САЙФЕР
Системы защиты информации
Интернет-банкинг

Сайфер ПРО, ТОВ
04107, Київ, вул. Нагірна 25/27, 3-ій поверх

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

Дата модифікації: 24/10/2019

Шифр-CaaS

Настанова з установки та експлуатації Агенту ЄСКО (Java)

ЗМІСТ

Вступ

В цьому документі описано порядок дій користувача для використання програмного комплексу «Шифр-CaaS», а саме Агенту ЄСКО (Java) його функціональні можливості та необхідні відомості для роботи з ним.

Системні вимоги

Перед початком встановлення та роботи з програмним застосуванням необхідно переконатися, що програмне та апаратне забезпечення відповідає рекомендаціям розробника.

Мінімальні вимоги до апаратного забезпечення:

- Оперативна пам'ять: 512 МБ та вище;
- Процесор – 1,2 ГГц;
- LAN: 10 Мбіт/с.

Мінімальні вимоги до програмного забезпечення:

- Вимоги до ОС:
  - ОС Windows (Windows XP і вище, Windows Server 2008 R2 з SP1 і вище)
  - ОС Linux (Ubuntu Linux 12.04 і вище, CentOS 6 і вище та ін.)
  - ОС MacOS X (10.7.3 і вище)
- Браузери, що підтримуються:
  - Internet Explorer 11;
  - Mozilla Firefox;
  - Google Chrome.
- Java:
  - ОС Windows XP (лише 8u111).
  - ОС Windows 7/8/10 (8u152 і вище).
  - ОС Linux (8u25 вище та ін.)

Підготовка робочого місця для роботи з сервісом

Введення

Програмний комплекс «Агент Єдиного сервісу криптографічних операцій» реалізований мовою програмування Java, що дозволяє виконувати запуск на таких платформах:

- ОС Linux.
- ОС Windows.
- ОС MacOS.

Основною умовою для користування «Агентом Єдиного сервісу криптографічних операцій» 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 комплексу неможливий, тому необхідно інсталювати її. Для початку потрібно завантажити дистрибутив відповідної компоненти (JRE) з офіційного сайту Java за посиланням java.com та слідувати відповідним інструкціям.

Якщо встановлена операційна система Windows XP, то з останніми версіями Java, «Агент Єдиного сервісу криптографічних операцій» 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 Агент «Шифр-CaaS» у вигляді Java Web Start Application використовує в своїй роботі проксі-сервер, який вказаний в 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:

1) Автоматичне налаштування. За допомогою DNS-сервера 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.**

2) Задання скрипта з налаштуваннями проксі вручну аналогічне п.1, але адреса скрипта (файлу) вказується вручну.

3) 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 Агенту «Шифр-CaaS» 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.

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.

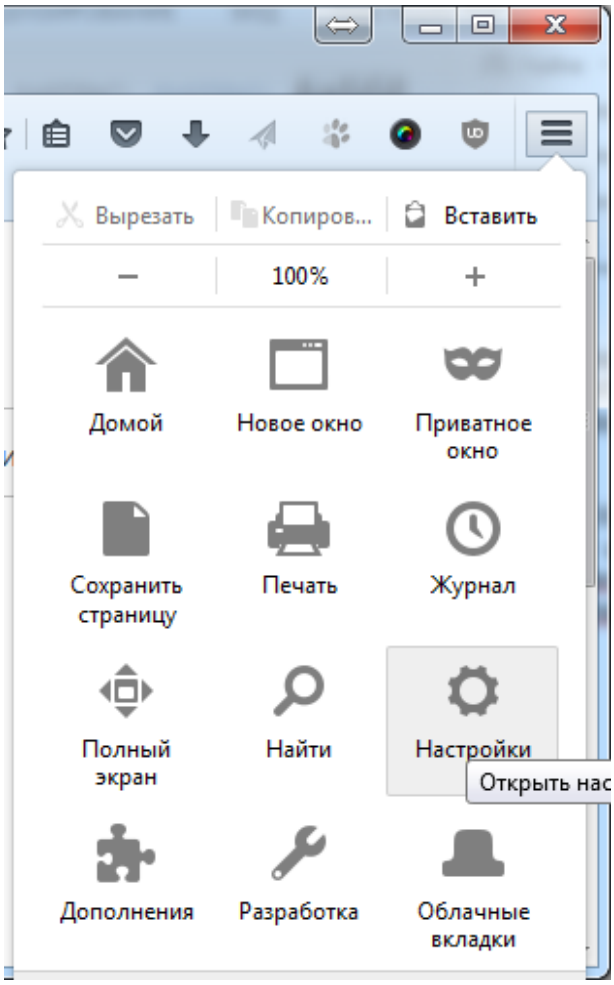

Рис. 1. Налаштування браузера Firefox

Далі послідовно обрати Налаштування: «Дополнительные->Сеть->Настроить», Рис. 2.

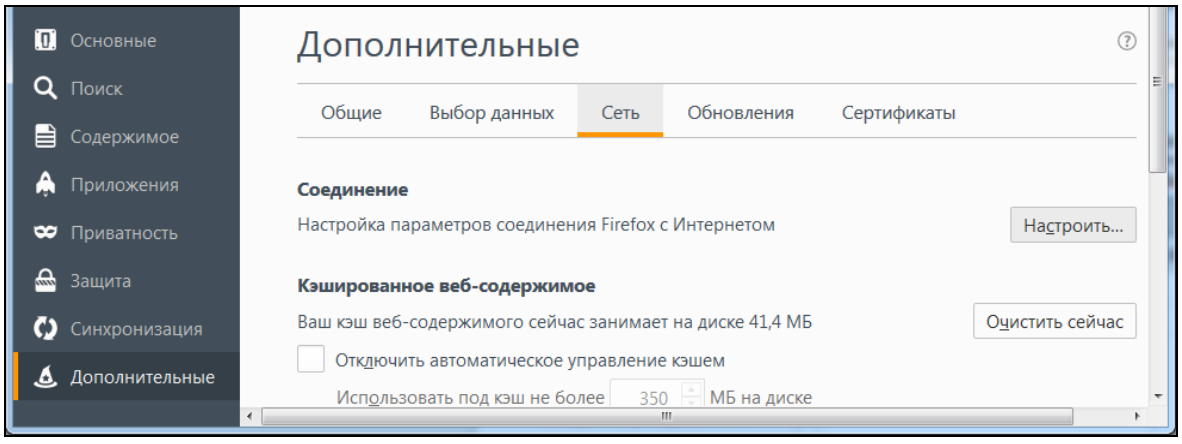

Рис. 2. Додаткові мережеві налаштування браузера

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

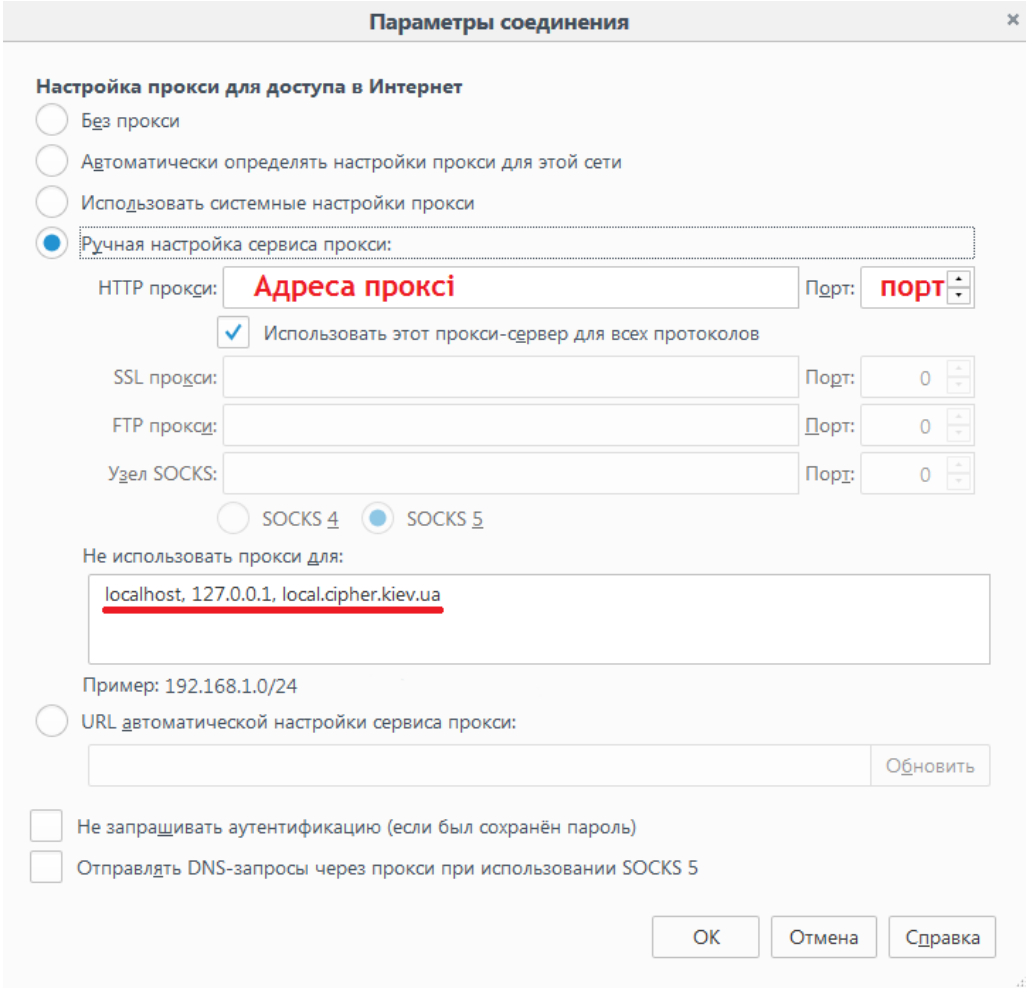

Рис. 3. Додаткові параметри з’єднання

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.

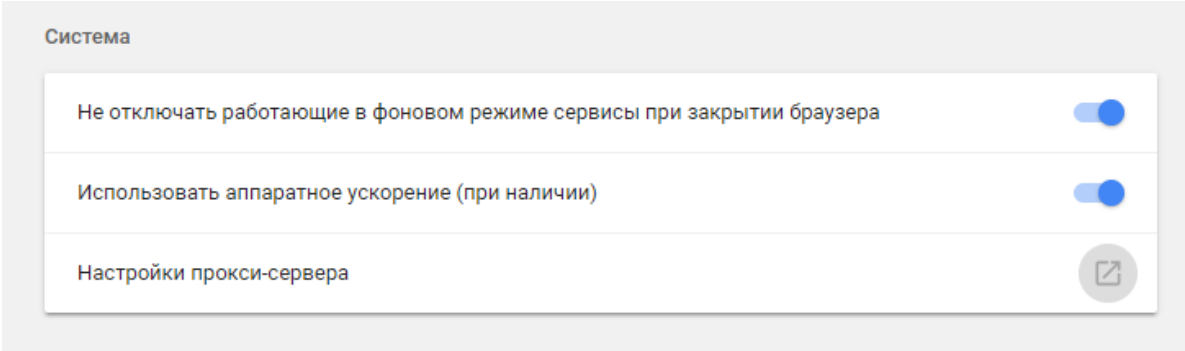

Рис. 4 Налаштування браузера Google Chrome

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

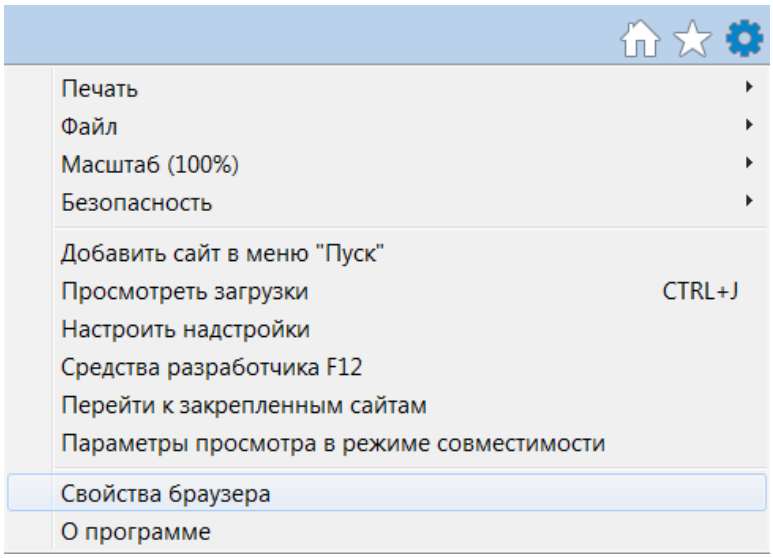

Рис. 5 Налаштування браузера Internet Explorer

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.

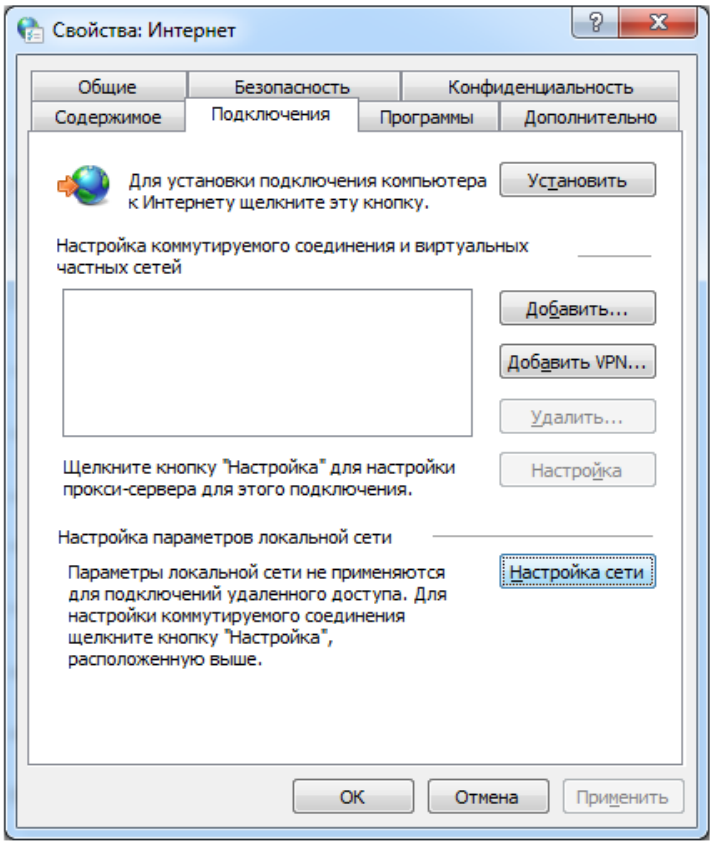

Рис. 6. Системні налаштування мережі

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

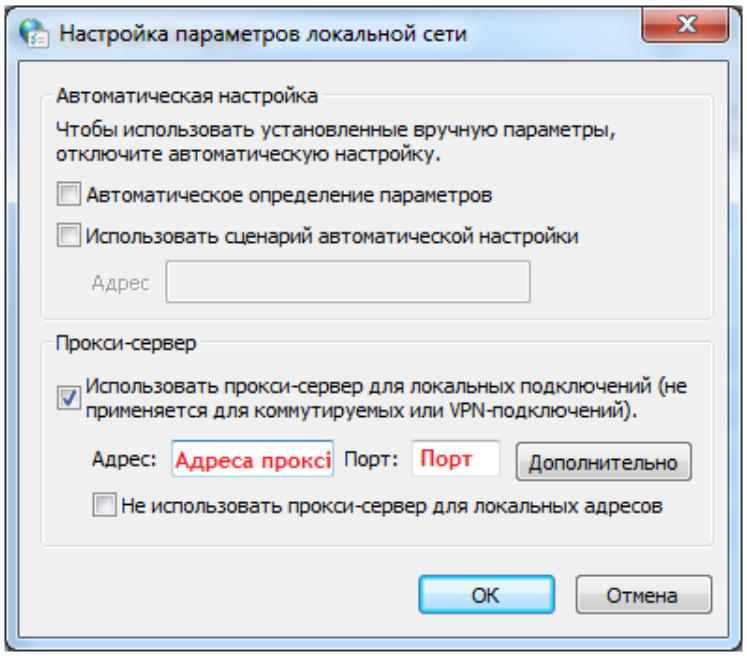

Рис. 7. Налаштування параметрів локальної мережі

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

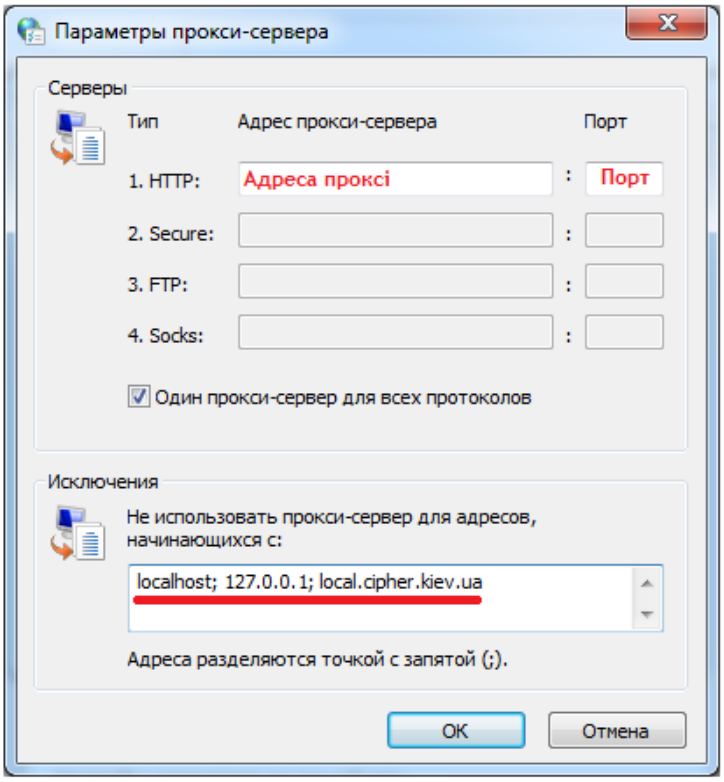

Рис. 8. Параметри проксі-сервера

Середовище Java

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

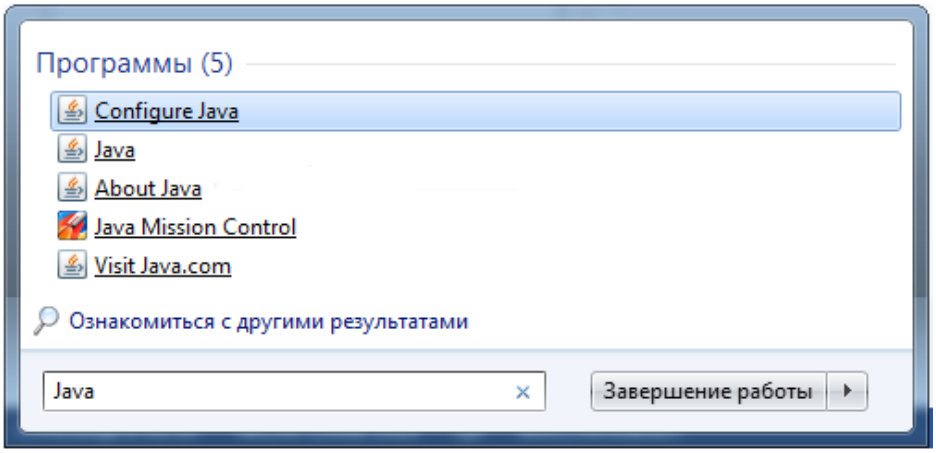

Рис. 9. Конфігурування java-середовища

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

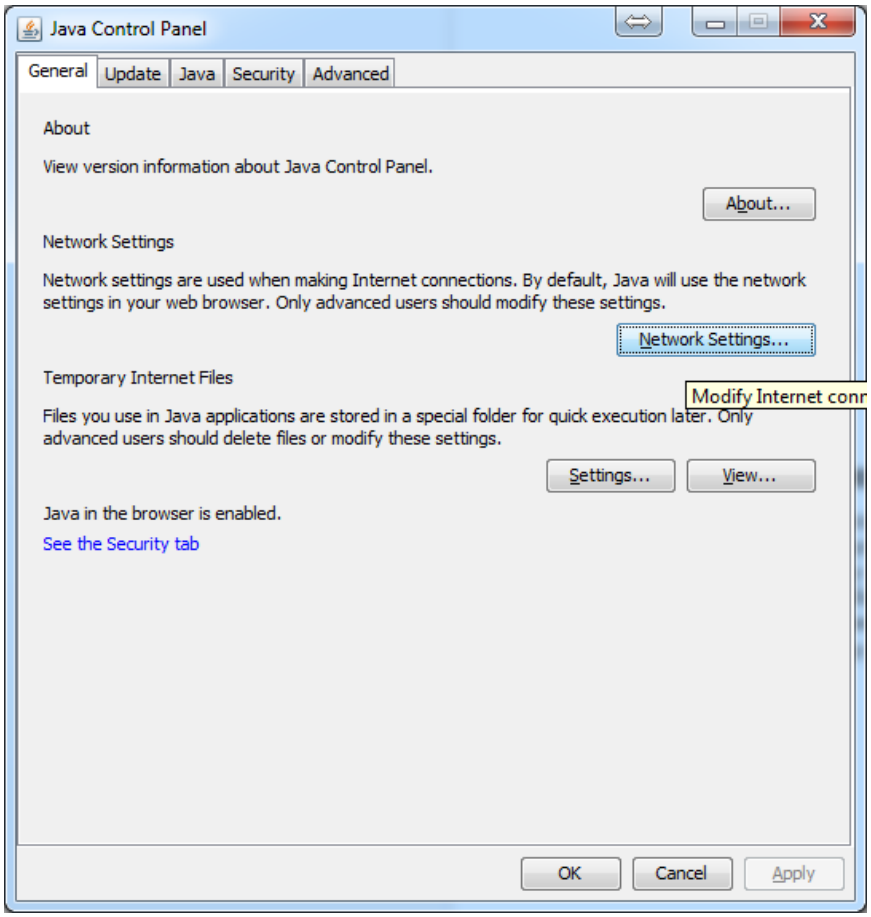

Рис. 10. Панель управління Java

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

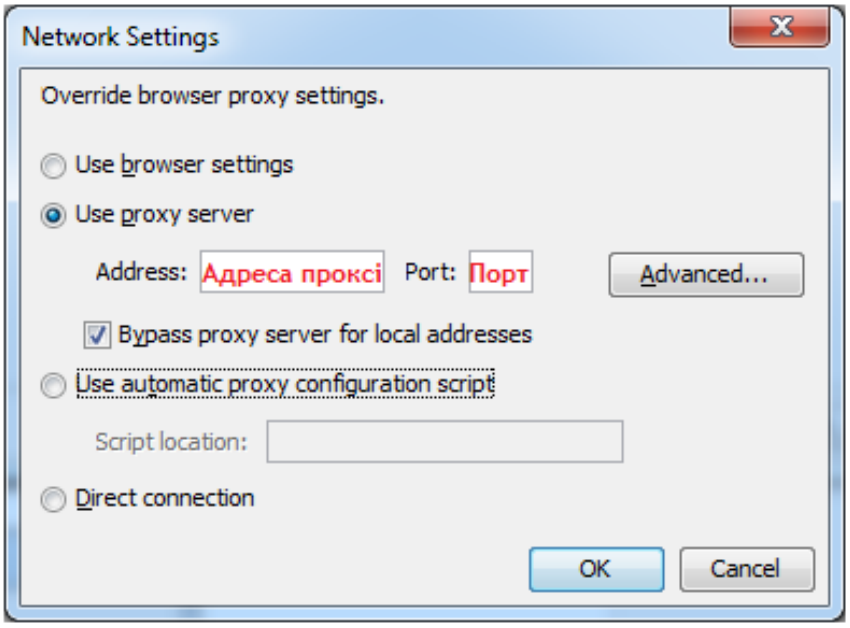

Рис. 11. Налаштування мережі

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

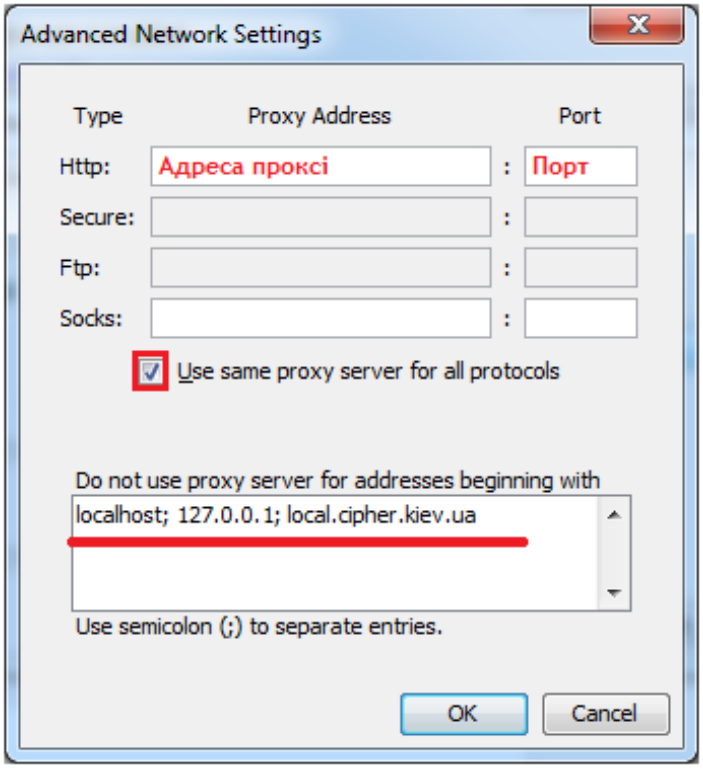

Рис. 12. Налаштування адрес-виключень

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:

- ОС Windows: C:\Windows\System32\drivers\etc\hosts.
- ОС Linux: */etc/hosts*.

Для внесення змін – у файлі hosts додати рядок:

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

Зберегти зміни в документі.

Слід зауважити, що перед рядком, який необхідно додати немає необхідності додавати знак «решітки» - #, оскільки це є знак коментаря.

Підтримка захищених носіїв

Агент Єдиного сервісу криптографічних операцій підтримує роботу із захищеними носіями.

Захищений апаратний носій у пасивному режимі – підтримує збереження особистого ключа у захищеному ключовому контейнері. Доступ до ключа здійснюється за допомогою інтерфейсу PKCS#11. До таких носіїв відносяться:

- Avest Avest-Key.
- Efit Key.
- Author Secure Token-337 Series, Author Smart Card-337 Series (обов’язкове розміщення бібліотеки у залежності від розрядності Java).
- Gemalto IDPrime.
- Gemalto eToken, SafeNet eToken, Aladdin eToken.
- jaCarta.
- eAladdin eToken.
- G&D StarSign Token, G&D StarSign Card.
- ІІТ Алмаз (обов’язкове встановлення ПЗ: EKAlmaz1CInstall.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- ІІТ Кристал (обов’язкове встановлення ПЗ: EKeyCrystal1Install.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).

Захищений апаратний носій у активному режимі – самостійно здійснює створення ЕП за допомогою особистого ключа у захищеному контейнері. Виконання операції з ЕП здійснюється за допомогою PKCS#11 інтерфейсу. До таких носіїв відносяться:

- Avest Avest-Key.
- Efit Key.
- Author Secure Token-337 Series, Author Smart Card-337 Series (обов’язкове розміщення бібліотеки у залежності від розрядності Java).
- ІІТ Алмаз (обов’язкове встановлення ПЗ: EKAlmaz1CInstall.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- ІІТ Кристал (обов’язкове встановлення ПЗ: EKeyCrystal1Install.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- Plasticard TEllipse (обов’язкове встановлення ПЗ та розміщення бібліотеки у залежності від розрядності Java).

Avtor Secure Token – 337

Для роботи із захищеними носіями Avtor Secure Token у Агенті Єдиного сервісу криптографічних операцій, 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:

1. 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.***

Завантажити архів можна за посиланням - x86_Av337CryptokiD.rar

2. 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.***

Завантажити архів можна за посиланням - x64_Av337CryptokiD.rar

Для продовження роботи, необхідно повернутися до «Агенту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити **Агент ЄСКО**.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши «**...**».
- Вказати **PIN-код** до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Якщо захищений носій не виявлено, зверніться до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника «Агенту Єдиного сервісу криптографічних операцій».

Подальша робота «Агенту Єдиного сервісу криптографічних операцій» 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».

Робота з Агентом Єдиного сервісу криптографічних операцій

Запуск

У веб-браузері перейти за посиланням - https://cryptocenter.cipher.kiev.ua/ до Клієнту Єдиного сервісу криптографічних операцій.

Покрокова інструкція та ознайомлення з інтерфейсом програмного комплексу:

1. Стартове вікно Клієнту Єдиного сервісу криптографічних операцій у веб-браузері показано на Рис. 13.

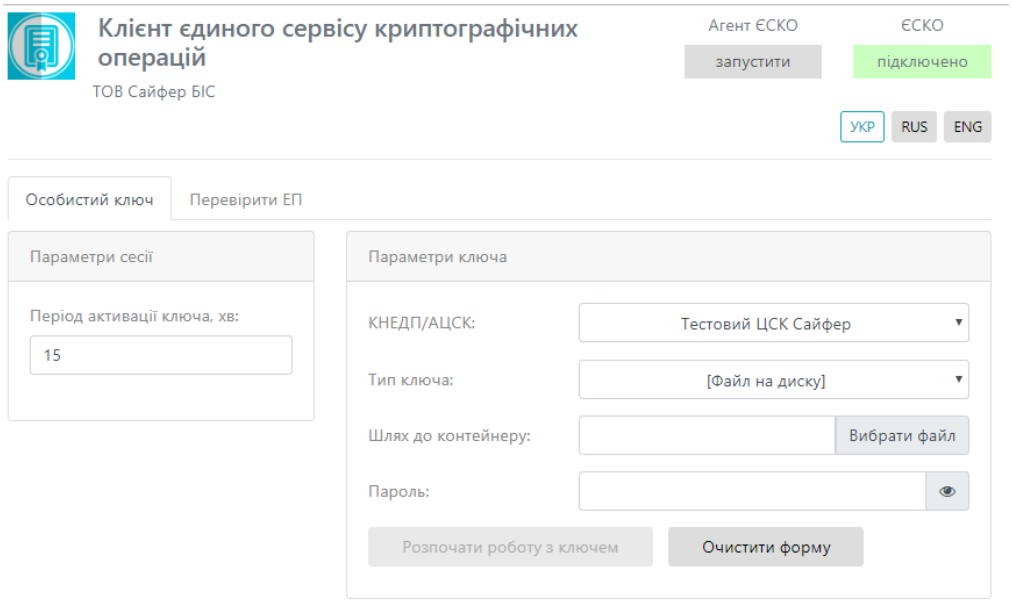

Рис. 13. Стартове вікно ЄСКО

2. Наступним кроком слід відкрити Агент ЄСКО, натиснувши у правому верхньому куті під написом Агент ЄСКО кнопку «запустити», Рис. 14.

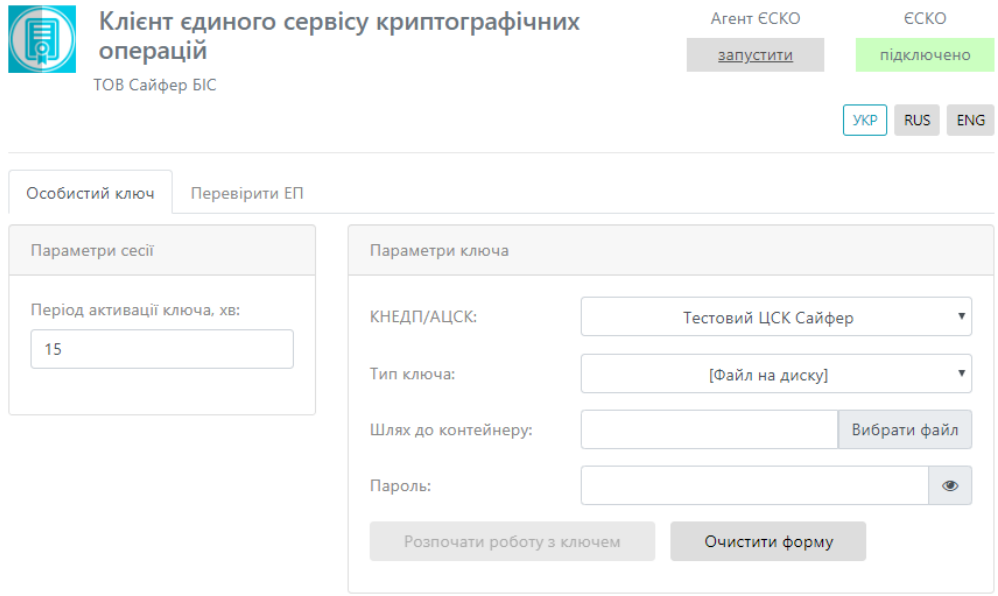

Рис. 14. Запуск Агенту ЄСКО

3. Далі відкривається вікно Агенту Єдиного сервісу криптографічних операцій, Це означає що Агент запущено, все працює коректно, його слід згорнути та повернутися до веб-браузера, Рис. 15.

