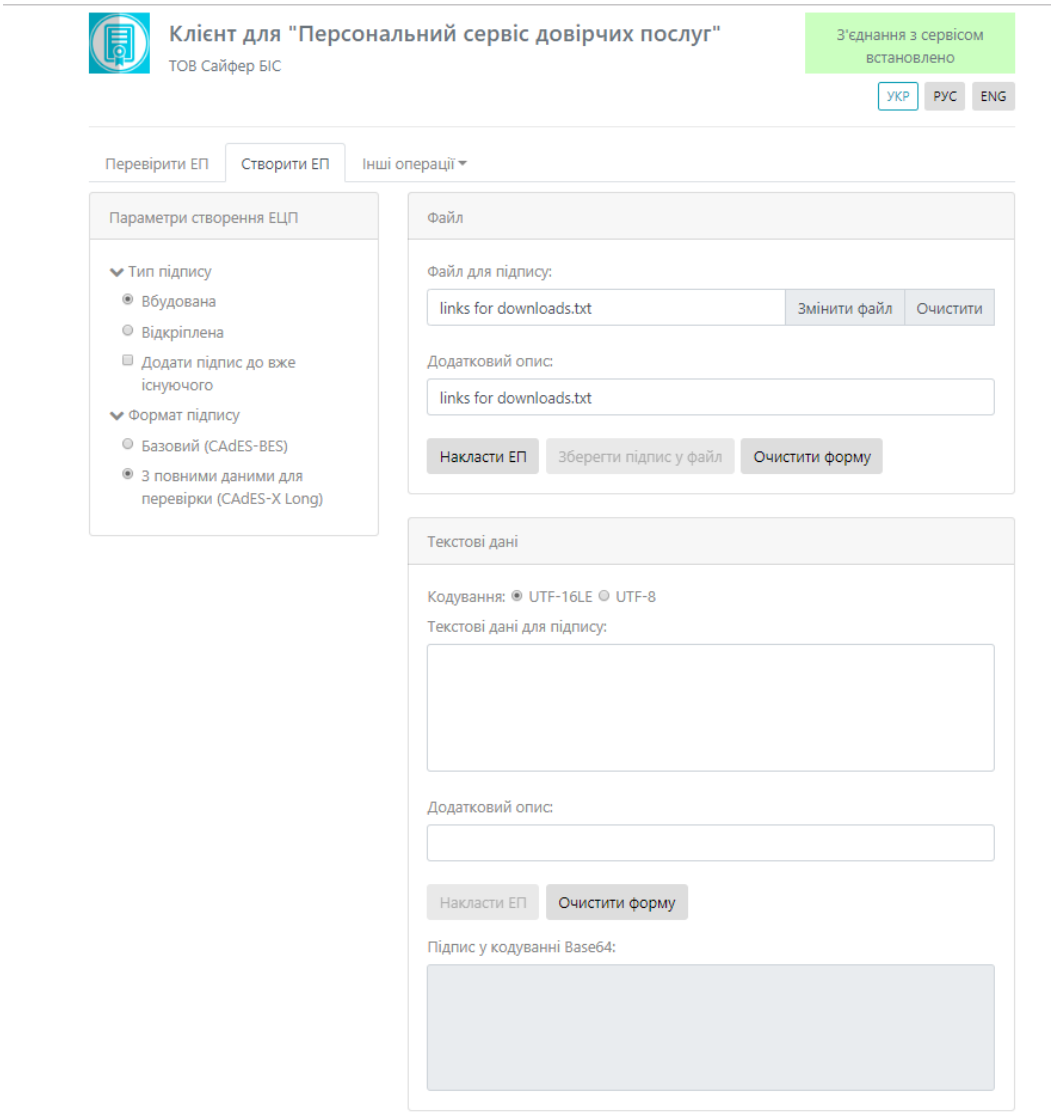

Рис. 54. Створення ЕП

Після натискання з’являється вікно про дозвіл на використання ЕП у кількості 1 раз, Рис. 55.

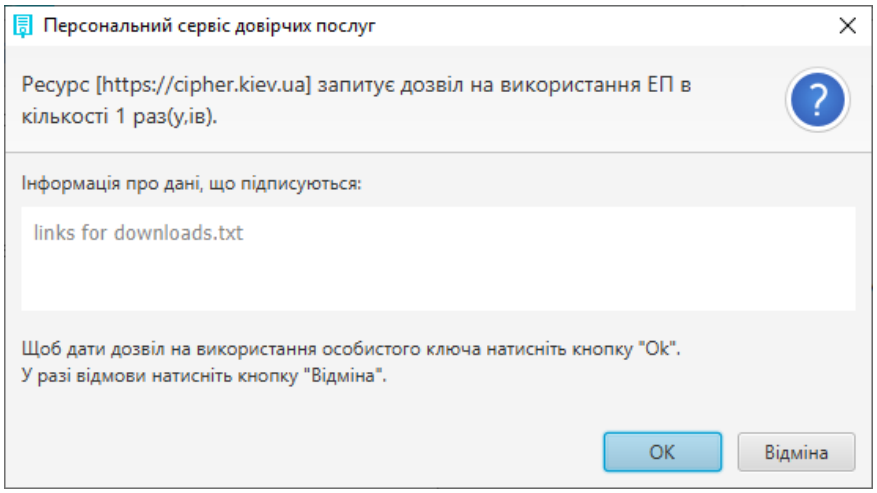

Рис. 55. Підтвердження використання ЕП

З’являється повідомлення про успішне створення електронного підпису, Рис. 56.

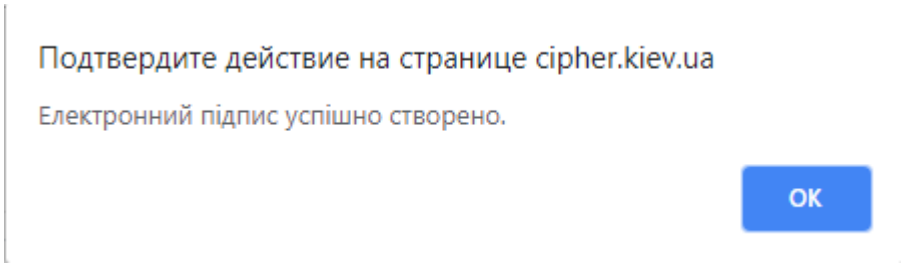

Рис. 56. Повідомлення про створення електронного підпису

Необхідно зберегти електронний підпис у файл, завдяки кнопки «Зберегти підпис у файл», Рис. 57. За необхідності можна змінити файл.

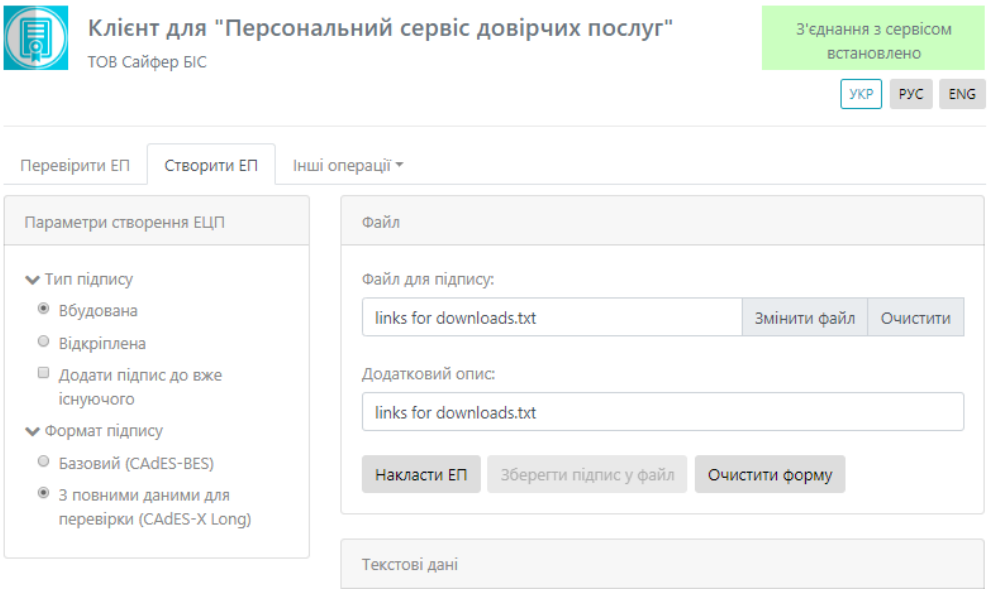

Рис. 57. Збереження підпису у файл

Після натискання кнопки, з’являється вікно з пропозицією зберегти файл, Рис. 58. Далі обираємо шлях збереження файлу та очищаємо форму.

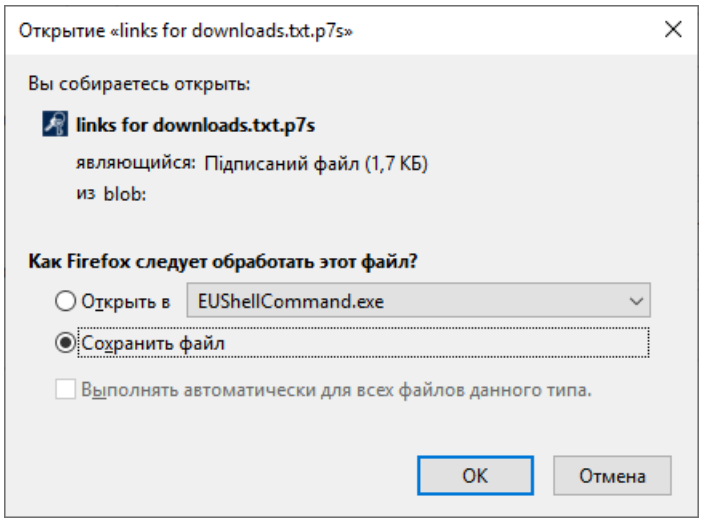

Рис. 58. Вікно з пропозицією збереження файлу

Перевірка ЕП

Вкладка «Перевірити ЕП» містить розділи: Параметри перевірки ЕП, Файл та Текстові дані, Рис. 59.

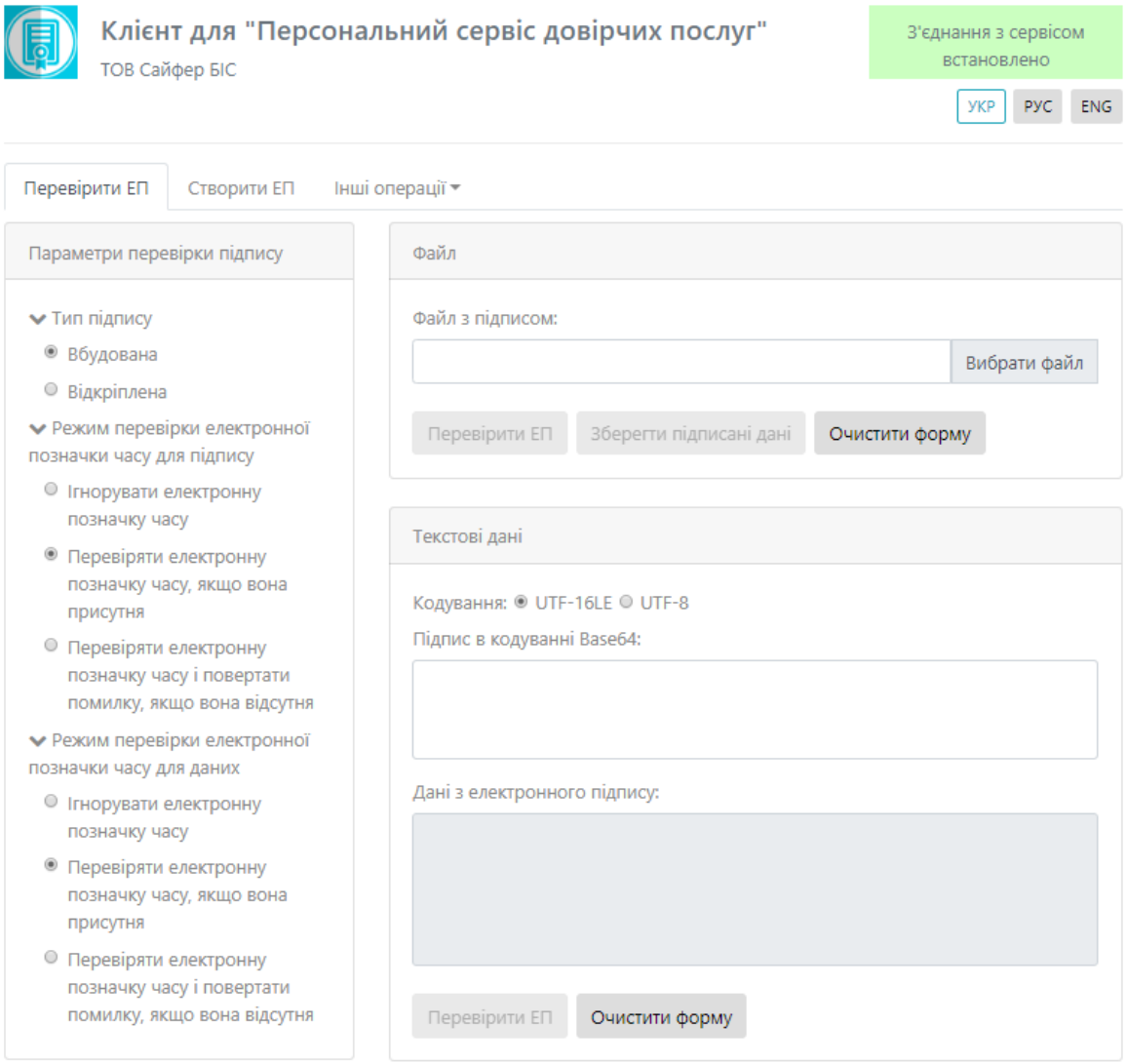

Рис. 59. Вкладка «Перевірити ЕП»

Розділ «Параметри перевірки ЕП», який у свою чергу включає:

1. Поле «Тип ЕП», яке містить:

- Вбудована (переглянути відеоінструкцію можливо за посиланням);
- Відкріплена (переглянути відеоінструкцію можливо за посиланням);

2. Режим перевірки позначки часу для ЕП, який вказується за необхідності ігнорувати, перевіряти її наявність, чи повертати помилку за її відсутності.
3. Режим перевірки позначки часу для даних, який вказується за необхідності ігнорувати, перевіряти її наявність, чи повертати помилку за її відсутності.

