Дата модифікації: 25/10/2024

Єдиний Криптографічний Центр

Настанова з установки та експлуатації Агенту ЄКЦ

ЗМІСТ

Вступ

В цьому документі описано порядок дій користувача для використання програмного комплексу «Єдиного Криптографічного Центру», а саме Агенту ЄКЦ 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: 3 ГБ та вище;
- Процесор – 1,2 ГГц;
- LAN: 100 Мбіт/с.

Мінімальні вимоги до програмного забезпечення:

- Вимоги до ОС:
    - ОС Windows (Windows 10 і вище, Windows Server 2016 і вище);
    - ОС Ubuntu, Oracle Linux;
    - MacOS - Sonoma (2023) та вище.
- Браузери, що підтримуються:
    - Mozilla Firefox;
    - Google Chrome;
    - Safari.

Підтримка захищених носіїв

Агент Єдиного криптографічного центру 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:

- Author Secure Token-338, 337 Series, Author Smart Card-337 Series.
- Plasticard TEllipse 3/4 (обов'язкове встановлення ПЗ).
- ІІТ Алмаз-1К (обов'язкове встановлення ПЗ: EKAlmaz1CInstall.exe (завантажити за посиланням) та EUInstall.exe (доступне за посиланням), також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- ІІТ Кристал-1 (обов'язкове встановлення ПЗ: EKeyCrystal1Install.exe (завантажити за посиланням) та EUInstall.exe (доступне за посиланням), також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- Avest AvestKey.
- Efit Key.

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:

- Author Secure Token-338, 337 Series, Author Smart Card-337 Series.
- Plasticard TEllipse 3/4 (обов'язкове встановлення ПЗ).
- ІІТ Алмаз-1К (обов'язкове встановлення ПЗ: EKAlmaz1CInstall.exe (завантажити за посиланням) та EUInstall.exe (доступне за посиланням), також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- ІІТ Кристал-1 (обов'язкове встановлення ПЗ: EKeyCrystal1Install.exe (завантажити за посиланням) та EUInstall.exe (доступне за посиланням), також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- Avest AvestKey.
- Efit Key.

Підготовка робочого місця для роботи із застосунком «Агент ЄКЦ

Завантаження файлу дистрибутиву застосунку «Агент ЄКЦ»

У веб-браузері перейти за посиланням - https://cryptocenter.kredobank.com.ua/ до Клієнту Єдиного Криптографічного Центру. Рис. 1.

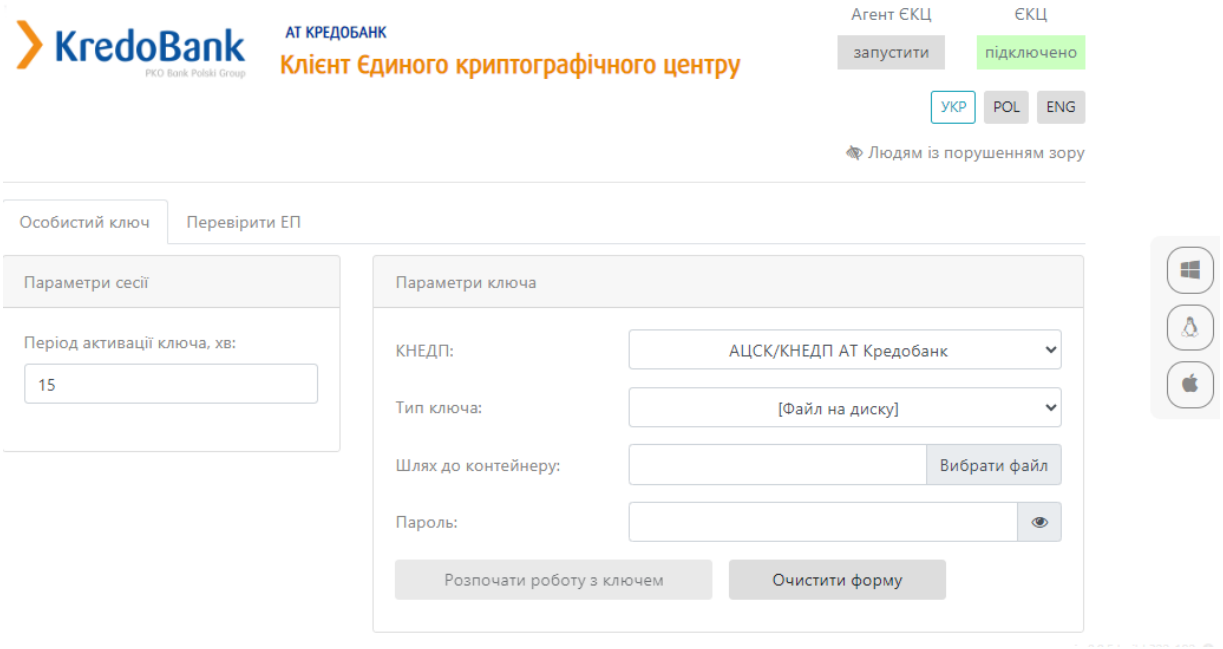

Рис. 1. Стартове вікно ЄКЦ

Навести на піктограму відповідної операційної системи, для якої необхідно завантажити дистрибутив (Рис. 2) та натиснути на неї. Розпочнеться завантаження файлу дистрибутиву в папку *Завантаження*.

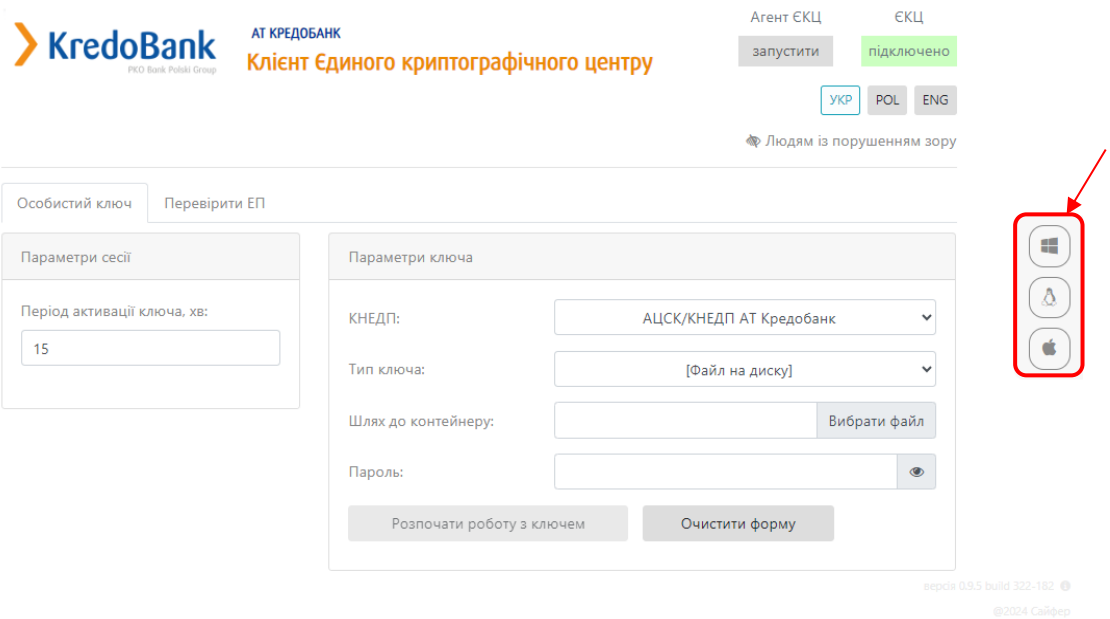

Рис. 2. Піктограми ОС для завантаження дистрибутиву

Встановлення застосунку «Агент ЄКЦ» з дистрибутива

Операційна система Windows

Для інсталяції застосунку для ОС Windows (наведено приклад для ОС Windows 10 x64) необхідно послідовно виконати наступні дії.