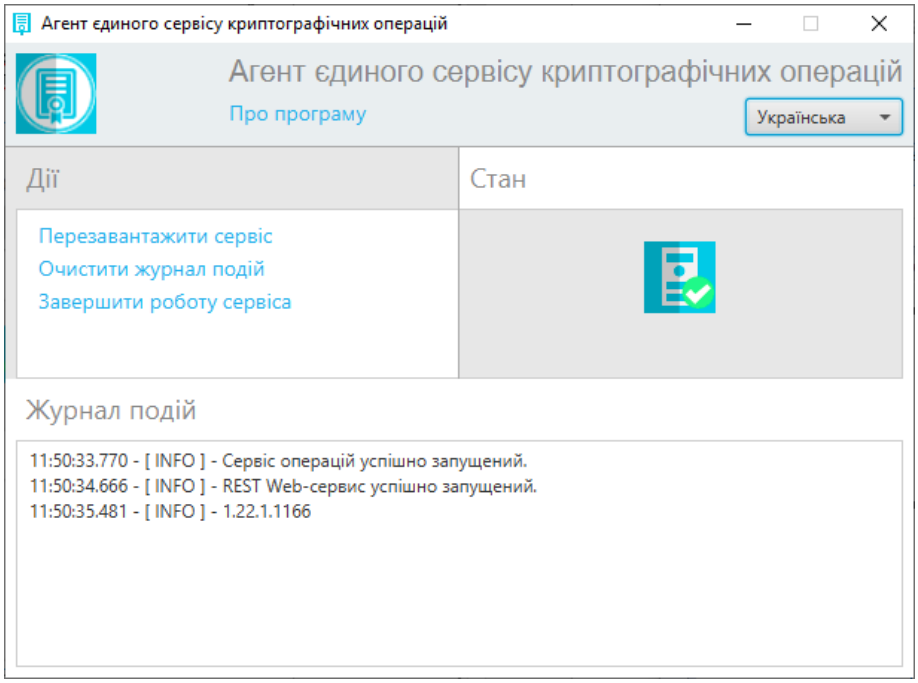

Рис. 15. Вікно «Агенту Єдиного сервісу криптографічних операцій»

4. У веб-сторінці одразу помітні зміни. Статус Агенту ЄСКО змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 16.

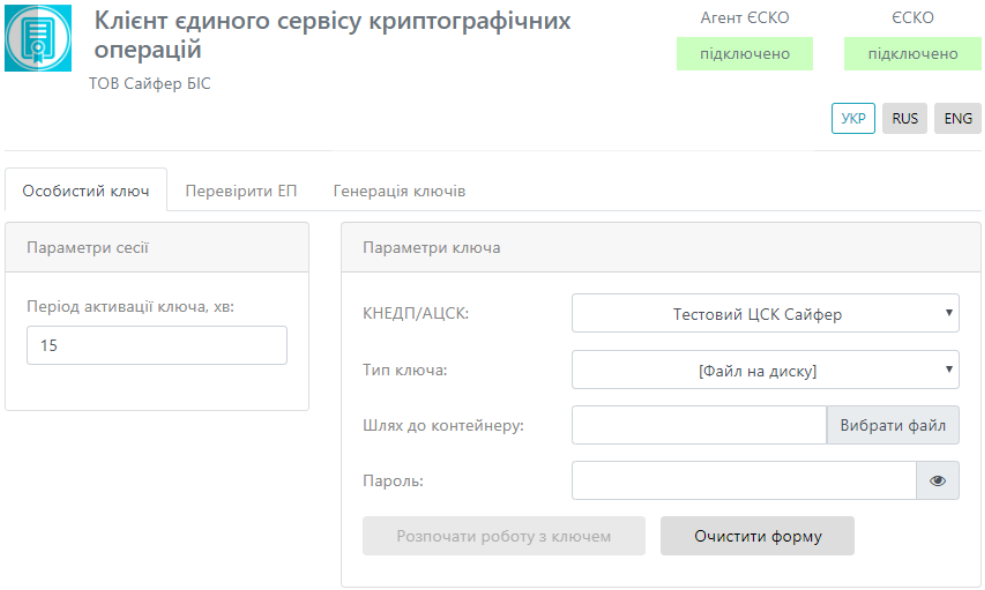

Рис. 16. Стартове вікно Агент ЄСКО

5. На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа, за замовчуванням 15 хв.
6. На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:
   1. ***АЦСК/КНЕДП***, у якому було отримано ключ;

Перелік АЦСК/КНЕДП, які підтримуються «Агентом Єдиного сервісу криптографічних операцій»:

- Тестовий ЦСК Сайфер;
- Тестовий ЦСК Сайфер (проксі);
- Тестовий ЦСК ІІТ;
- АЦСК/КНЕДП Національного банку України;
- АЦСК/КНЕДП ІДД ДФС;
- АЦСК/КНЕДП органів юстиції України;
- АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- АЦСК/КНЕДП ПАТ «КБ «Приватбанк»;
- АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- АЦСК/КНЕДП Збройних Сил;
- АЦСК/КНЕДП Міністерства внутрішніх справ України;
- АЦСК/КНЕДП Державної прикордонної служби;
- АЦСК/КНЕДП Укрзалізниці;
- АЦСК/КНЕДП ринку електричної енергії;
- АЦСК/КНЕДП ПАТ «Національний депозитарій України»;
- АЦСК/КНЕДП ТОВ «Ключові системи»;
- АЦСК/КНЕДП ДП «Українські спеціальні системи»;
- АЦСК/КНЕДП ПАТ «Ощадбанк»;
- АЦСК/КНЕДП Генеральної прокуратури України.

2. ***Тип ключа***:
   - файл на диску;
   - PKCS#11 пристрої – активний режим;
   - PKCS#11 пристрої – пасивний режим;
   - MobileID.
3. ***Шлях до контейнеру***;
4. ***Пароль*** до ключа чи PIN до захищеного носія, Рис. 17.

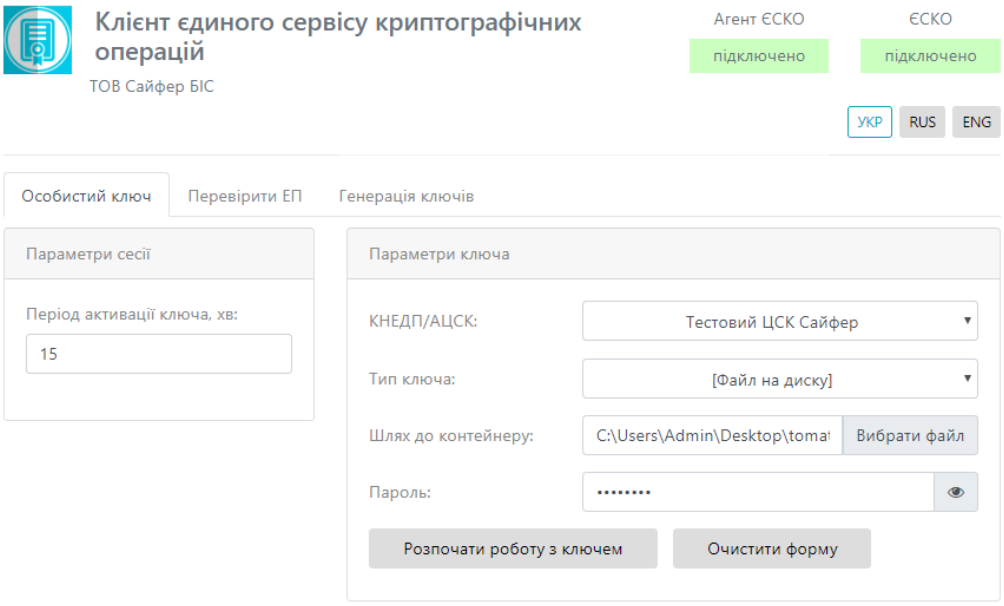

Рис. 17. Заповнення розділу «Параметри ключа»

7. Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу створюється криптографічний контекст, де відкривається робоча область, де стають доступні всі функції та операції в Агенту ЄСКО, Рис. 18.

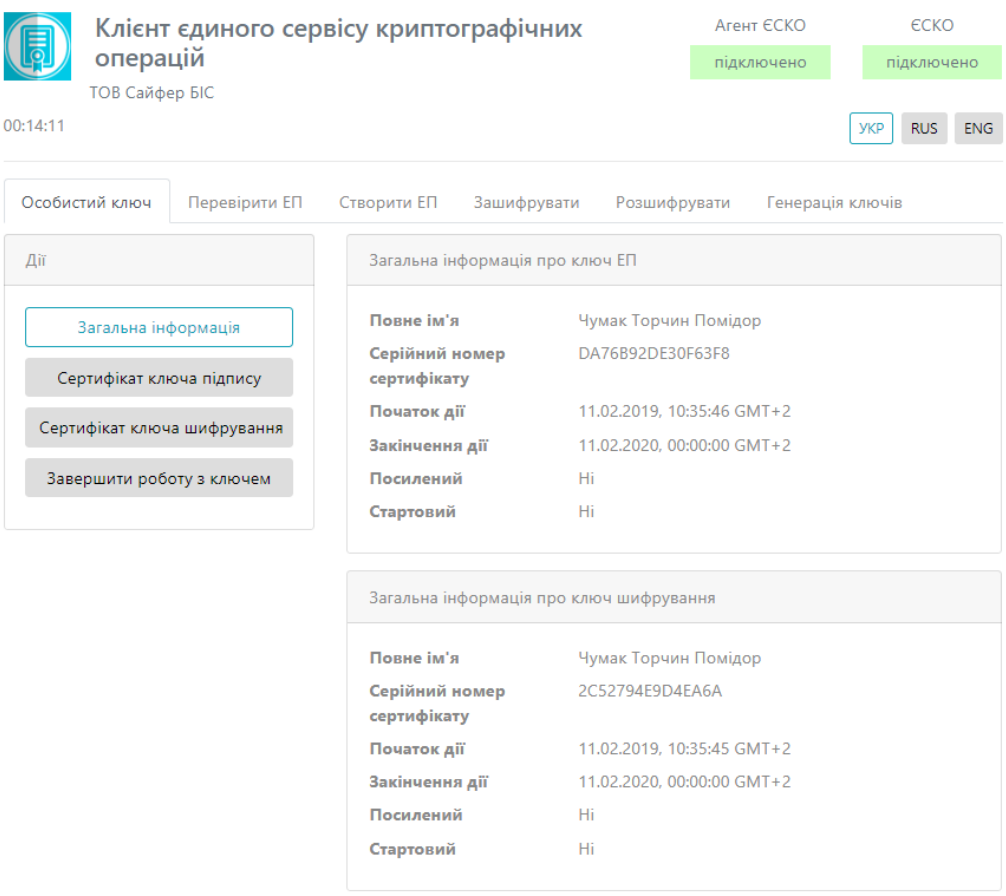

Рис. 18. Робоча область Агенту ЄСКО

Службові функції та опції ЄСКО

Після завантаження даних ключового контейнеру у вікні «Клієнту Єдиного сервісу криптографічних операцій» з'являються такі поля та відповідні опції, Рис. 19:

1. Вкладка «Особистий ключ», яка містить кнопки:
   - «Загальна інформація» - коротка інформація про ключі.
   - «Сертифікат ключа ЕП» - повна інформація про сертифікат ключа ЕП.
   - «Сертифікат ключа шифрування» - повна інформація про сертифікат ключа шифрування.
   - «Завершити роботу з ключем» - завершується сесія.
2. Вкладка «Перевірити ЕП».

На даній вкладці є можливість здійснити перевірку ЕП, доступні такі розділи:

- «Параметри перевірки ЕП» включає в себе:
  - Можна вказати Тип ЕП (Вбудована чи Відкріплена).
  - Режим перевірки електронної позначки часу для ЕП (Ігнорувати електронну позначку часу чи перевіряти електронну позначку часу, якщо вона присутня чи повертати помилку, якщо вона відсутня).
  - Режим перевірки електронної позначки часу для даних (Ігнорувати електронну позначку часу чи перевіряти електронну позначку часу, якщо вона присутня чи повертати помилку, якщо вона відсутня).
- Розширення ЕП.
- «Файл» включає в себе 2 поля, якщо:

- Тип ЕП - Відкріплена: файл для перевірки (файл на який було створено підпис) та файл з підписом (файл, який містить підпис).
- Тип ЕП – Вбудована: файл з підписом (файл який містить підпис).

- «Текстові дані» включає в себе 2 поля, якщо:
  - Кодування UTF-16LE та UTF-8.
  - Тип ЕП - Відкріплена: текстові дані для перевірки (текст на який було створено підпис) та підпис у кодуванні Base64 (текст, який містить підпис).
  - Тип ЕП – Вбудована: підпис у кодуванні Base64 (текст, який містить підпис) та дані з електронного підпису (виведення даних без підпису).

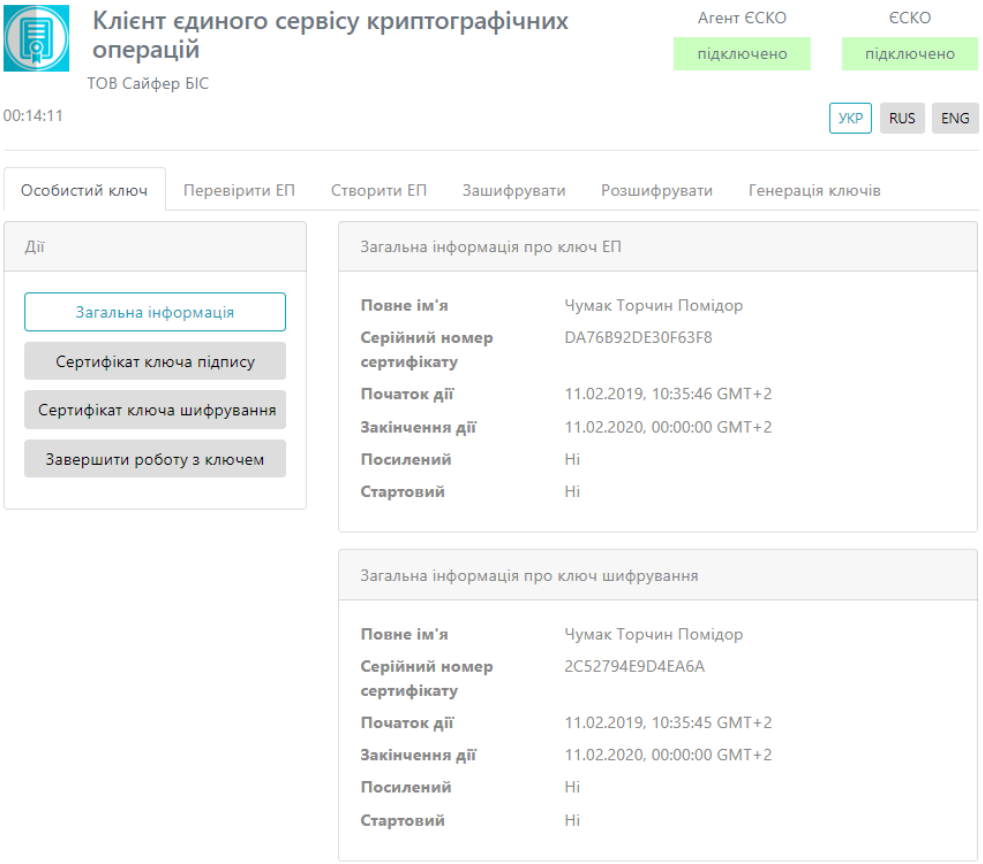

Рис. 19. Робоча область Агенту ЄСКО

3. Вкладка «Створити ЕП».

На даній вкладці є можливість здійснити створення ЕП, доступні такі розділи:

- «Параметри створення ЕП» включає в себе:
  - Тип ЕП (Вбудована чи Відкріплена), за необхідності вказати позначку «Додати підпис до вже існуючого» (таким чином, можуть підписувати один файл кілька осіб).
  - Формат ЕП (CAdES-BES чи CAdES-X Long).
- «Файл». Включає в себе 2 поля:
  - Файл/Файли для підпису (файл, який необхідно підписати).
  - Додатковий опис (назва файлу підпису).
- «Текстові дані». Включає в себе поля:
  - Кодування UTF-16LE та UTF-8.
  - Текстові дані для підпису (текст, який необхідно підписати).
  - Додатковий опис (назва тексу підпису).
  - Підпис у кодуванні Base64.

4. Вкладка «Зашифрувати».

На даній вкладці є можливість здійснити зашифрування даних, доступні такі розділи:

- «Параметри зашифрування». Слід визначитися з параметром, який слід додати при зашифруванні:
  - Сертифікат відправника та сертифікати видавців.
  - Сертифікат відправника.
  - Не додавати сертифікат відправника та сертифікати видавців.
- «Сертифікат отримувача». Поле, де слід вказати сертифікат отримувача зашифрованих даних.
- «Файл». Поле, де слід вказати файл/файли для зашифрування.
- «Текстові дані».
  - Кодування UTF-16LE та UTF-8.
  - «Текст для зашифрування». Поле, де слід вказати текст для зашифрування.
  - «Зашифровані дані у кодування Base64». Виведення зашифрованої інформації.

5. Вкладка «Розшифрувати».

На даній вкладці є можливість здійснити розшифрування даних, доступний такий розділ:

- «Файл». Слід вказати файл, який необхідно розшифрувати.
- «Текстові дані»:
  - Кодування UTF-16LE та UTF-8.
  - «Зашифровані дані у кодування Base64». Поле, де слід вказати зашифрований текст.
  - «Розшифрований текст». Виведення розшифрованої інформації.

6. Вкладка «Генерація ключів».

На даній вкладці є можливість здійснити генерацію ключів попередньо обравши відповідний профіль генерації ключів.

Профілі генерації ключів:

- Співробітник банку.
- Технолог.
- Посадова особа клієнта iFOBS.
- Клієнт iFOBS (ФОП).

Генерація ключів відбувається як файл на диску так і на захищений носій.

7. Час до кінця сесії – відлік у реальному часі до закінчення сесії (знаходиться у лівому верхньому куті).
8. Статус роботи програмного комплексу «Агенту ЄСКО» - знаходиться у правій верхній частині вікна. За допомогою «Агент ЄСКО» є можливість працювати не лише із файлами на диску, але із захищеними носіями.

Можливі статуси «Агенту ЄСКО»:

- «Запустити». Для початку роботи із «Агентом ЄСКО», необхідно натиснути дану кнопку та для подальшої роботи слід відкрити іншу інструкцію «Агент Єдиного сервісу криптографічних операцій. Настанова з установки та експлуатації».
- «Підключено». Працює у звичайному режимі.
- «Відключено». Слід звернутися до системного адміністратора.

9. Статус роботи програмного комплексу «ЄСКО» - знаходиться у правій верхній частині вікна.

Можливі статуси ЄСКО:

- «Підключено». Працює у звичайному режимі.
- «Відключено». Слід звернутися до системного адміністратора.

10. Зміна мови - знаходиться у правій верхній частині вікна можна змінити мову веб-інтерфейсу ЄСКО. Доступні мови: українська, російська та англійська.

Основна форма «Агенту Єдиного сервісу криптографічних операцій» містить такі поля та відповідні опції, Рис. 20.

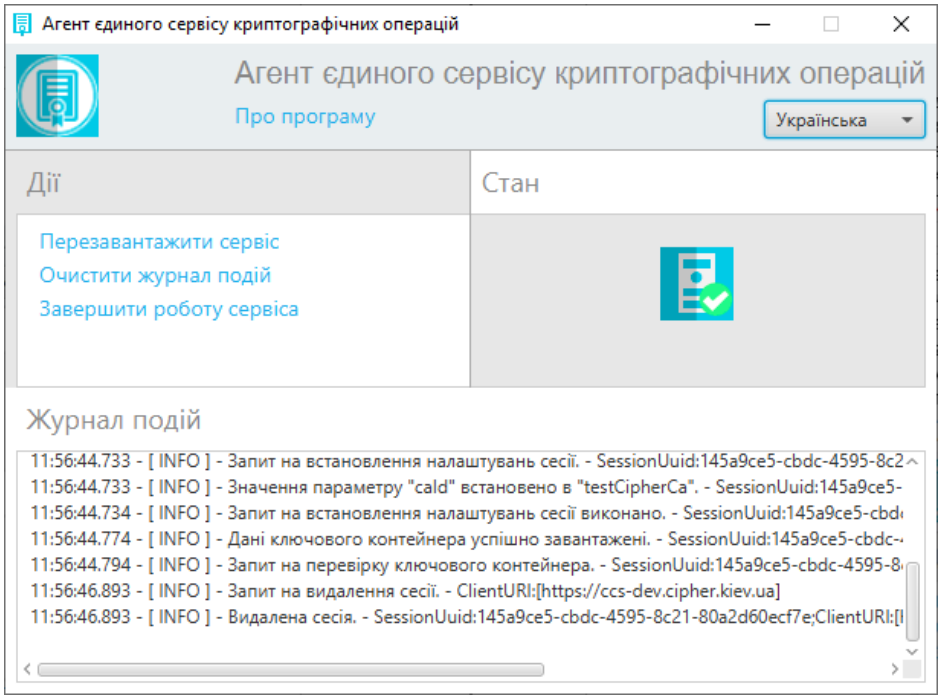

Рис. 20. Агент Єдиного сервісу криптографічних операцій

1. Даний розділ містить:
   - назву Програмного комплексу.
   - гіперпосилання «Про програму», яке відкриває нове вікно з інформацією про розробників, версію продукту, Рис. 21.
   - Випадаючий список зі зміною мови, доступні мови: Українська, Англійська, Російська.

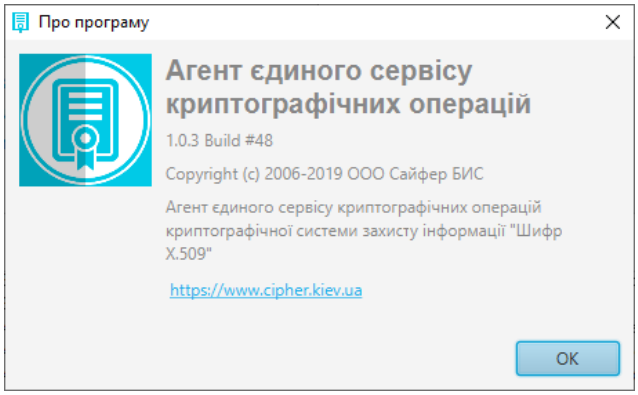

Рис. 21. Вікно «Про програму»

2. Розділ «Дії» містить гіперпосилання:
   - «Перезавантажити сервіс».
   - «Очистити журнал подій».
   - «Завершити роботу сервісу».
3. Розділ «Стан» містить інформацію про стан роботи сервісу, що він працює.

4. Розділ «Журнал подій» містить повну інформацію про дії, які виконуються у веб-браузері, під час роботи з Агентом ЄСКО.

Вибір ключа ЕП – файл

Відеоінструкція знаходиться за посиланням.

1. Стартове вікно Клієнту Єдиного сервісу криптографічних операцій у веб-браузері показано на Рис. 22.

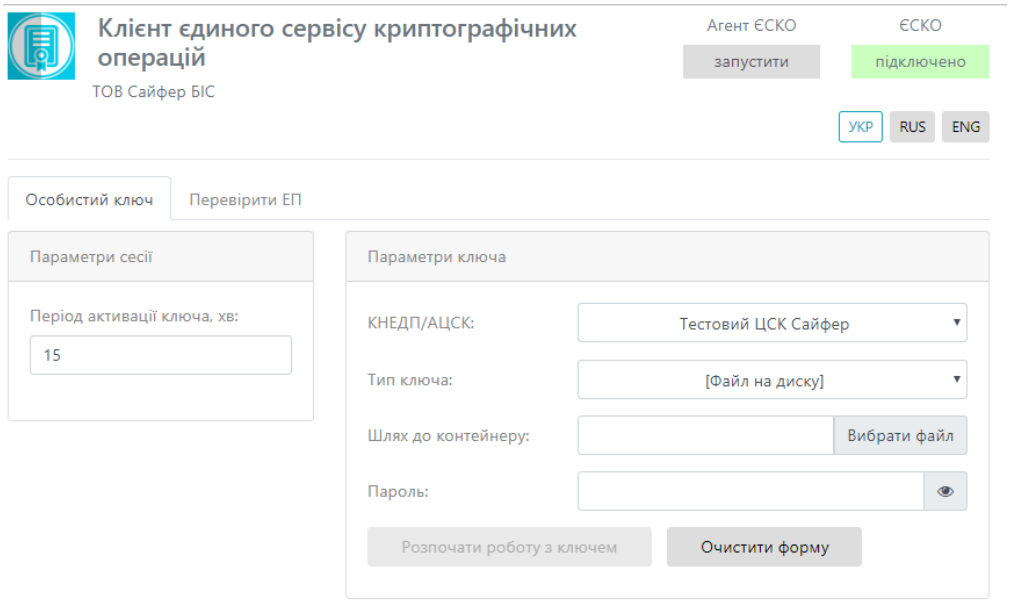

Рис. 22. Стартове вікно ЄСКО

2. Наступним кроком слід відкрити Агент ЄСКО, натиснувши у правому верхньому куті під написом Агент ЄСКО кнопку «запустити», Рис. 23.

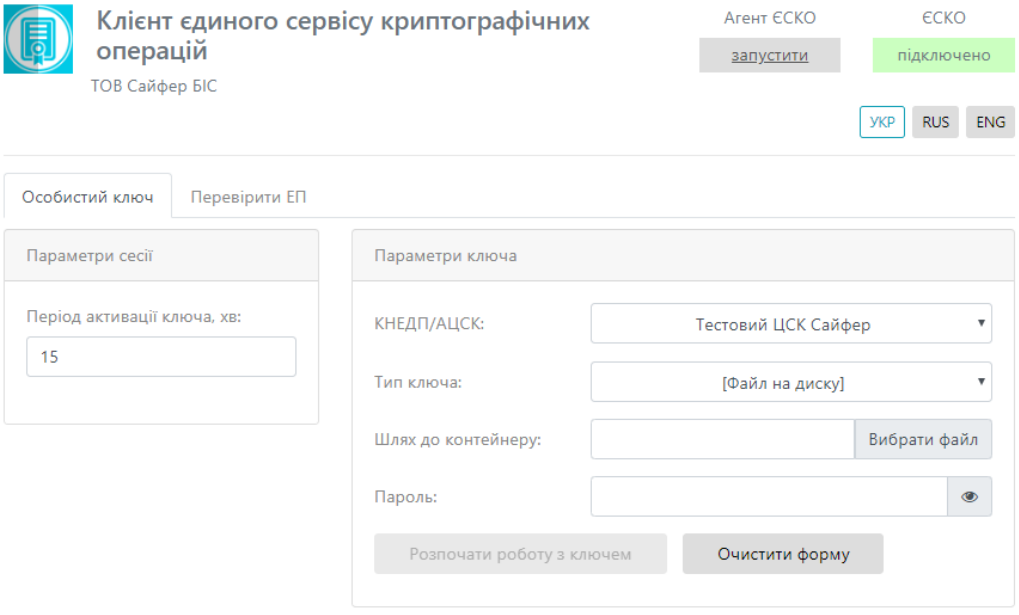

Рис. 23. Запуск Агенту ЄСКО

3. Далі відкривається вікно Агенту Єдиного сервісу криптографічних операцій, його слід згорнути та повернутися до веб-браузера, Рис. 24.

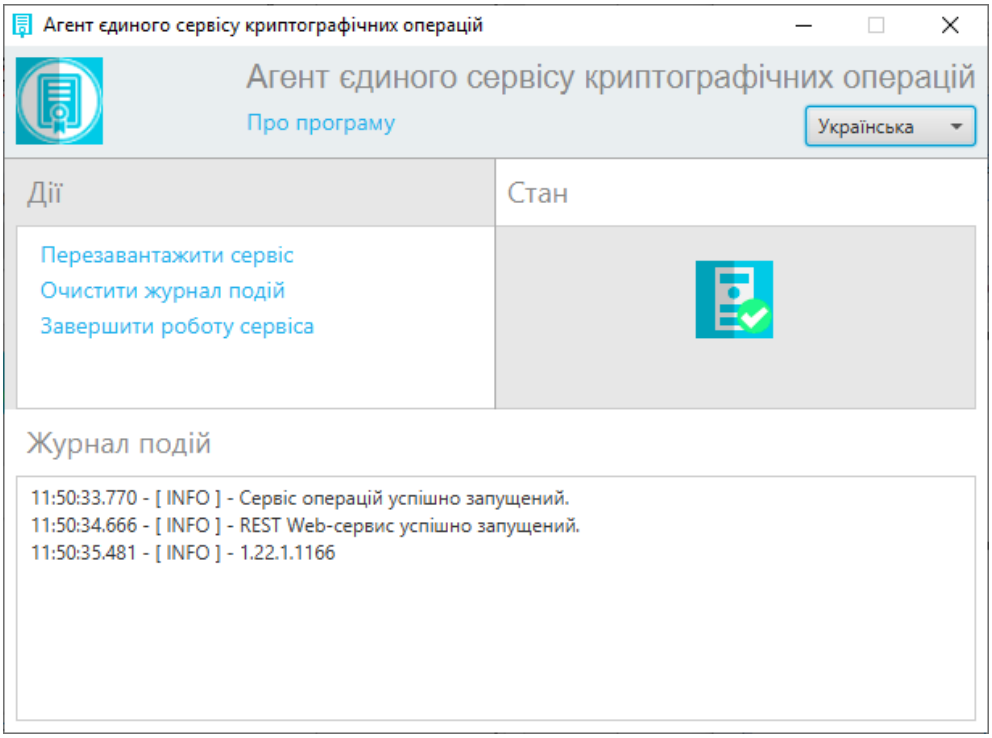

Рис. 24. Агент Єдиного сервісу криптографічних операцій

4. У веб-сторінці одразу помітні зміни. Статус Агенту ЄСКО змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 25.

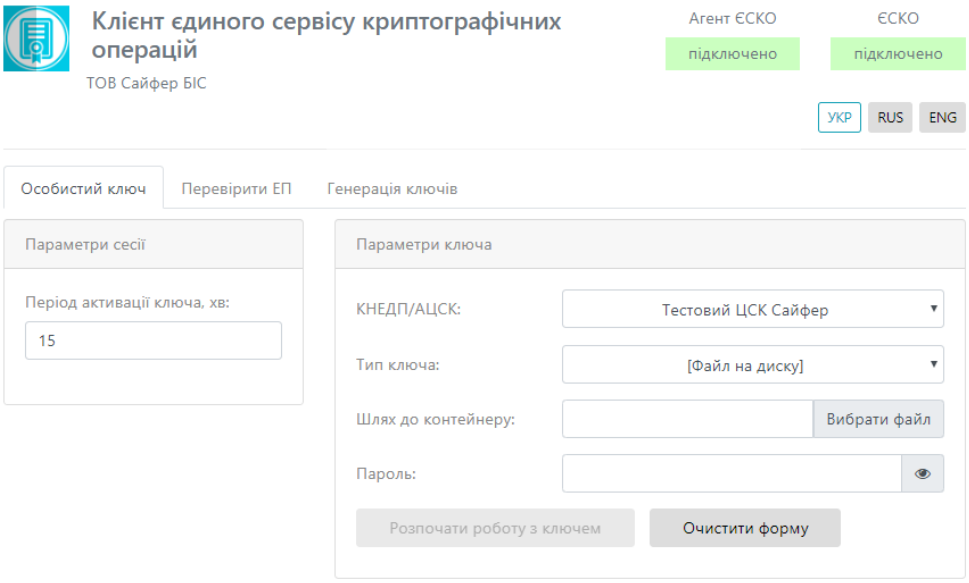

Рис. 25. Стартове вікно Агент ЄСКО

5. На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа, за замовчуванням 15 хв.
6. На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:
   1. ***АЦСК/КНЕДП***, у якому було отримано ключ;

Перелік АЦСК/КНЕДП, які підтримуються «Агентом Єдиного сервісу криптографічних операцій»:

- Тестовий ЦСК Сайфер;
- Тестовий ЦСК Сайфер (проксі);
- Тестовий ЦСК ІІТ;
- АЦСК/КНЕДП Національного банку України;
- АЦСК/КНЕДП ІДД ДФС;
- АЦСК/КНЕДП органів юстиції України;
- АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- АЦСК/КНЕДП ПАТ «КБ «Приватбанк»;
- АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- АЦСК/КНЕДП Збройних Сил;
- АЦСК/КНЕДП Міністерства внутрішніх справ України;
- АЦСК/КНЕДП Державної прикордонної служби;
- АЦСК/КНЕДП Укрзалізниці;
- АЦСК/КНЕДП ринку електричної енергії;
- АЦСК/КНЕДП ПАТ «Національний депозитарій України»;
- АЦСК/КНЕДП ТОВ «Ключові системи»;
- АЦСК/КНЕДП ДП «Українські спеціальні системи»;
- АЦСК/КНЕДП ПАТ «Ощадбанк»;
- АЦСК/КНЕДП Генеральної прокуратури України.

2. ***Тип ключа***:
   - файл на диску;
   - PKCS#11 пристрої – активний режим;
   - PKCS#11 пристрої – пасивний режим;
   - MobileID.
3. ***Шлях до контейнеру***;
4. ***Пароль*** до ключа, Рис. 26.