Розділ «Файл», який у свою чергу включає:

Якщо перевіряється файл за типом ЕП – **Вбудована**.

1. Поле «Файл з підписом» (обирається файл, який містить підпис з типом ЕП Вбудована).
2. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
3. Кнопка «Зберегти підписані дані» (здійснює збереження файлу, який не містить підпис);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми).

Якщо перевіряється файл за типом ЕП – **Відкріплена**.

1. Поле «Файл для перевірки» (обирається файл, який не містить підпис – початковий файл);
2. Поле «Файл з підписом» (обирається файл, який містить підпис з типом ЕП Відкріплена);
3. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису за допомогою завантаженого файлу з підписом для файлу для перевірки);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми).

Розділ «Текстові дані», який у свою чергу включає:

Якщо перевіряється файл з типом ЕП – **Вбудована**.

- Кодування (обираємо стандарт кодування тексту): UTF-16LE чи UTF-8;
- Поле «Підпис в кодуванні Base64» (вносимо зашифровані дані);
- Поле «Дані з електронного підпису» (відображаються розшифровані дані);
- Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
- Кнопка «Очистити форму» (здійснює очищення всієї форми).

Якщо перевіряється файл з типом ЕП – **Відкріплена**.

- Кодування (обираємо стандарт кодування тексту): UTF-16LE чи UTF-8;
- Поле «Текстові дані для перевірки» (вносимо вихідні дані);
- Поле «Підпис в кодуванні Base64» (вносимо зашифровані дані);
- Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
- Кнопка «Очистити форму» (здійснює очищення всієї форми).

Процес Перевірки ЕП починається з того, що обираються «Параметри для створення ЕП», обирається файл/текст для підпису, натискаємо кнопку «Перевірити ЕП». За необхідності можна змінити файл.

Якщо перевіряється файл з типом ЕП – **Вбудована**.

Вносимо «Параметри перевірки ЕП», вказуємо файл з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 60.

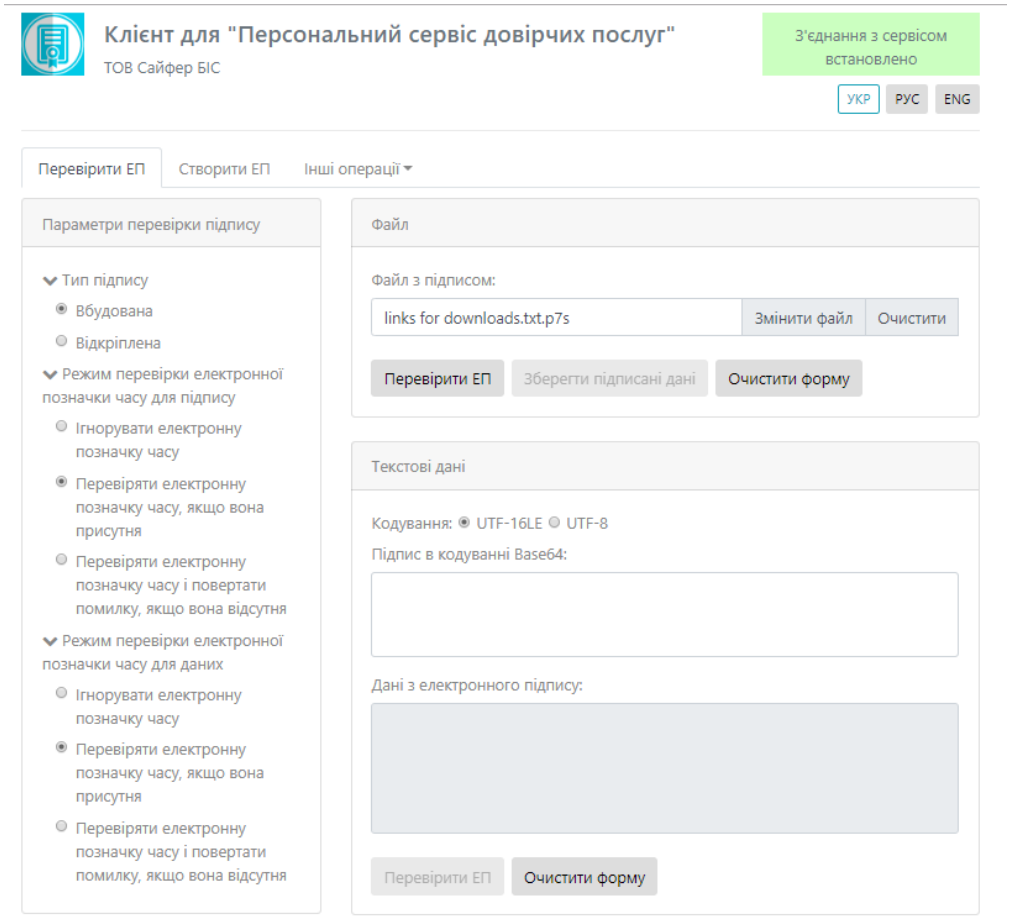

Рис. 60. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення про дійсність електронного підпису, Рис. 61.

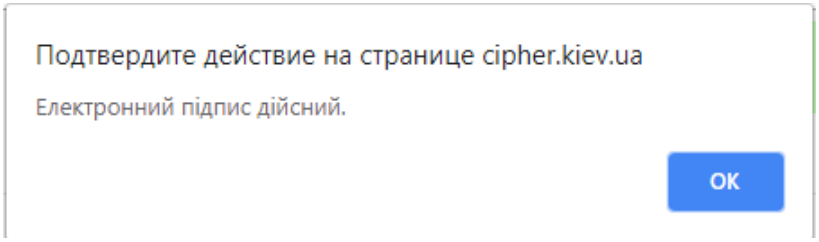

Рис. 61. Повідомлення про дійсність електронного підпису

Після натискання «ок», з'являється повідомлення про успішне отримання даних з вбудованого електронного підпису, Рис. 62.

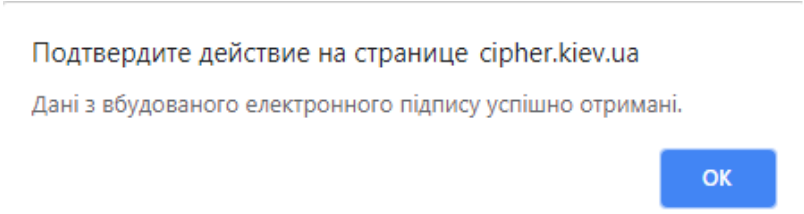

Рис. 62. Повідомлення про успішне отримання даних з вбудованого електронного підпису

Після натискання «ок», з’являється інформація про дійсність підпису, вказується інформація про підписанта та інформація про позначки часу та даних, які були вказані при накладанні ЕП, Рис. 63. Після чого, натискаємо кнопку «Очистити форму».

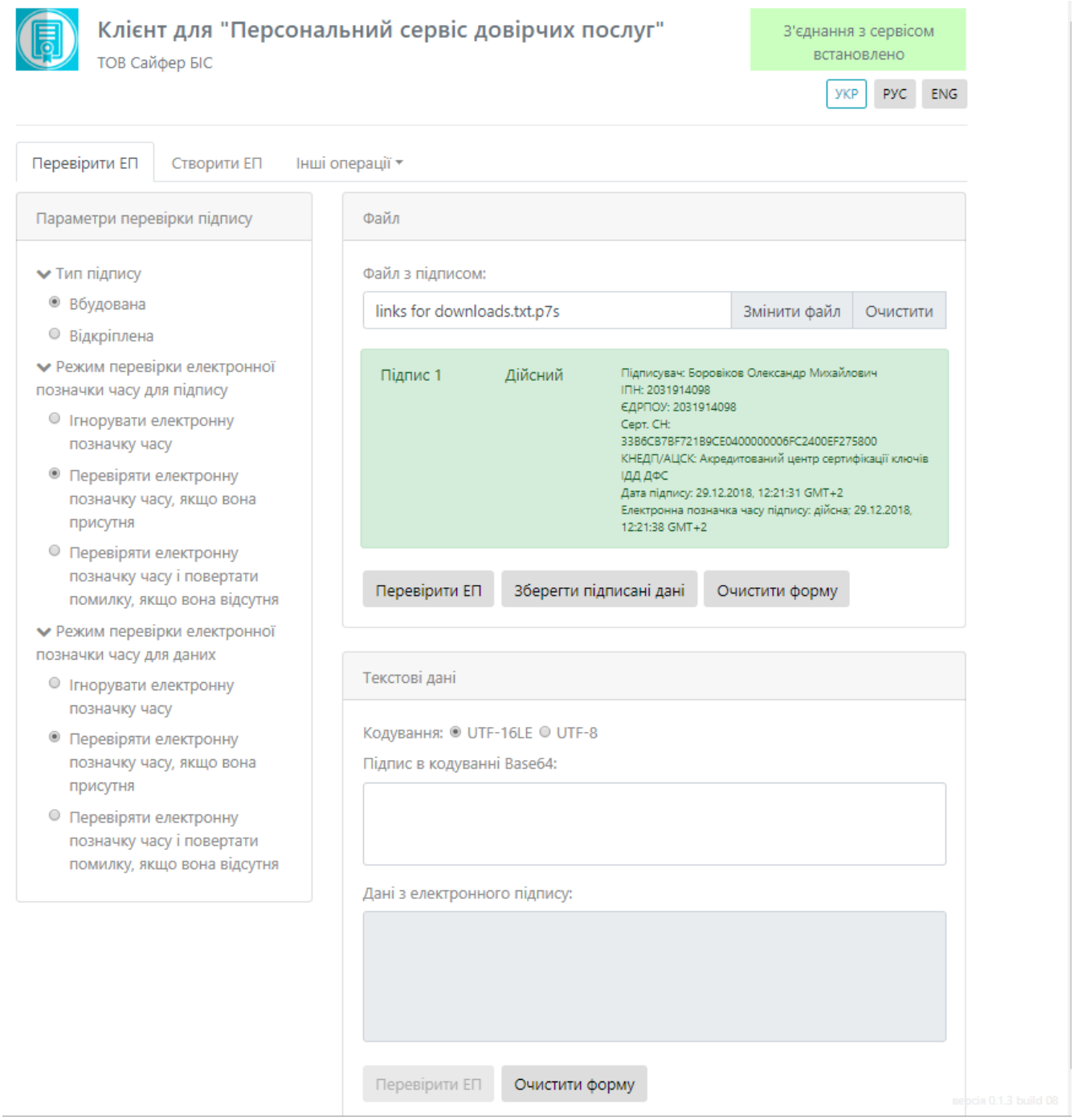

Рис. 63. Результат перевірки

Якщо перевіряється файл з типом ЕП – **Відкріплена**.

Вносимо «Параметри перевірки ЕП», вказуємо файл з вихідними даними та файл з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 64. За необхідності, є можливість змінити файл.