Запустити завантажений файл дистрибутиву (наприклад, файл дистрибутиву *Agent_UOS_windows-x32_3_0_5-b148.exe*) від імені Адміністратора та слідувати підказкам «Майстра установки».

Після появи стартового вікна, необхідно обрати мову та натиснути «ОК», Рис. 3.

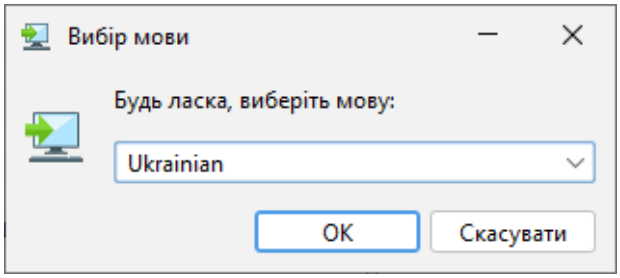

Рис. 3. Стартове вікно «Майстра установки»

У вікні вітання майстра встановлення застосунку натиснути «Далі», Рис. 4.

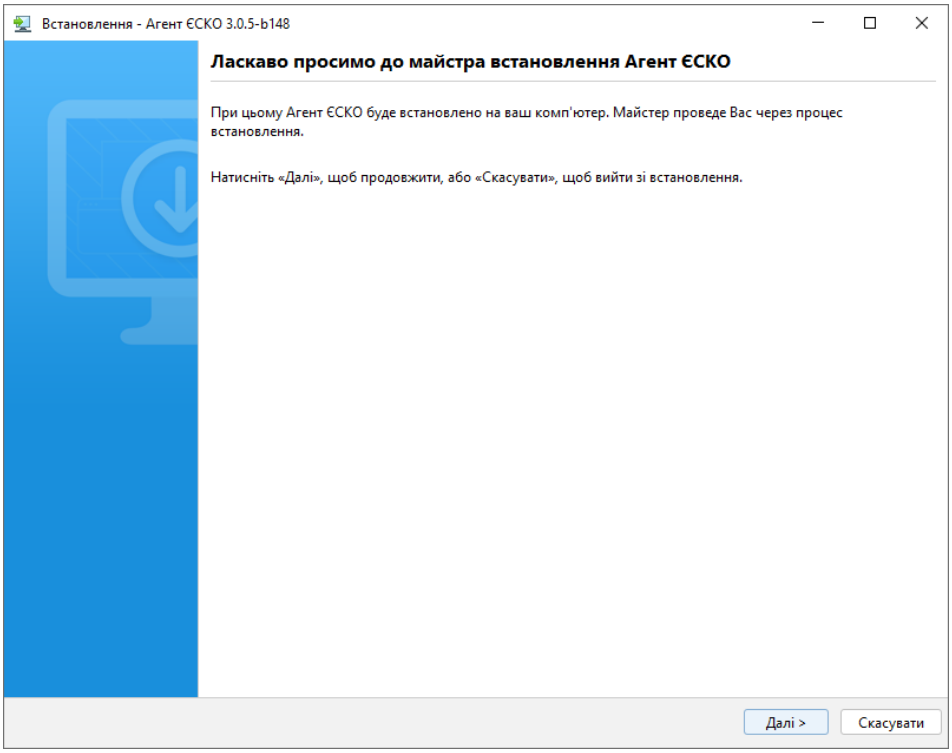

Рис. 4. Вітання майстра встановлення застосунку

У наступному вікні обрати пункт «Я приймаю умови угоди» та натиснути «Далі», Рис. 5.

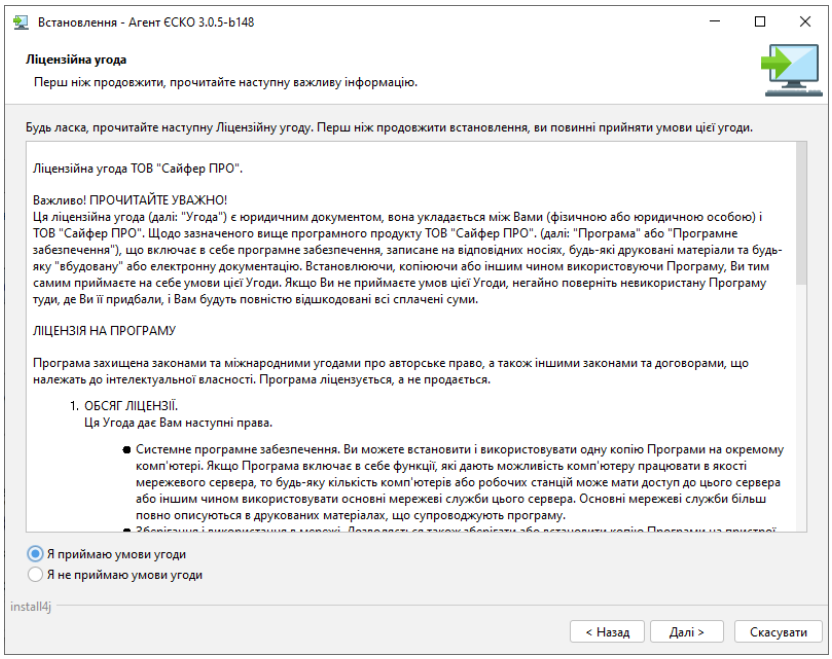

Рис. 5. Вікно ліцензійної угоди

У наступному вікну надається змога налаштувати параметри проксі-сервера, якщо доступ до мережі Інтернет з робочого місця користувача здійснюється за його допомогою. Для цього необхідно натиснути на поле «Потрібне налаштування проксі» та виконати певні налаштування, Рис. 6.

Якщо доступ до мережі Інтернет з робочого місця користувача здійснюється без використання проксі-сервера, необхідно натиснути «Далі».

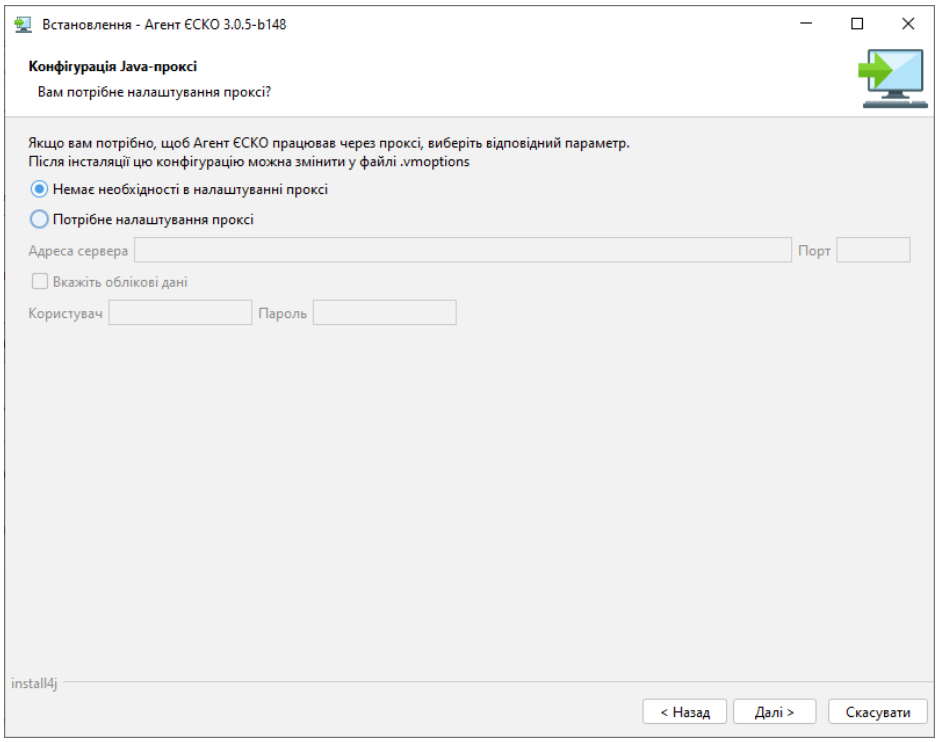

Рис. 6. Налаштування параметрів проксі-сервера

Вибір каталогу для інсталяції застосунку (Майстром установки запропонований каталог «за замовчуванням», за необхідності його можна змінити, натиснувши кнопку «Перегляд» та обрати необхідний каталог). Після цього натиснути «Далі», Рис. 7.