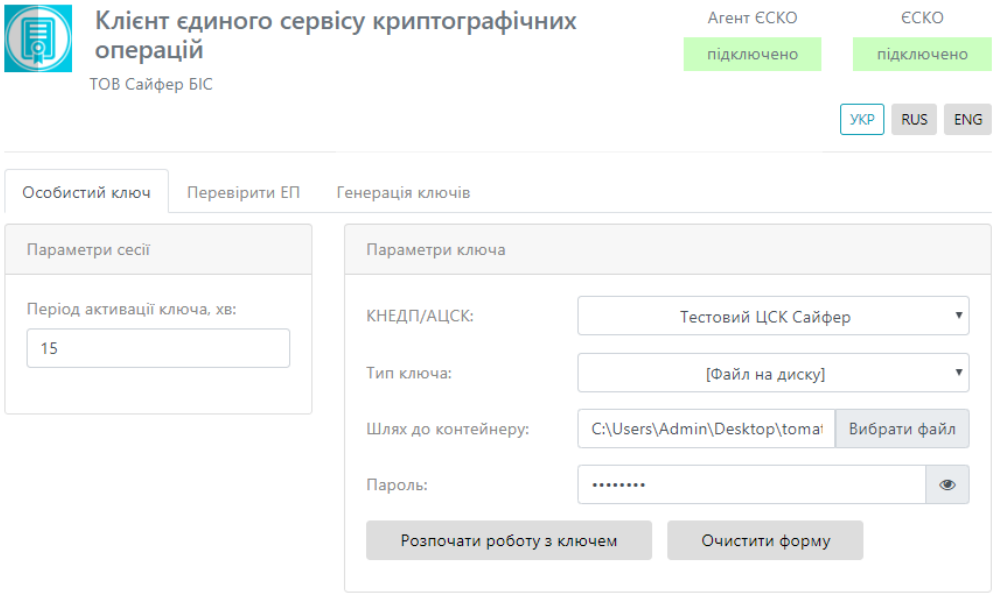

Рис. 26. Заповнення розділу «Параметри ключа»

7. Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу створюється криптографічний контекст, де відкривається робоча область, де стають доступні всі функції та операції в Агенту ЄСКО, Рис. 27.

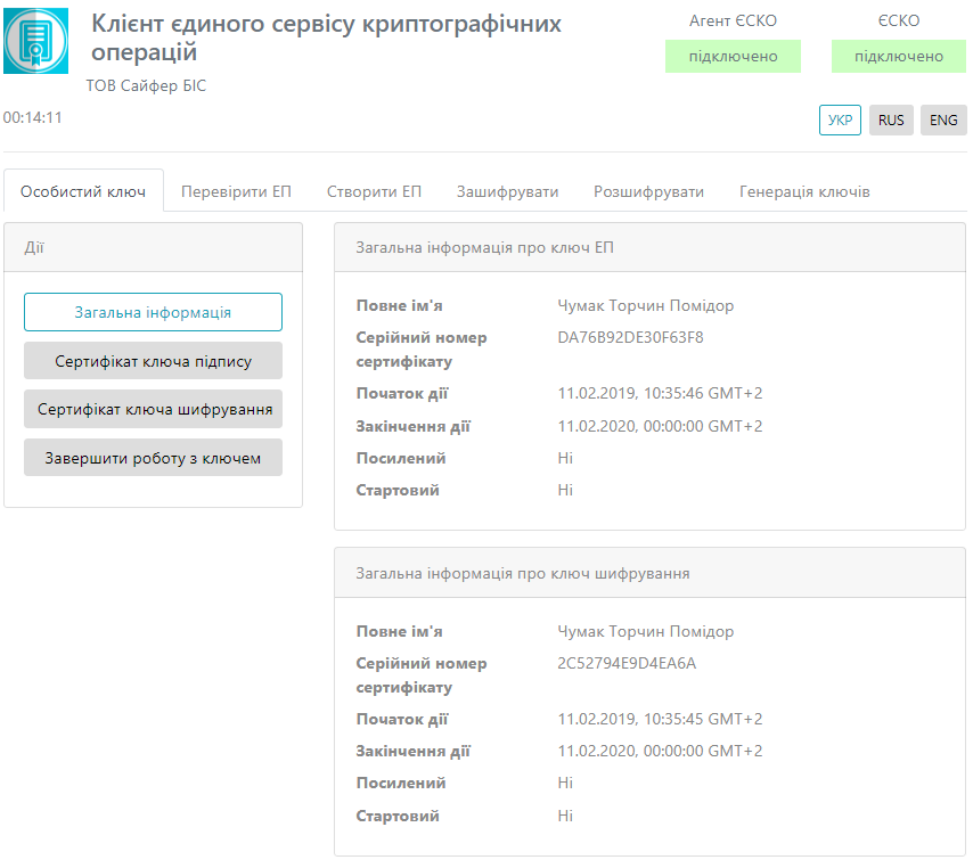

Рис. 27. Робоча область Агенту ЄСКО

Вибір ключа ЕП – захищений носій

Відеоінструкція знаходиться за посиланням.

1. Стартове вікно Клієнта Єдиного сервісу криптографічних операцій у веб-браузері показано на Рис. 28.

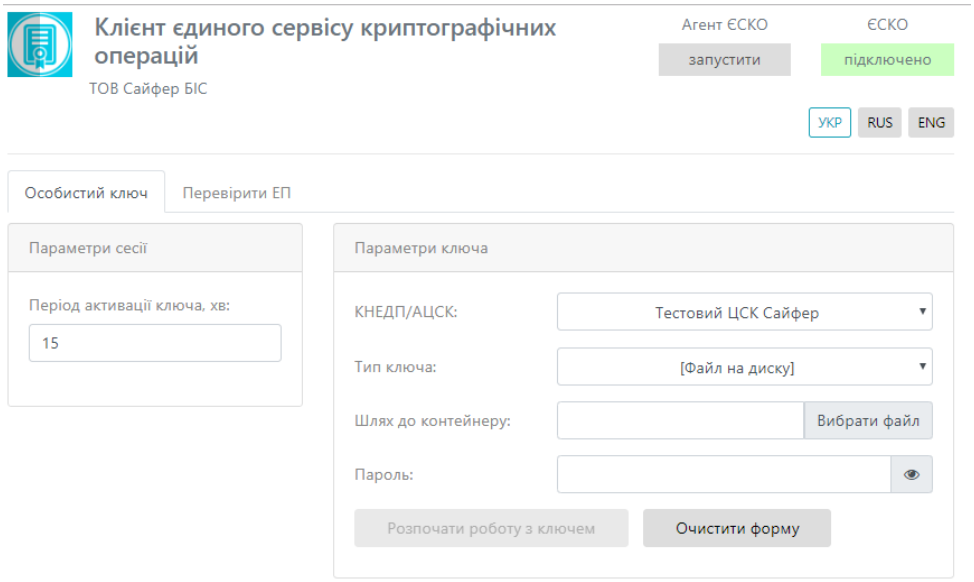

Рис. 28. Стартове вікно ЄСКО

2. Наступним кроком слід відкрити Агент ЄСКО, натиснувши у правому верхньому куті під написом Агент ЄСКО кнопку «запустити», Рис. 29.

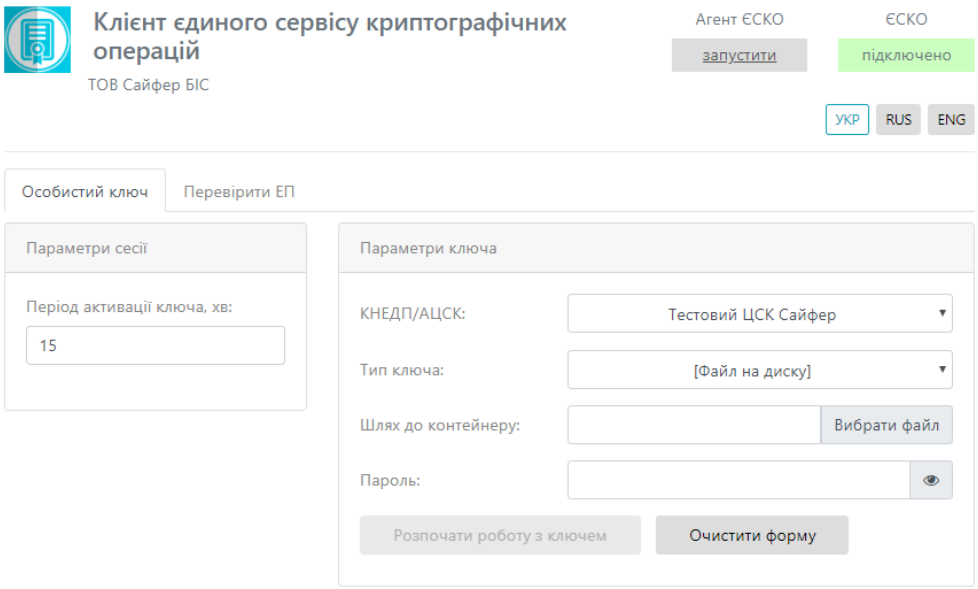

Рис. 29. Запуск Агенту ЄСКО

3. Далі відкривається вікно Агенту Єдиного сервісу криптографічних операцій, його слід згорнути та повернутися до веб-браузера, Рис. 30.

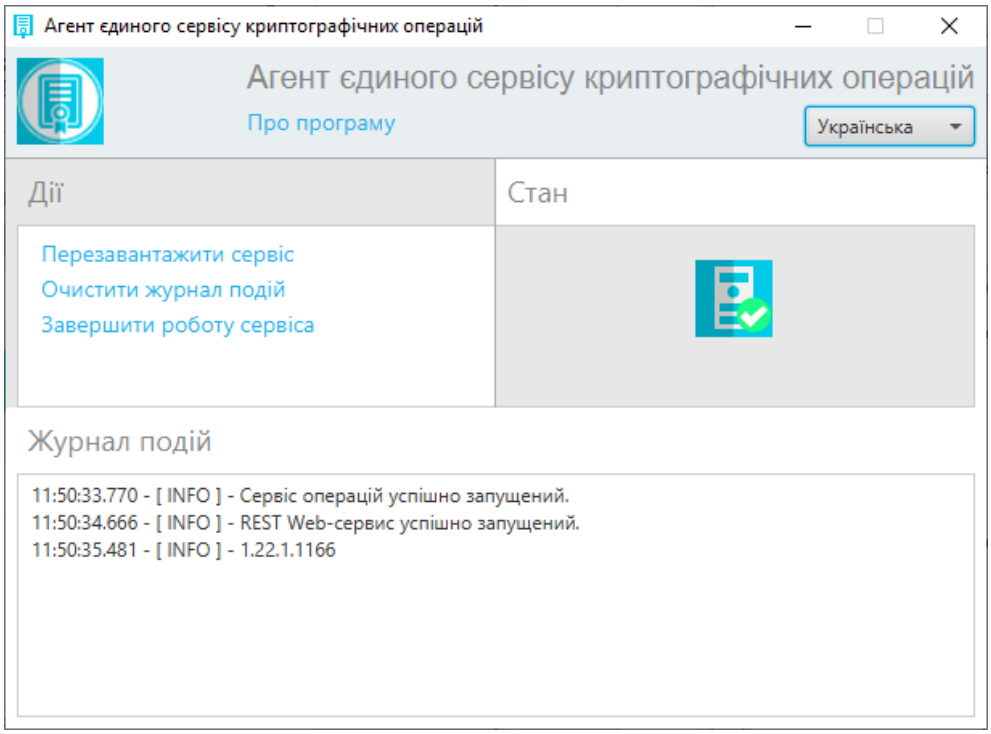

Рис. 30. Агент Єдиного сервісу криптографічних операцій

4. У веб-сторінці одразу помітні зміни. Статус Агенту ЄСКО змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 31.

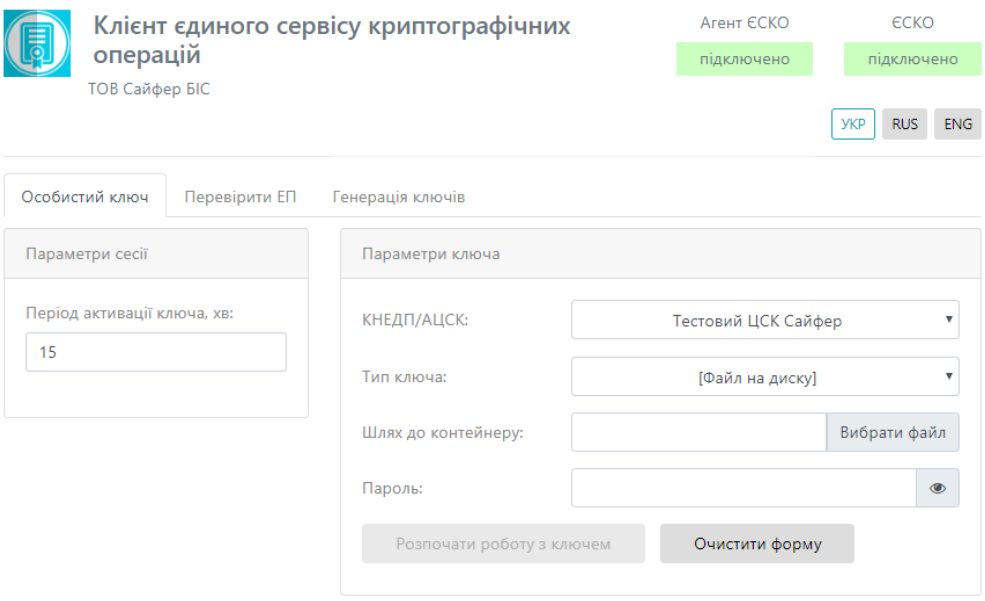

Рис. 31. Стартове вікно Агент ЄСКО

5. На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа, за замовчуванням 15 хв.
6. На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:
   1. ***АЦСК/КНЕДП***, у якому було отримано ключ;

Перелік АЦСК/КНЕДП, які підтримуються «Агентом Єдиного сервісу криптографічних операцій»:

- Тестовий ЦСК Сайфер;
- Тестовий ЦСК Сайфер (проксі);
- Тестовий ЦСК ІІТ;
- АЦСК/КНЕДП Національного банку України;
- АЦСК/КНЕДП ІДД ДФС;
- АЦСК/КНЕДП органів юстиції України;
- АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- АЦСК/КНЕДП ПАТ «КБ «Приватбанк»;
- АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- АЦСК/КНЕДП Збройних Сил;
- АЦСК/КНЕДП Міністерства внутрішніх справ України;
- АЦСК/КНЕДП Державної прикордонної служби;
- АЦСК/КНЕДП Укрзалізниці;
- АЦСК/КНЕДП ринку електричної енергії;
- АЦСК/КНЕДП ПАТ «Національний депозитарій України»;
- АЦСК/КНЕДП ТОВ «Ключові системи»;
- АЦСК/КНЕДП ДП «Українські спеціальні системи»;
- АЦСК/КНЕДП ПАТ «Ощадбанк»;
- АЦСК/КНЕДП Генеральної прокуратури України.

   2. ***Тип ключа***:
      - файл на диску;
      - PKCS#11 пристрої – активний режим;
      - PKCS#11 пристрої – пасивний режим;
      - MobileID.
   3. **Шлях до контейнеру**, Рис. 32;

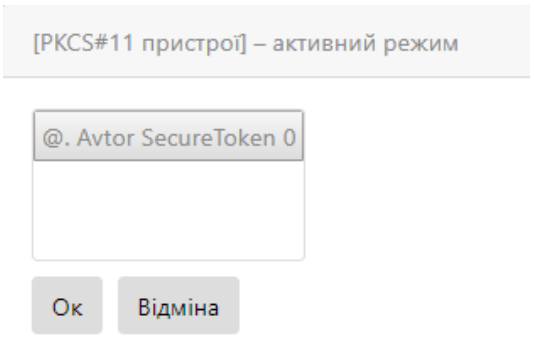

Рис. 32. Вказівка «Шлях до контейнера»

4. ***PIN*** до захищеного носія, Рис. 33.

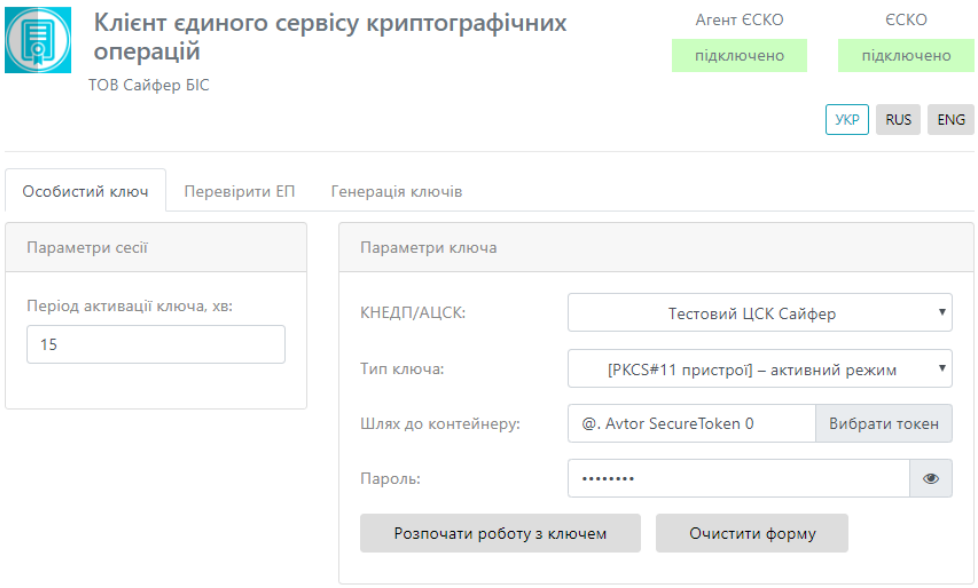

Рис. 33. Форма «Агент ЄСКО»

7. Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу створюється криптографічний контекст, де відкривається робоча область, де стають доступні всі функції та операції в Агенту ЄСКО, Рис. 34.

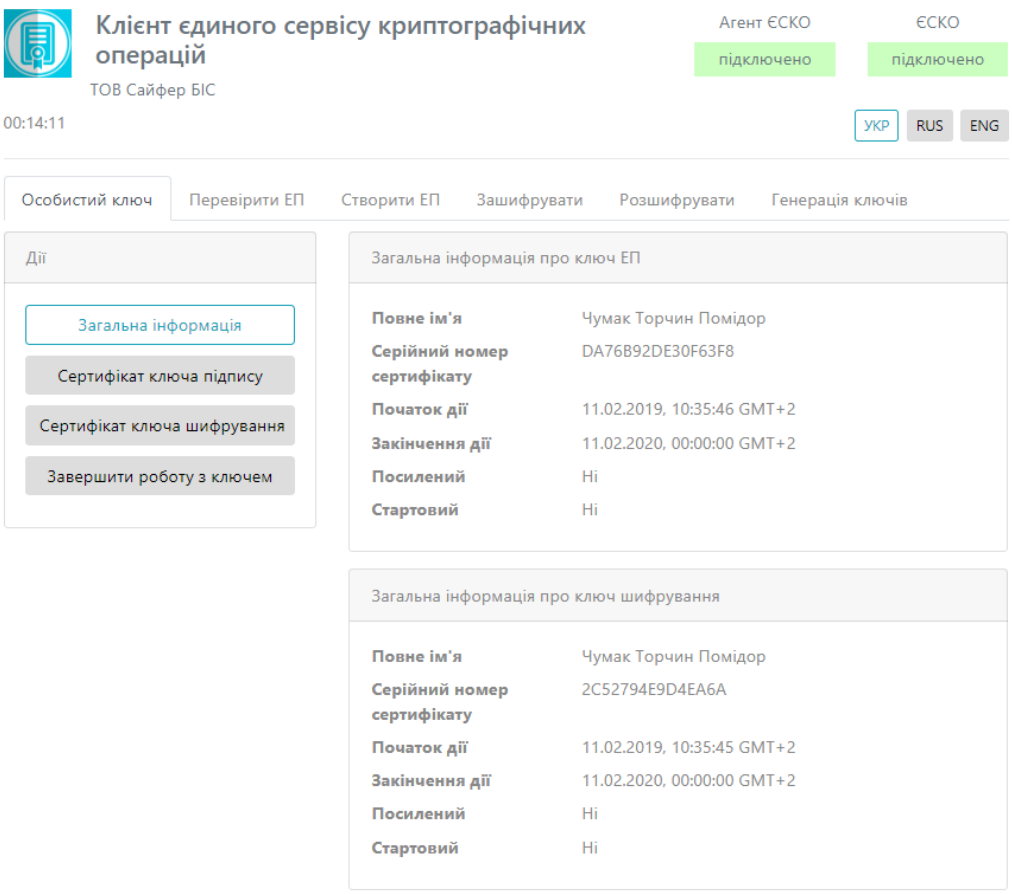

Рис. 34. Робоча область Агенту ЄСКО

Створення ЕП

Вкладка «Створення ЕП» містить розділи: Параметри створення ЕП, Текстові дані та Файл, Рис. 35.

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

1. Поле «Тип ЕП», яке містить:
   - Вбудована;
   - Відкріплена;
   - Додати підпис до вже існуючого (накладається підпис на файл, на який вже попередньо накладено ЕП).
2. Поле «Формат ЕП», яке містить:
   - CAdES-BES. Або «Базова ЕП» використовується для автентифікації підписанта та перевірки цілісності електронного документа в період чинності сертифіката відкритого ключа (сертифікат). Формат «Базовий ЕП» не надає можливості встановити дійсність підпису у випадку, якщо ЕП перевіряється після закінчення строку чинності сертифіката або скасування сертифіката після формування ЕП;
   - CAdES-X Long. Або «ЕП з повним набором даних перевірки» 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 «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

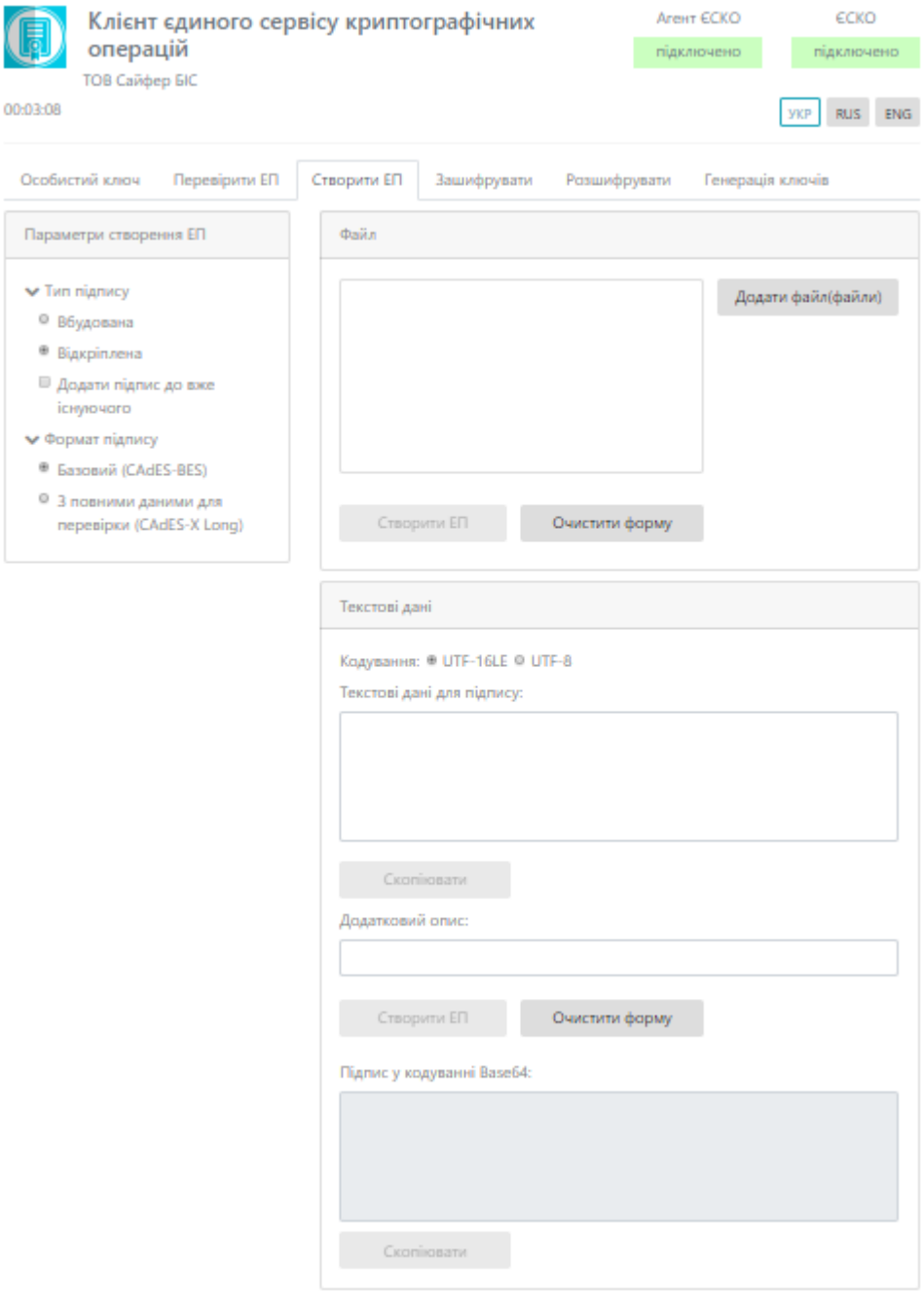

Рис. 35. Вкладка «Створення ЕП»

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

- Кодування UTF-16LE та UTF-8.
- Текстові дані для підпису (у поле слід внести текстові дані);
- Додатковий опис (опис до текстових даних);

- Кнопка «Створити ЕП» (здійснює накладання ЕП на текстові дані, який завантажено);
- Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.
- Підпис у кодування Base64 (виведення підписаних текстових даних).

Створення ЕП за типом «Вбудована» на файл

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Вбудована» та Формат ЕП (CAdES-BES чи CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 36. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об'єм всіх файлів не повинен перевищувати 100Мб.

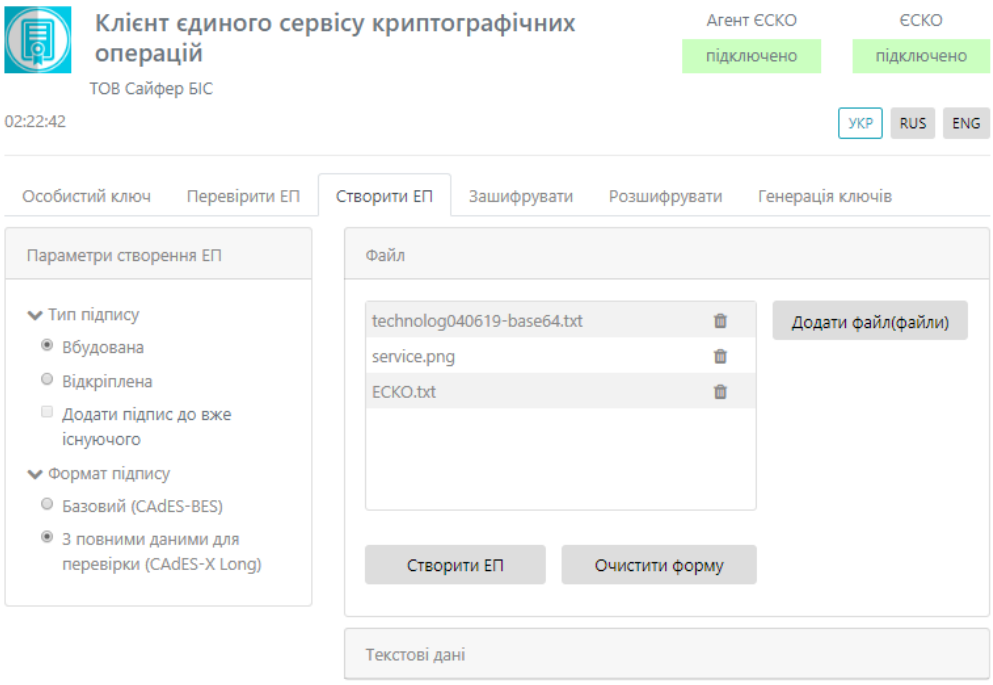

Рис. 36. Створення ЕП

Після натискання на кнопку «Створити ЕП» з'являється вікно із запитом дозволу на використання ЕП, для того, щоб дати дозвіл необхідно натиснути «ОК», Рис. 37. Якщо натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена.

Після натискання кнопки «ОК» з'являється вікно про успішне створення електронного підпису, Рис. 38.

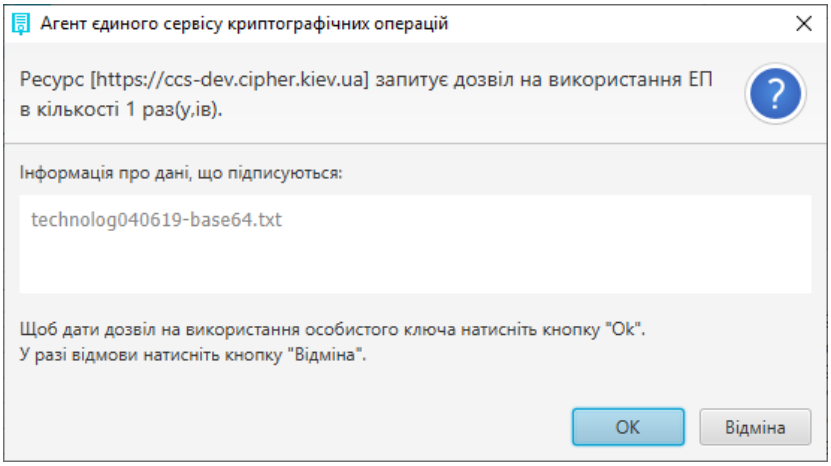

Рис. 37. Дозвіл на використання ЕП

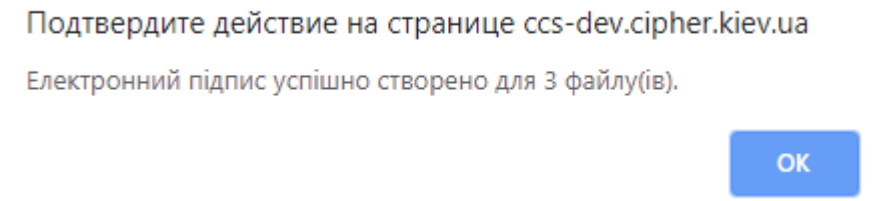

Рис. 38. Повідомлення про створення електронного підпису

Далі зберігається файл з підписом за допомогою кнопки «стрілки вниз», яка з'являється біля кожного файлу на який накладено підпис, Рис. 39.

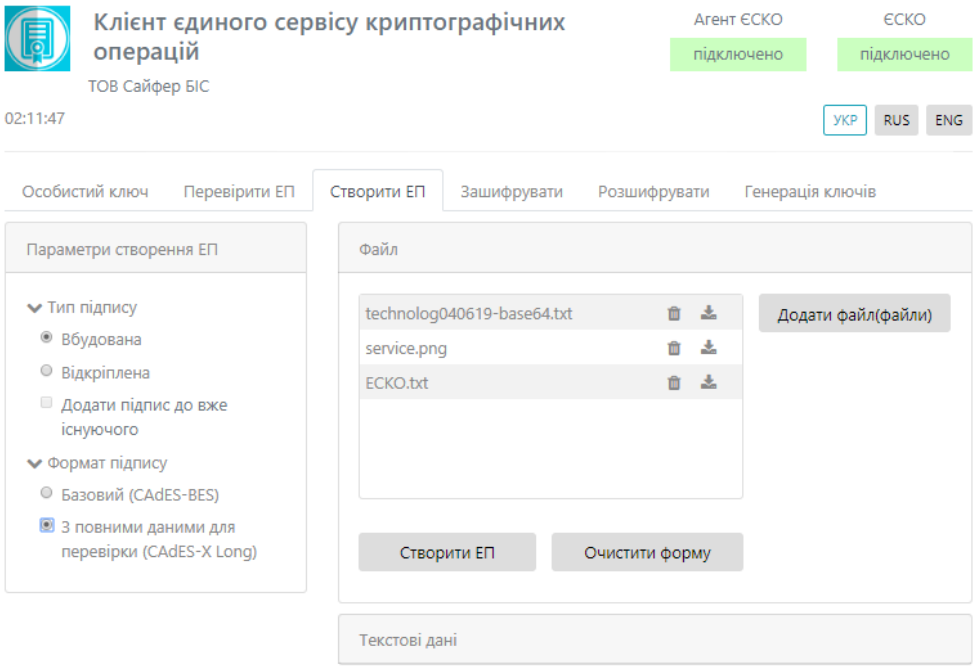

Рис. 39. Збереження підпису у файл

За необхідності вказуємо шлях для збереження та очищаємо форму, Рис. 40.

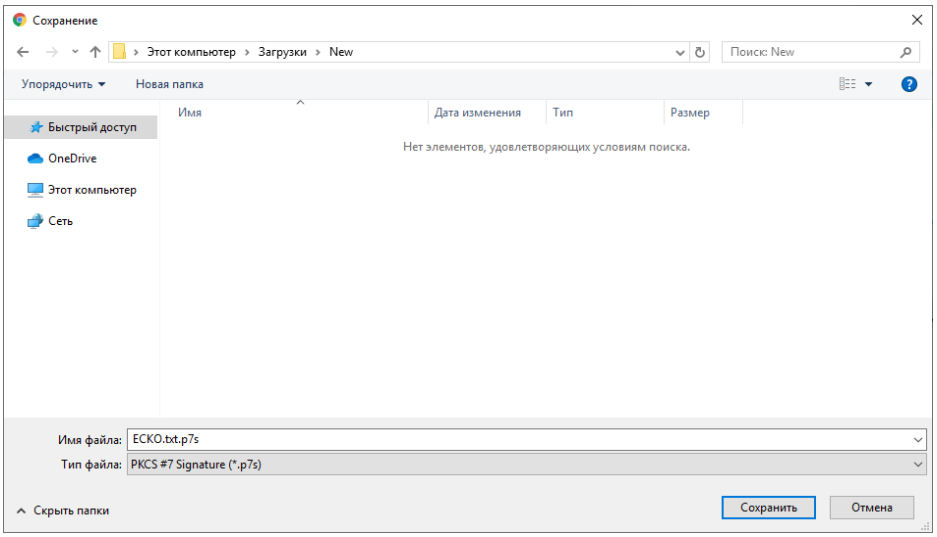

Рис. 40. Збереження файлу

Створення ЕП за типом «Відкріплена» на файл

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Відкріплена» та Формат ЕП (CAdES-BES чи CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 41. За необхідності можна змінити файл. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об’єм всіх файлів не повинен перевищувати 100Мб.