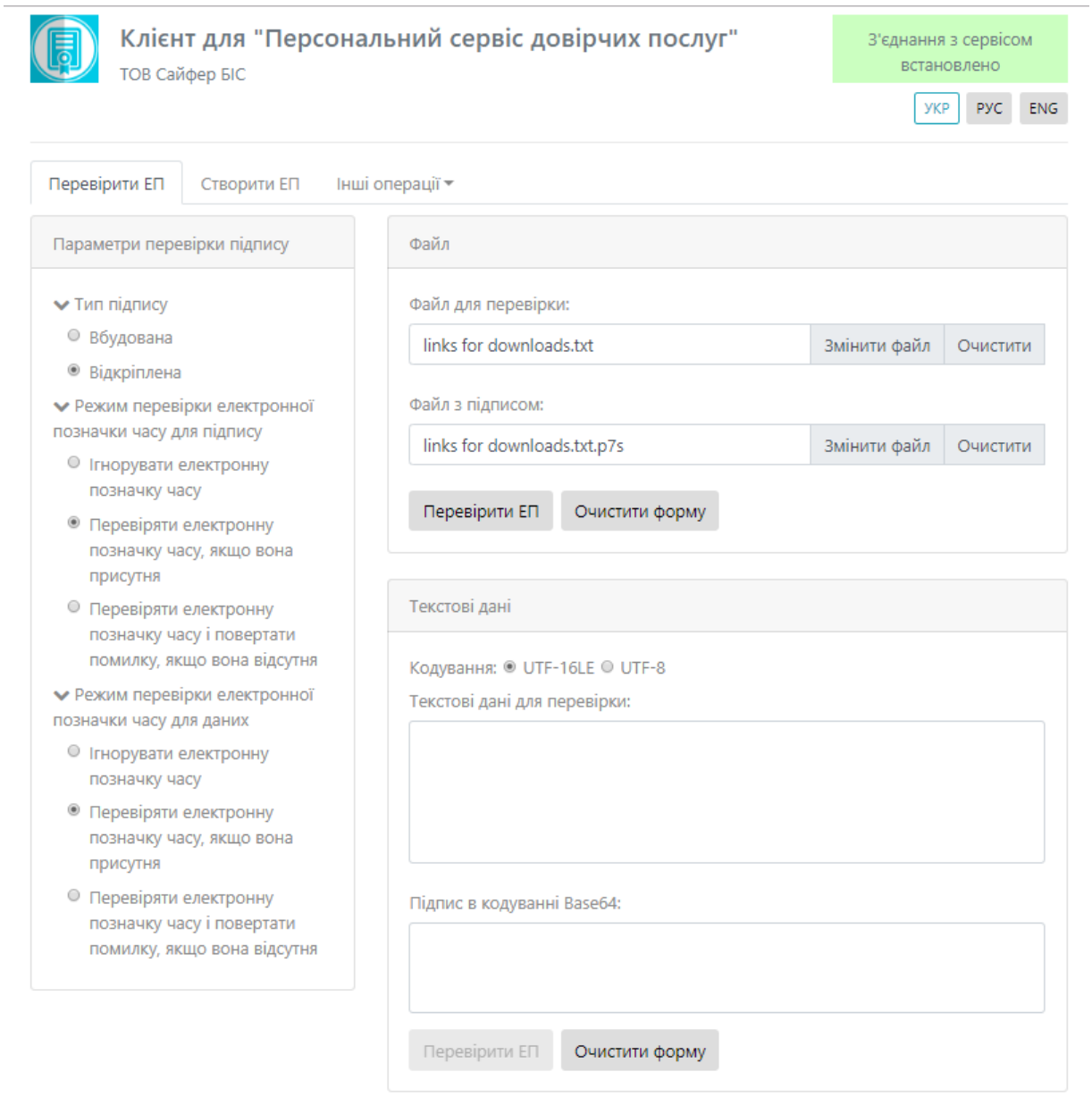

Рис. 64. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення про дійсність електронного підпису, Рис. 65.

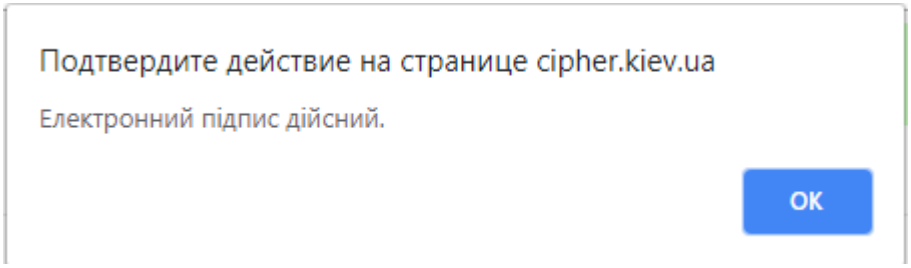

Рис. 65. Повідомлення про дійсність електронного підпису

Після натискання «ок», з’являється інформація про дійсність підпису, вказується інформація про підписанта та інформація про позначки часу та даних, які були вказані при накладанні ЕП, Рис. 66. Після чого, натискаємо кнопку «Очистити форму».

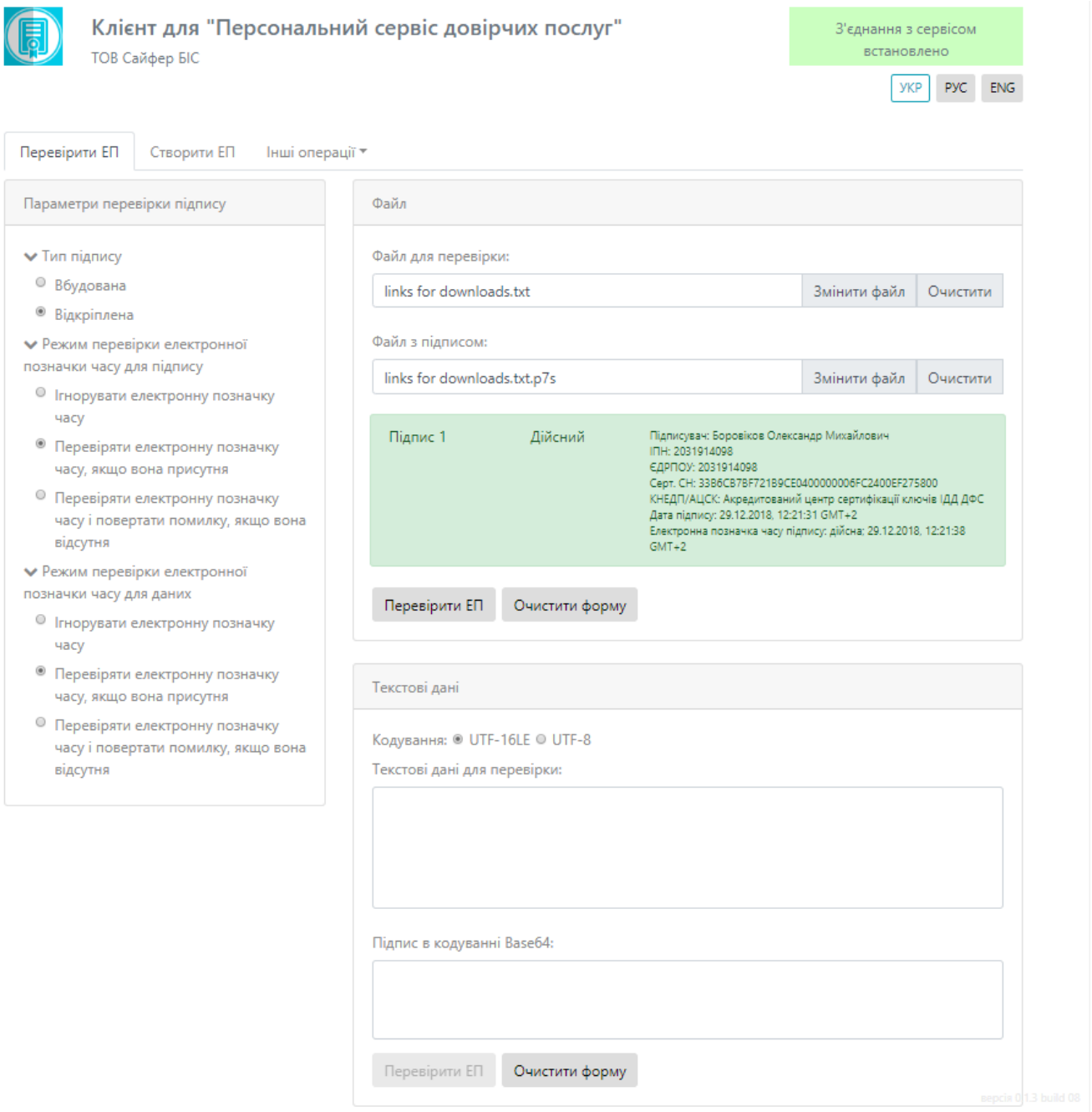

Рис. 66. Результат перевірки

Інші операції

Інші операції включають в себе: дані про сертифікат ключа підпису, дані про сертифікат ключа шифрування та вказати електронну позначку часу.

Дані про сертифікат ключа підпису

Містить у собі серійний номер сертифікату, початок та дату закінчення, чи посилений сертифікат. Також міститься інформація про власника, видавця та про відкритий ключ у окремих полях, Рис. 67.

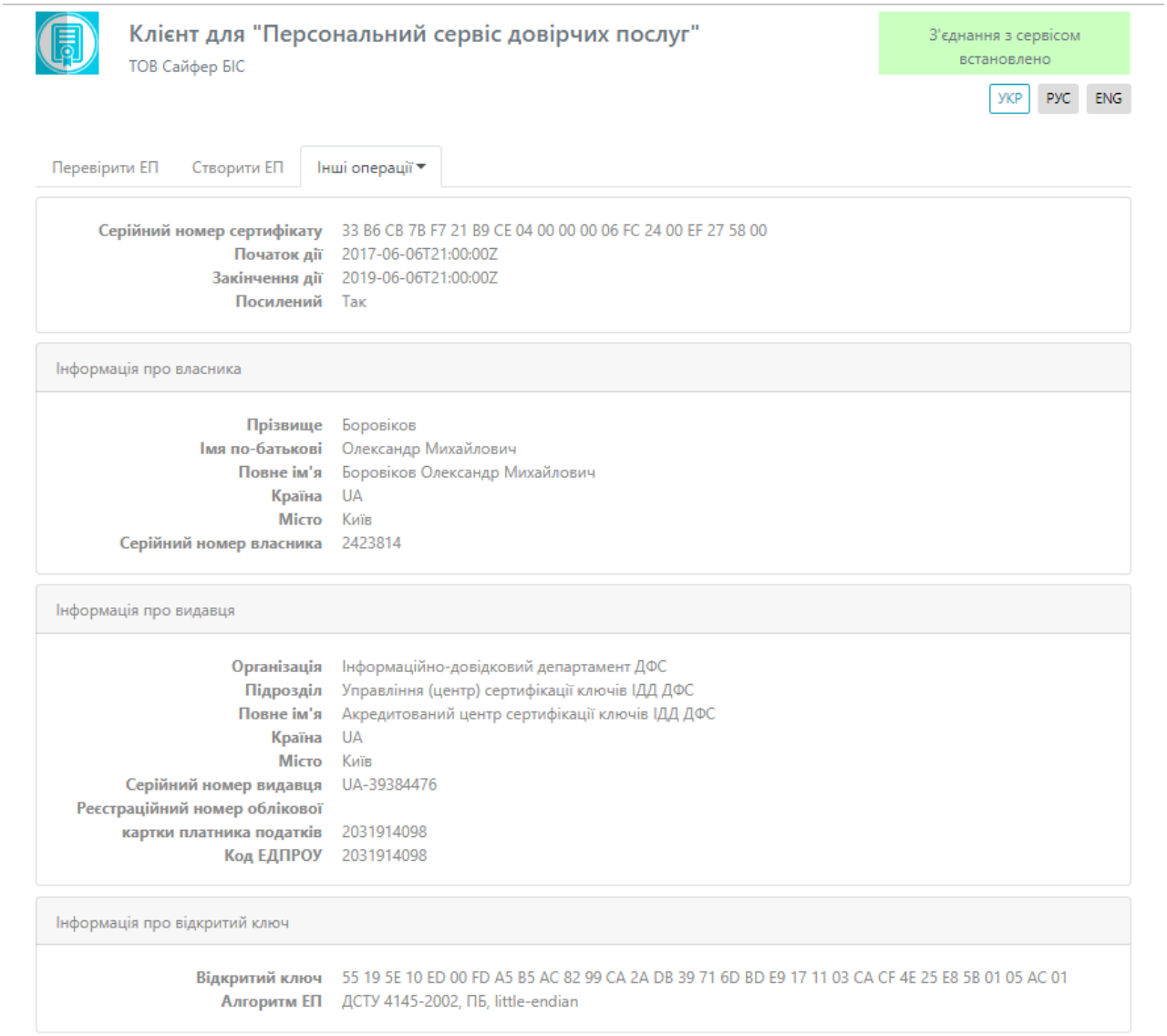

Рис. 67. Дані про сертифікат ключа підпису

Сертифікат ключа шифрування

Містить у собі серійний номер сертифікату, початок та дату закінчення, чи посилений сертифікат. Також міститься інформація про власника, видавця та про відкритий ключ у

окремих полях, Рис. 68. Присутня кнопка «Зберегти сертифікат у файл», який зберігається з розширенням crt.