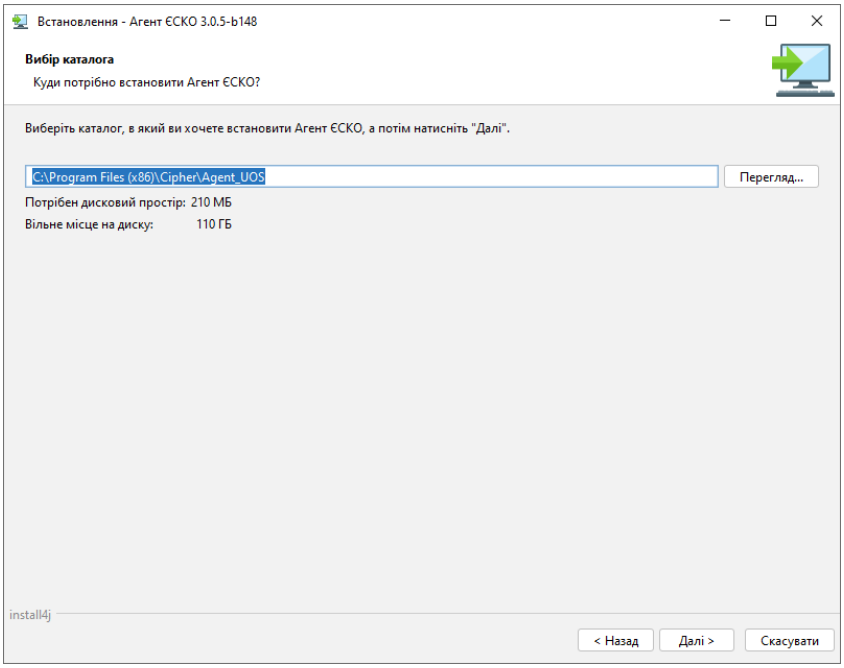

Рис. 7. Вибір шляху для встановлення застосунку

Вибір каталогу для розміщення ярликів застосунку (Майстром установки запропонований каталог «за замовчуванням», за необхідності його можна змінити, вказавши назву у відповідному полі). Також є можливість не створювати каталог для розміщення ярликів застосунку, створити ярлики тільки для користувача, який безпосередньо встановлює дистрибутив застосунку на ПК та працює під власним профілем в ОС або для всіх користувачів водночас. Для цього необхідно відмітити відповідні поля, Рис. 8. Після цього натиснути «Далі».

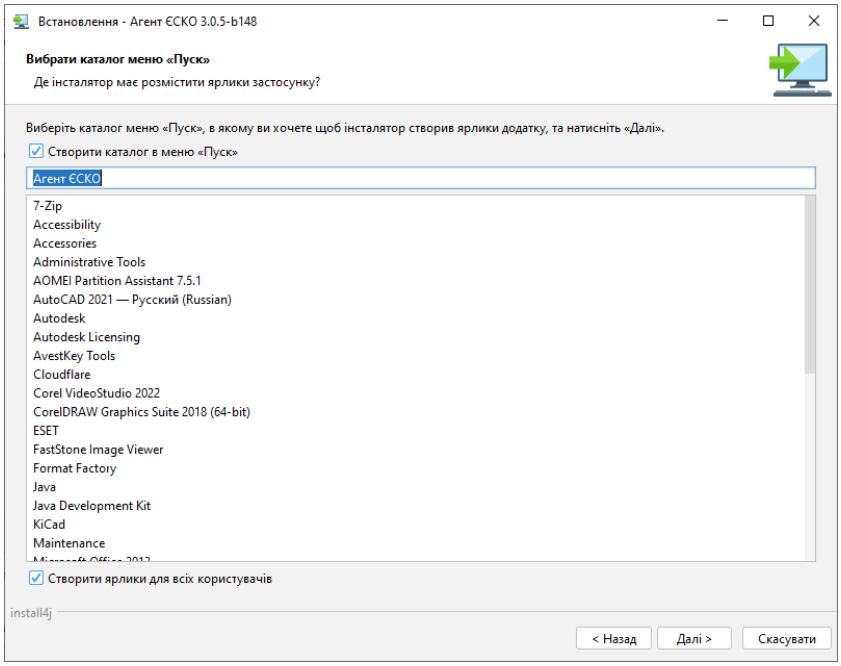

Рис. 8. Вибір шляху для встановлення ярликів застосунку

В наступному вікні є можливість не створювати ярлик для застосунку на робочому столі, для цього необхідно зняти відмітку у відповідному полі. За замовчуванням ярлик створюється. Після чого натиснути «Далі», Рис. 9.

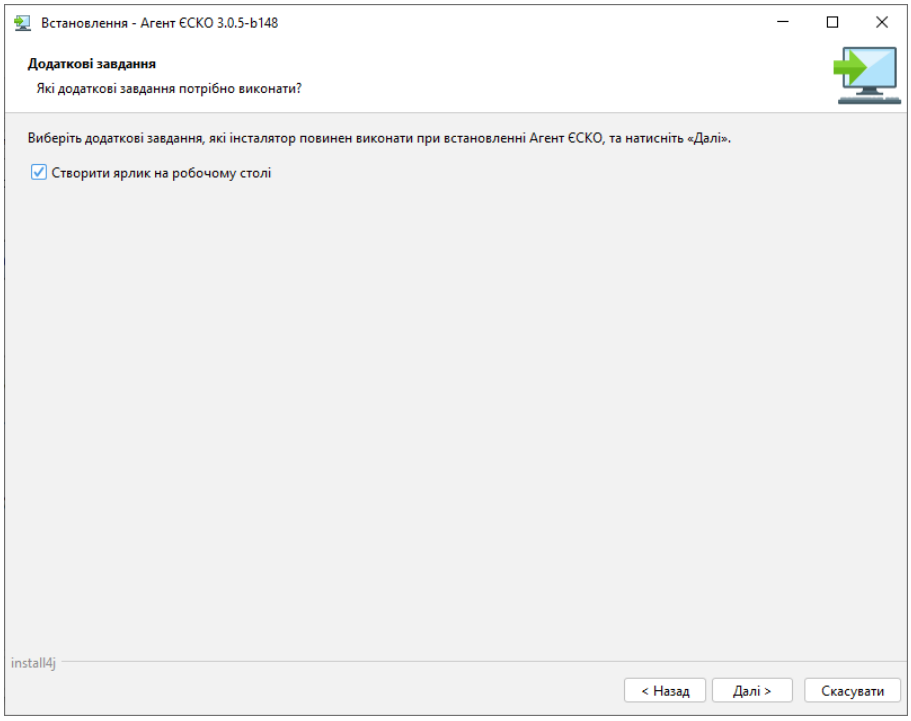

Рис. 9. Налаштування додаткових параметрів ярлика застосунку

Далі починається розпакування та запис файлів на ПК, Рис. 10.