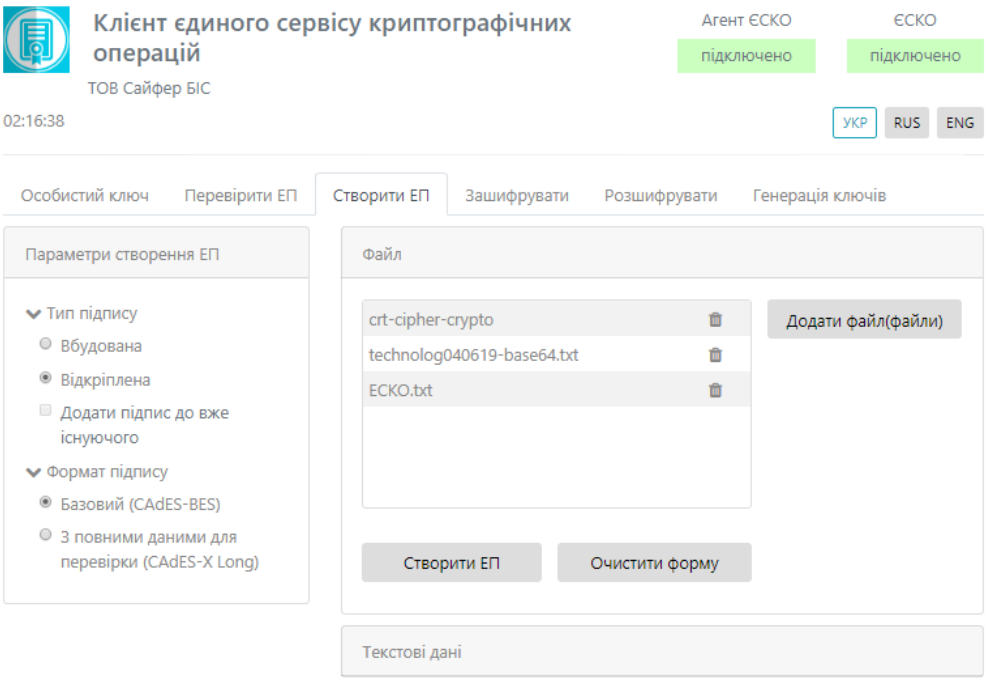

Рис. 41. Створення ЕП

Після натискання на кнопку «Створити ЕП» з’являється вікно із запитом дозволу на використання ЕП, для того, щоб дати дозвіл необхідно натиснути «ОК», Рис. 42. Якщо натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена.

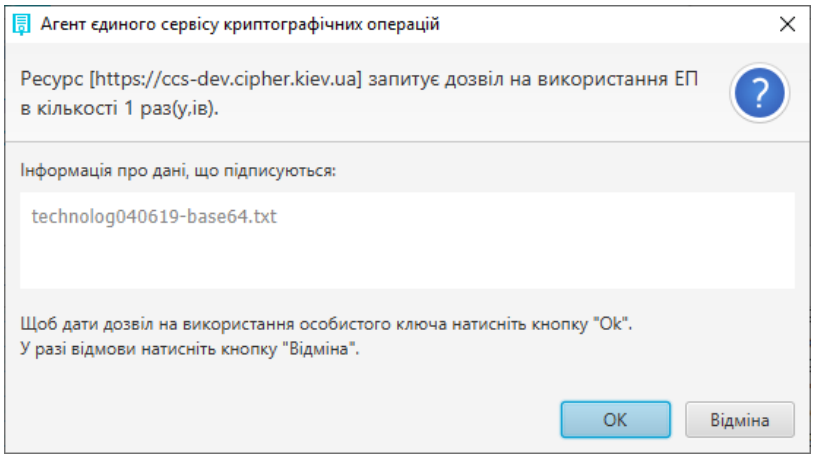

Рис. 42. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з'являється вікно про успішне створення електронного підпису, Рис. 43.

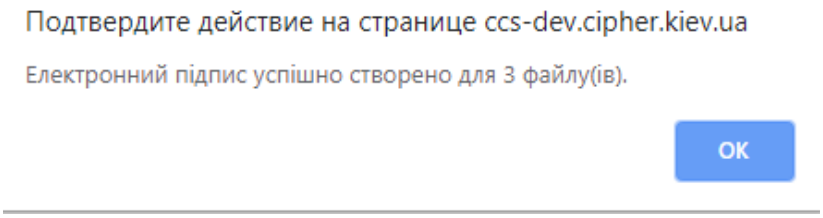

Рис. 43. Повідомлення про створення електронного підпису

Далі зберігається файл з підписом за допомогою кнопки «стрілки вниз», яка з'являється біля кожного файлу на який накладено підпис, Рис. 44.

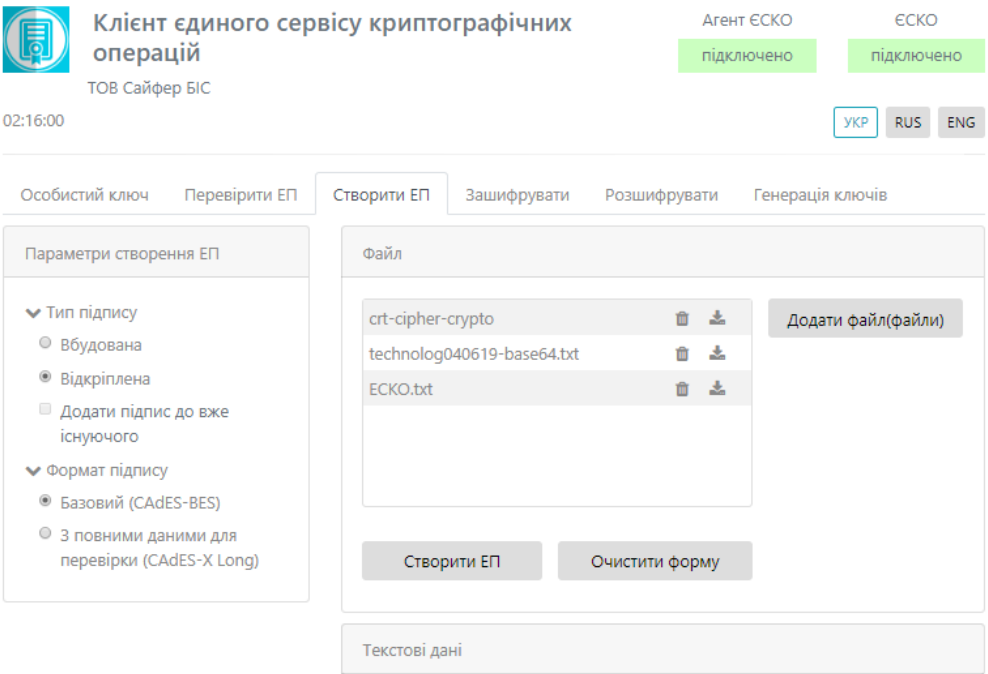

Рис. 44. Збереження підпису у файл

Далі обираємо шлях збереження файлу та очищаємо форму, Рис. 45.

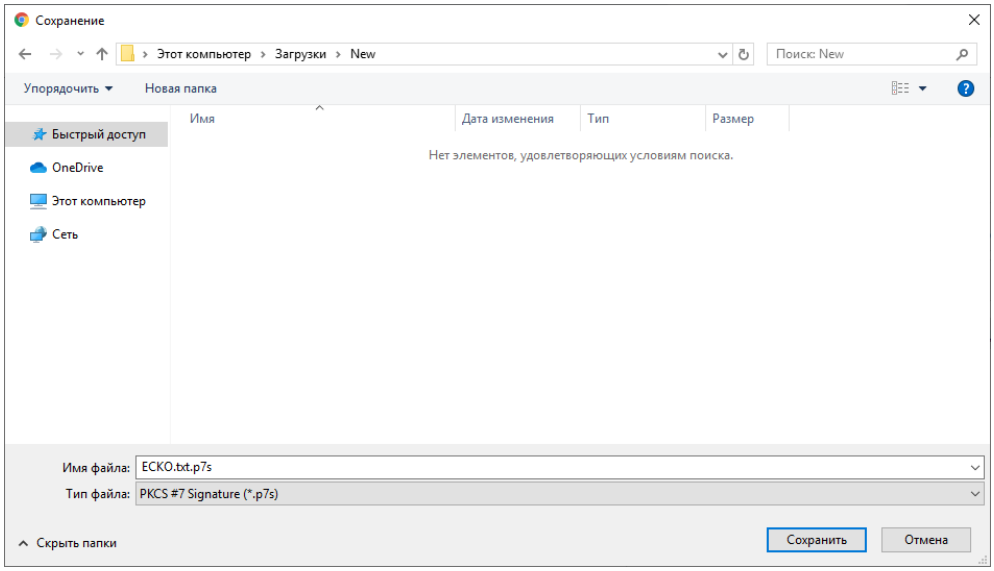

Рис. 45. Збереження файлу

Створення ЕП за типом «Вбудована» на текстові дані

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Вбудована» та Формат ЕП (CAdES-BES чи CAdES-X Long), тип кодування, вказується текст для підпису, натискаємо кнопку «Створити ЕП», Рис. 46.

Після натискання на кнопку «Створити ЕП» з’являється вікно із запитом дозволу на використання ЕП, для кожного файлу, який було додано для накладення підпису, щоб дати дозвіл необхідно натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена, Рис. 47.

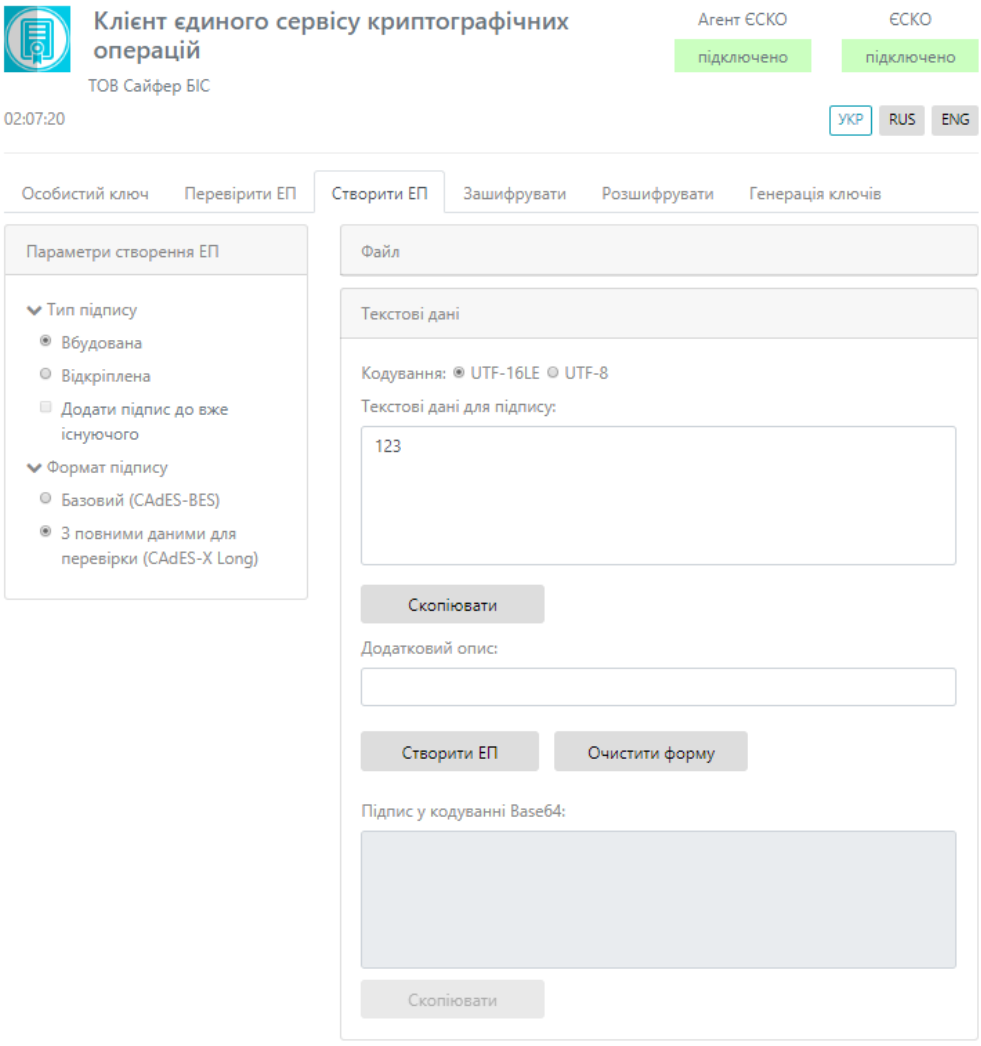

Рис. 46. Створення ЕП

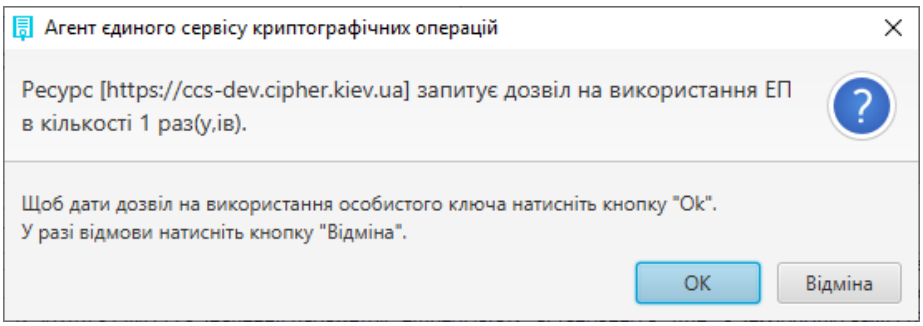

Рис. 47. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з’являється вікно про успішне створення електронного підпису, Рис. 48.

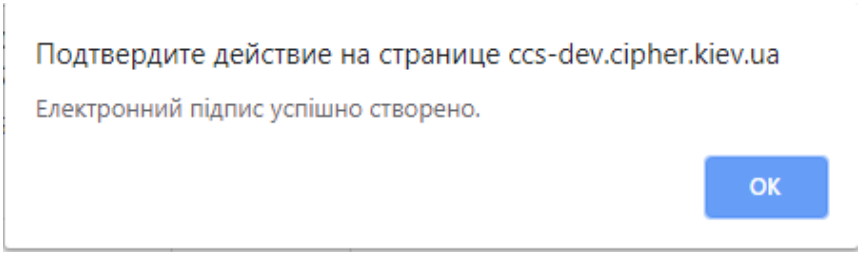

Рис. 48. Повідомлення про створення електронного підпису

Далі у полі «Підпис у кодуванні Base64» з'являється текст з підписом, Рис. 49, далі за необхідності очищаємо форму.

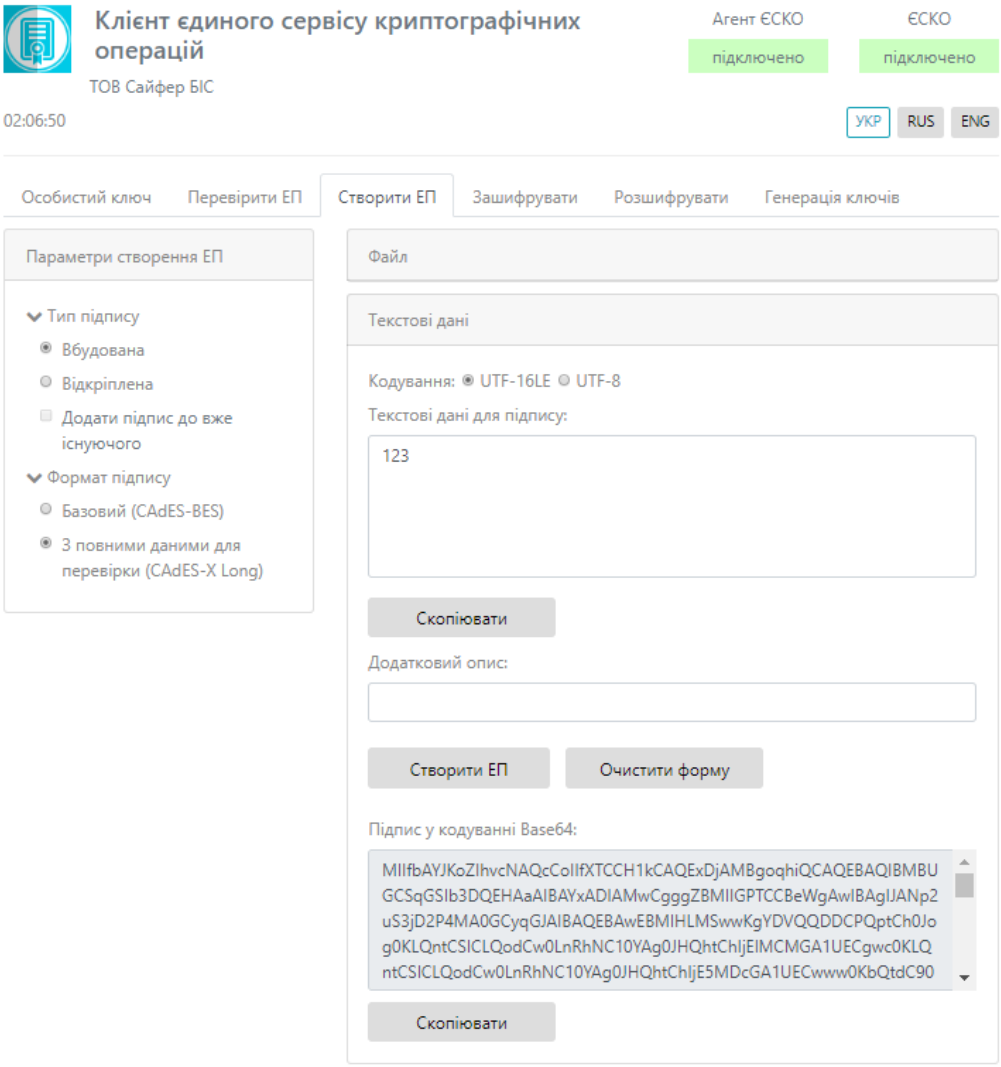

Рис. 49. Результат підпису тестових даних

Створення ЕП за типом «Відкріплена» на текстові дані

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Відкріплена» та Формат ЕП (CAdES-BES чи CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 50.

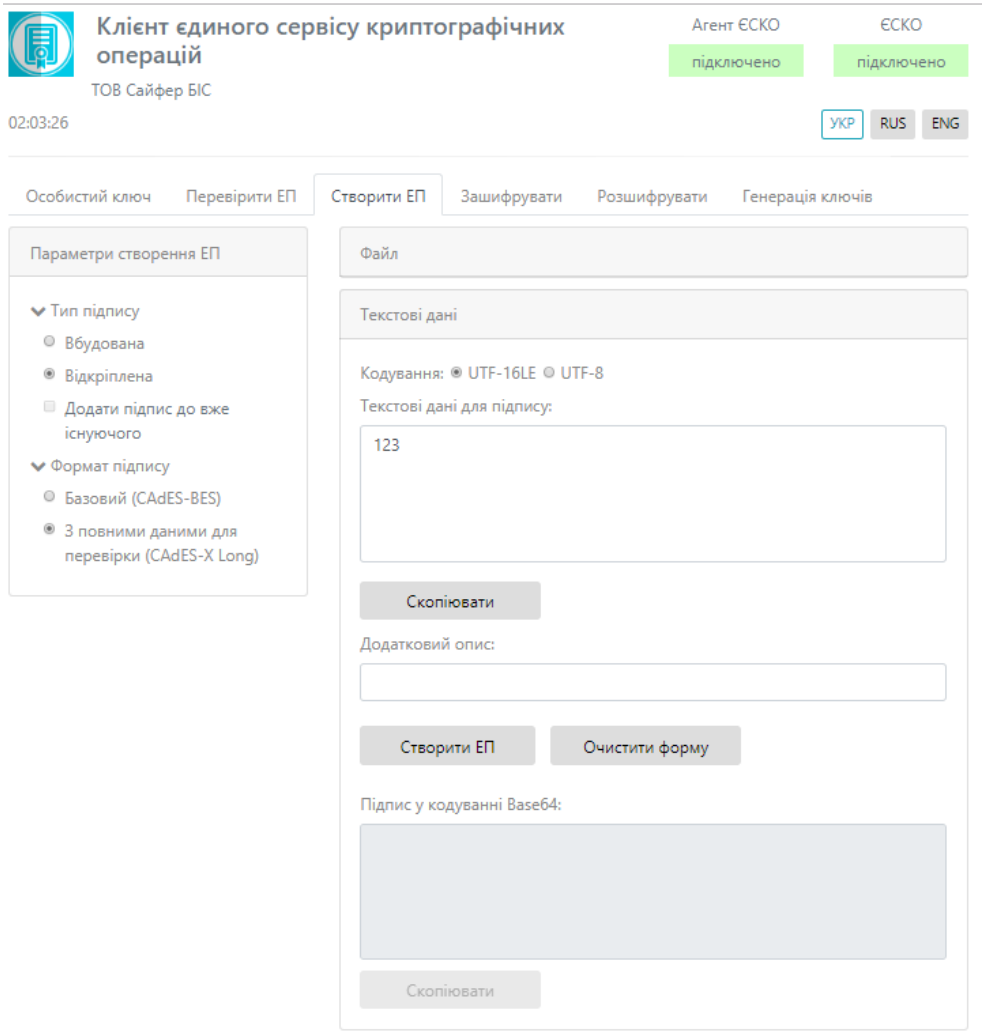

Рис. 50. Створення ЕП

Після натискання на кнопку «Створити ЕП» з'являється вікно із запитом дозволу на використання ЕП, для кожного файлу, який було додано для накладення підпису, щоб дати дозвіл необхідно натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена, Рис. 51.

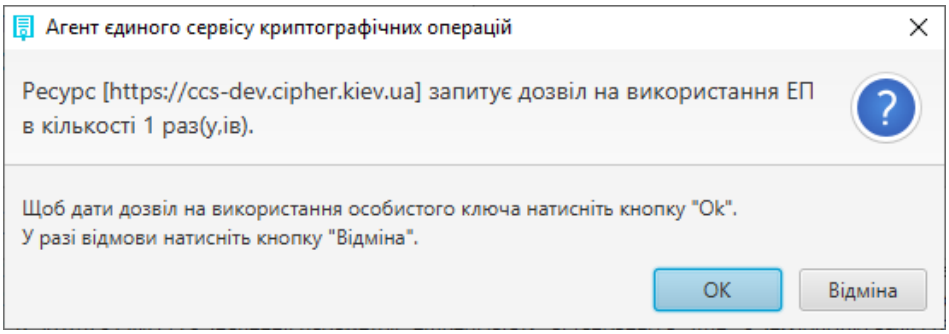

Рис. 51. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з'являється вікно про успішне створення електронного підпису, Рис. 52.

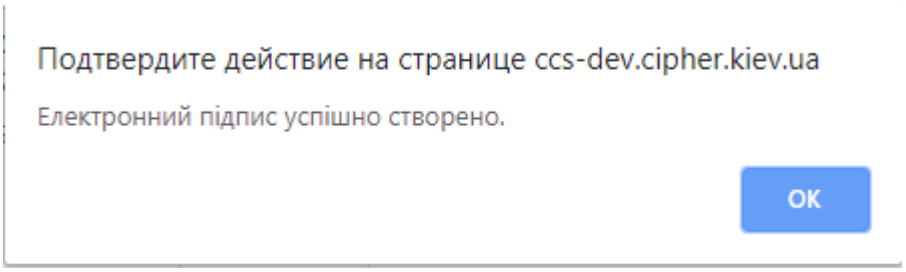

Рис. 52. Повідомлення про створення електронного підпису

Далі у полі «Підпис у кодуванні Base64» з'являється текст з підписом, Рис. 53. Далі за необхідності очищаємо форму.

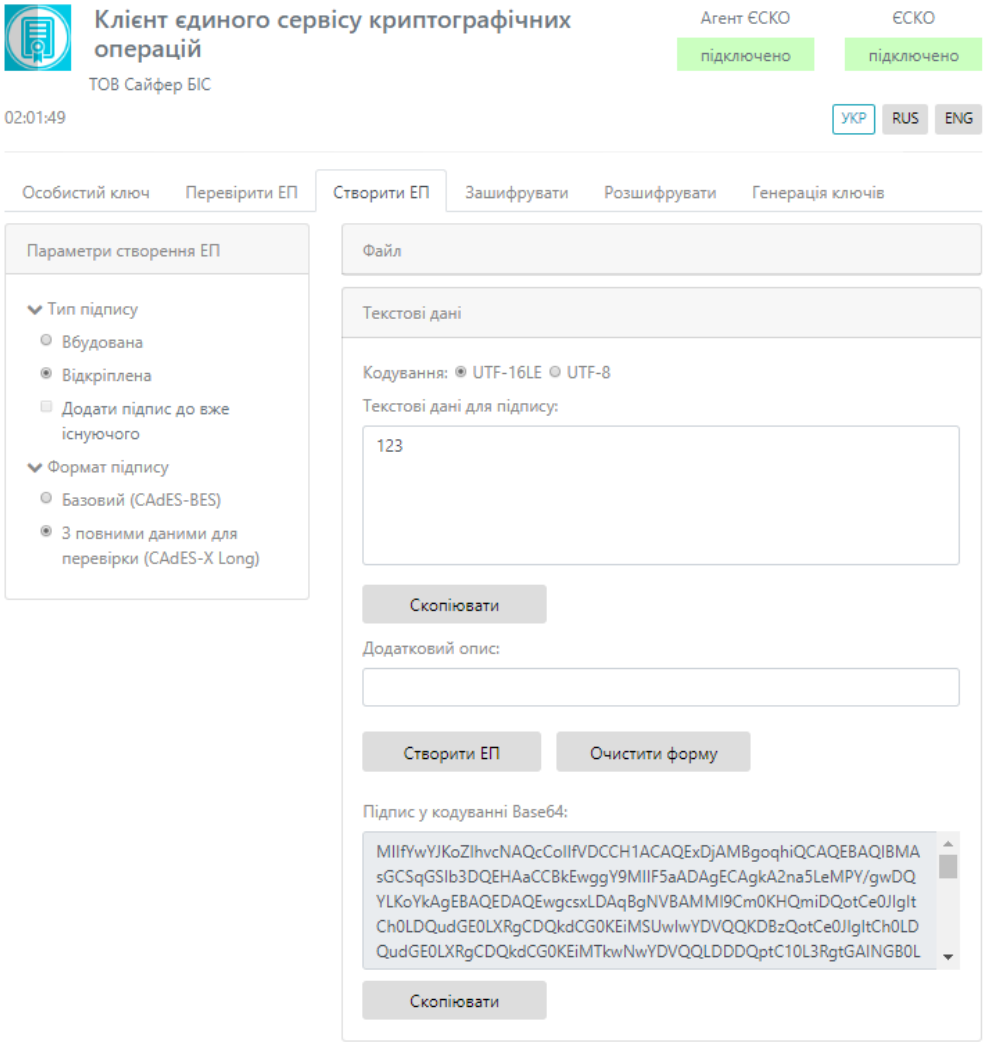

Рис. 53. Результат підпису тестових даних

Перевірка ЕП

Дана функція є доступною і без ключа.

Вкладка «Перевірити ЕП» містить розділи: Параметри перевірки ЕП, Текстові дані та Файл, Рис. 54-Рис. 55.

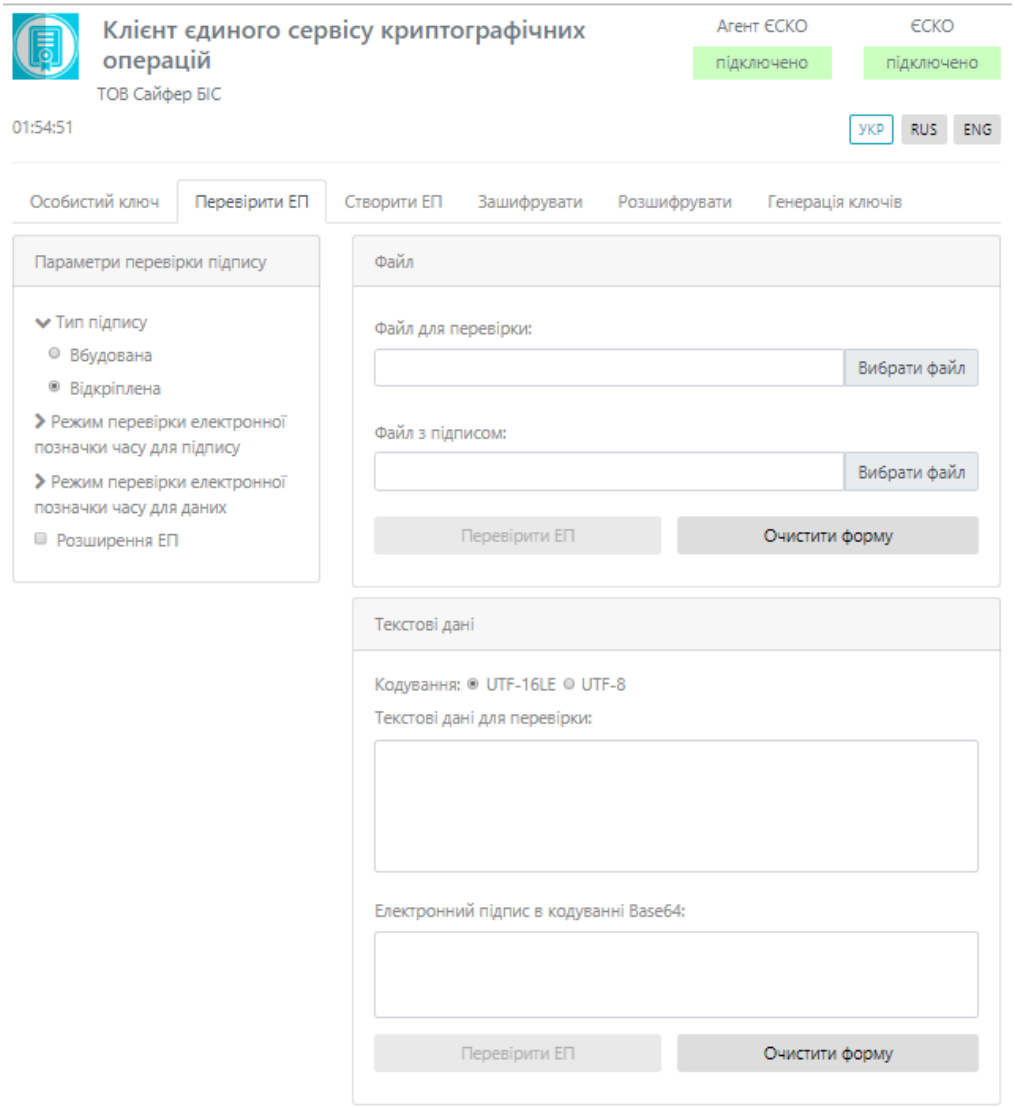

Рис. 54. Вкладка «Перевірити ЕП»

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

1. Поле «Тип ЕП», яке містить:
   - Вбудована;
   - Відкріплена;
2. Режим перевірки електронної позначки часу для ЕП, який вказується за необхідності ігнорувати, перевіряти її наявність, чи повертати помилку за її відсутності.
3. Режим перевірки електронної позначки часу для даних, який вказується за необхідності ігнорувати, перевіряти її наявність, чи повертати помилку за її відсутності.
4. Позначка «Розширити ЕП».