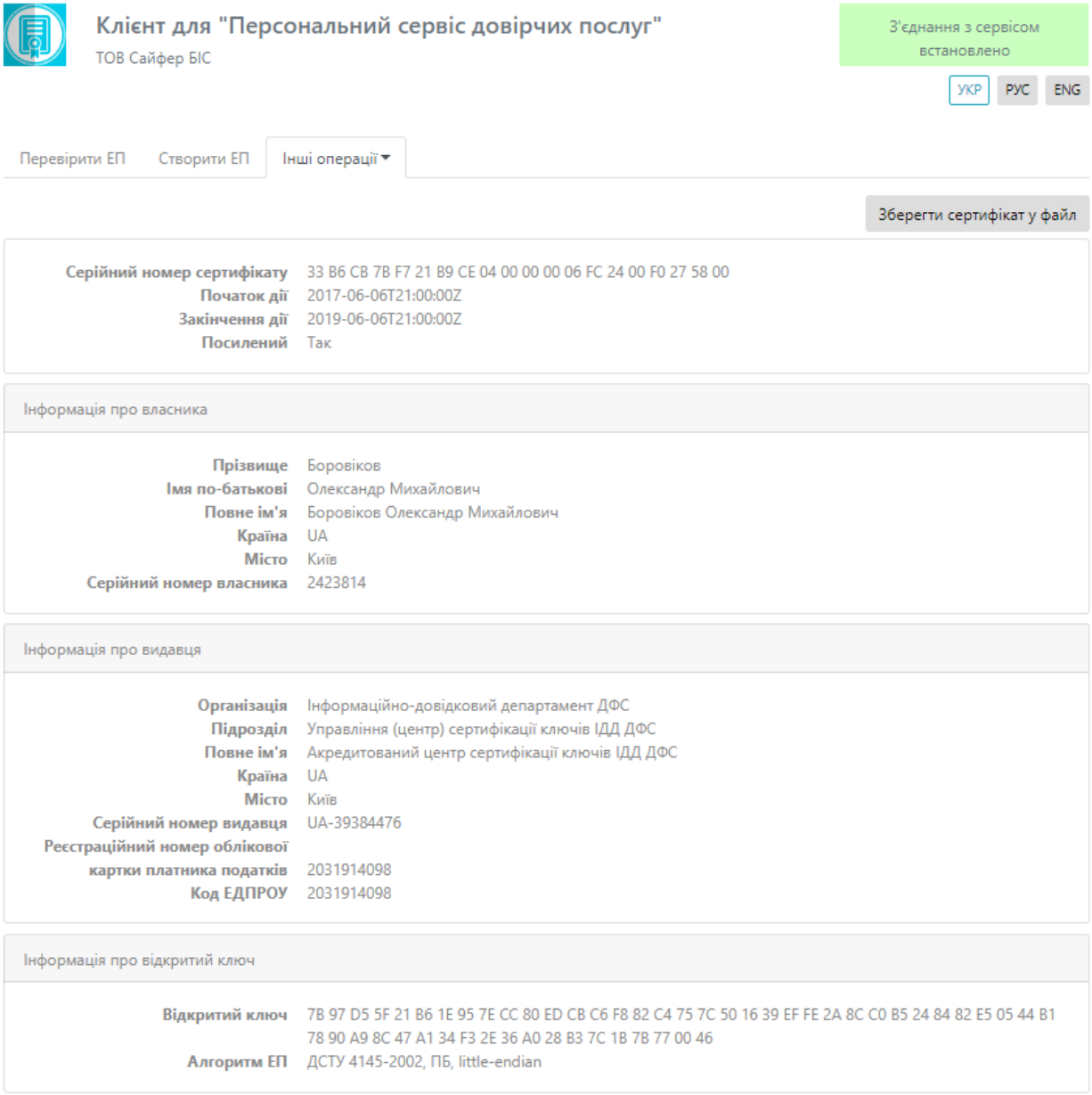

Рис. 68. Сертифікат ключа шифрування

Зашифрувати

Дана вкладка містить такі поля: Параметри при зашифруванні, Сертифікат отримувача, Файл та Текстові дані, Рис. 69.

Відеоінструкцію для зашифрування даних можна переглянути за посиланням Персональний сервіс довірчих послуг. Зашифрувати та розшифрувати файл.

Розділ «Параметри зашифрування», який включає:

1. Додати при зашифруванні:

- Сертифікат відправника та сертифікати видавців;
- Сертифікати відправника;
- Не додавати сертифікат відправника та сертифікати видавців.

Розділ «Сертифікат отримувача», який включає:

1. Поле «Сертифікат отримувача зашифрованих даних» (завантажуємо файл-сертифікат).

Розділ «Файл», який включає:

1. Поле «Файл для зашифрування»;
2. Кнопка «Зашифрувати» (здійснює зашифрування файлу);
3. Кнопка «Зберегти зашифровані дані у файл» (зберігає зашифровані дані у файл);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми).

Розділ «Текстові дані», який включає:

1. Кодування (обираємо стандарт кодування тексту): UTF-16LE чи UTF-8;
2. Поле «Текст для зашифрування» (вносимо дані для зашифрування);
3. Кнопка «зашифрувати» (здійснює зашифрування текстових даних);
4. Кнопка «Очистити форму» (здійснює очищення всіє форми);
5. Поле «Зашифровані дані в кодуванні Base64» (отримуємо зашифровані дані).

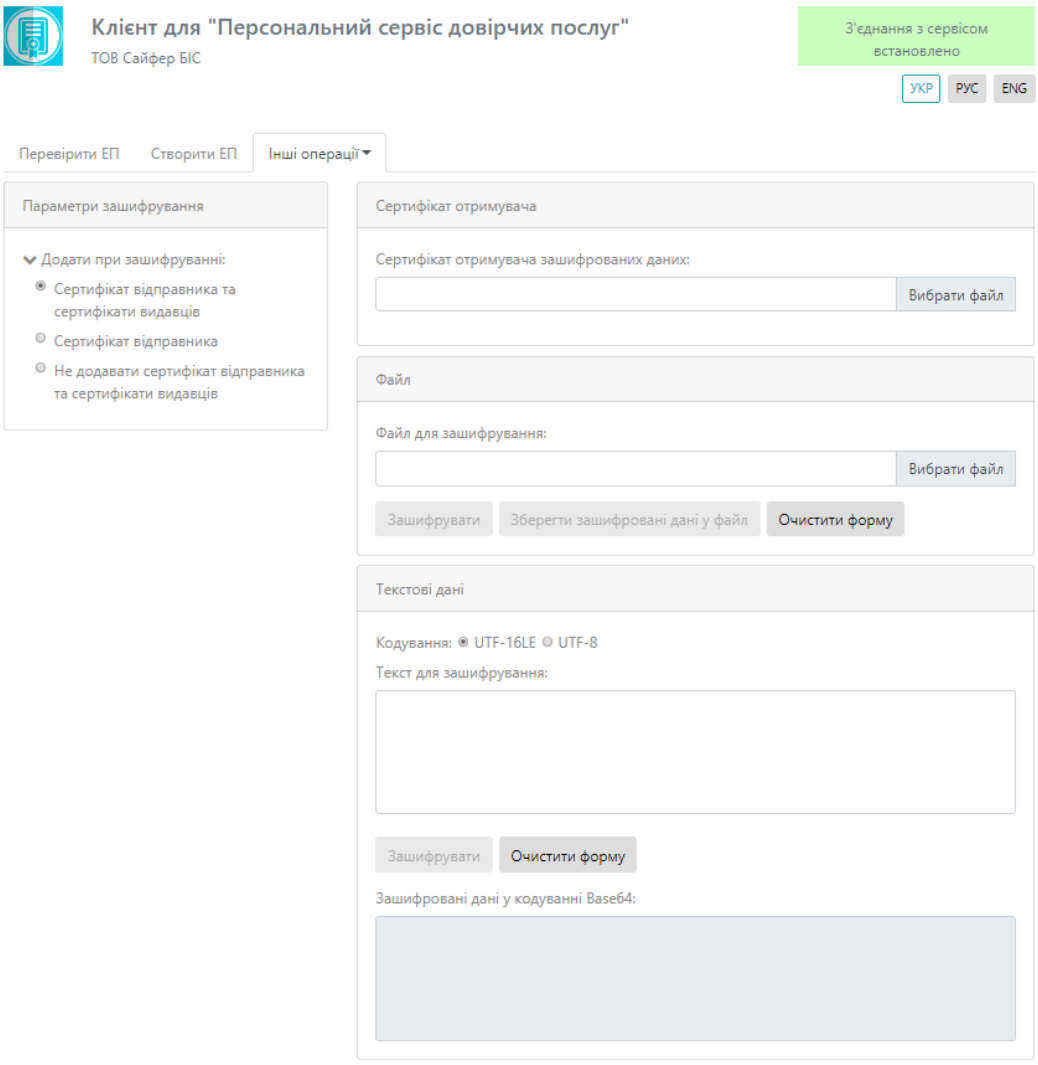

Рис. 69. Вкладка «Зашифрування»

Процес Зашифрування починається з того, що обираються «Параметри зашифрування», додається сертифікат отримувача зашифрованих даних, обирається тип кодування, вноситься текст для зашифрування, натискаємо кнопку «Зашифрувати», Рис. 70. Після, очищаємо форму.

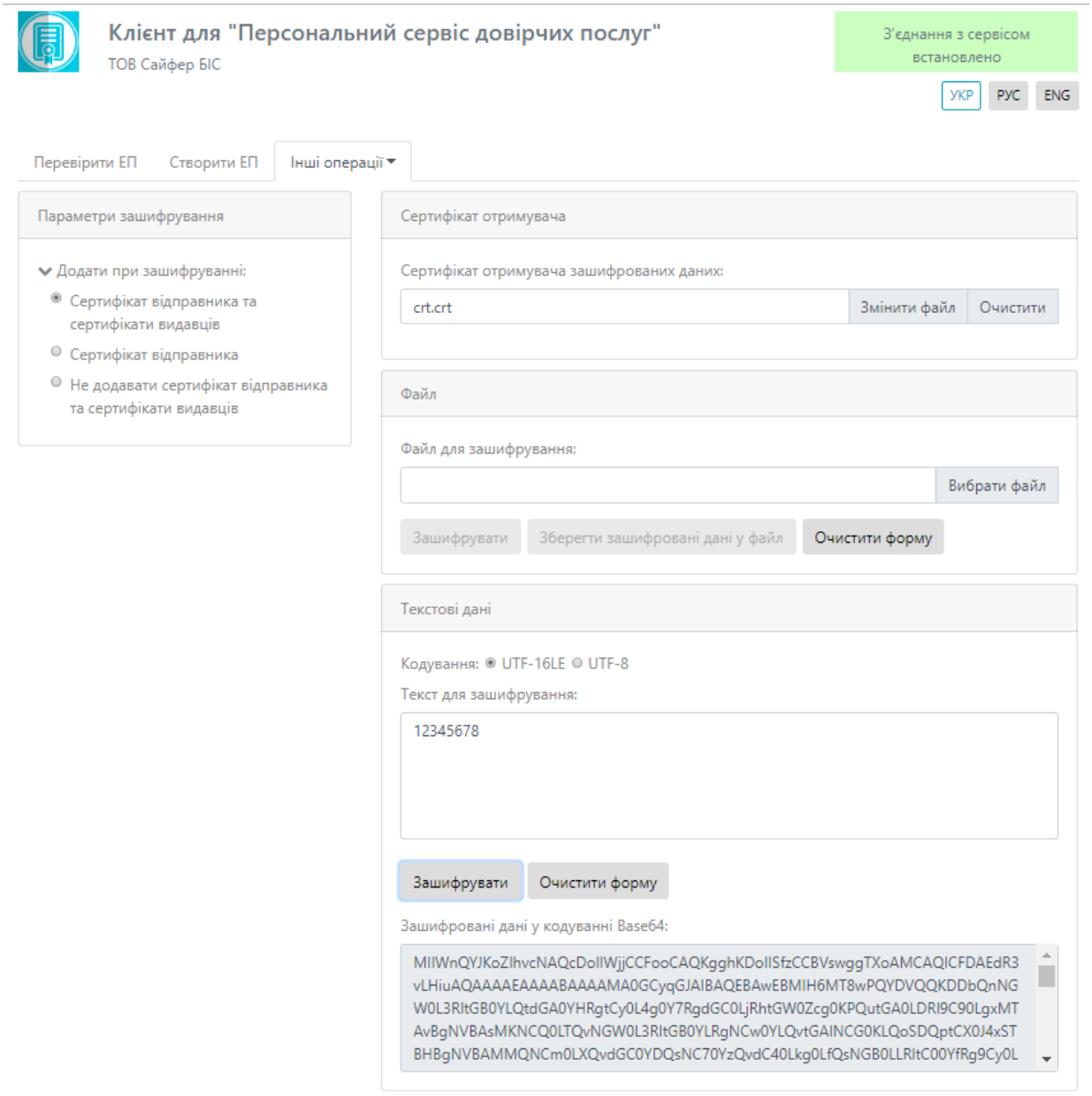

Рис. 70. Зашифрування

Розшифрування

Дана вкладка містить такі поля: Файл та Текстові дані.