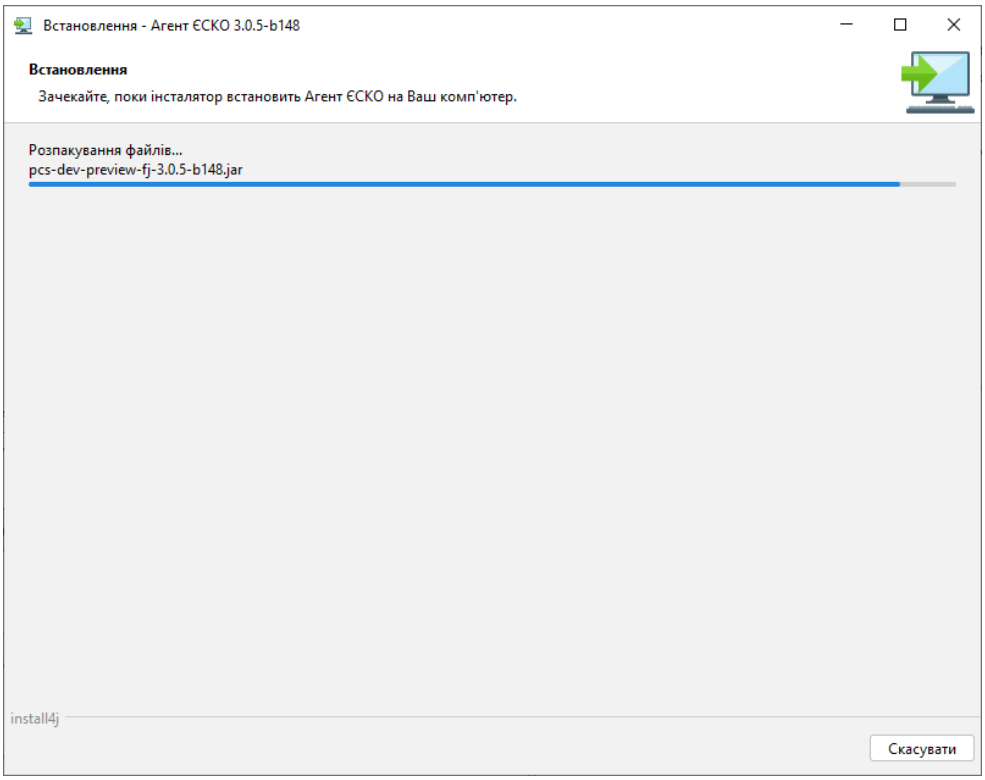

Рис. 10. Процес встановлення застосунку

Після завершення встановлення застосунку є можливість відразу його запустити, для чого необхідно натиснути «Готово», Рис. 11. У разі, коли немає потреби у його запуску необхідно зняти відмітку у відповідному полі.

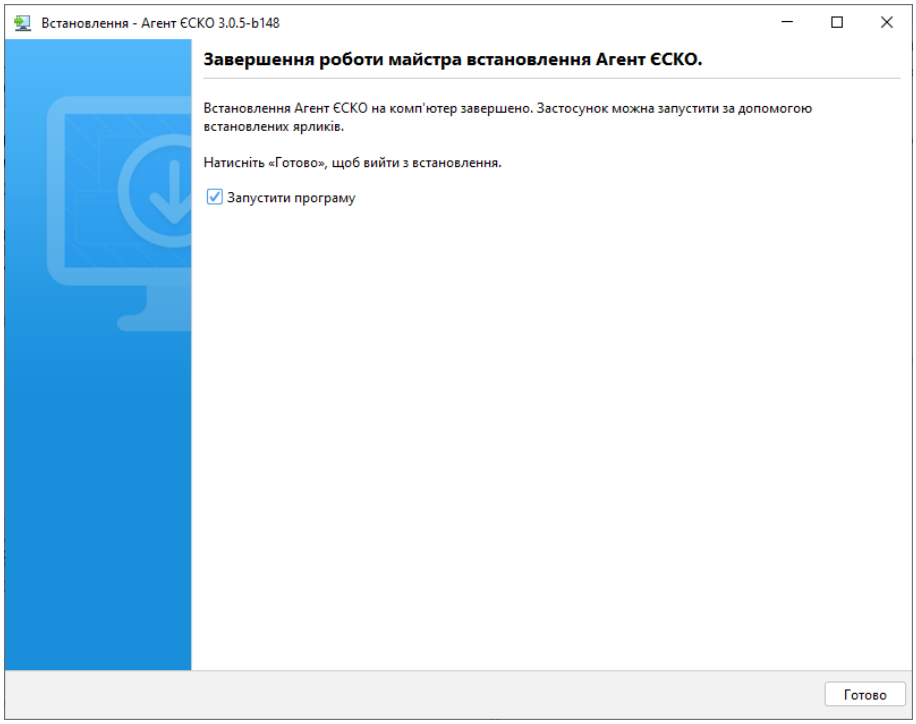

Рис. 11. Завершення процесу встановлення застосунку

Для початку роботи слід запустити застосунок «Агент_UOS», натиснувши на ярлик на робочому столі або запустити його, обравши зі списку встановлених на ПК програм, Рис. 12.

Рис. 12. Запуск застосунку «Агент ЄКЦ»

*. У випадку, якщо доступ до мережі Інтернет з робочого місця користувача здійснюється за допомогою проксі-сервера, необхідно додати у виключення: Не використовувати проксі-сервер для адрес (*127.0.0.1; local.cipher.kiev.ua; localhost)*

Операційна система Linux

Для інсталяції застосунку для ОС Linux (наведено приклад для ОС OracleLinux 9.3 x64) необхідно послідовно виконати наступні дії.

Для встановлення завантаженого дистрибутиву в ОС (наприклад, файл дистрибутиву *Agent_UOS_unix-3_0_5-b148.sh*), необхідно запустити програму "Термінал" (Ctrl+Alt+T) та в командному рядку ввести команди:

- для здійснення переходу до каталогу, в який був завантажений дистрибутив:

```
cd /home/xxx/Downloads
```

- для запуску процесу інсталяції дистрибутива застосунку:

```
sh Agent_UOS_unix-3_0_5-b148.sh
```

Після появи стартового вікна, необхідно обрати мову та натиснути «ОК», Рис. 13.

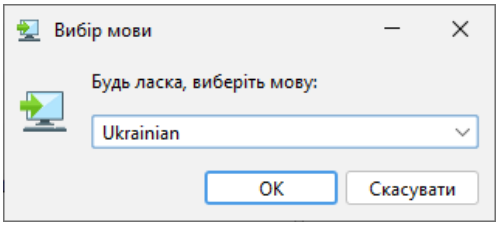

Рис. 13. Стартове вікно «Майстра установки»

Далі необхідно ввести пароль від імені суперкористувача та натиснути «Аутентифікація», Рис. 14.

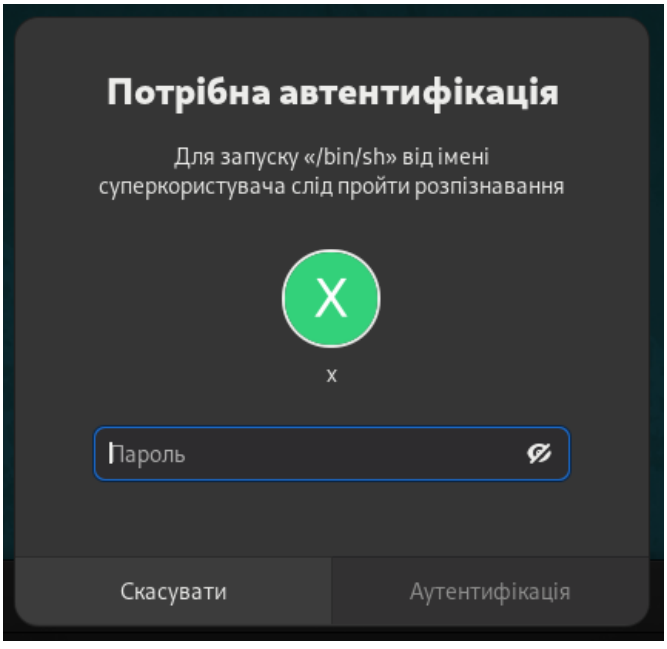

Рис. 14. Вікно автентифікації супер користувача

У вікні вітання майстра встановлення застосунку натиснути «Далі», Рис. 15.