Розділ «Файл», який у свою чергу включає:

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

1. Поле «Файл з підписом» (обирається файл, який містить підпис за типом ЕП Вбудована).
2. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
3. Кнопка «Зберегти підписані дані» (дозволяє зберегти дані без підпису);

4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов’язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

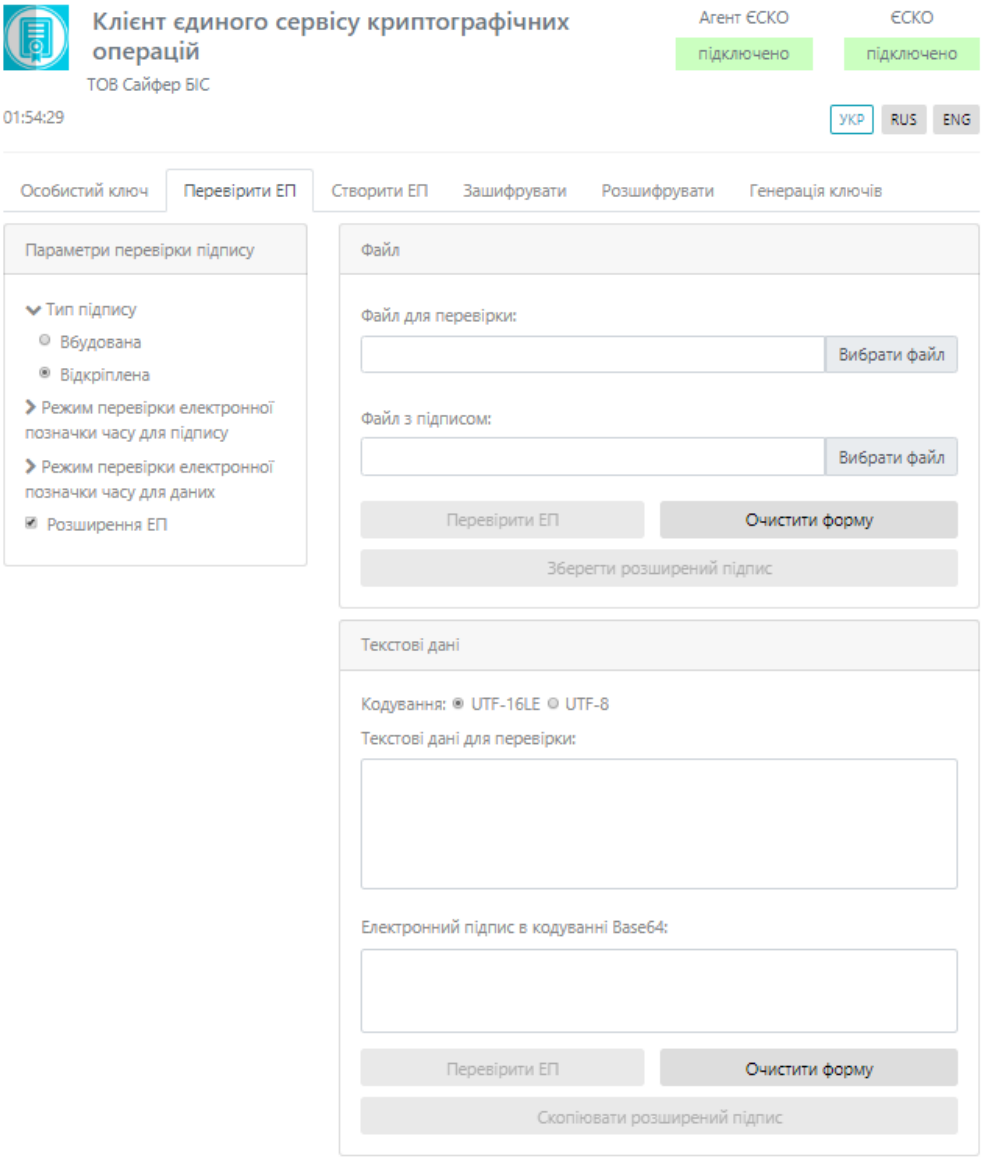

Рис. 55. Вкладка «Перевірити ЕП» зі вказівкою позначки «Розширення ЕП»

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 за 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). Очищення форми щоразу не є обов’язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

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

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

1. Кодування: UTF-16LE та UTF-8.
2. Поле «Підпис у кодування Base64» (вказується текст, який містить підпис за типом ЕП Вбудована).
3. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
4. Поле «Дані з електронного підпису» (виведення текст без підпсиу);
5. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

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

1. Кодування: UTF-16LE та UTF-8.
2. Поле «Текстові дані для перевірки» (вказуються текстові дані, який не містить підпис – початкові дані);
3. Поле «Підпис у кодуванні Base64» (вказуються текстові дані з підписом, за типом ЕП Відкріплена);
4. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
5. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Процес Перевірки ЕП починається з того, що обираються «Параметри перевірки ЕП», обирається файл з підписом, натискаємо кнопку «Перевірити ЕП». За необхідності можна змінити файл.

Перевірка ЕП за типом «Вбудована», файл

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Вбудована» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Вбудована, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо файл з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 56.

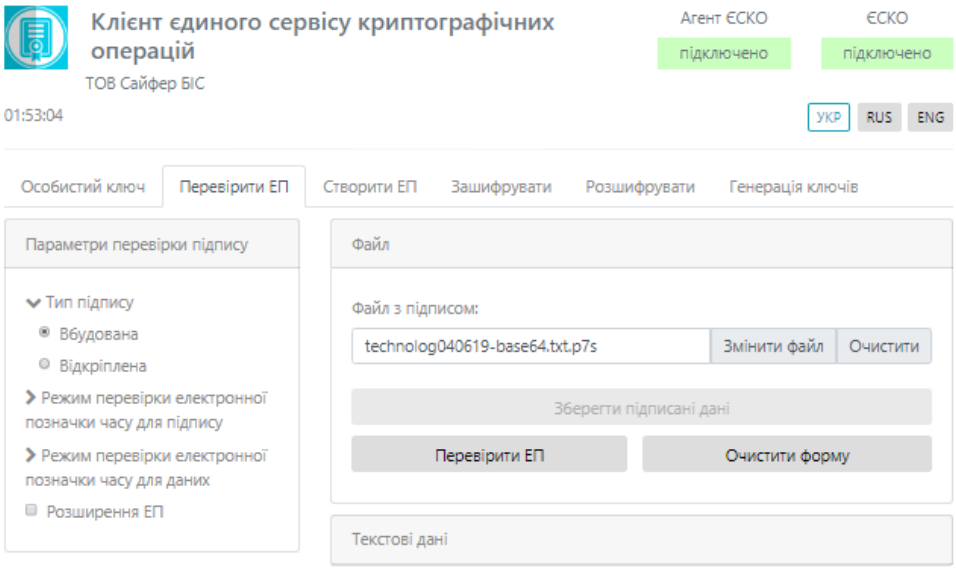

Рис. 56. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 57.

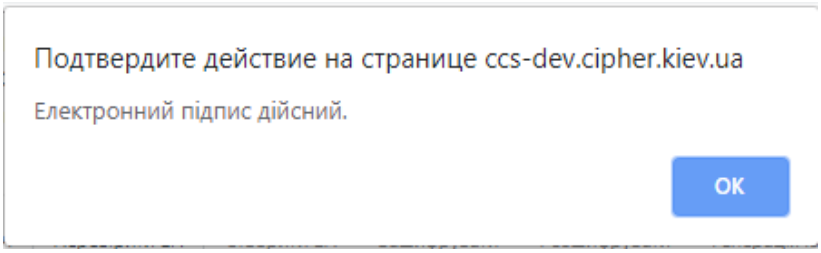

Рис. 57. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дату підпису, Рис. 58. За необхідності зберегти первинні дані (без підпису), натиснувши на кнопку «Зберегти підписані дані». Після чого, натискаємо кнопку «Очистити форму».

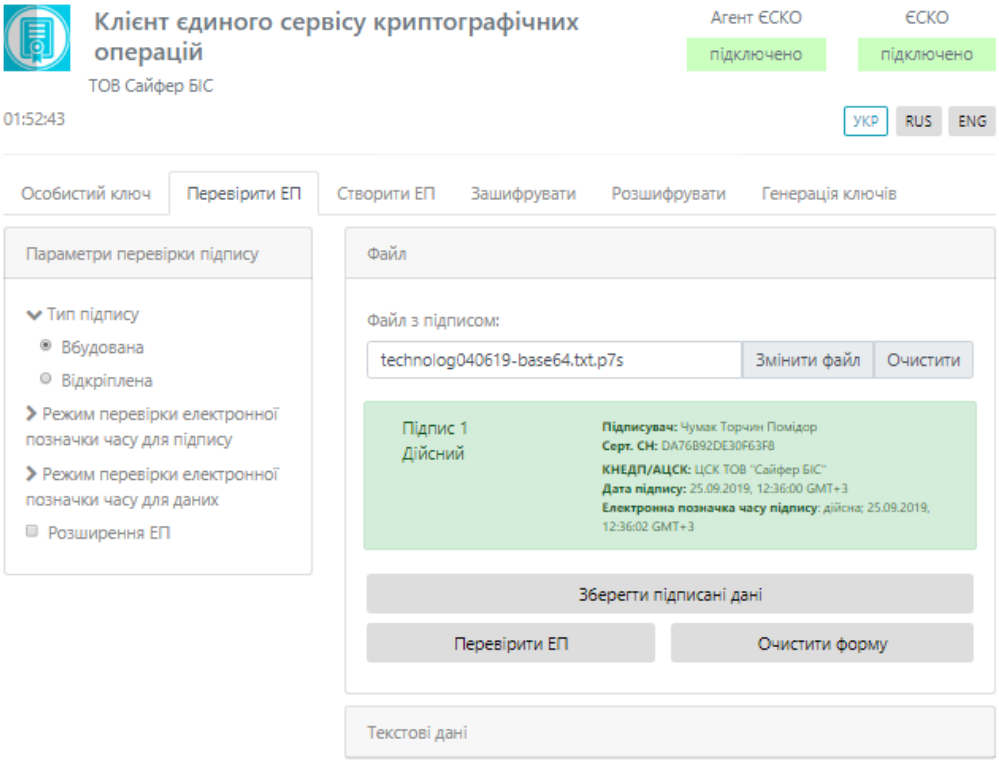

Рис. 58. Результат перевірки

Перевірка ЕП за типом «Відкріплена», файл

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Відкріплена» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Відкріплена, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо файл з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 59.

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 60.

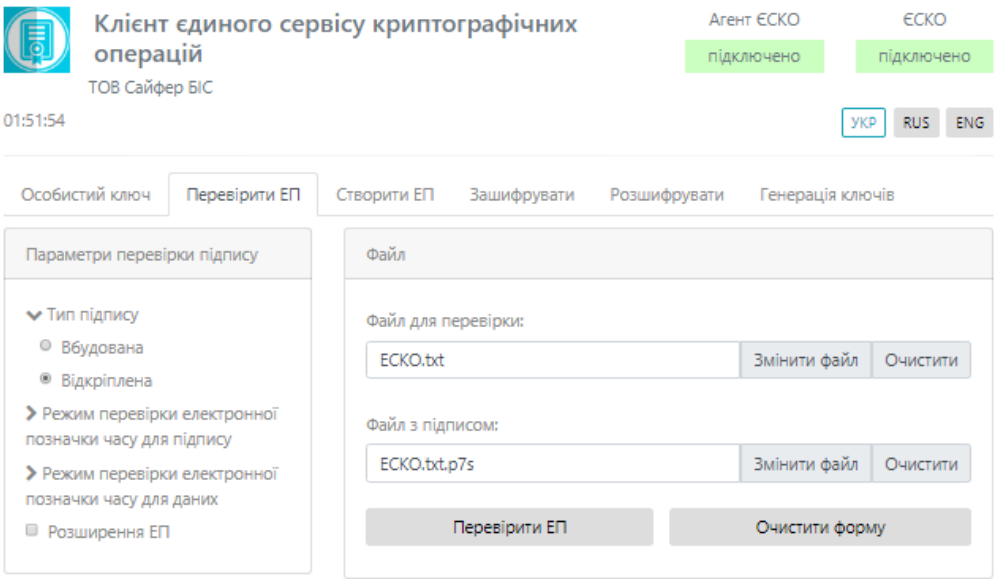

Рис. 59. Перевірка ЕП

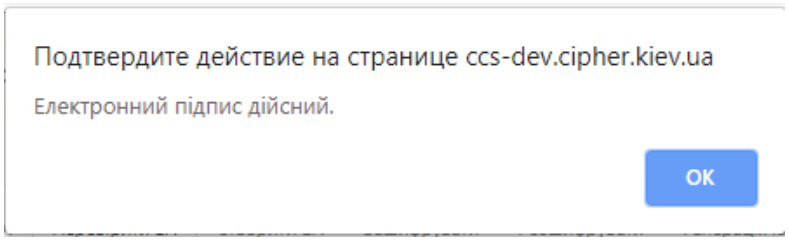

Рис. 60. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з’являється інформація про дійсність підпису, вказується інформація про підписанта та дата підпису, Рис. 61. Після чого, натискаємо кнопку «Очистити форму».

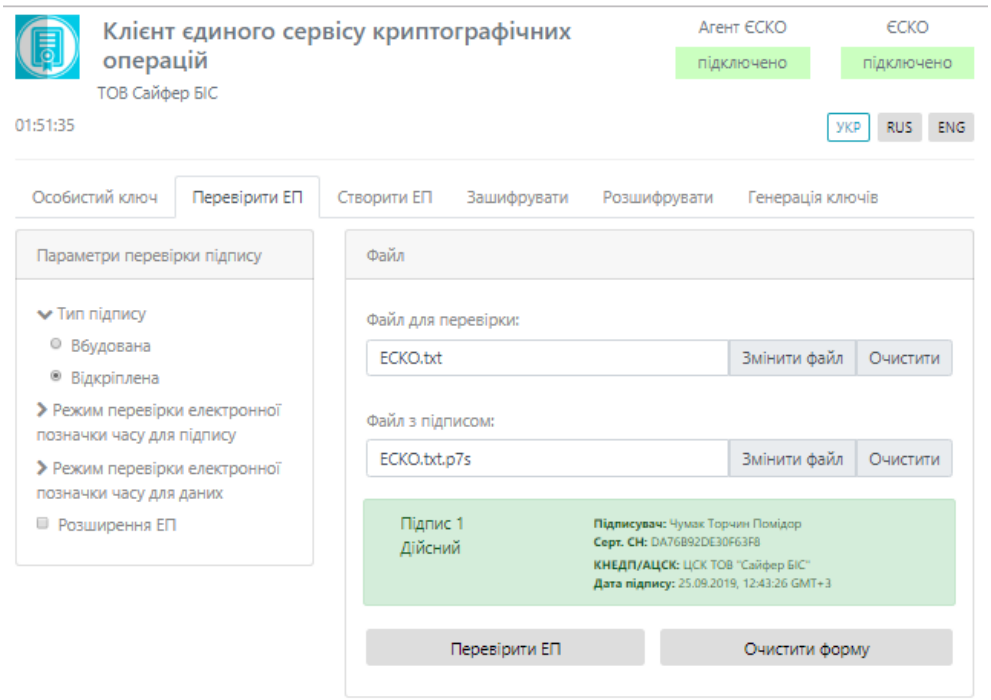

Рис. 61. Результат перевірки

Перевірка ЕП за типом «Вбудована», текстові дані

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Вбудована» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Вбудована, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо текст з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 62.

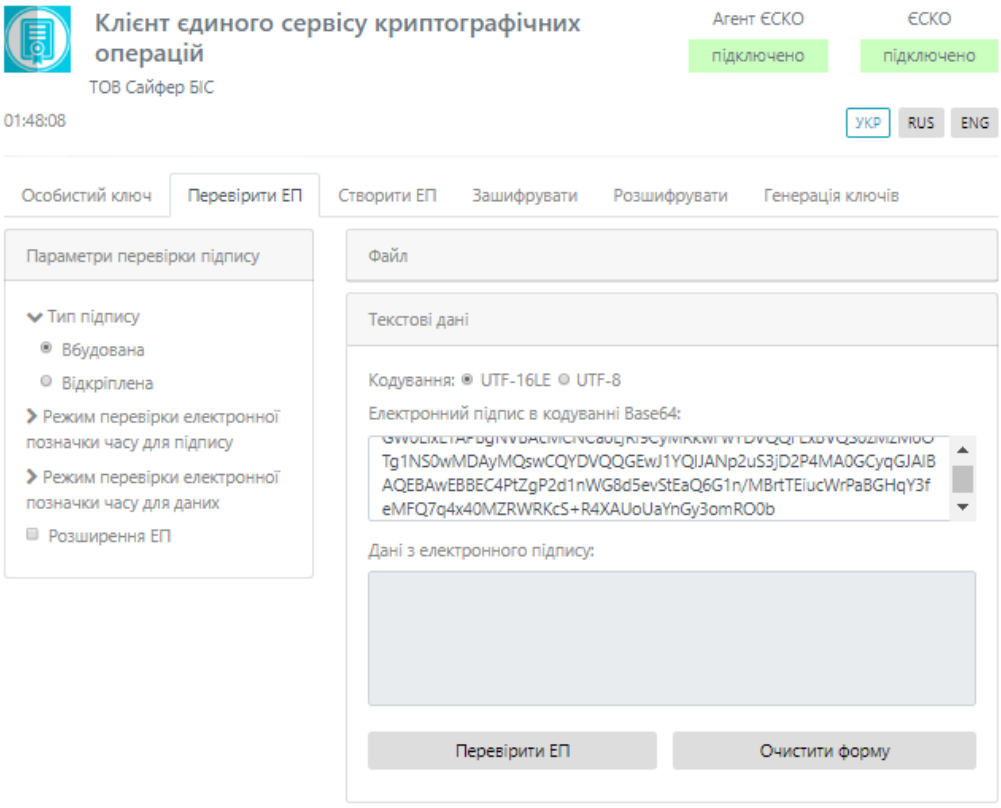

Рис. 62. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 63.

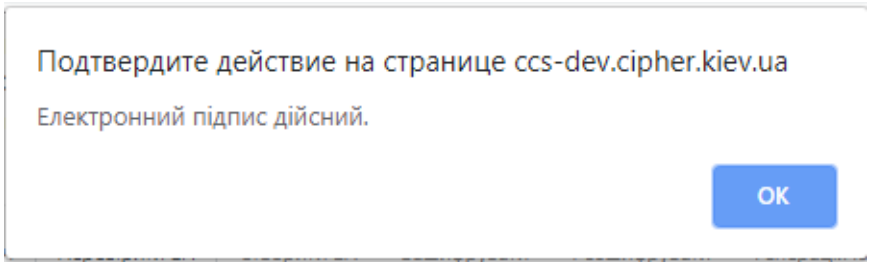

Рис. 63. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дату підпису, Рис. 64. Після чого, натискаємо кнопку «Очистити форму».

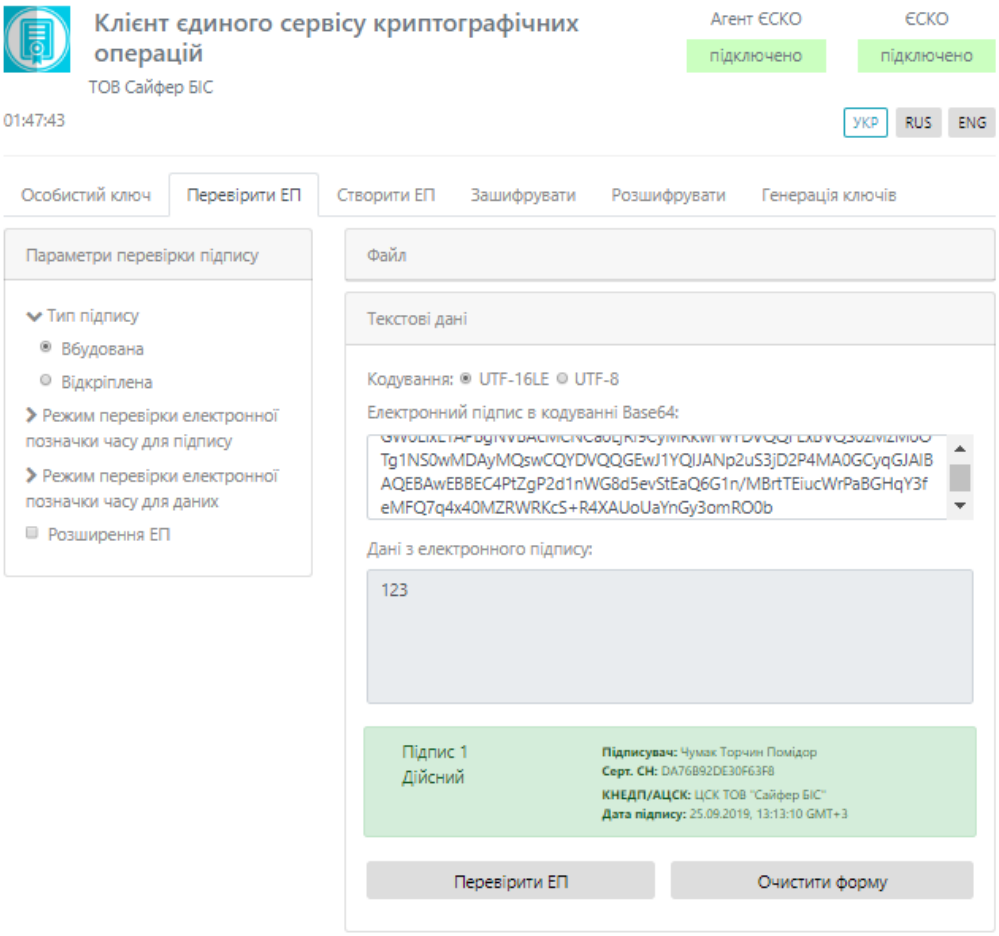

Рис. 64. Результат перевірки

Перевірка ЕП за типом «Відкріплена», текстові дані

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Відкріплена» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Відкріплена, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо текст з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 65.

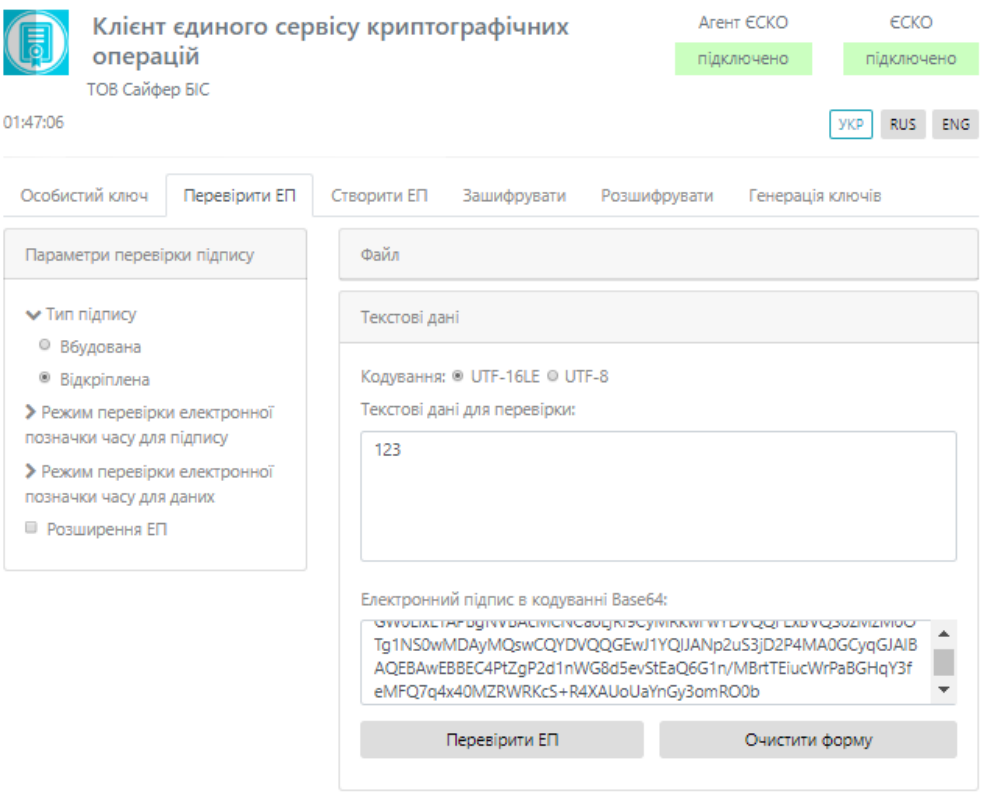

Рис. 65. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з’являється повідомлення з результатами перевірки електронного підпису, Рис. 66.

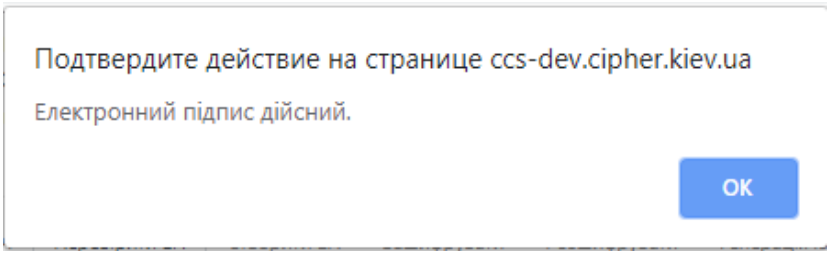

Рис. 66. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з’являється інформація про дійсність підпису, вказується інформація про підписанта та дата підпису, Рис. 67. Після чого, натискаємо кнопку «Очистити форму».

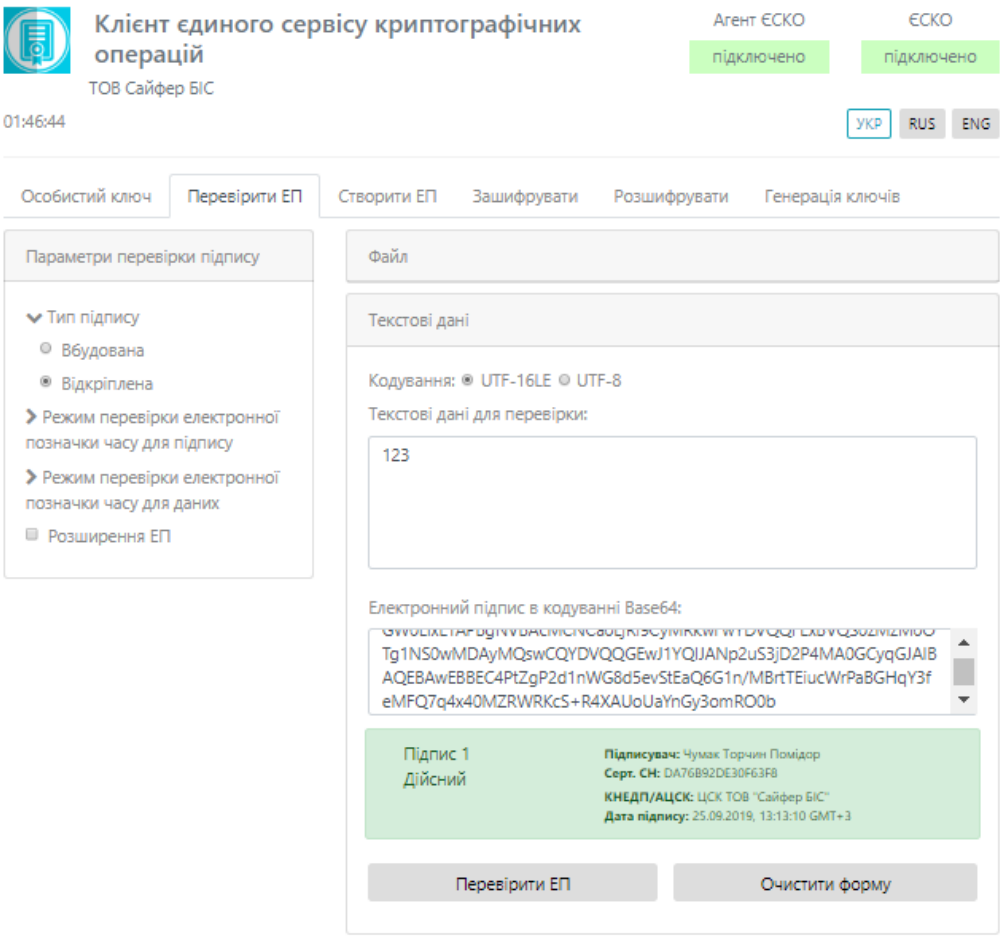

Рис. 67. Результат перевірки

Розширення ЕП

Вкладка «Перевірити ЕП» містить додаткову позначку «Розширити ЕП», при її вказівці, зовнішній вигляд сторінки видозмінюється та стають доступні нові кнопки, Рис. 68.

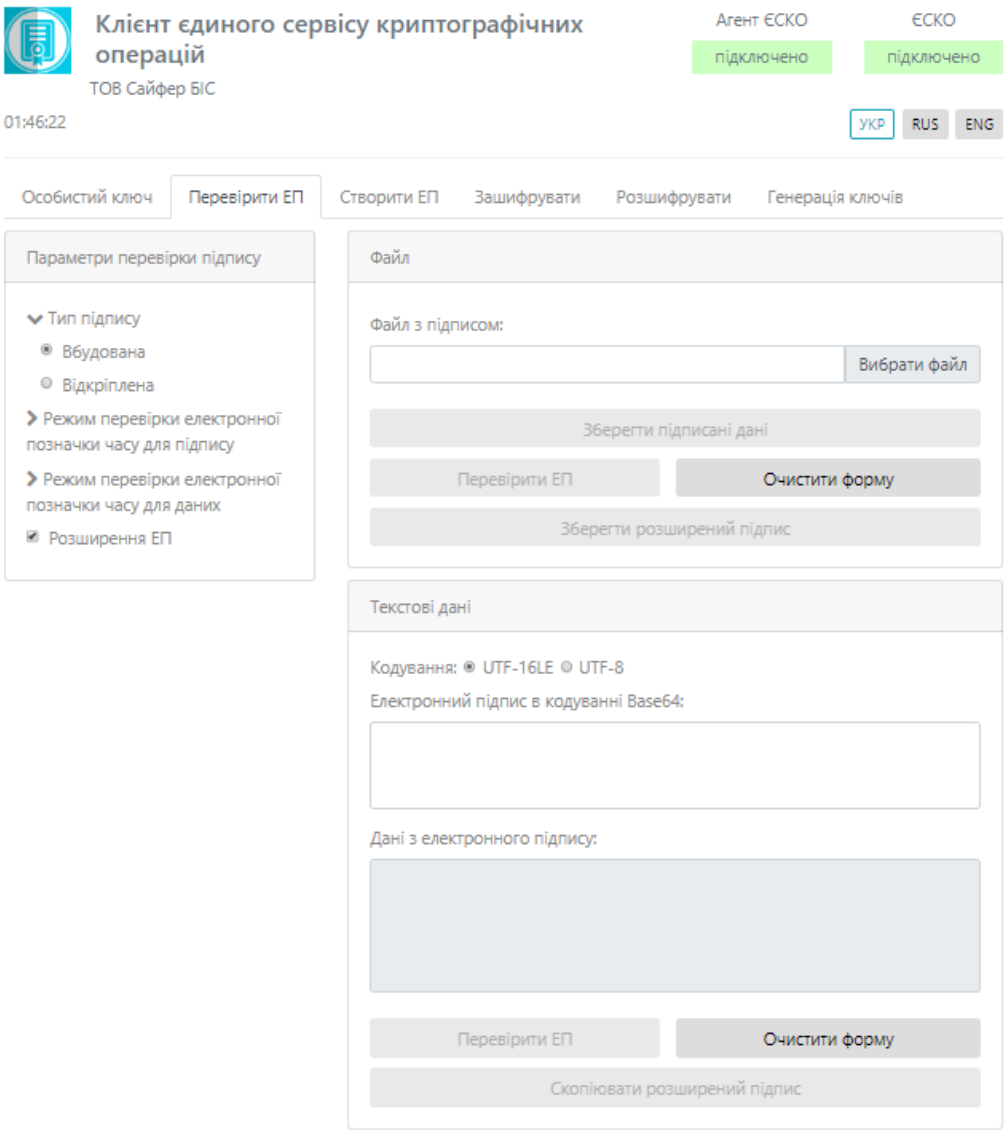

Рис. 68. Вкладка «Перевірити ЕП» з позначкою «Розширення ЕП»

Розширення ЕП для файлу

Відеоінструкція знаходиться за посиланням.

На прикладі вбудованого електронного підпису, який отримано раніше. Слід обрати файл та натиснути кнопку «Перевірити ЕП», Рис. 69.

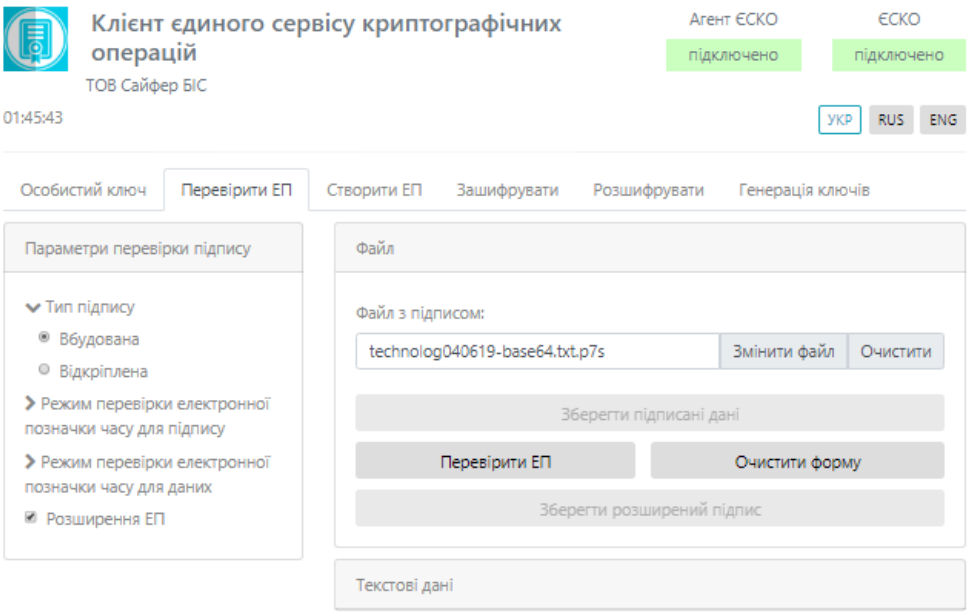

Рис. 69. Розширення вбудованого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 70.