Відеоінструкцію для розшифрування даних можна переглянути за посиланням Персональний сервіс довірчих послуг. Зашифрувати та розшифрувати файл.

Розділ «Файл», який включає, Рис. 71:

1. Поле «Файл для розшифрування» (обирається файл, який необхідно розшифрувати);
2. Кнопка «Розшифрувати» (здійснює розшифрування файлу);
3. Кнопка «Зберегти розшифровані дані у файл» (здійснює збереження розшифрованих даних у файл);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми).

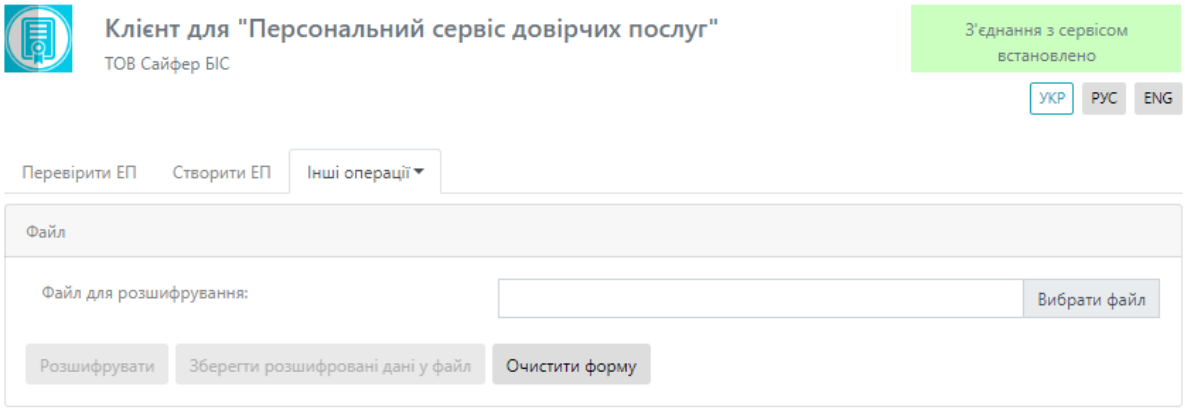

Рис. 71. Вкладка «Розшифрування», розділ «Файл»

Розділ «Текстові дані», який включає, Рис. 72:

1. Кодування (обираємо стандарт кодування тексту): UTF-16LE чи UTF-8;
2. Поле «Зашифровані дані в кодуванні Base64» (вносимо дані для розшифрування);
3. Кнопка «Розшифрувати» (здійснює розшифрування текстових даних);
4. Кнопка «Очистити форму» (здійснює очищення всіє форми);
5. Поле «Розшифрований текст» (отримуємо розшифровані дані).

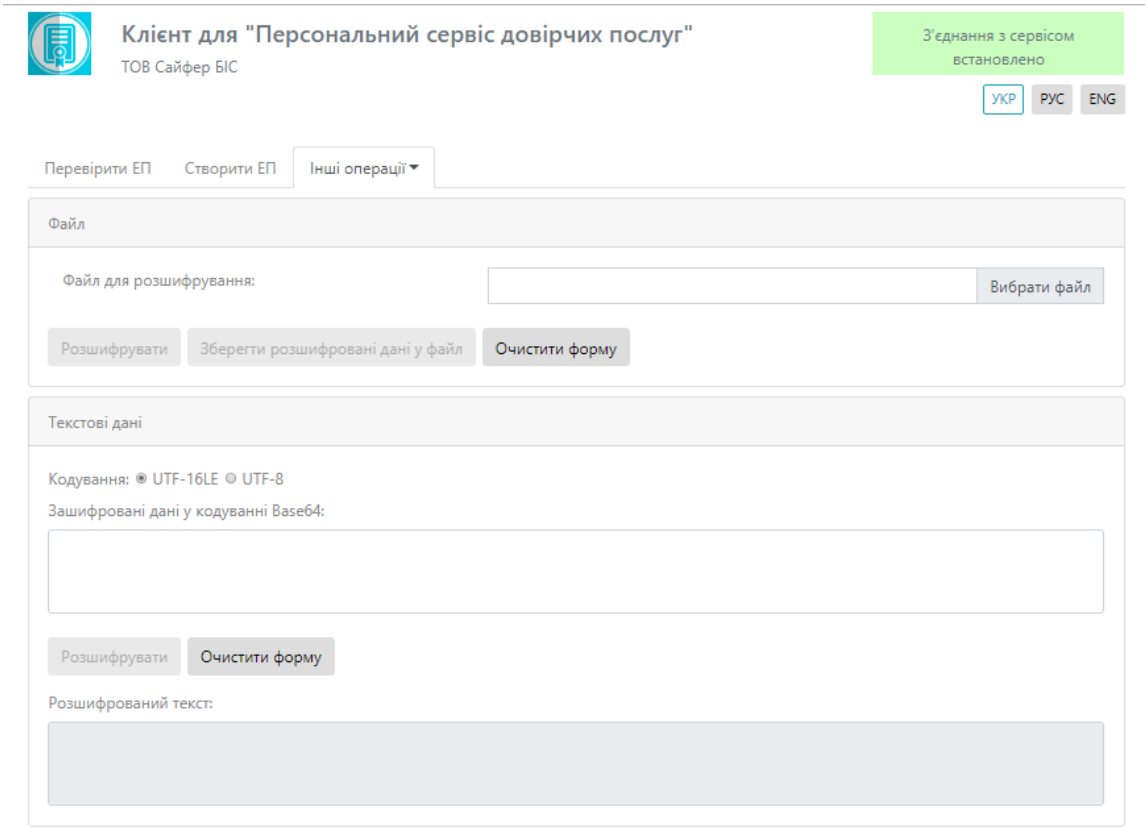

Рис. 72. Вкладка «Розшифрування», розділ «Текстові дані»

Процес Розшифрування починається з того, що обирається тип кодування, вноситься текст для розшифрування, натискаємо кнопку «Розшифрувати», Рис. 73. Після, очищаємо форму.

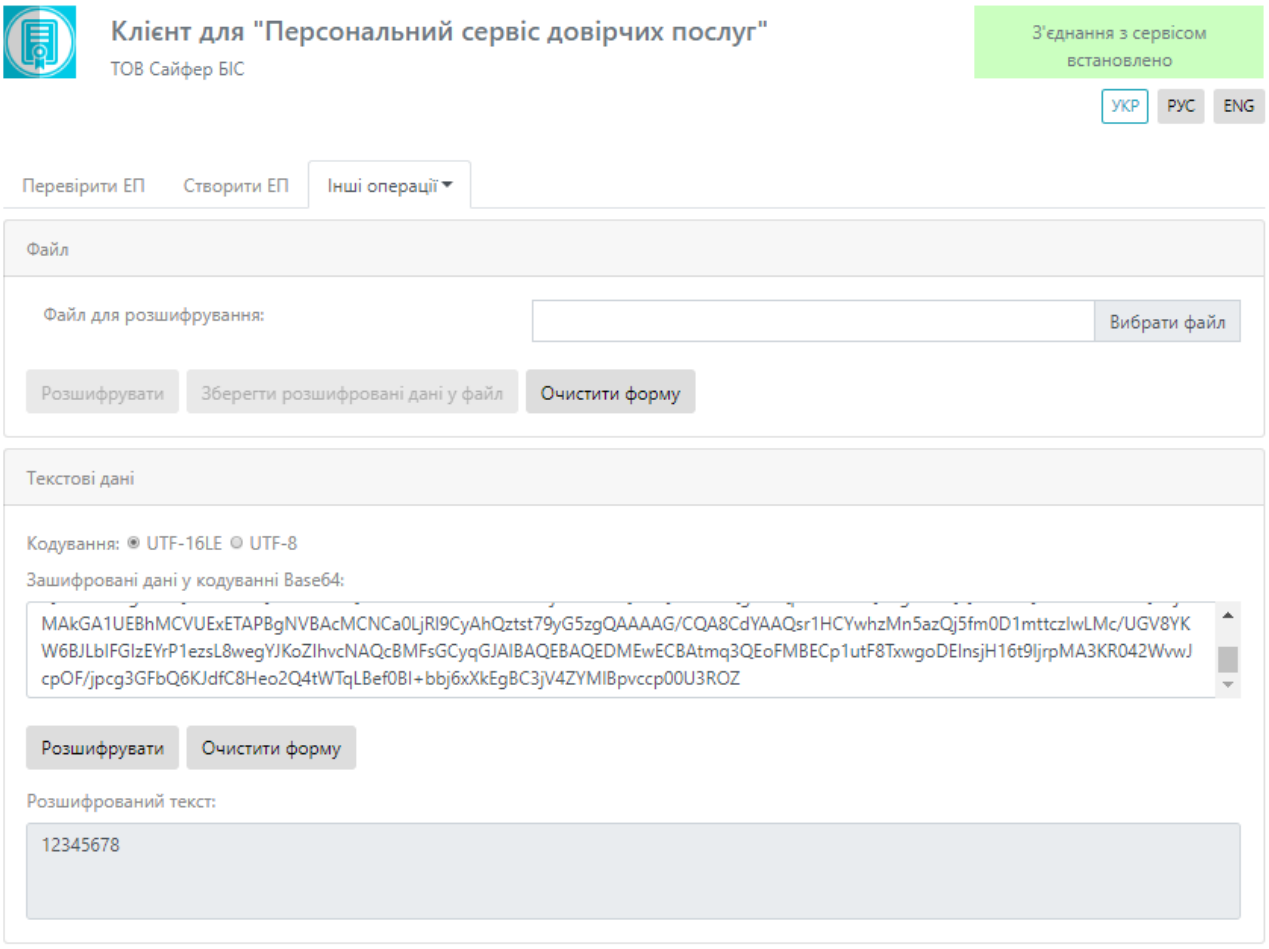

Рис. 73. Розшифрування

Електронна позначка часу

Дана вкладка містить такі поля: Створення електронної позначки часу та Перевірка електронної позначки часу, Рис. 74.

Переглянути відеоінструкцію можливо за посиланням.

Розділ «Створення електронної позначки часу», який містить:

1. Поле «Файл з даними» (обираємо файл, для якого необхідно створити електронну позначку часу);
2. Кнопка «Створити електронну позначку часу» (здійснює створення електронної позначки часу для завантаженого файлу);
3. Кнопка «Зберегти позначку у файлу» (здійснює збереження позначки у файл);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми).

Розділ «Перевірка електронної позначки часу», який містить:

1. Поле «Файл для перевірки» (обираємо файл, без електронної позначки часу);
2. Поле «Файл з електронною позначкою часу» (обираємо файл, який містить електронну позначку часу);

3. Кнопка «Перевірити електронну позначку часу» (здійснюється перевірка електронної позначки часу);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми).

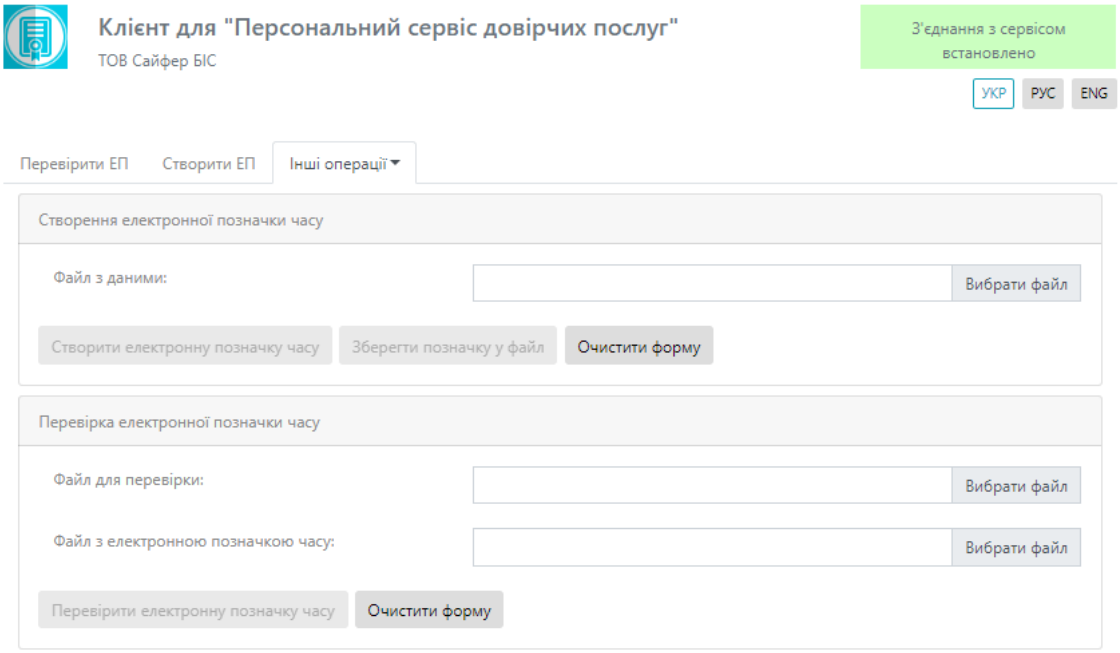

Рис. 74. Електронна позначка часу

Процес Створення електронної позначки часу починається з того, що обирається файл з даними, натискаємо кнопку «Створити електронну позначку часу», Рис. 75.