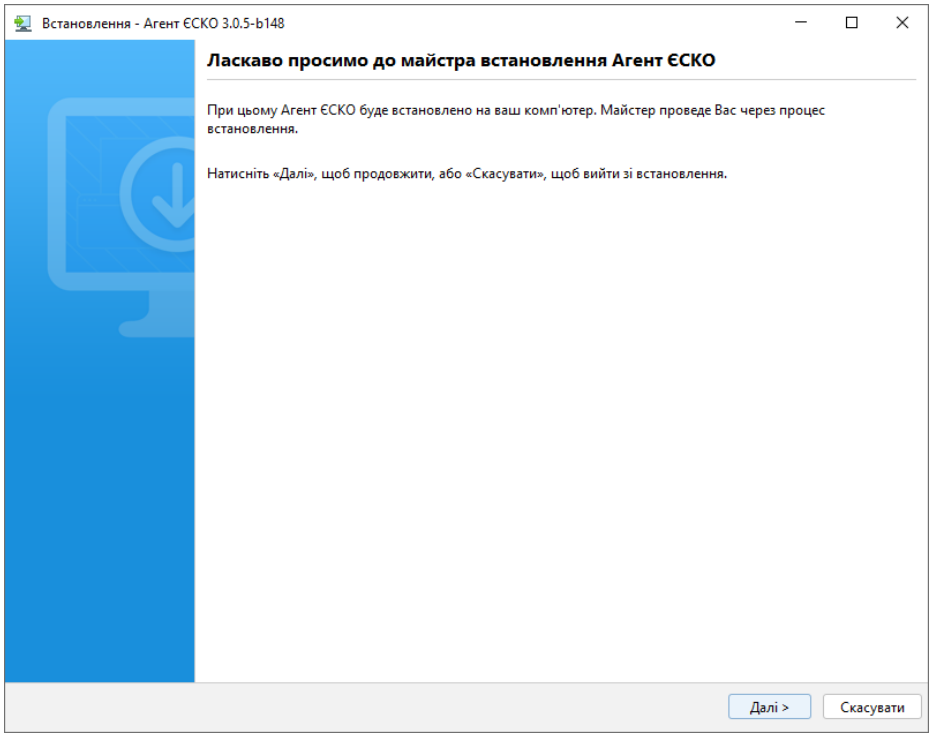

Рис. 15. Вітання майстра встановлення застосунку

У наступному вікні обрати пункт «Я приймаю умови угоди» та натиснути «Далі», Рис. 16.

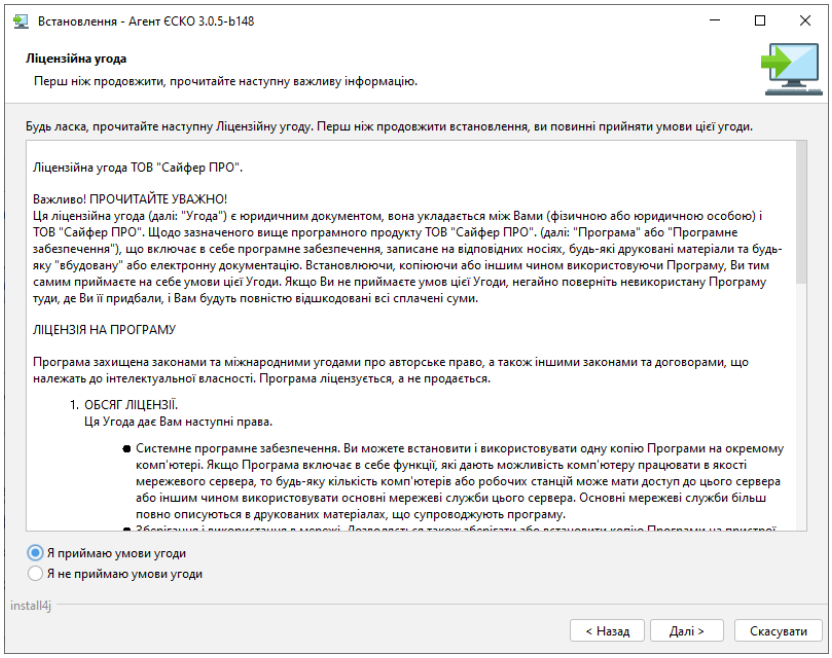

Рис. 16. Вікно ліцензійної угоди

У наступному вікну надається змога налаштувати параметри проксі-сервера, якщо доступ до мережі Інтернет з робочого місця користувача здійснюється за його допомогою. Для цього необхідно натиснути на поле «Потрібне налаштування проксі» та виконати певні налаштування, Рис. 17.

Якщо доступ до мережі Інтернет з робочого місця користувача здійснюється без використання проксі-сервера, необхідно натиснути «Далі».

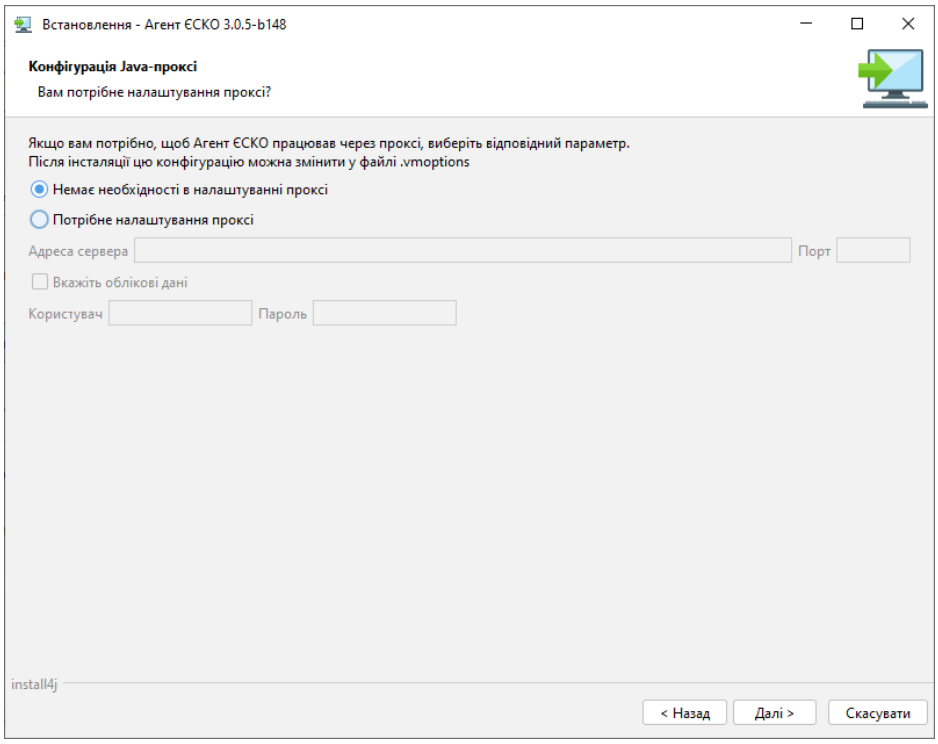

Рис. 17. Налаштування параметрів проксі-сервера

Вибір каталогу для інсталяції застосунку (Майстром установки запропонований каталог «за замовчуванням», за необхідності його можна змінити, натиснувши кнопку «Перегляд» та обрати необхідний каталог). Після цього натиснути «Далі», Рис. 18.