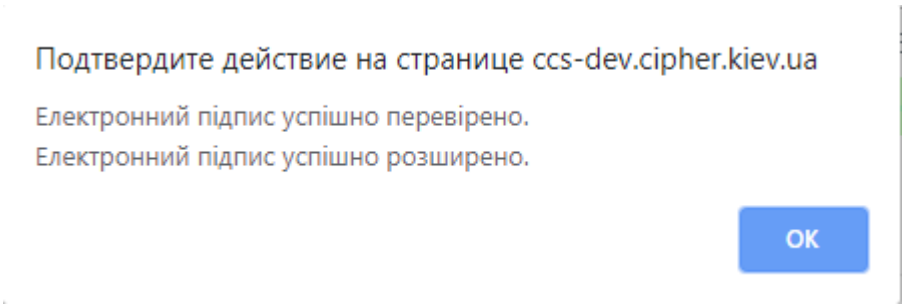

Рис. 70. Повідомлення про результат перевірки та розширення ЕП

Отримати результат перевірки електронного підпису, Рис. 71.

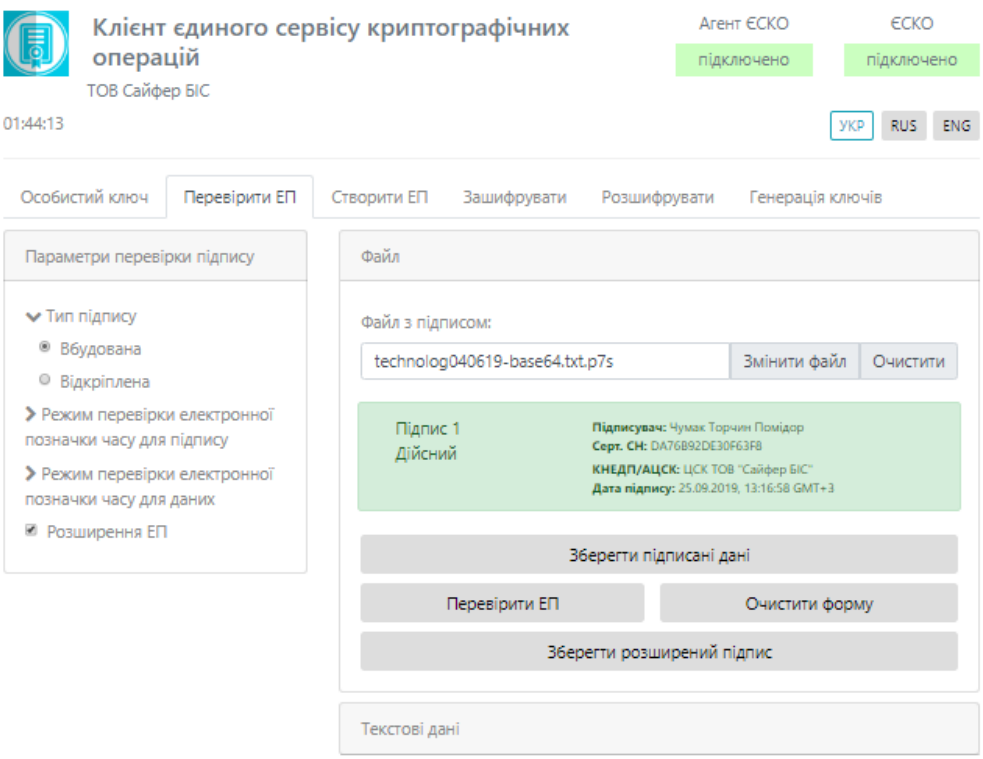

Рис. 71. Розширення вбудованого ЕП

За умови, якщо було завантажено файл вже з повними даними для перевірки, то з’явиться повідомлення про це, Рис. 72.

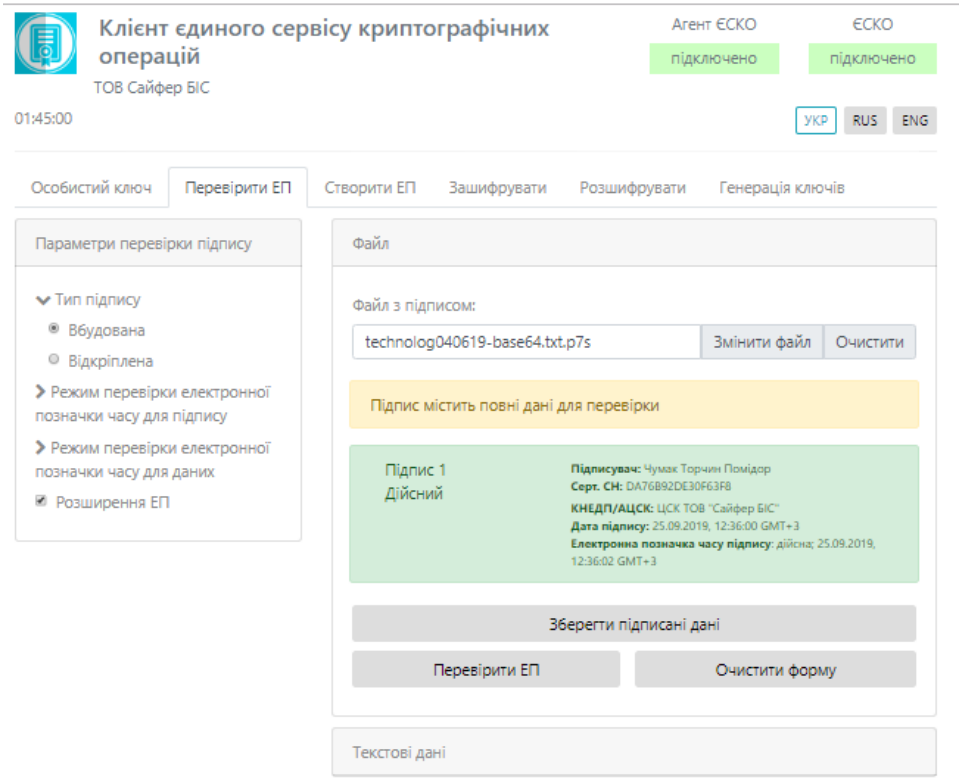

Рис. 72. Результати розширення підпису з повними даними для перевірки

Розширення ЕП для текстових даних

Відеоінструкція знаходиться за посиланням.

На прикладі відкріпленого електронного підпису, який отримано раніше. Слід вказати підписані дані та натиснути кнопку «Перевірити ЕП», Рис. 73.

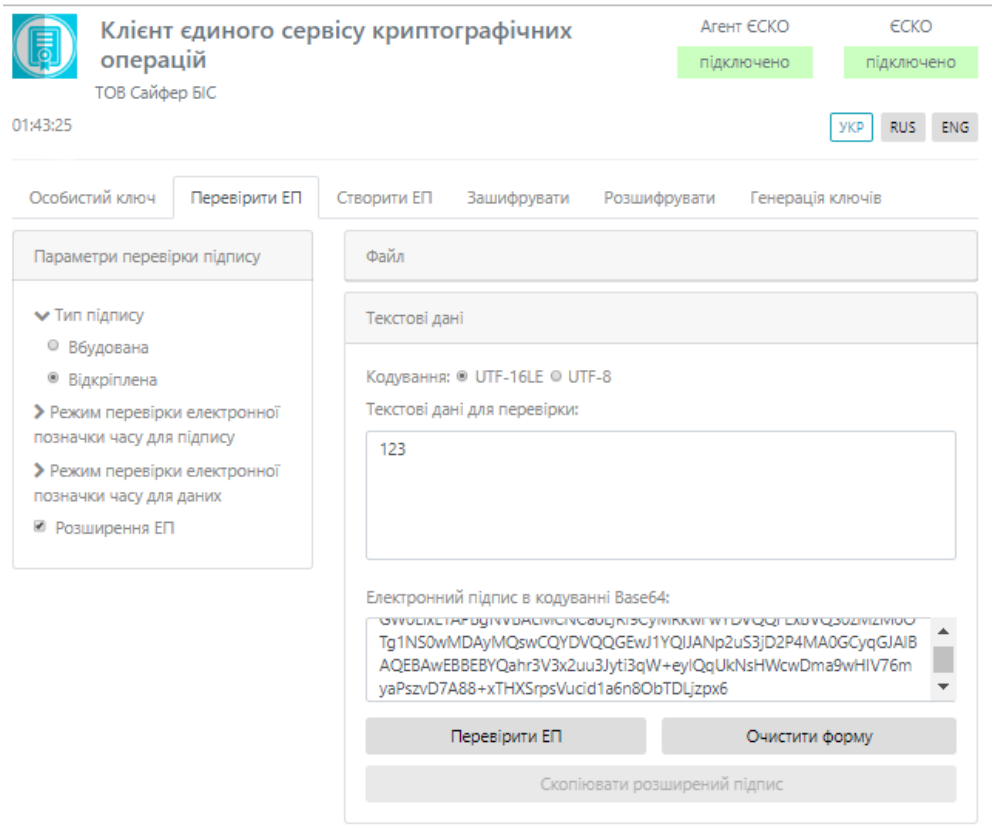

Рис. 73. Розширення відкріпленого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 74.

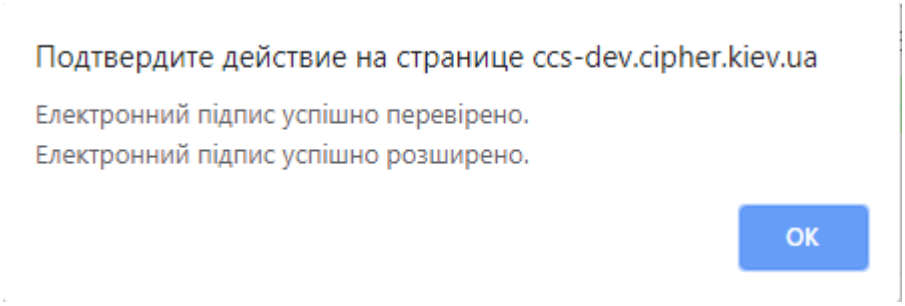

Рис. 74. Повідомлення про перевірку та розширення підпису

Отримати результат перевірки електронного підпису, Рис. 75.

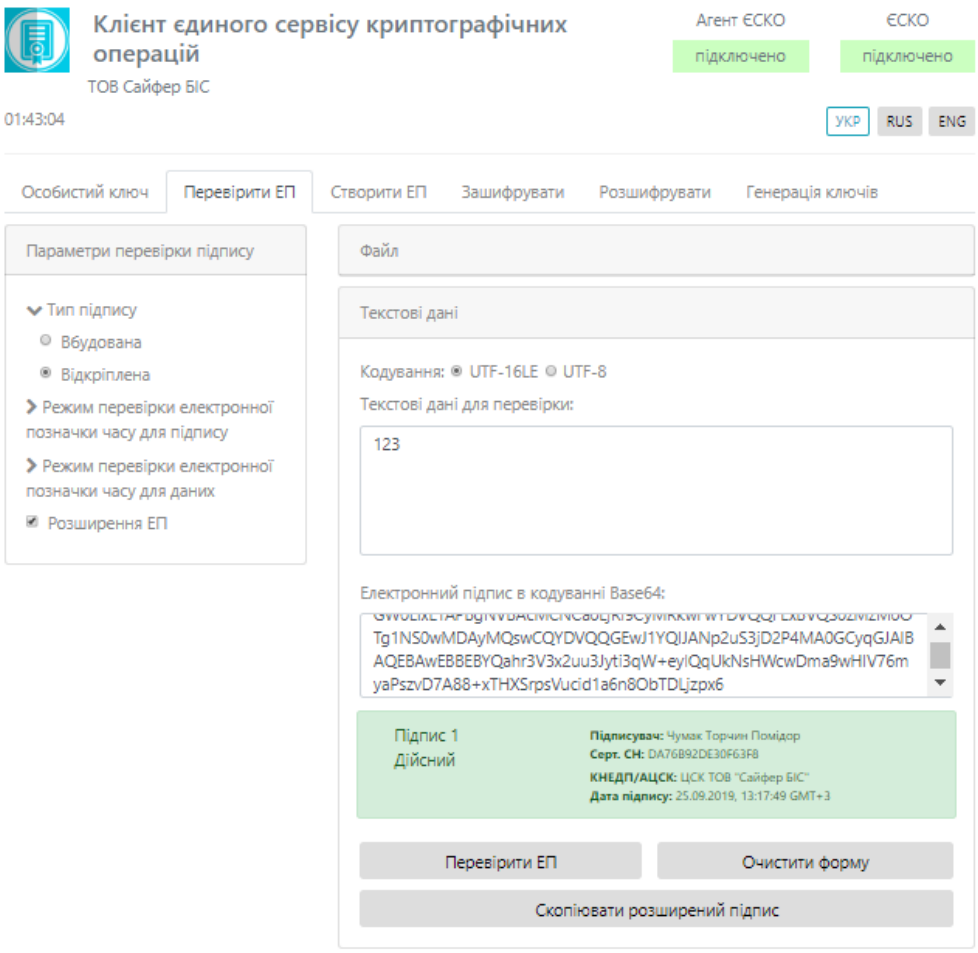

Рис. 75. Результат розширення та перевірки ЕП

За умови, якщо було завантажено текстові дані вже з повними даними для перевірки, то з’явиться повідомлення про це, Рис. 76.

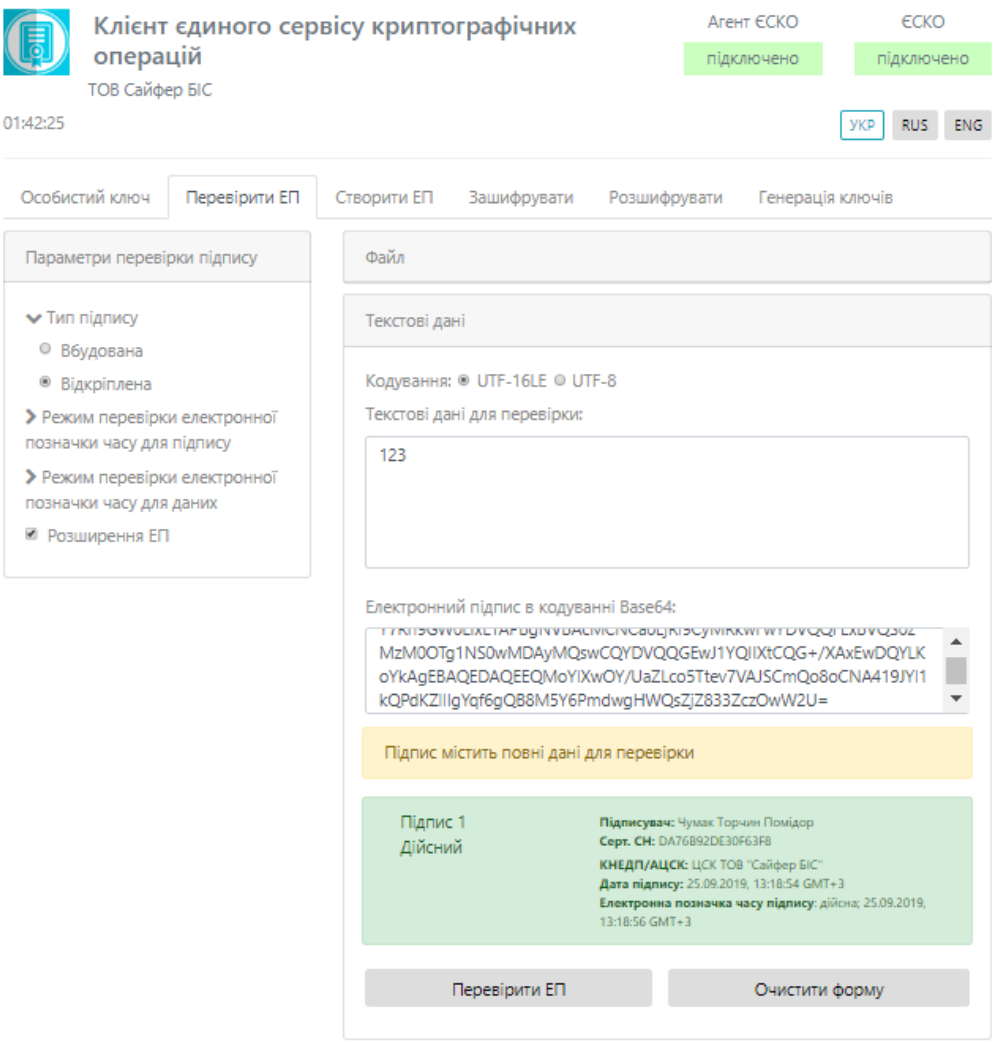

Рис. 76. Результати розширення підпису з повними даними для перевірки

Зашифрувати

Процес зашифрування здійснюється із застосуванням захищеного носія (в активному та пасивному режимі) чи файлового ключового контейнеру.

За умови, якщо генерація ключа здійснювалася за допомогою Агенту ЄСКО у активному режимі – процес зашифрування здійснюється коректно, або самостійний запис ключа за допомогою «Модуля роботи з ключовим контейнером» у пасивному режимі.

Вкладка «Зашифрувати» містить такі розділи: Параметри шифрування, Сертифікат отримувача, Текстові дані та Файл, Рис. 77.

Розділ «Параметри шифрування», який включає:

1. Додати при шифруванні:
   - 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 отримувача).

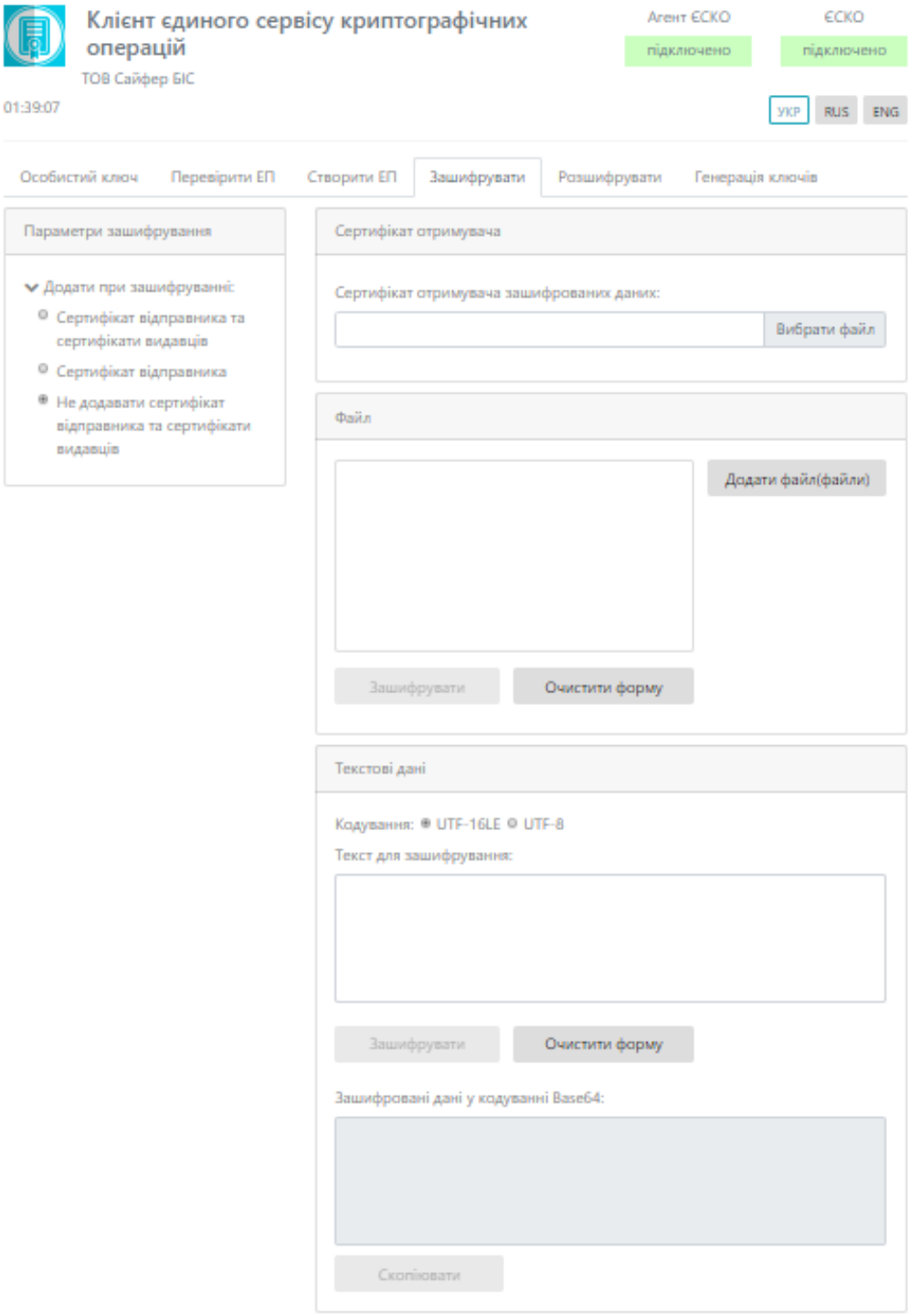

Рис. 77. Вкладка «Зашифрувати»

Розділ «Файл», який включає:

1. Поле «Файл для шифрування»;
2. Кнопка «Зашифрувати» (здійснює зашифрування файлу);
3. Кнопка «Зберегти шифровані дані у файл» (зберігає шифровані дані у файл);

4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов’язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Розділ «Текстові дані», який включає:

1. Тип кодування UTF-16LE та UTF-8.
2. Поле «Текст для зашифрування»;
3. Кнопка «Зашифрувати» (здійснює зашифрування тексту);
4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов’язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.
5. Поле «Зашифровані дані у кодуванні Base64».

Процес зашифрування файлу

Відеоінструкція знаходиться за посиланням.

Для того, щоб зашифрувати файл, у розділі «Параметри шифрування», обрати один з пунктів (сертифікат відправника та сертифікати видавців чи сертифікат відправника чи не додавати сертифікат відправника та сертифікати видавців), у розділі «Сертифікат отримувача» додати сертифікат отримувача зашифрованих даних, у розділі «Файл» обрати файл для шифрування, натиснути кнопку «Зашифрувати», Рис. 78.

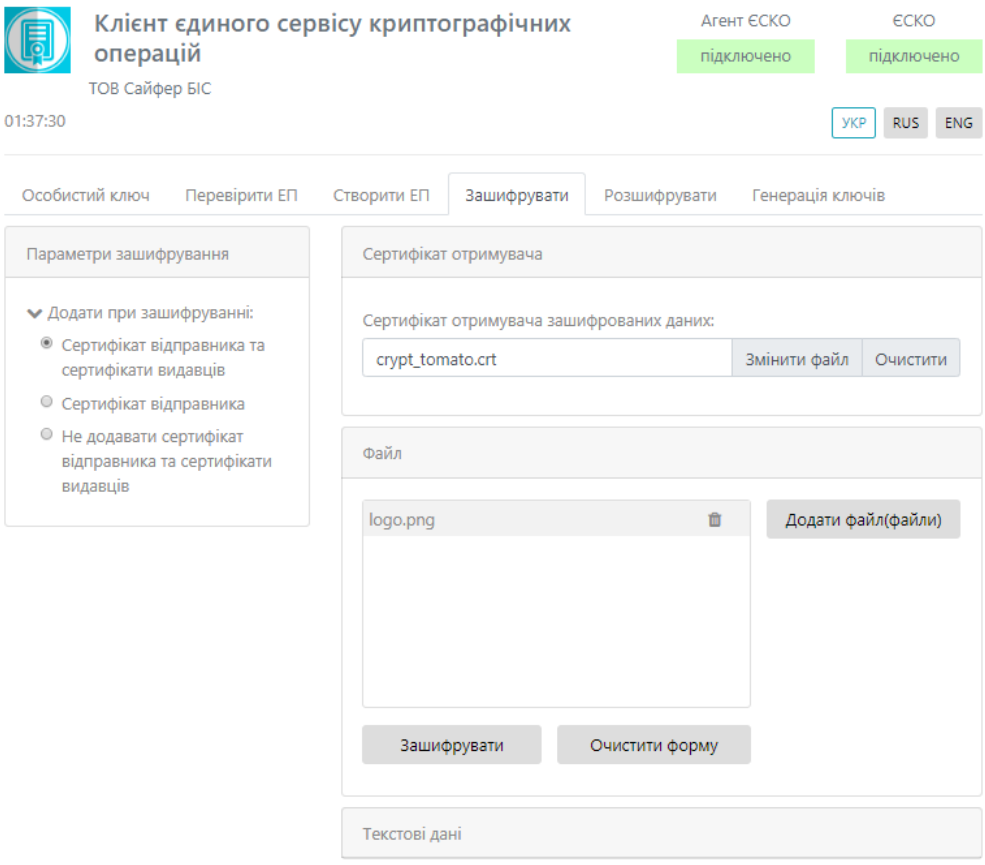

Рис. 78. Процес зашифрування

Після натискання на кнопку «Зашифрувати» з’являється вікно з повідомленням з результатом зашифрування, Рис. 79.

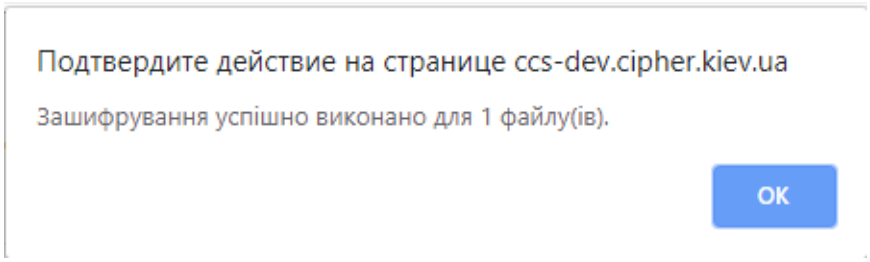

Рис. 79. Повідомлення про успішне зашифрування даних

Після, зберігаємо зашифровані дані у файл та очищаємо форму.

Після, за допомогою відповідної кнопки «стрілка вниз» можна зберегти зашифрований файл та очищаємо форму, Рис. 80.

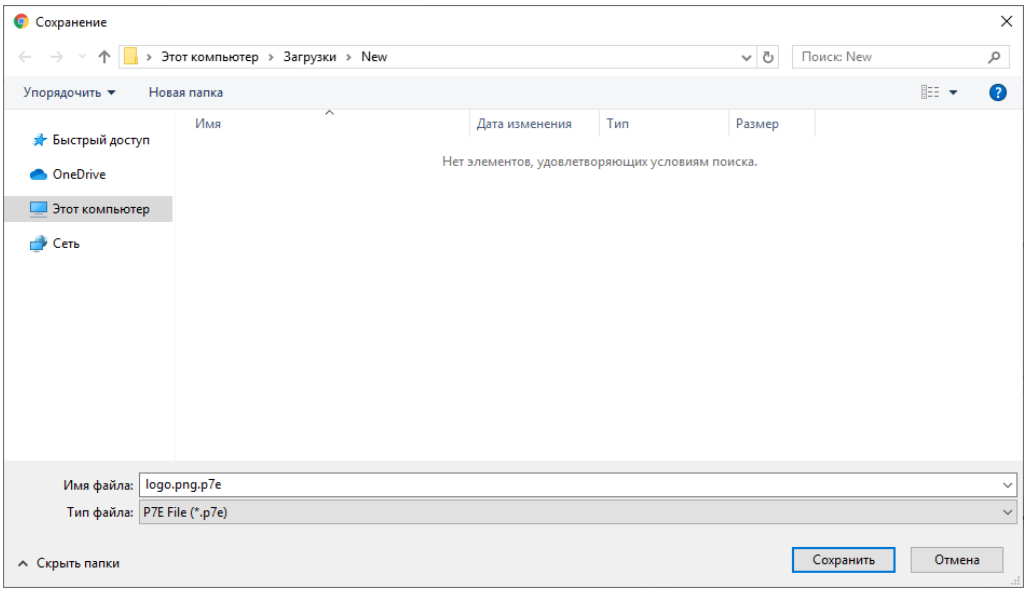

Рис. 80. Збереження зашифрованого файлу

Процес зашифрування текстових даних

Відеоінструкція знаходиться за посиланням.

Для того, щоб зашифрувати текстові дані, у розділі «Параметри шифрування», обрати один з пунктів (сертифікат відправника та сертифікати видавців чи сертифікат відправника чи не додавати сертифікат відправника та сертифікати видавців), у розділі «Сертифікат отримувача» додати сертифікат отримувача зашифрованих даних, у розділі «Текстові дані» вказати текст для шифрування, натиснути кнопку «Зашифрувати», Рис. 81.

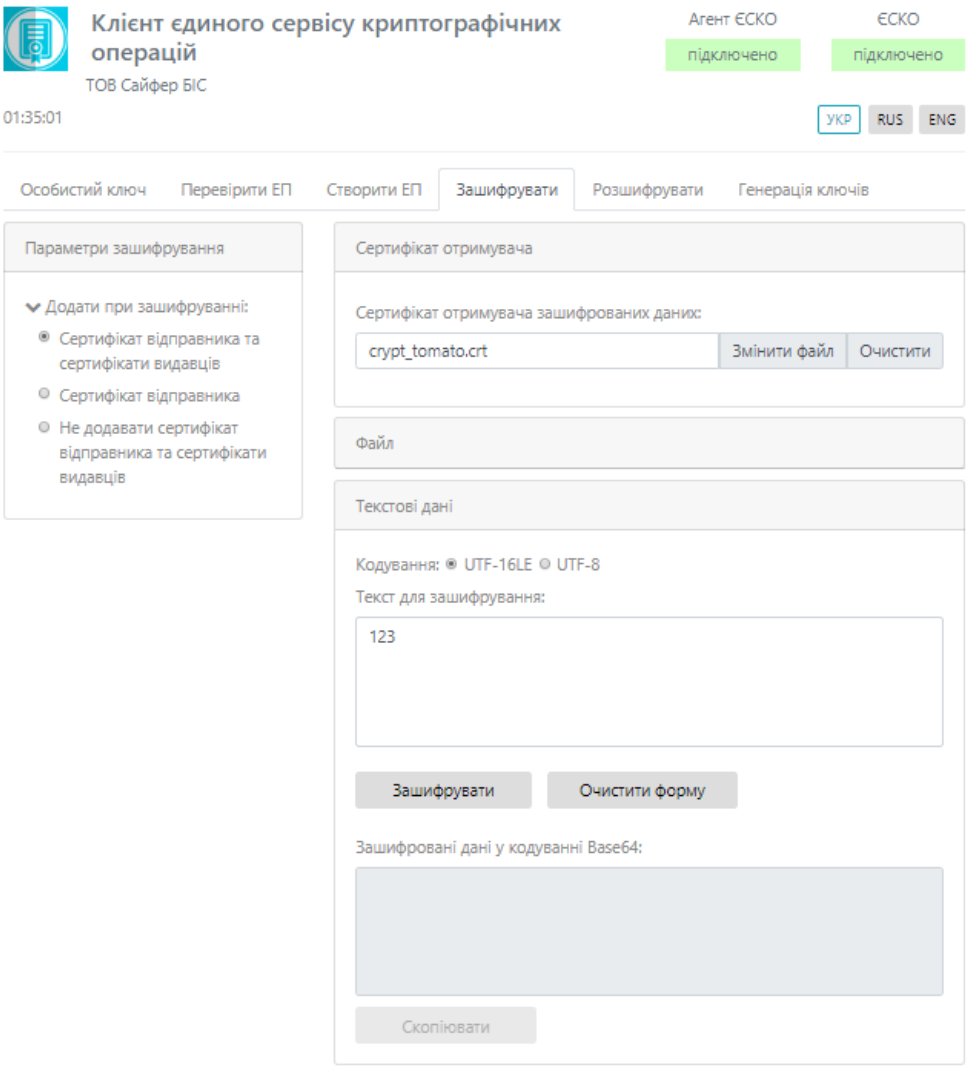

Рис. 81. Процес зашифрування

Після натискання на кнопку «Зашифрувати» з’являється у полі «Зашифровані дані у кодуванні Base64», Рис. 82.

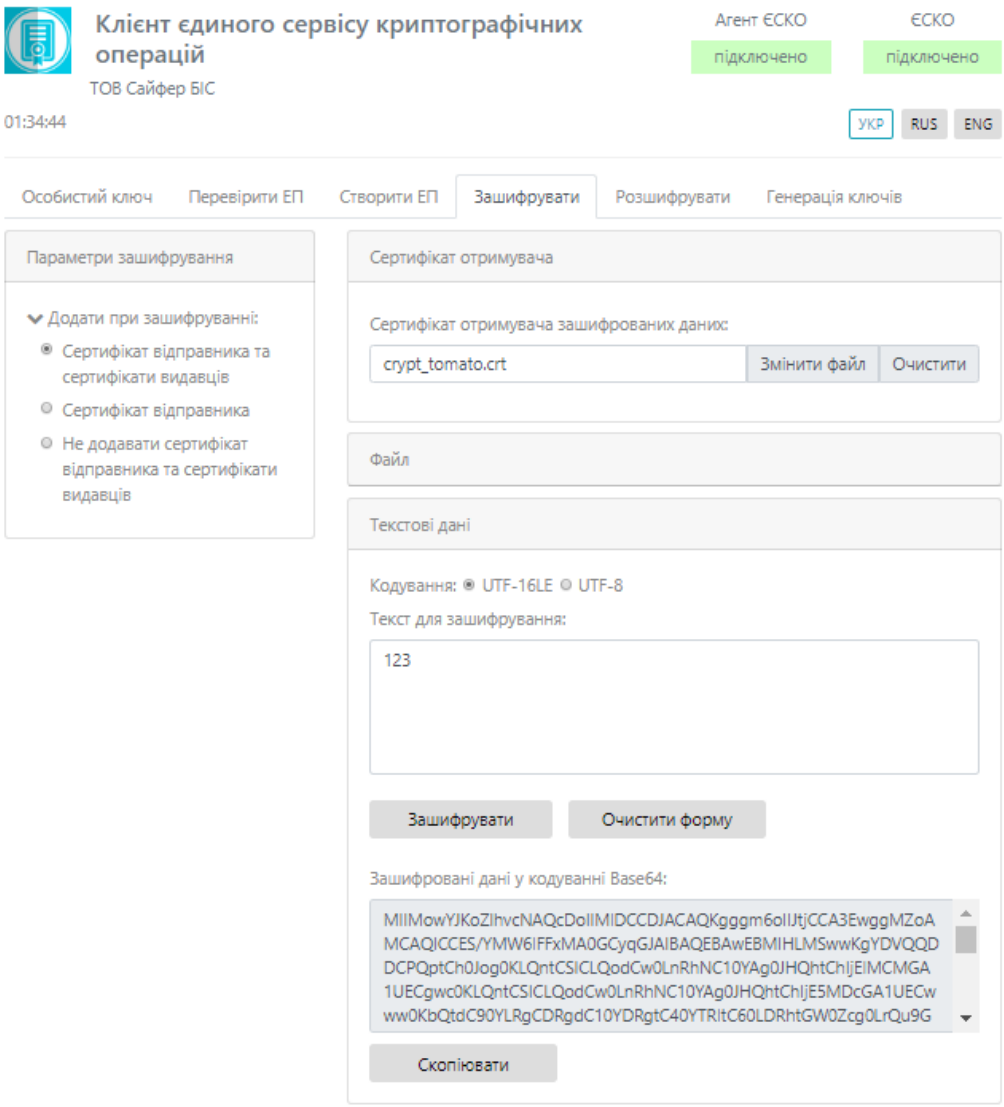

Рис. 82. Повідомлення про успішне зашифрування даних

Розшифрувати

Процес розшифрування здійснюється із застосуванням захищеного носія (в активному та пасивному режимі) чи файлового ключового контейнеру.