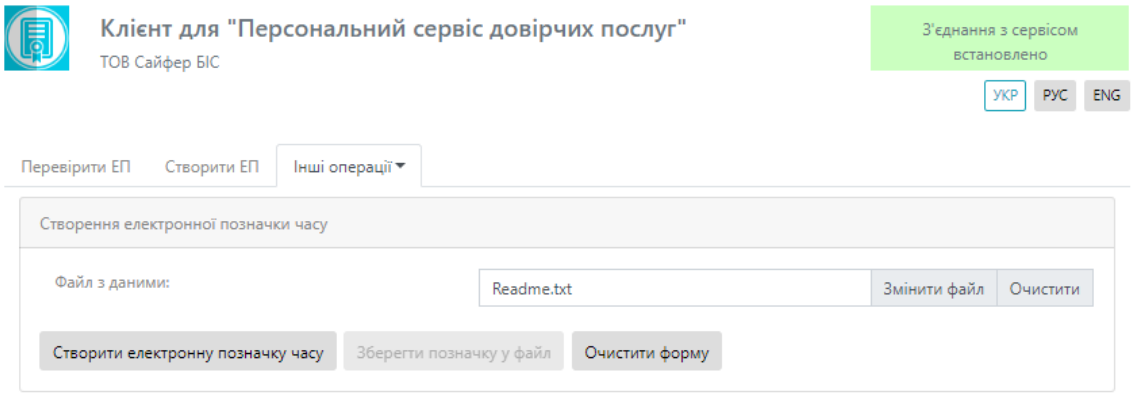

Рис. 75. Створення електронної позначки часу

Після натискання кнопки «Створити електронну позначку часу», з'являється повідомлення про успішне створення електронної позначки часу, Рис. 76.

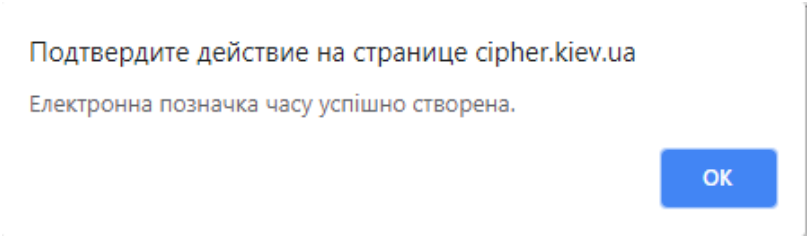

Рис. 76. Повідомлення про успішне створення електронної позначки часу

Після натискання «Ок», з’являється можливість зберегти позначку у файл, Рис. 77. Обираємо шлях для збереження та очищаємо форму.

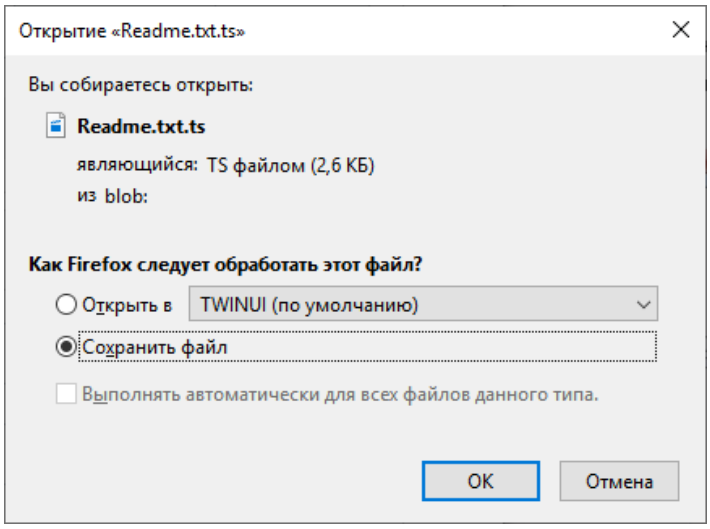

Рис. 77. Збереження файлу

Процес Перевірки позначки часу починається з того, що обирається файл з даними та файл з познакою часу, натискаємо кнопку «Перевірити електронну позначку часу», Рис. 78.

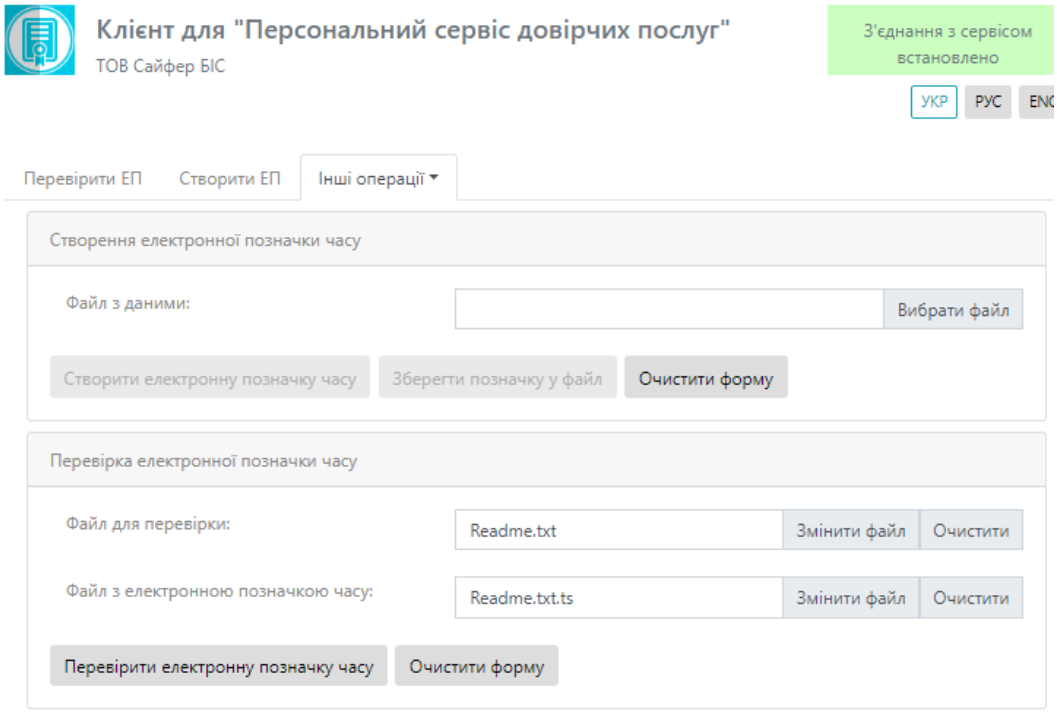

Рис. 78. Перевірка електронної позначки часу

Після натискання на кнопку «Перевірити електронну позначку часу», з’являється повідомлення про дійсність позначки часу, Рис. 79. Та очищаємо форму.

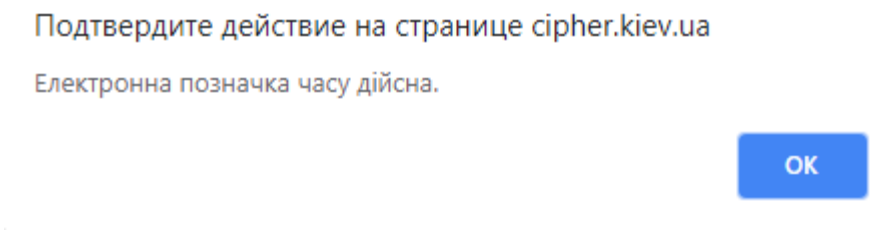

Рис. 79. Повідомлення про дійсність електронної позначки часу

Поширені запитання у роботі з Персональним сервісом довірчих послуг та шляхи їх вирішення

ВАЖЛИВО ЗНАТИ:

1. Для роботи із захищеними носіями рекомендується користуватися 32-розрядною версією Java.
2. Якщо ключ виданий КНЕДП/АЦСК Казначейства необхідно користуватися старим інтерфейсом, як вказано на сторінці, оскільки на даний момент «Персональний сервіс довірчих послуг» не працює з даним КНЕДП/АЦСК. Якщо це захищений носій, то створити ЕП Ви не матимете змогу.
3. «Персональний сервіс довірчих послуг» працює **некоректно** на платформі **ОС Microsoft Windows XP SP(1/2/3) 2002** у поєднанні з версіями **java старше 1.8.0_111**. Дана версія ОС вважається застарілою, про що повідомляється на офіційному ресурсі Java при спробі завантажити оновлену її версію. Для користувачів ОС Microsoft Windows XP SP(1/2/3) 2002 рекомендуємо завантажувати попередню версію за посиланням jre-8u111-windows-i586.exe.

ПОМИЛКИ, що виникають в роботі та методи їх усунення:

4. Файл завантажився, але додаток не розгортається –«нічого не відбувається».

4.1. Перевірити можливість блокування додатку брандмауером ОС (приклад для ОС Windows 7).

«Пуск» -> «Панель управления-брандмауэр Windows» -> «Изменение параметров уведомлений» -> вказати опцію «Уведомлять, когда брандмауэр блокирует новую программу», або взагалі його вимкнути завдяки позначки «Отключить брандмауэр Windows» на період накладання чи перевірки підпису, Рис. 80.

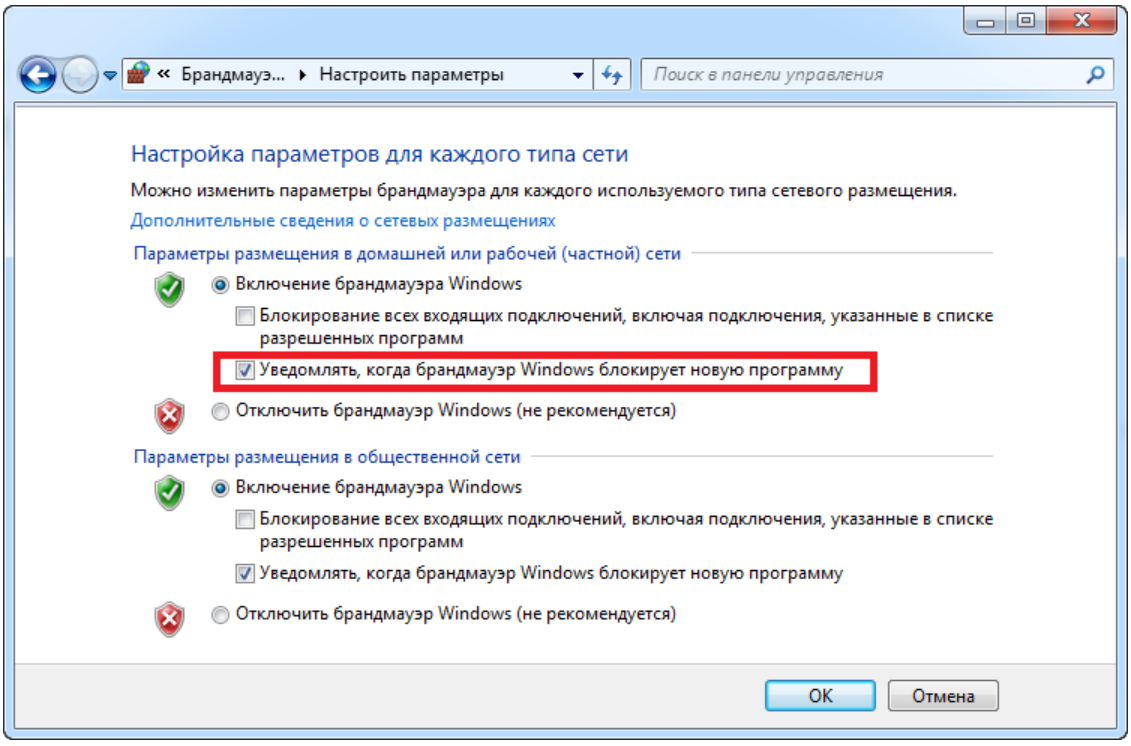

Рис. 80. Вікно налаштувань брандмауера

4.2. Перевірити чи правильно налаштовані асоціації для фалів та програм.