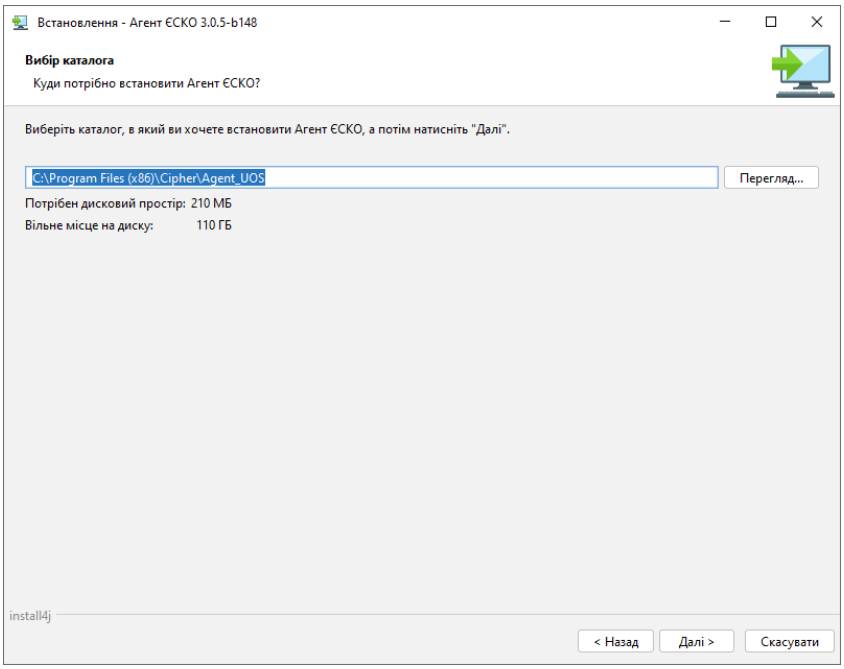

Рис. 18. Вибір шляху для встановлення застосунку

Вибір каталогу для розміщення ярликів застосунку (Майстром установки запропонований каталог «за замовчуванням», за необхідності його можна змінити, вказавши назву у

відповідному полі). Також є можливість не створювати каталог для розміщення ярликів застосунку, створити ярлики тільки для користувача, який безпосередньо встановлює дистрибутив застосунку на ПК та працює під власним профілем в ОС або для всіх користувачів водночас. Для цього необхідно відмітити відповідні поля, Рис. 19. Після цього натиснути «Далі».

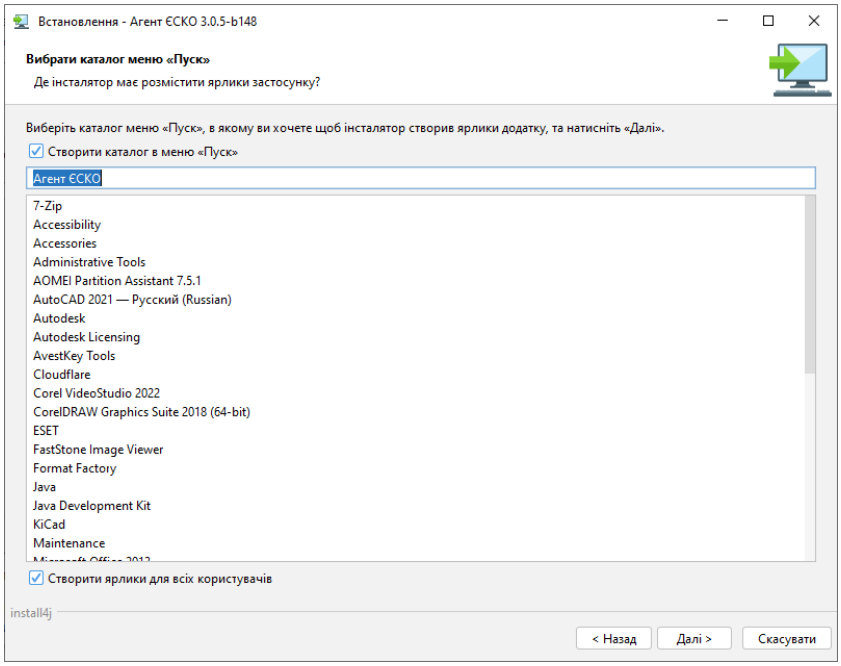

Рис. 19. Вибір шляху для встановлення ярликів застосунку

В наступному вікні є можливість не створювати ярлик для застосунку на робочому столі, для цього необхідно зняти відмітку у відповідному полі. За замовчуванням ярлик створюється. Після чого натиснути «Далі», Рис. 20.

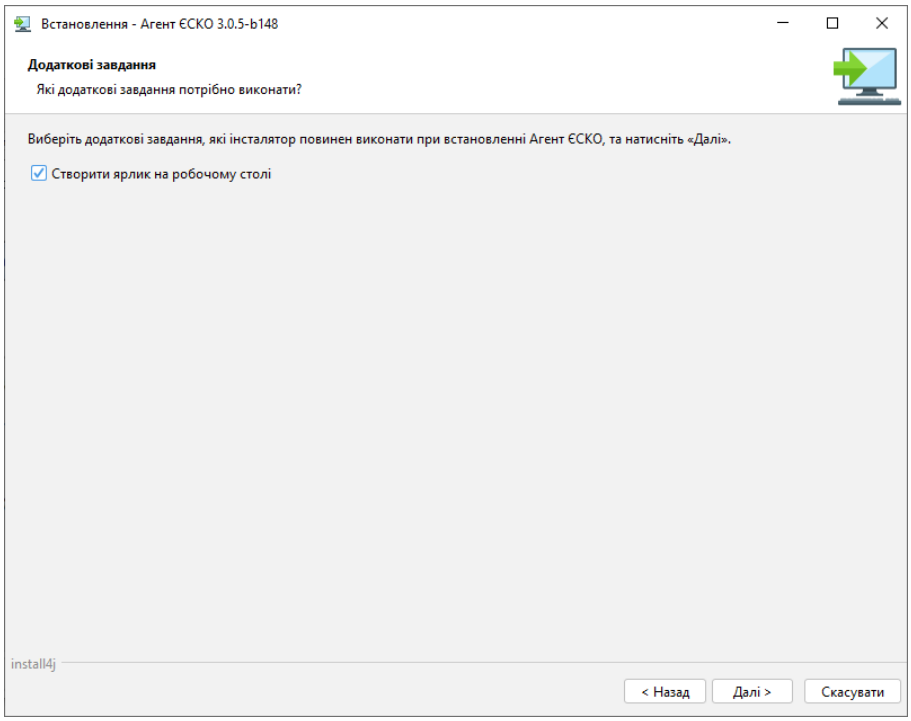

Рис. 20. Налаштування додаткових параметрів ярлика застосунку

Далі починається розпакування та запис файлів на ПК, Рис. 21.

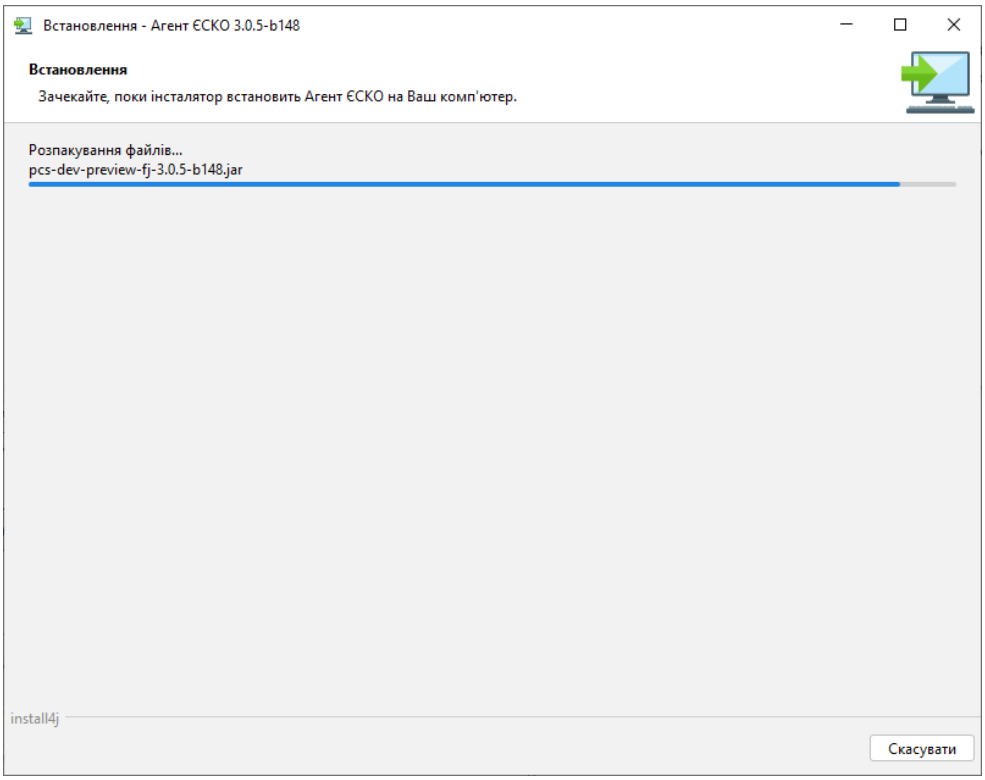

Рис. 21. Процес встановлення застосунку

Після завершення встановлення застосунку є можливість відразу його запустити, для чого необхідно натиснути «Готово», Рис. 22. У разі, коли немає потреби у його запуску необхідно зняти відмітку у відповідному полі.