За умови, якщо генерація ключа здійснювалася за допомогою Агенту ЄСКО у активному режимі – процес розшифрування здійснюється коректно, або самостійний запис ключа за допомогою «Модуля роботи з ключовим контейнером» у пасивному режимі.

Дана вкладка містить розділ Файл.

Розділ «Файл», який включає, Рис. 83:

1. Поле «Файл для розшифрування» (обирається файл, який необхідно розшифрувати);
2. Кнопка «Розшифрувати» (Здійснює дешифрування файлу);
3. Кнопка «Зберегти розшифровані дані у файл» (здійснює збереження розшифрованих даних у файл);

4. Кнопка «Очистити форму» (здійснює очищення форми). Очищення форми щоразу не є обов’язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Розділ «Текстові дані», який включає, Рис. 83:

1. Тип кодування: UFT-16LE та UTF-8.
2. Поле «Зашифровані дані у кодуванні Base64» (вказується текст, який необхідно розшифрувати);
3. Кнопка «Розшифрувати» (здійснює дешифрування текстових даних);
4. Кнопка «Очистити форму» (здійснює очищення форми). Очищення форми щоразу не є обов’язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

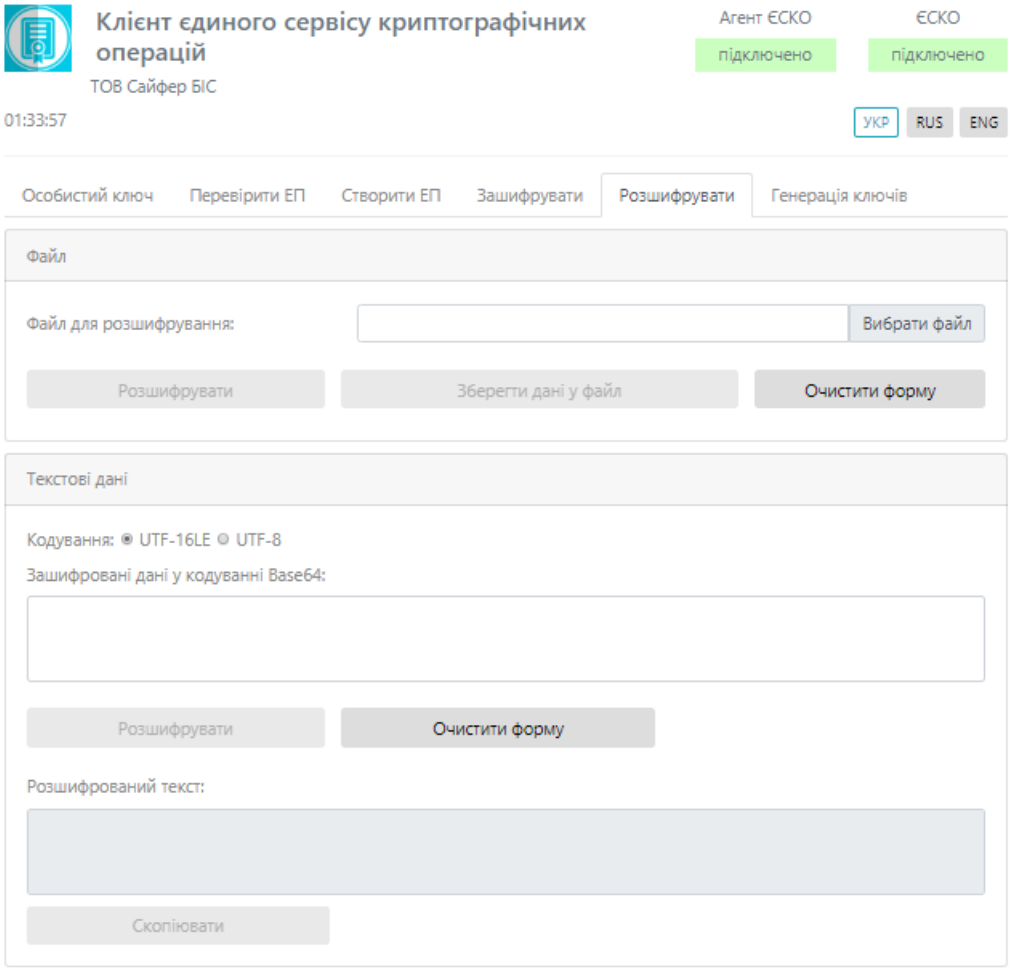

Рис. 83. Вкладка «Розшифрувати», розділ «Файл»

Процес розшифрування файлу

Відеоінструкція знаходиться за посиланням.

Для того, щоб розшифрувати файл, у розділі «Файл», необхідно вказати файл для розшифрування та натиснути кнопку «Розшифрувати», Рис. 84.

Після натискання на кнопку «Розшифрувати» з’являється вікно з повідомленням з результатом зашифрування, Рис. 85, де слід натиснути кнопку «ОК» та зберегти розшифровані дані у файл та очистити форму.

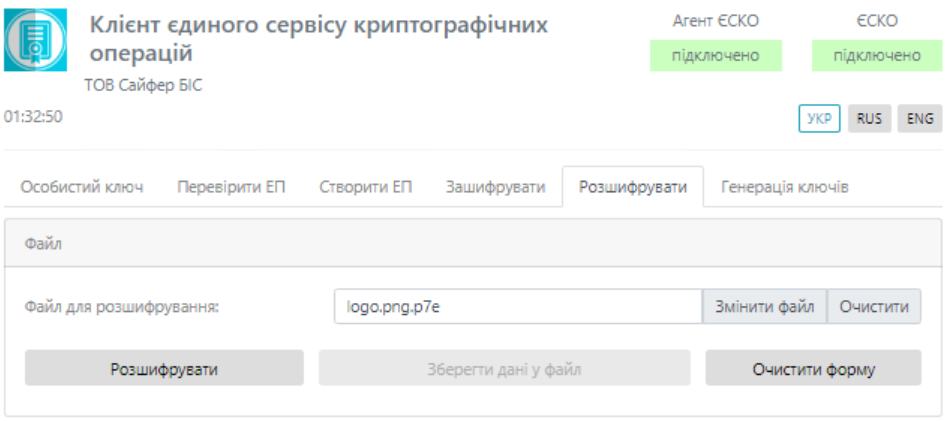

Рис. 84. Процес розшифрування

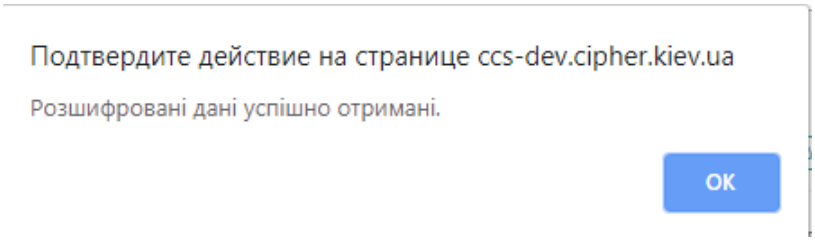

Рис. 85. Повідомлення про успішне розшифрування даних

Процес розшифрування текстових даних

Відеоінструкція знаходиться за посиланням.

Для того, щоб розшифрувати текст, у розділі «Текстові дані», необхідно вказати текст для розшифрування та натиснути кнопку «Розшифрувати», Рис. 86.

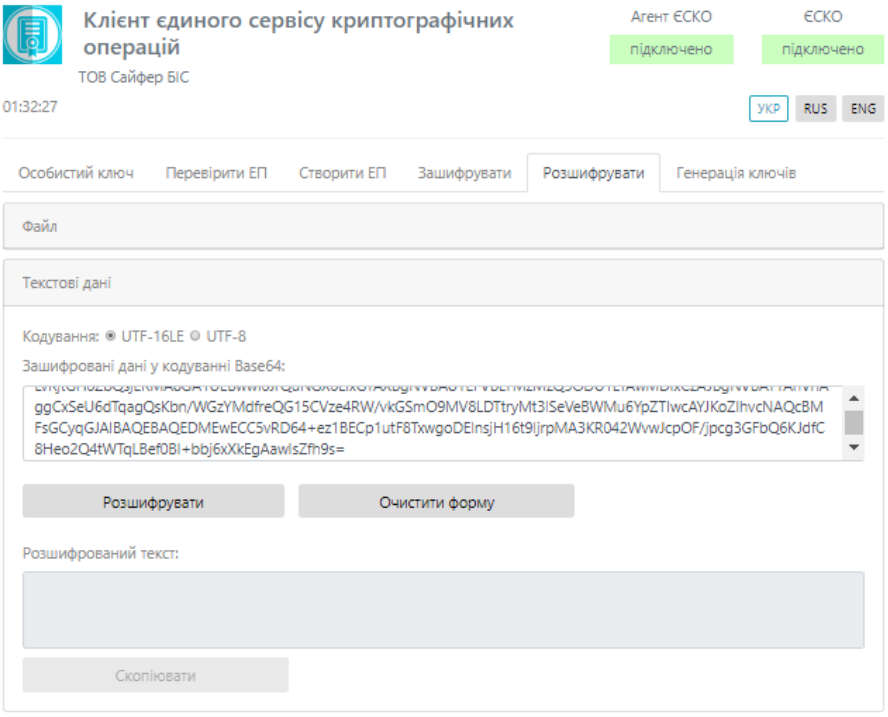

Рис. 86. Процес розшифрування

Після натискання на кнопку «Розшифрувати» з’являється розшифровані текстові дані у полі «Розшифрований текст», Рис. 87 та очистити форму.

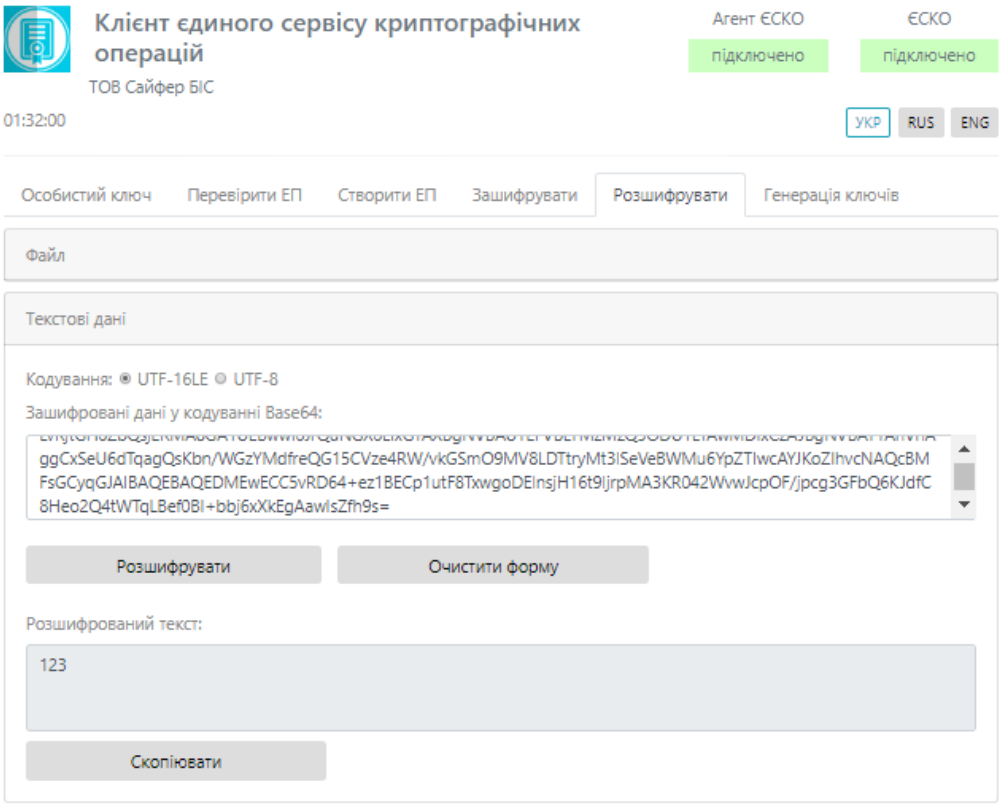

Рис. 87. Розшифровані текстові дані

Генерація ключів

Дана функція є доступною і без ключа.

Відеоінструкція знаходиться за посиланням.

Генерація ключів відбувається як у файл на диску так і на захищений носій.

На Рис. 88 показано вкладку «Генерація ключів», а саме вибір профілю. Дана вкладка містить розділ Профіль генерації ключів, які включає у себе:

- Співробітник банку.
- Технолог.
- Посадова особа клієнта iFOBS.
- Клієнт iFOBS (ФОП).

Дані профілі відрізняються один від одного полями та обов’язковими полями.

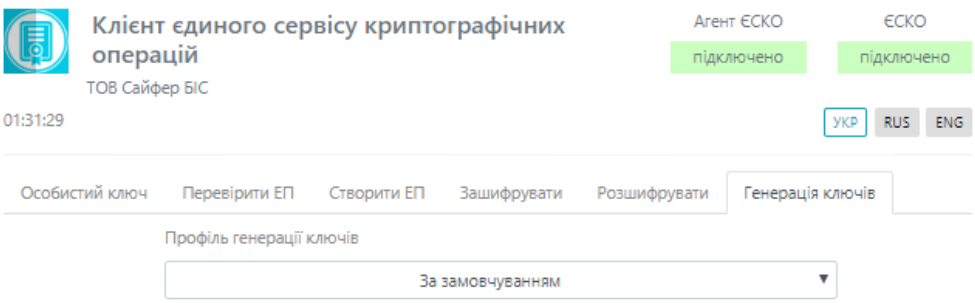

Рис. 88. Вкладка «Генерація ключів»

Після вибору з переліку необхідного профілю, Рис. 89 (у даному випадку буде розглядатися варіант генерації ключа для співробітника банку).

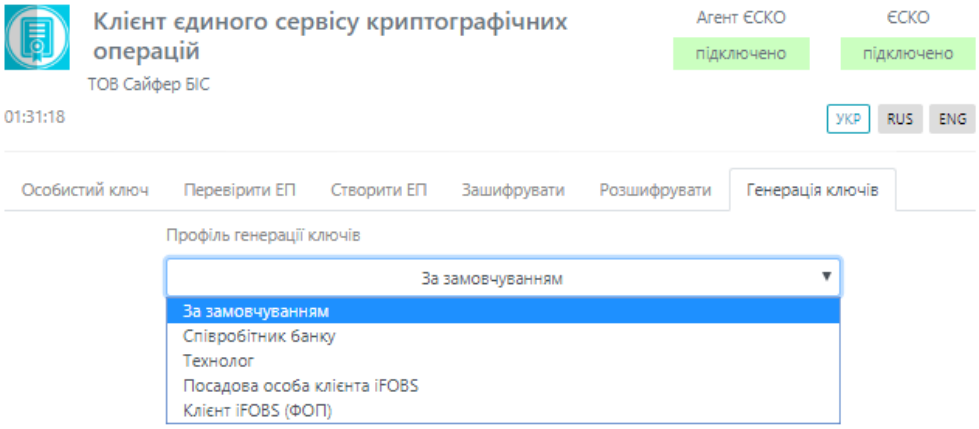

Рис. 89. Вибір профілю генерації ключів

Відкривається форма для заповнення персональних даних власника ключа. Слід звернути увагу, що є обов’язкові поля, якщо їх не вказати буде помилка, і підпис не буде створено. Форма профілю генерації ключів для Співробітника банку для заповнення персональних даних показана на Рис. 90.

Для профілю «Співробітник банку» необхідно вказати логін та пароль до MS Active Directory та натиснути кнопку «Отримати дані з корпоративного каталогу MS Active Directory». За умови, якщо дані не вірні чи не отримані з системи – слід звернутися до адміністратора системи (про це буде повідомлено у вікні).

Після уважного заповнення всіх полів, необхідно звернути увагу на CAPTCHA, яку теж необхідно вказати, якщо вона є не розбірливою, праворуч від поля для її введення, є кнопка для її зміни.

Наступним кроком є натискання на кнопку «Згенерувати ключі», Рис. 91.

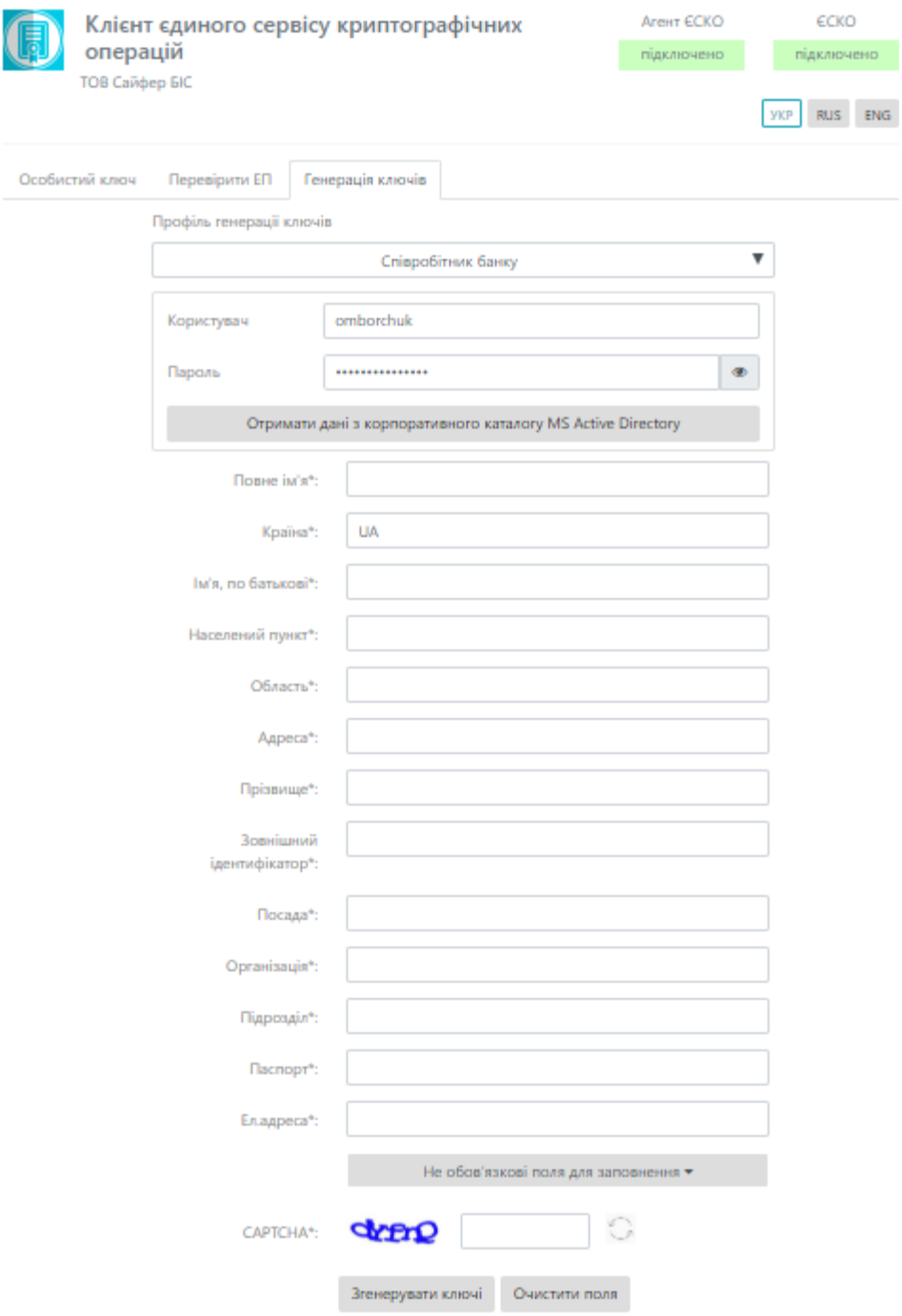

Рис. 90. Форма для персональних даних

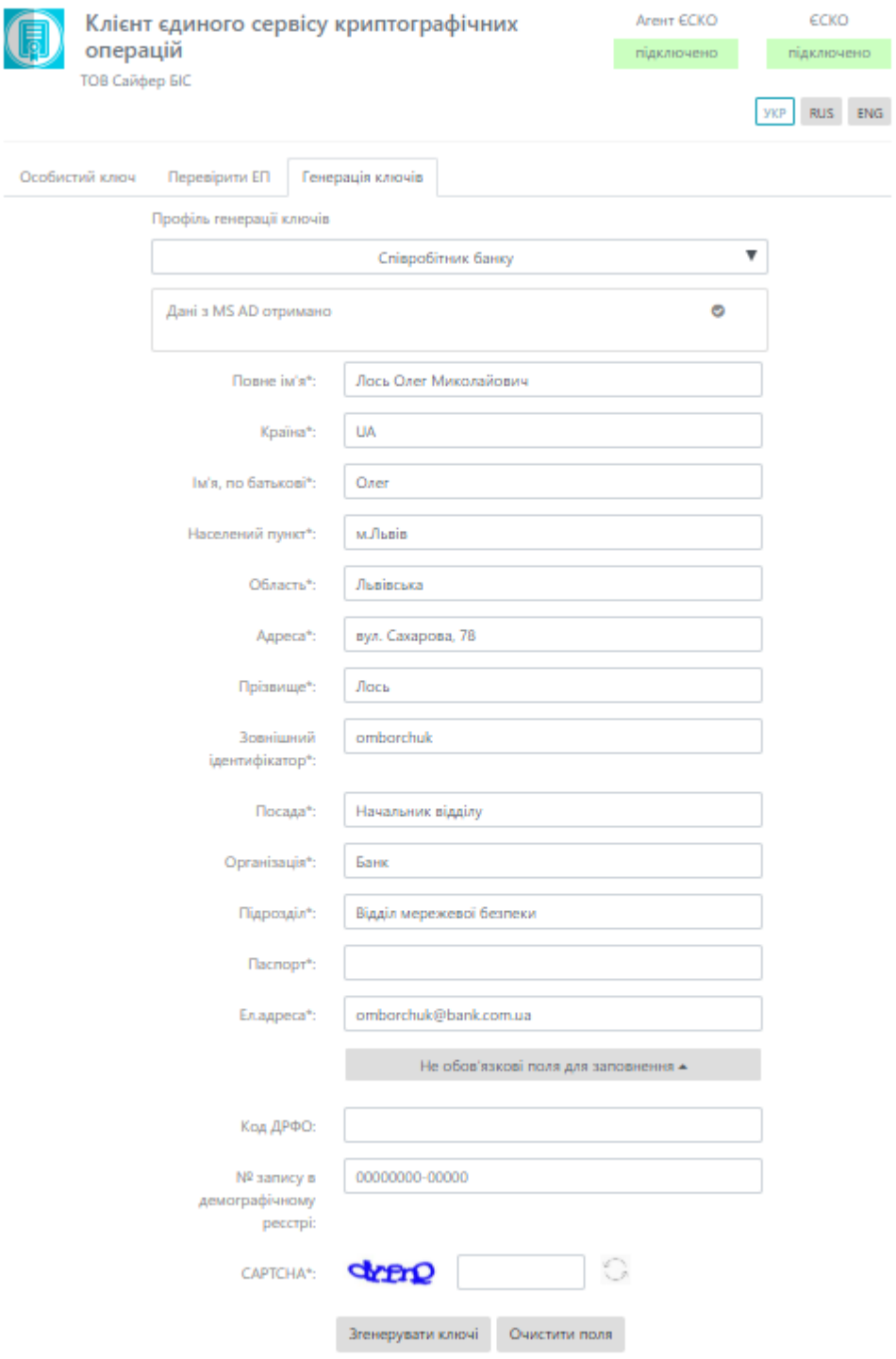

Рис. 91. Заповнена форма для персональних даних

З’являється нове вікно з параметрами нового ключового контейнеру, у залежності від того куди буде збережено ключ, то слід звернути увагу на різницю у параметрах, якщо:

- Збереження відбувається у файл на диску.

Необхідно для поля Тип вказати Файл на диску, для поля Шлях до контейнеру вказати місцерозташування для збереження файлу, для цього слід натиснути «…» та вказати шлях, двічі вказати пароль та натиснути «ОК», Рис. 92.

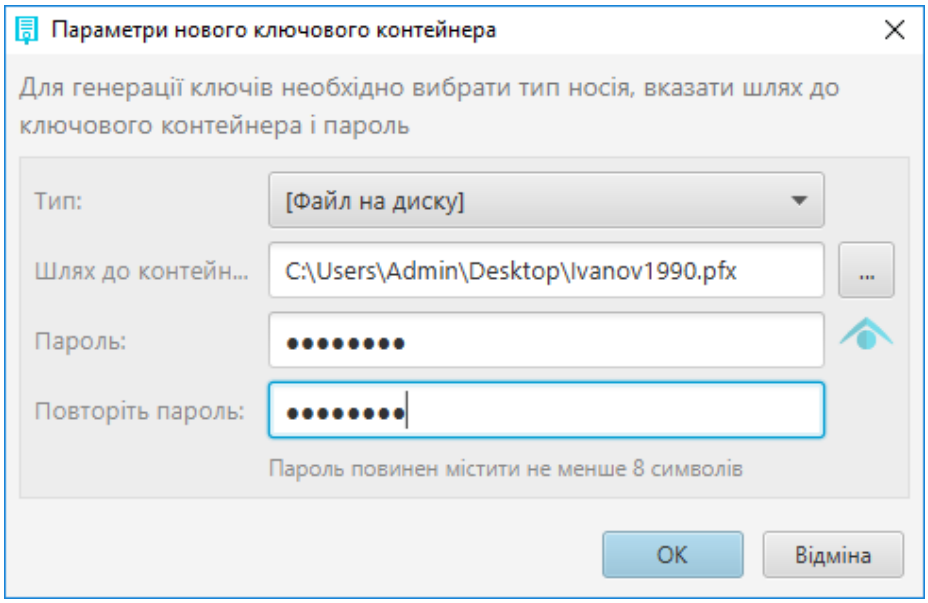

Рис. 92. Збереження ключа у файл на диску

- Збереження відбувається на захищений носій

Необхідно для поля Тип вказати активний чи пасивний режим, для поля Шлях до контейнеру вказати під'єднаний носій для збереження файлу, для цього слід натиснути «…», двічі вказати пароль та натиснути «ОК», Рис. 93.

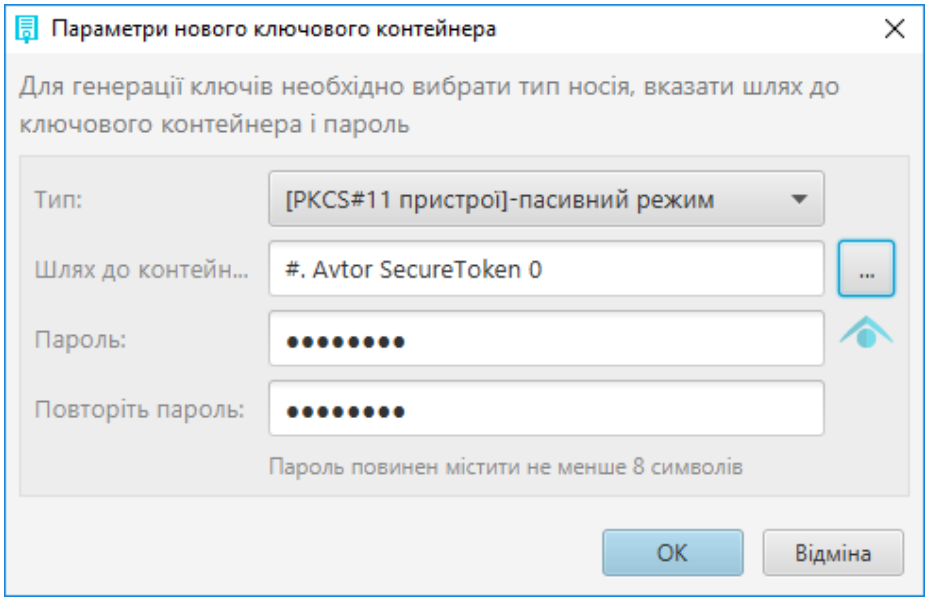

Рис. 93. Збереження ключа на захищений носій

Після коректного введення всіх даних у вікно «Параметри нового ключового контейнеру» з'являється віно з повідомлення про успішну генерацію ключів, Рис. 94.

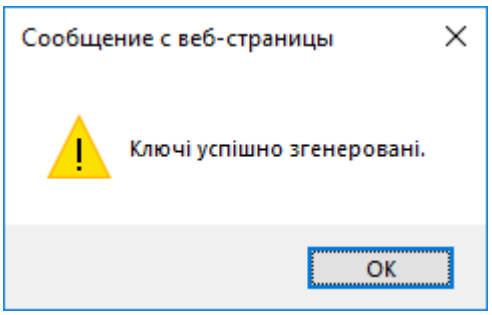

Рис. 94. Повідомлення про успішну генерацію ключів

Зміна ключів

Зміна ключів, до закінчення строку дії яких менше 14 днів

Для зміни ключів обов'язкове завантаження Агенту ЄСКО. Далі слід вказати КНЕДП/АЦСК, тип ключа, шлях до контейнера та пароль, Рис. 95.

Після завантаження ключа з'являється повідомлення про виконання зміни ключа, у повідомленні вказано кількість днів до завершення дії ключів, пропонується одразу виконати зміну, Рис. 96.

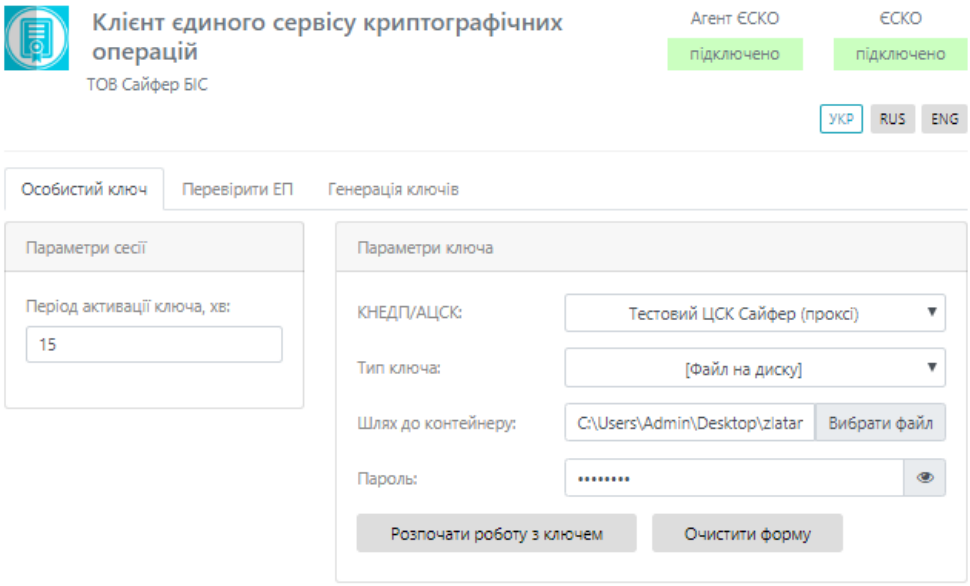

Рис. 95. Завантаження ключа

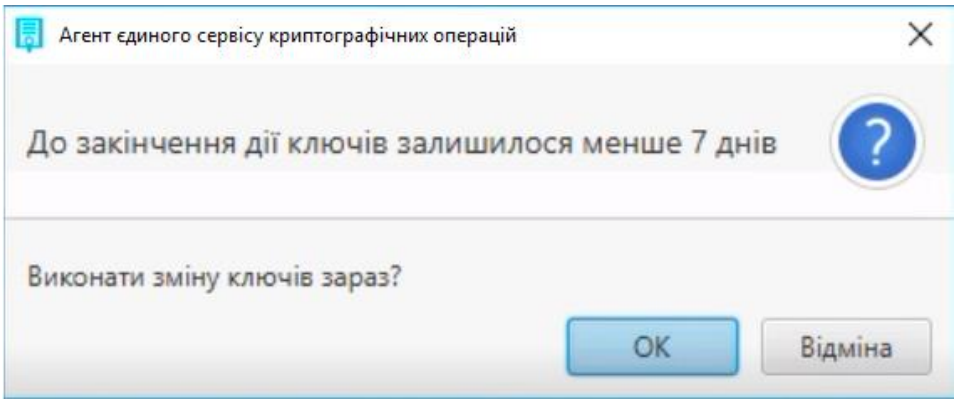

Рис. 96. Повідомлення про закінчення строку дії ключів

Слід зауважити, якщо до звершення строку дії ключів залишається один день, то здійснюється примусова зміна ключів, тобто повідомлення, яке зображене на Рис. 96 не виникає, одна пропонується зміна паролю до ключового контейнеру.