Для файлів формату .jnlp потрібно вказати програму Java WebStart Application (javaws):

- На прикладі браузера Mozilla FireFox, Рис. 81. «Меню» – «Настройки» – «Приложения»

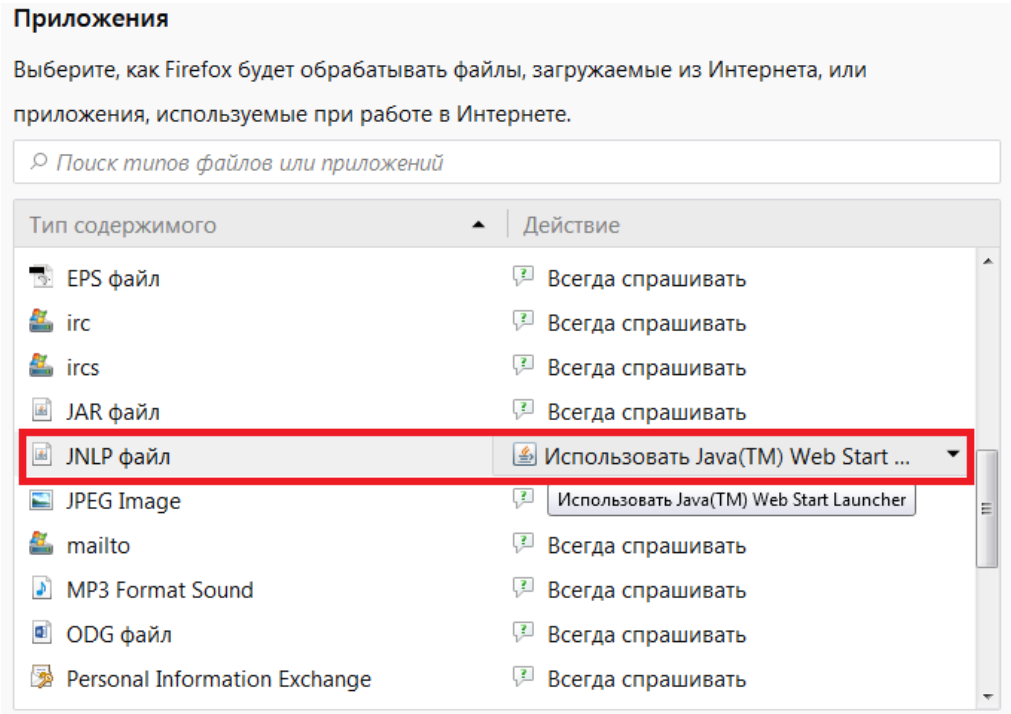

Рис. 81. Налаштування асоціацій у браузері Mozilla FireFox

- На прикладі системних налаштувань, Рис. 82. «Панель управления» -> «Программы по умолчанию -> «Сопоставление типов файлов или протоколов конкретным программам».

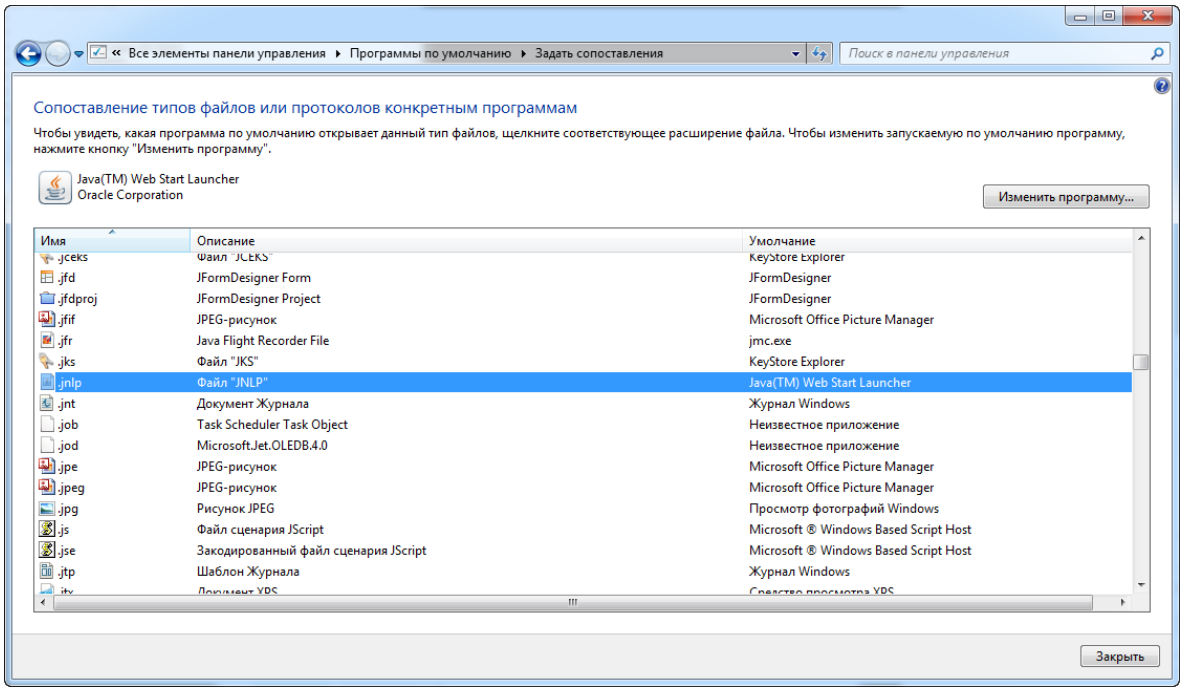

Рис. 82. Системні налаштування асоціацій

5. Помилка «Неможливо створити криптографічний контекст. У ключовому контейнері відсутній сертифікат ключа ЕП», Рис. 83.

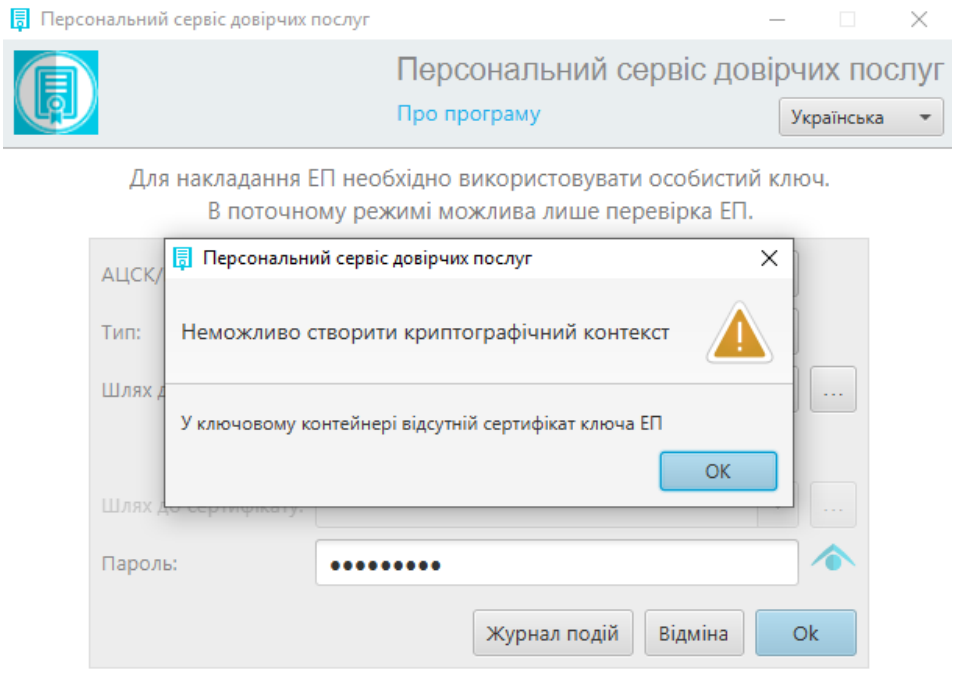

Рис. 83. Помилка «Неможливо створити криптографічний контекст. У ключовому контейнері відсутній сертифікат ключа ЕП»

5.1. Перевірити чи вірно був обраний КНЕДП/АЦСК, який надав користувачеві ЕП.

5.2. Чи був виданий Вам окремо сертифікат ключа ЕП? Якщо так – потрібно обрати опцію «Вказувати шлях до сертифікату», Рис. 84.

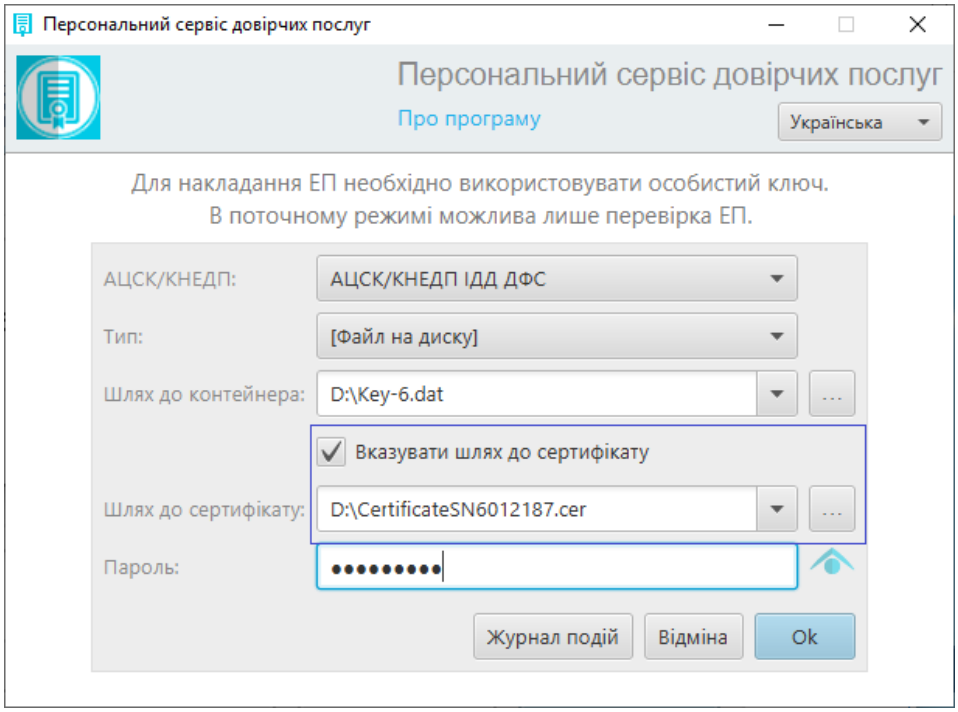

Рис. 84. Опція «Вказувати шлях до сертифікату»

5.3. В мережі використовується проксі, потрібно правильно налаштувати:

- задати системні налаштування;

- задати налаштування у браузері;

- задати налаштування для java середовища.

6. Помилка «Неможливо створити криптографічний контекст. Не знайдено файл ключового контейнера», Рис. 85.

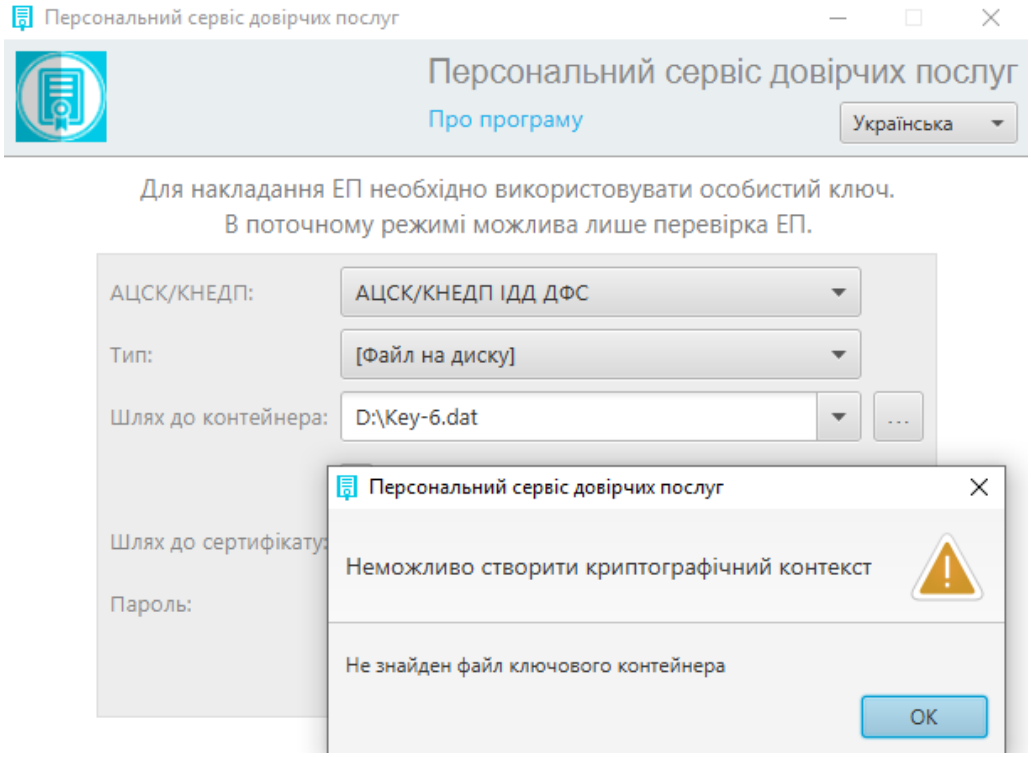

Рис. 85. Помилка «Неможливо створити криптографічний контекст. Не знайдено файл ключового контейнера»

6.1. Дана помилка пов’язана з розміщенням ключа ЕП, для вирішення даної проблеми, необхідно ключ розмістити у корені диску, чи папці, що містить цифри чи латинські літери.