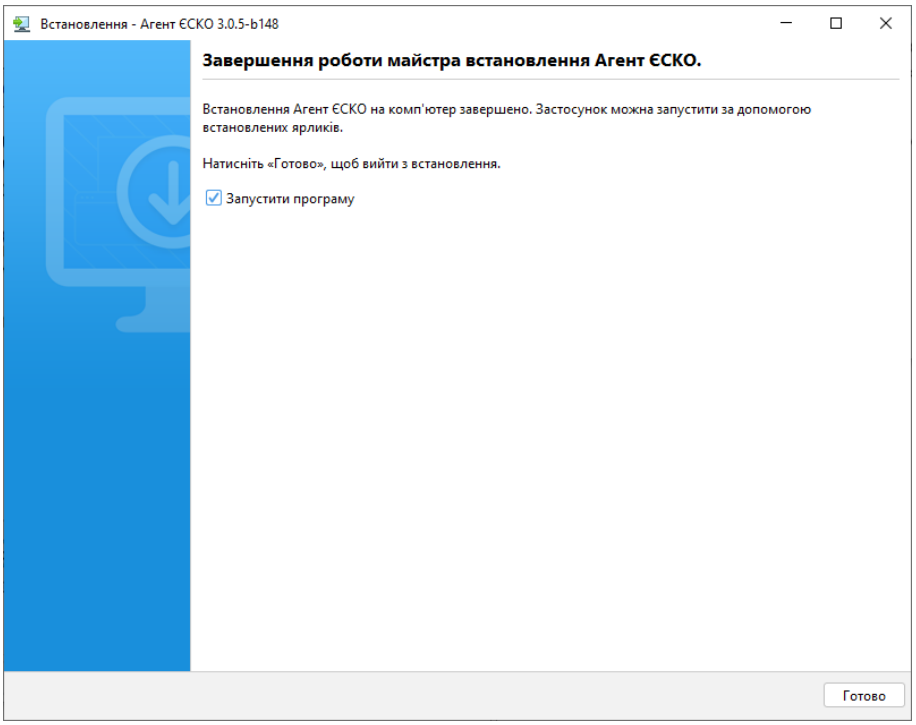

Рис. 22. Завершення процесу встановлення застосунку

Ярлик застосунку буде розміщений у загальному списку встановлених в операційній системі. Для початку роботи слід запустити застосунок «Агент_UOS», Рис. 23.

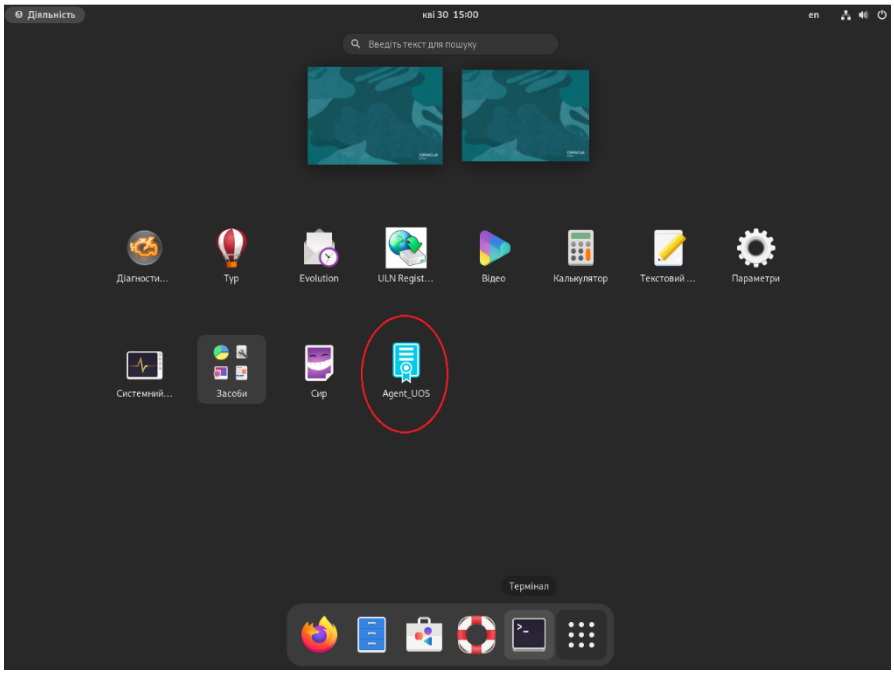

Рис. 23. Розміщення ярлику застосунку

Операційна система MacOS

Для інсталяції застосунку для MacOS (наведено приклад для MacOS Sonoma 14.4.1) необхідно послідовно виконати наступні дії.

Запустити завантажений файл дистрибутиву (наприклад, файл дистрибутиву *Agent_UOS_macos_3_0_5-b148.dmg*), Рис. 24. Натискаємо двічі на значку.

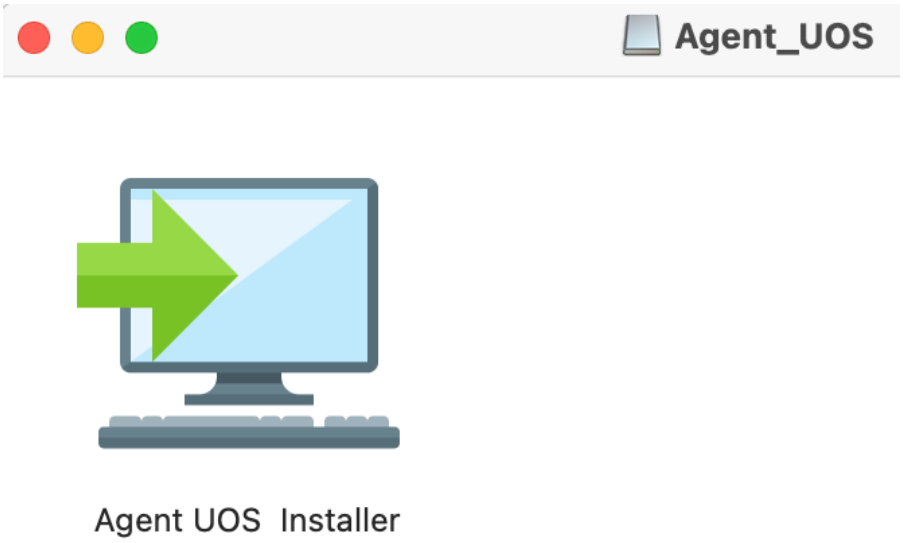

Рис. 24. Завантажений файл дистрибутиву застосунку

З'являється вікно, де зазначено про те, що цей дистрибутив з недовіреного джерела, так як він буде завантажений не з App Store, натискаємо «ОК», Рис. 25.