Пропонується вказати пароль до ключа двічі до ключового контейнеру, Рис. 97.

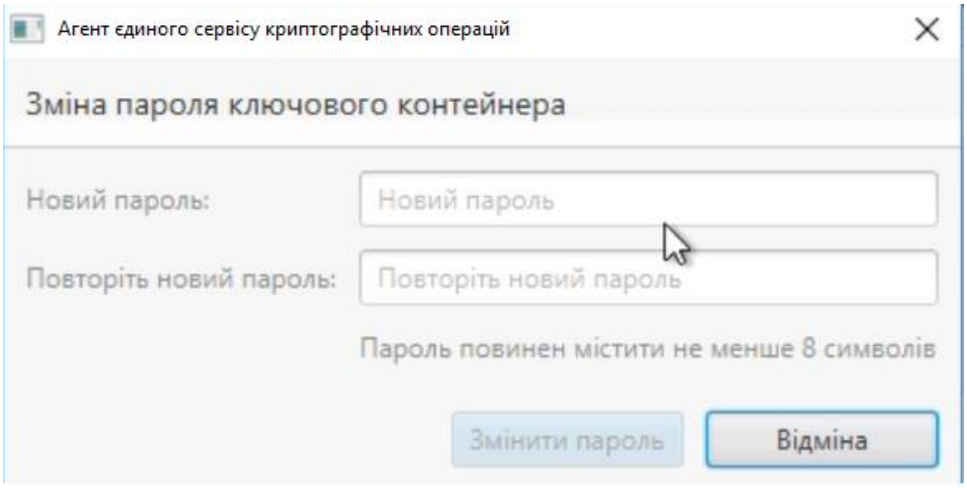

Рис. 97. Введення паролю до ключового контейнеру

Після вказівки паролю до ключового контейнеру з'являється повідомлення про відправлення запиту на зміну ключа ЕП та шифрування до Центру сертифікації, Рис. 98 та Рис. 99.

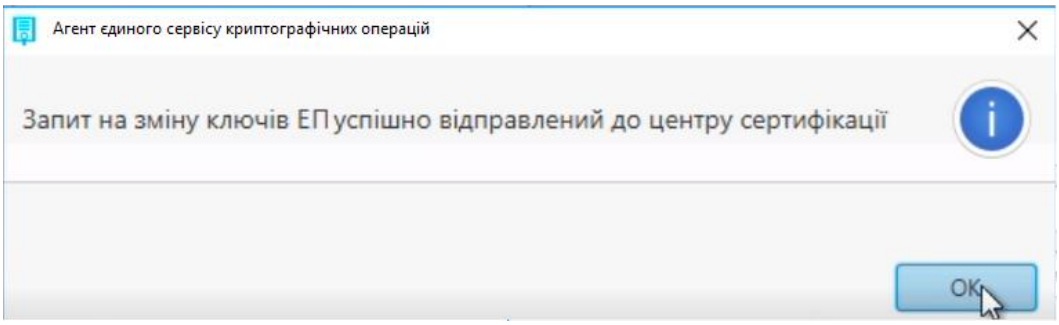

Рис. 98. Запит на зміну ключів ЕП успішно відправлений до Центру сертифікації

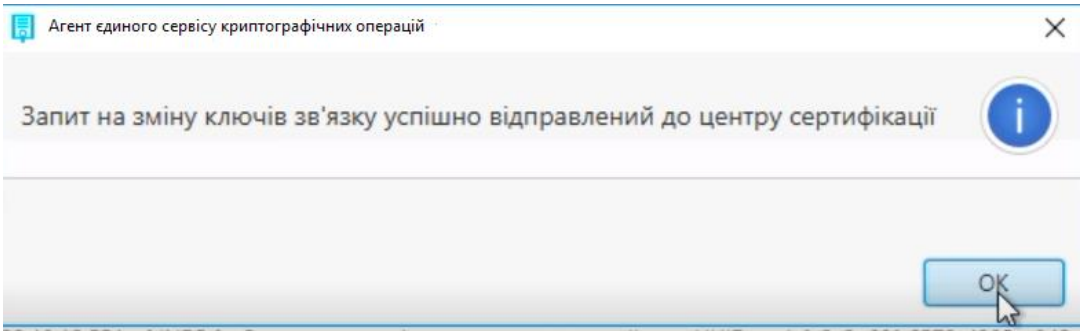

Рис. 99. Запит на зміну ключів зв’язку успішно відправлений до Центру сертифікації

Далі створюється контекст, Рис. 100, з ключем строк дії, якого ще не закінчився, після того як у Центрі сертифікації буде засвідчено запити, то дати до ключа зміняться та не будуть з’влятися повідомлення про повторне відправлення запиту на зміну ключів.

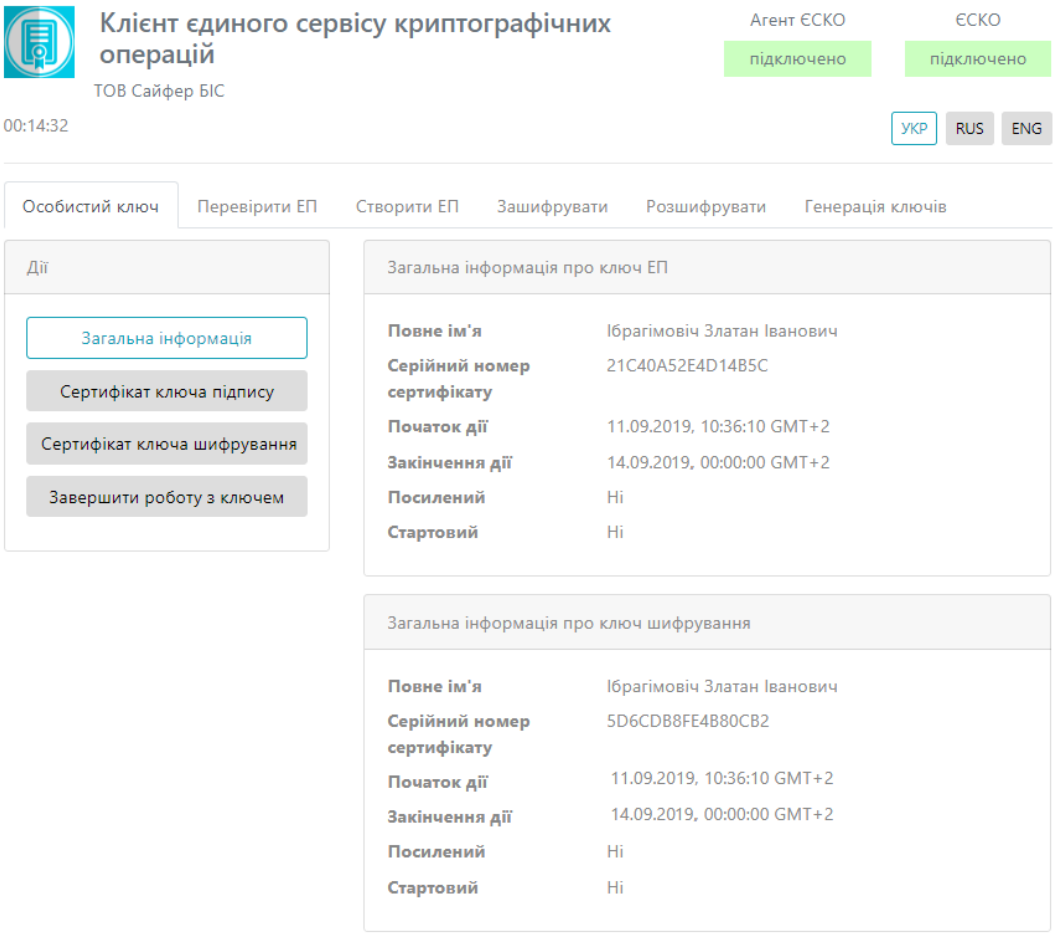

Рис. 100. Створення контексту з ключем

Зміна стартових ключів

Для зміни ключів обов’язкове завантаження Агенту ЄСКО. Далі слід вказати КНЕДП/АЦСК, тип ключа, шлях до контейнера та пароль, Рис. 101.

Після завантаження ключа з’являється повідомлення про виконання зміни ключа, у повідомленні вказано, що ключі є стартовими, пропонується одразу виконати зміну, Рис. 102.

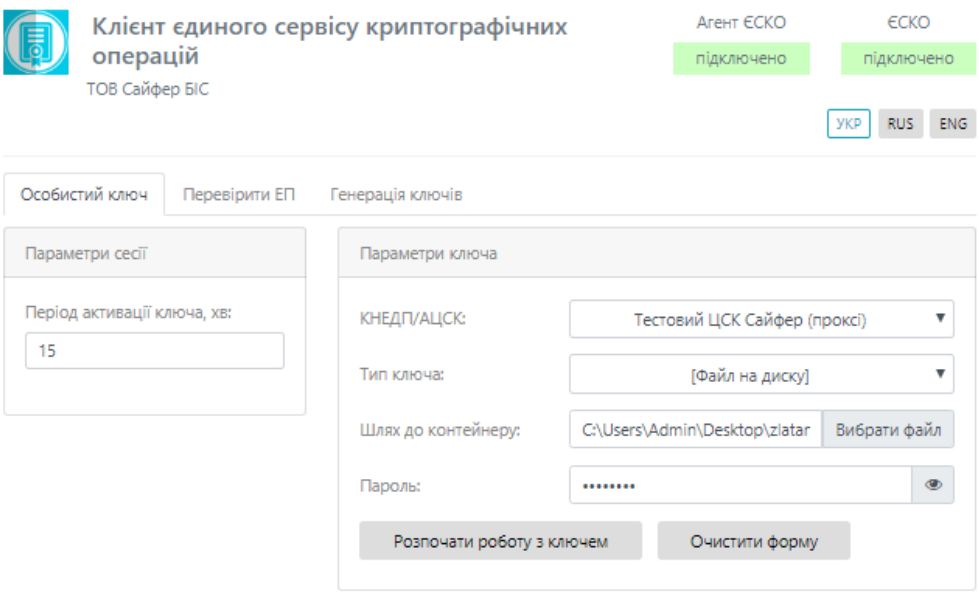

Рис. 101. Завантаження ключа

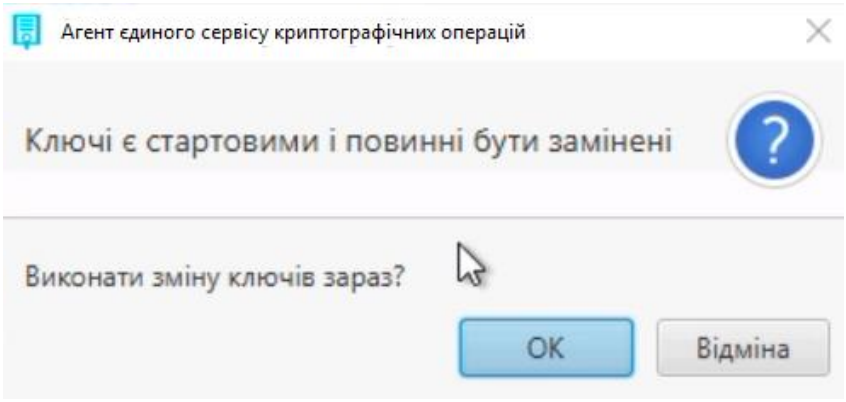

Рис. 102. Повідомлення про те, що ключі є стартовими

Пропонується вказати пароль до ключа двічі до ключового контейнеру, Рис. 103.

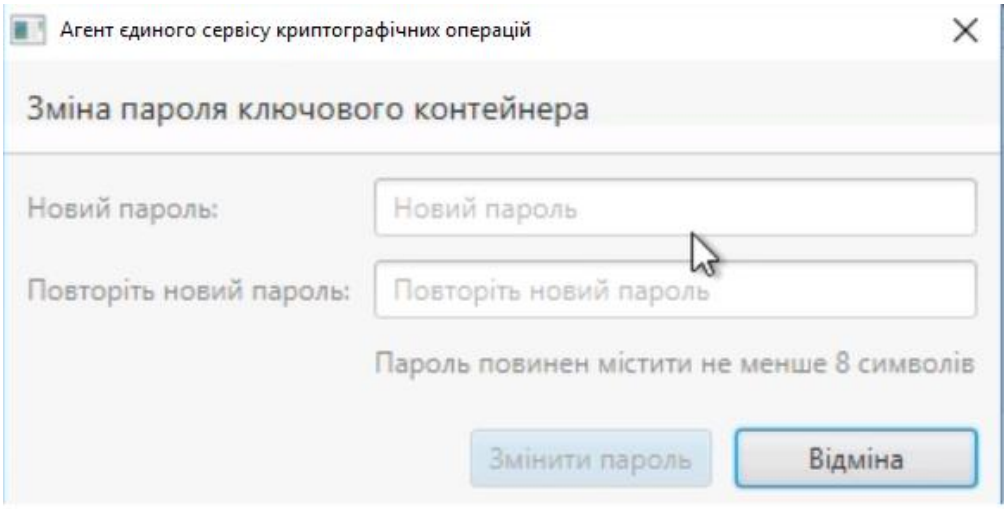

Рис. 103. Введення паролю до ключового контейнеру

Після вказівки паролю до ключового контейнеру з’являється повідомлення про відправлення запиту на зміну ключа ЕП та шифрування до Центру сертифікації, Рис. 104 та Рис. 105.

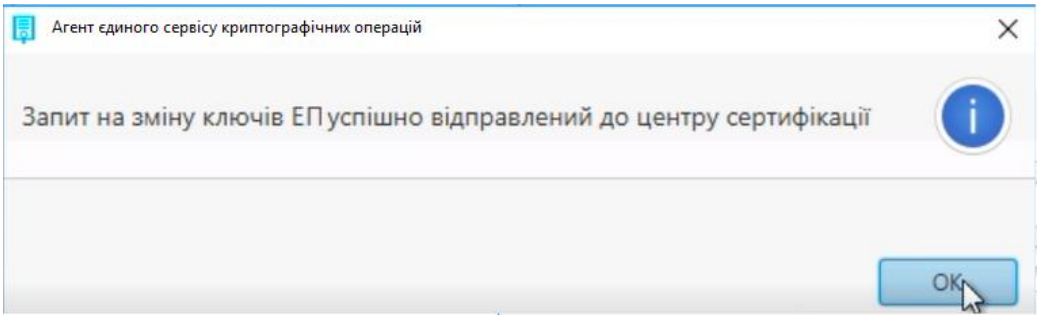

Рис. 104. Запит на зміну ключів ЕП успішно відправлений до Центру сертифікації

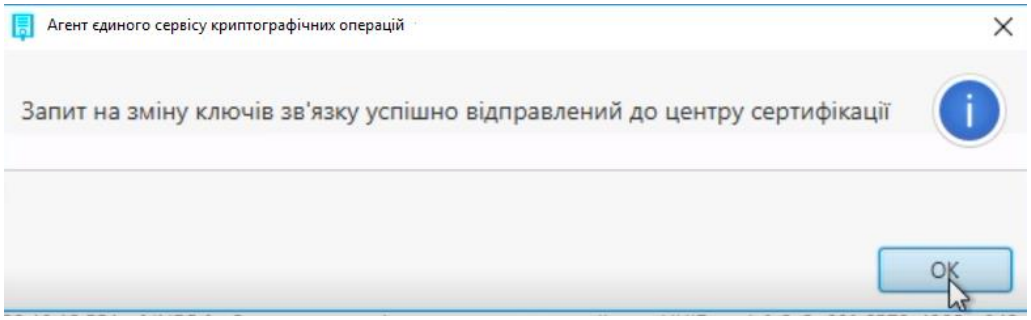

Рис. 105. Запит на зміну ключів зв’язку успішно відправлений до Центру сертифікації

Після засвідчення запитів у Центрі сертифікації, можна створювати контекст та працювати з ключем у звичному режимі.

MobileID

Відеоінструкція знаходиться за посиланням.

Для авторизації з ключем, який знаходиться на SIM-карті в ЄСКО, необхідно змінити «Тип ключа» на «Мобільний ЕП (MobileID)», Рис. 106.

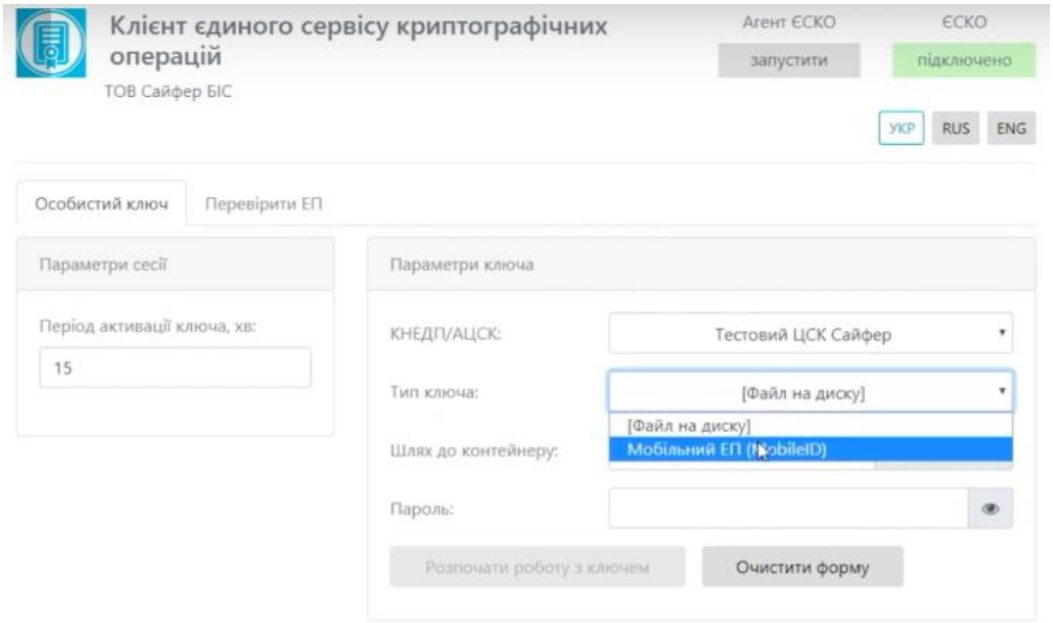

Рис. 106. Вибір «Мобільного ЕП»

Після зміни типу ключа, видозмінюється вікно «Параметри ключа», де слід вказати оператора та номер телефону, Рис. 107-Рис. 108.

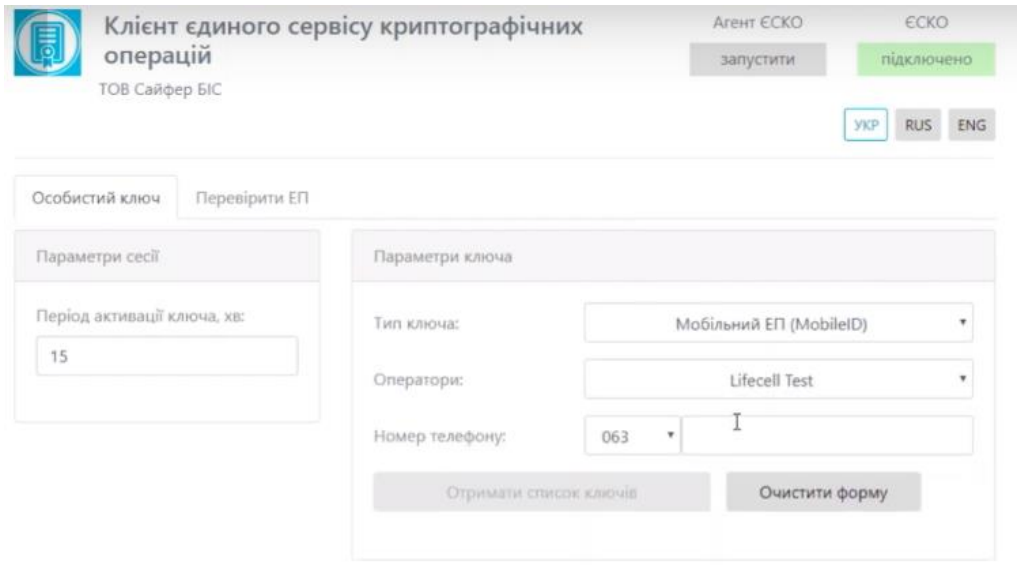

Рис. 107. Заповнення поля «Оператор»

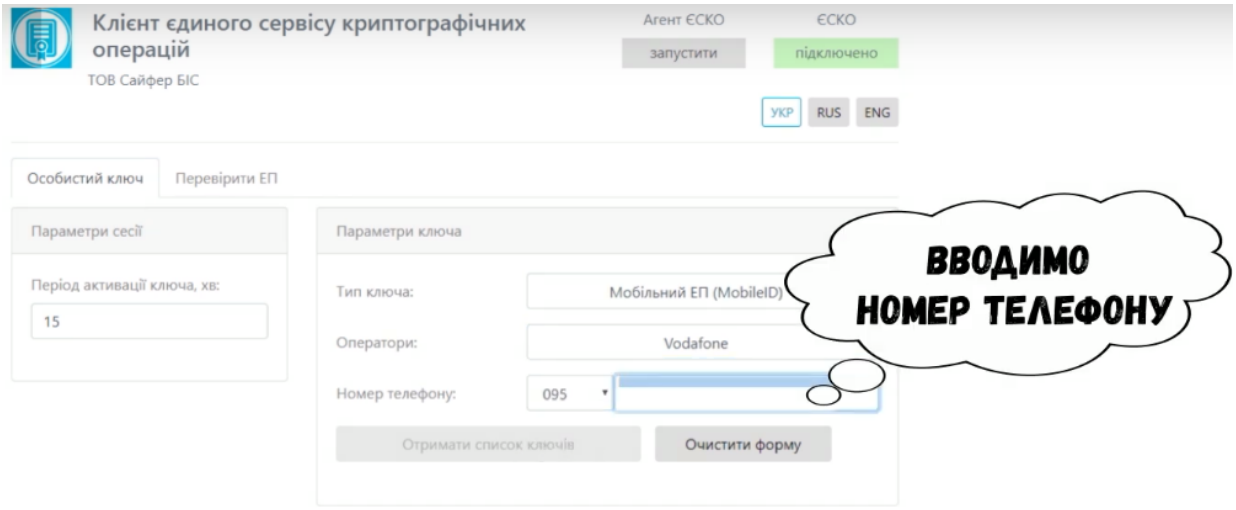

Рис. 108. Заповнення поля «Номер телефону»

Наступним кроком є отримання списку ключів, натиснувши відповідну кнопку у вікні «Параметри ключа», Рис. 109.

Одночасно на телефон приходить повідомлення про надання дозволу відображення посад додатку (Рис. 110), де необхідно «Дозволити» та ввести ПІН-код до ключа, Рис. 111.

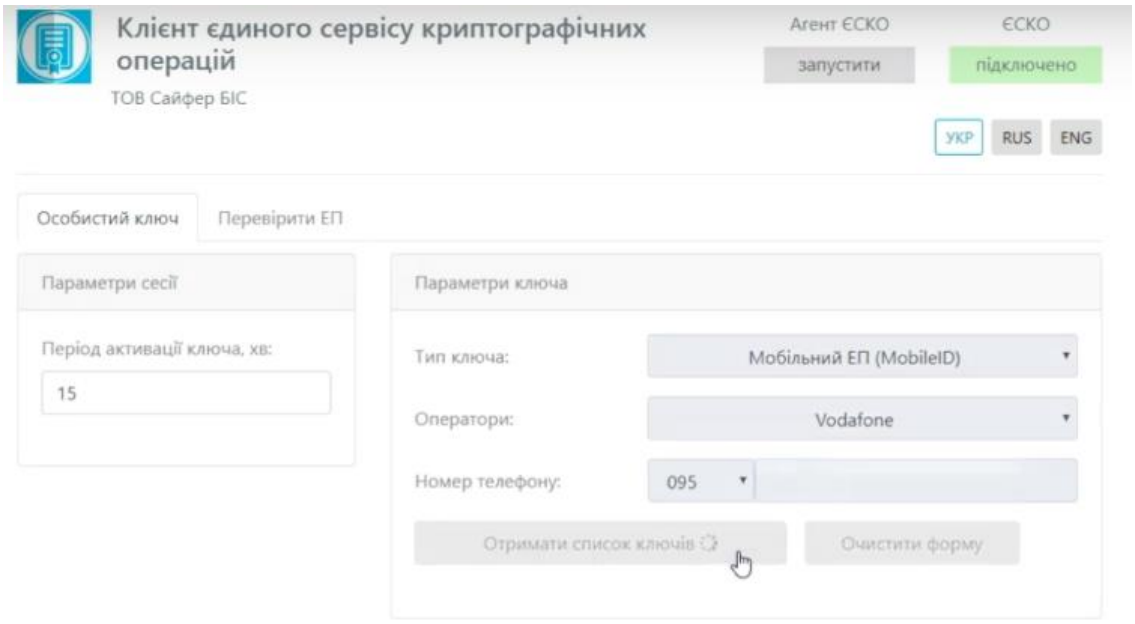

Рис. 109. Отримання списку доступних ключів

Рис. 110. Дозвіл на відображення посад додатку

Рис. 111. Введення ПІН-коду

Після успішного введення ПІН-коду, у браузері з'являється нове поле «Ключ», де необхідно обрати ключ, який необхідно використовувати (на SIM-карті може бути кілька ключів), Рис. 112.

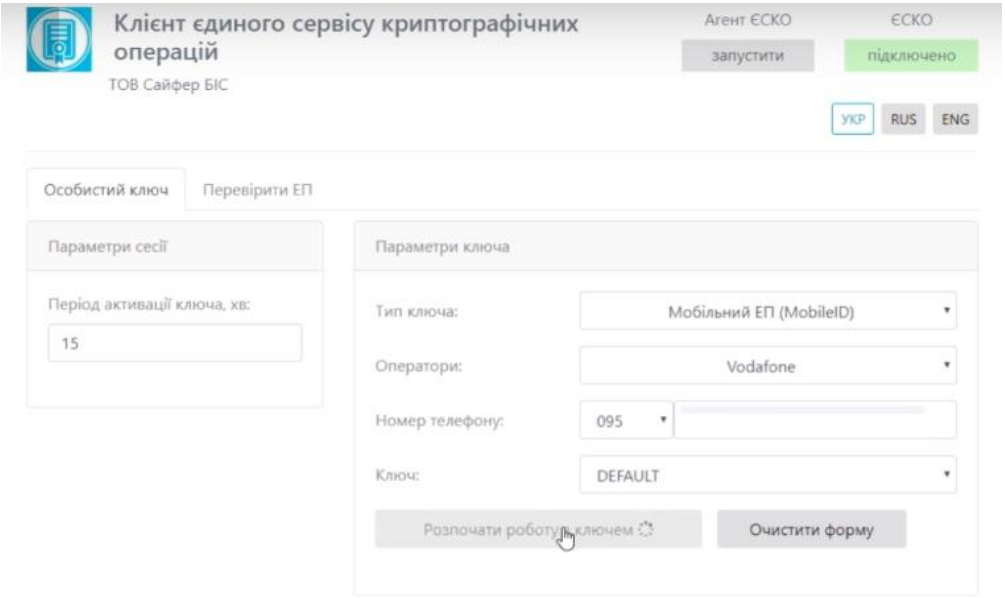

Рис. 112. Вибір ключа

Натиснувши кнопку «Розпочати роботу з ключем» створюється криптографічний контекст, де можна виконати наступні дії:

- Переглянути інформацію про сертифікат ключа ЕП, Рис. 113;
- Перевірити ЕП (доступно і без ключа);

- Створити ЕП.

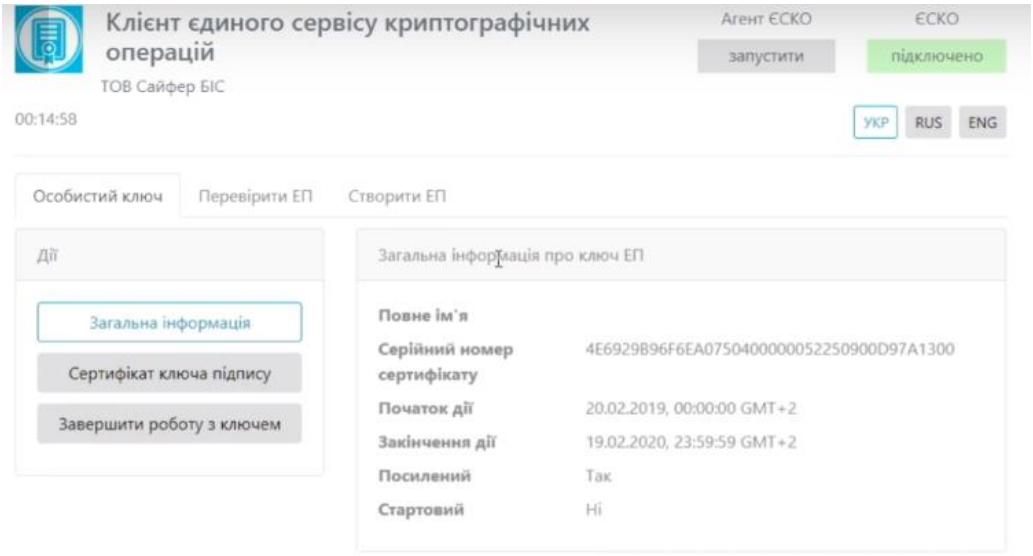

Рис. 113. Перегляд загальної інформації про ключ

Створення мобільного ЕП

За аналогією, як і при створенні звичайного підпису (за допомогою файлового контейнеру), необхідно завантажити файл/файли/текстові дані та натиснути кнопку «Створити ЕП», Рис. 114.
На телефон приходить повідомлення про підтвердження створення ЕП та введення ПІН-коду, Рис. 115-Рис. 116.
Про успішне створення мобільного ЕП повідомляється у відповідному повідомлені, Рис. 117.

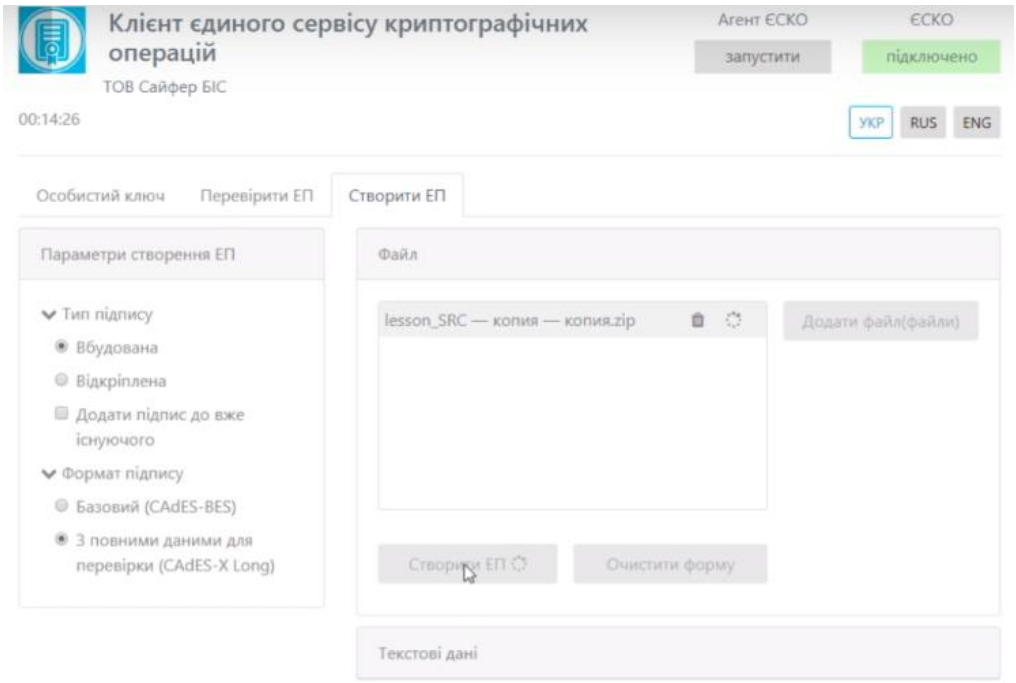

Рис. 114. Створення мобільного ЕП

Рис. 115. Підтвердження створення мобільного ЕП

Рис. 116. Введення ПІН-коду

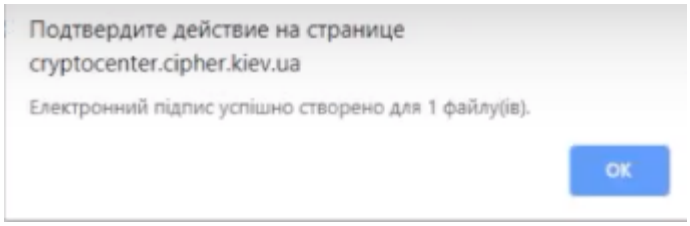

Рис. 117. Повідомлення про створення ЕП