6.2. Також, дана помилка може виникнути, якщо Ви натиснули «стрілочку вниз» напроти поля «Шлях до контейнеру», та обрали з нижче вказаного переліку ключовий контейнер. Цей список означає, що Ви раніше вже використовували ці ключі для авторизації, і якщо Ви виберете одного з них, то можливе виникнення помилки «не знайдено файл ключового контейнеру». Оскільки Ви могли раніше використовуваний файл та згодом перемістити до іншої папки. Томі слід щоразу обирати файл з початку, натиснувши кнопку «…» напроти поля «Шлях до контейнеру».

7. Помилка «Неможливо створити криптографічний контекст. Помилка розшифрування ключового контейнеру», Рис. 86.

Дана помилка пов’язана з тим, що немає необхідності вказувати «Шлях до сертифікату», тому необхідно прибрати позначку з пункту «Вказувати шлях до сертифікату».

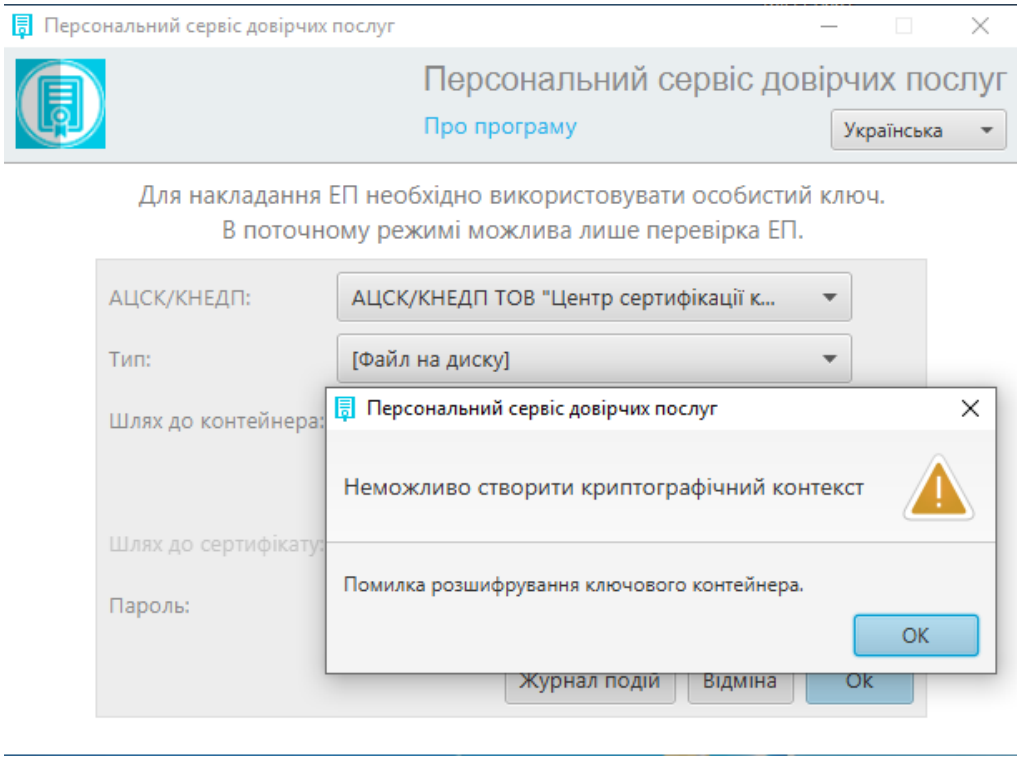

Рис. 86. Помилка «Неможливо створити криптографічний контекст. Помилка розшифрування ключового контейнеру»

8. Помилка, яка виникає при відкритті JNLP-файлу “Unable to launch the application”, Рис. 87.

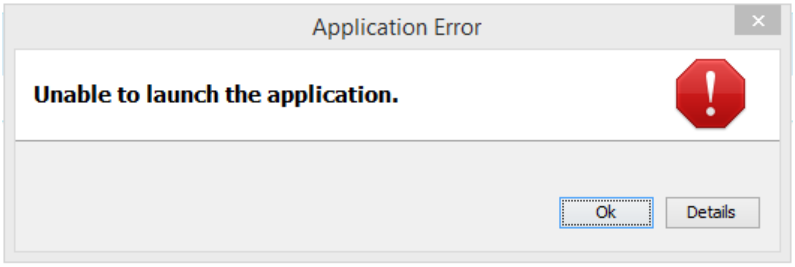

Рис. 87. Помилка при відкритті JNLP-файлу “Unable to launch the application”

8.1. Пов’язана з тим, що необхідно налаштувати проксі для Java та для браузера, який використовується:

- задати системні налаштування;

- задати налаштування у браузері;

- задати налаштування для java середовища.

8.2. Пов'язана з тим, що є необхідність внести зміни у системні налаштування hosts.

Увага! Для того, щоб бути впевненим у необхідності внесення змін, під час роботи з «Персональним сервісом довірчих послуг» необхідно у браузері натиснути кнопку F12 та перейти на вкладку «Сеть», якщо відображається «перекреслений замок», як показано на Рис. 88, то переходимо за на розділ системні налаштування hosts.

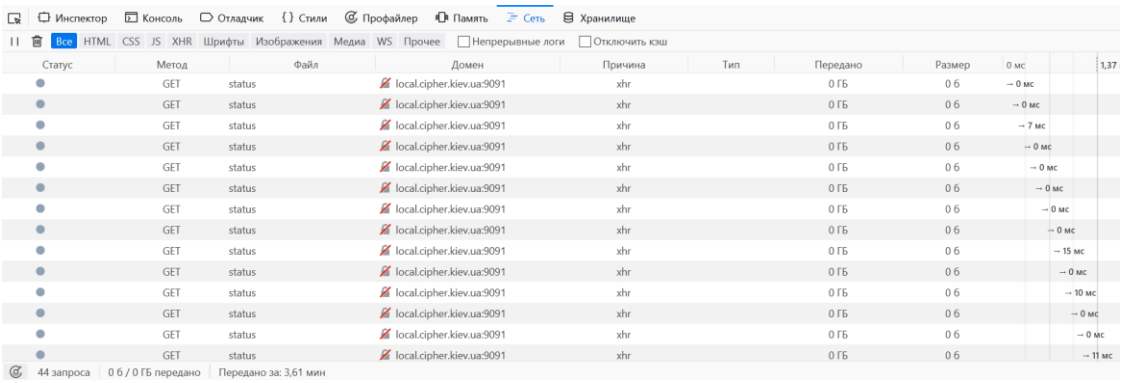

Рис. 88. Вкладка «Сеть» у браузері до змін

Після внесених змін, необхідно перевірити, натиснувши повторно кнопку F12, та перевірити вигляд «замків» та статус – 200, як показано на Рис. 89.

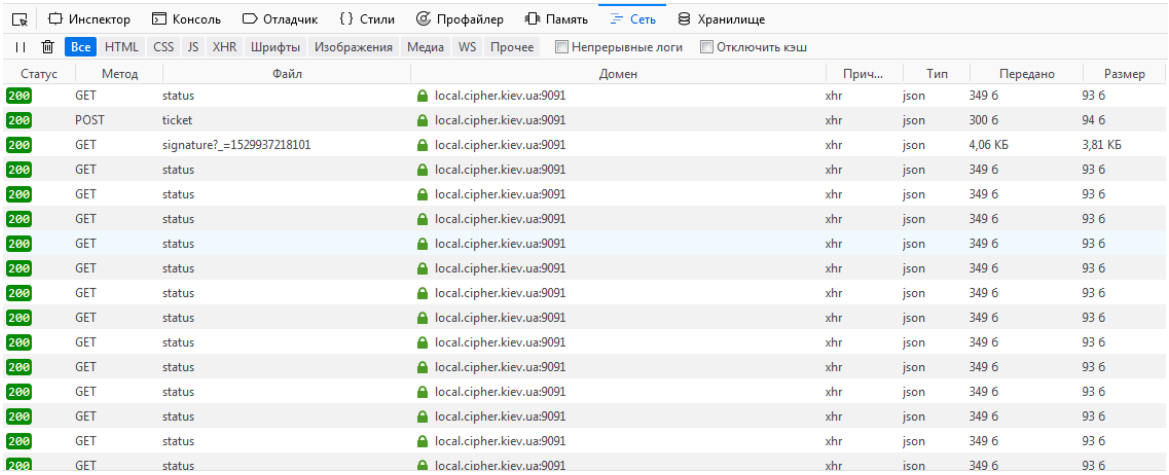

Рис. 89. Вкладка «Сеть» у браузері після змін

9. Помилка на Рис. 90 пов’язана з тим, при перевірці накладеного підпису за типом «Відкріплена», у поле «Файл для перевірки» необхідно внести файл на який було накладено підпис (початковий), у поле «Файл з підписом» необхідно внести файл, який має підпис.

У прикладі, у поле «Файл з підписом» – додано ключ.

Якщо Ви накладали підпис за типом «Вбудована», у поле «Файл з підписом» необхідно внести лише файл на який накладено підпис. Поле «Файл для перевірки» – відсутнє.

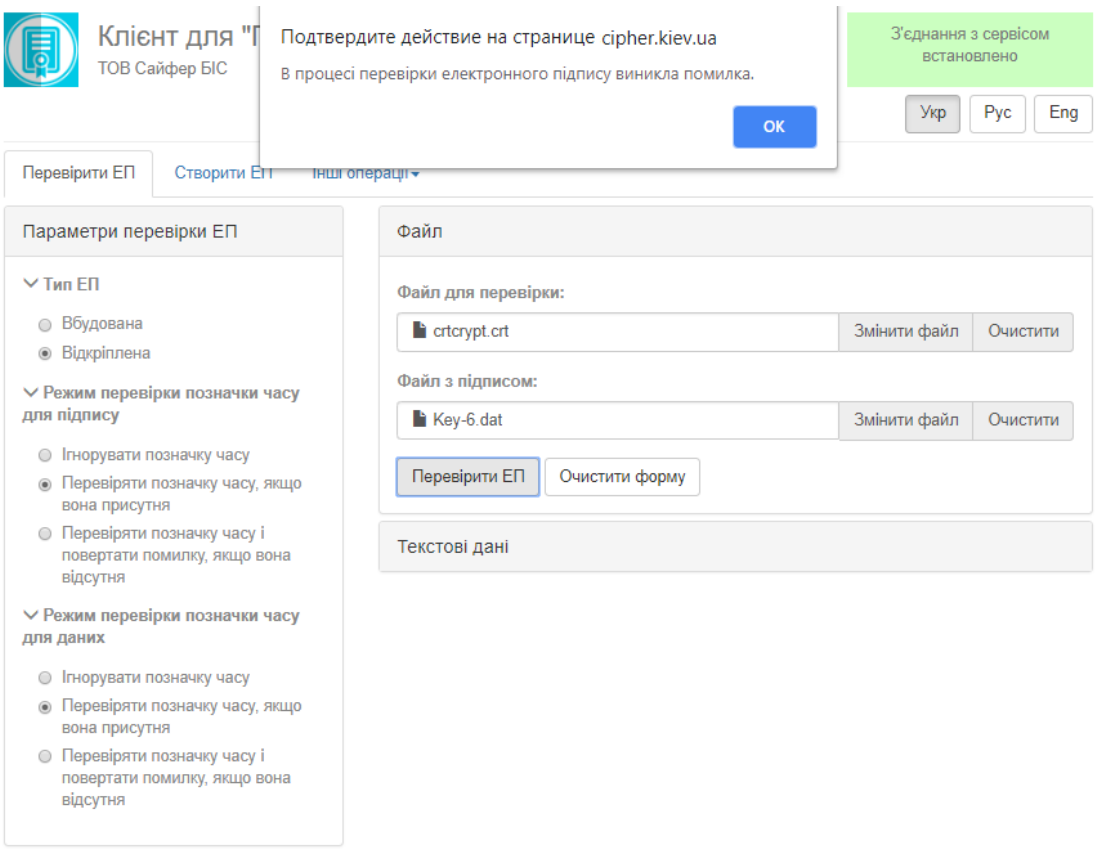

Рис. 90. Повідомлення про помилку

Примітка. Під час роботи «Персонального сервісу довірчих послуг» можуть виникати інші помилки, тому для їх вирішення розробникам необхідно отримати від користувача:

1. Знімок екрану з помилкою.
2. Вміст «Журналу роботи» у вікні «Персонального сервісу довірчих послуг», скопіювати у текстовий документ з розширенням txt.
3. Вміст Java Console, скопіювати у текстовий документ з розширенням txt. Щоб відкрити Java Console є два варіанти:
   - Перейти у папку, де встановлена Java (скоріш за все - C:\Program Files\Java\jre1.8.0_181\bin), знайти файл javacpl.exe. Перейти на вкладку «Advanced» -> «Java console» -> «Show console» -> «ok». Перезавантажити «Персональний сервіс довірчих послуг».

АБО

- «Пуск» –> «Панель управления» -> «Java» -> «Advanced» -> «Java console» -> «Show console» -> «ok». Перезавантажити «Персональний сервіс довірчих послуг».