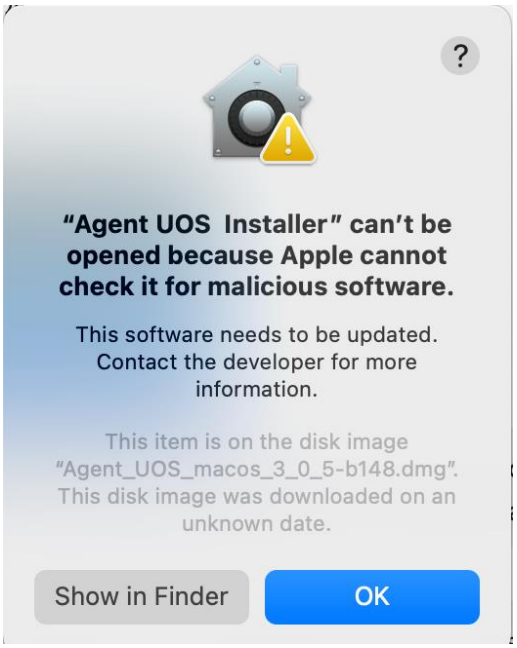

Рис. 25. Вікно-повідомлення про неможливість запустити дистрибутив

Далі необхідно перейти у розділ налаштувань ПК «Privacy&Security» та натиснути на кнопку «Open Anyway», Рис. 26.

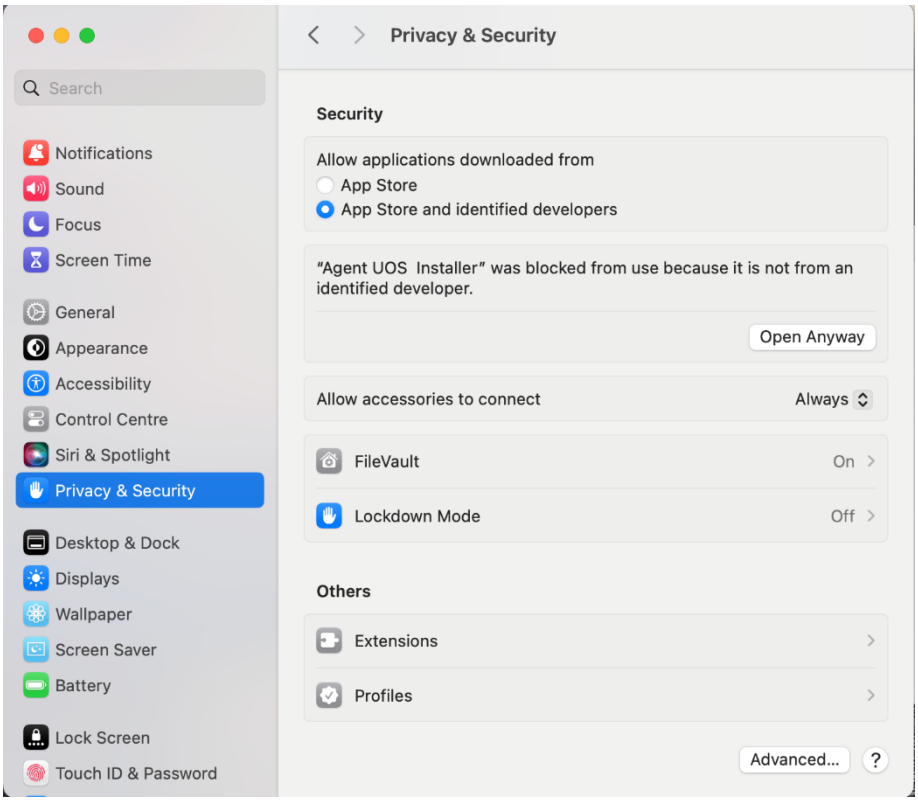

Рис. 26. Вікно-повідомлення про неможливість запустити дистрибутив

Після цього з'явиться вікно, в якому необхідно ввести пароль/відбиток пальця для продовження встановлення, натиснувши «Use Password», Рис. 27.

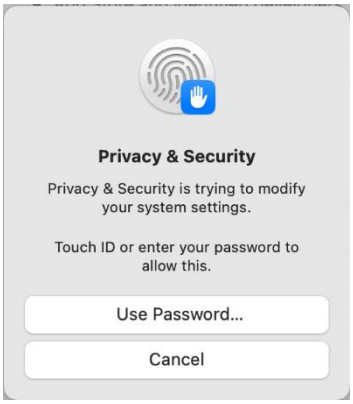

Рис. 27. Введення паролю/вказівка відбитка пальцю

Повторно з'являється повідомлення про те, що дистрибутив завантажено з недовіреного ресурсу, знову треба погодитися натиснувши «Open», Рис. 28.

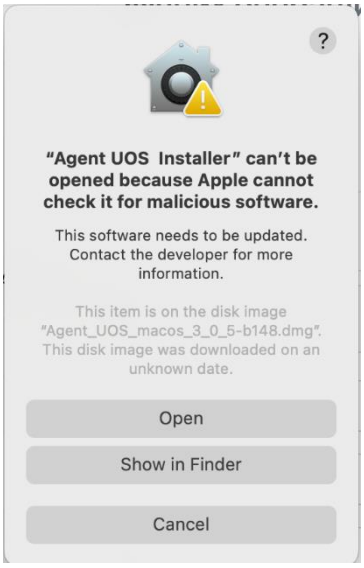

Рис. 28. Вікно-повідомлення про встановлення інсталятору з недовіреного ресурсу

Після цього запуститься «Майстер установки». Після появи стартового вікна, необхідно обрати мову та натиснути «ОК», Рис. 29.

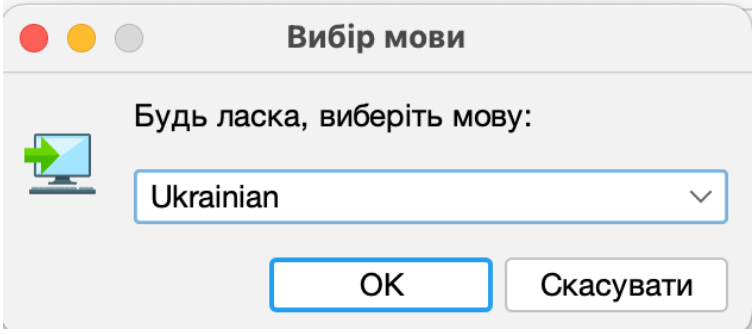

Рис. 29. Стартове вікно «Майстра установки»

У вікні вітання майстра встановлення застосунку натиснути «Далі», Рис. 30.

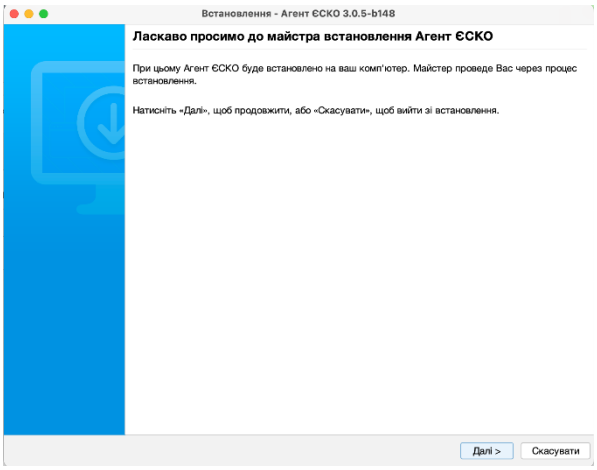

Рис. 30. Вітання майстра встановлення застосунку

У наступному вікні обрати пункт «Я приймаю умови угоди» та натиснути «Далі», Рис. 31.

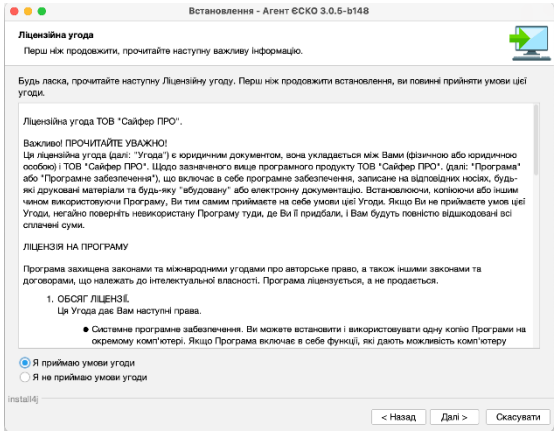

Рис. 31. Вікно ліцензійної угоди

У наступному вікну надається змога налаштувати параметри проксі-сервера, якщо доступ до мережі Інтернет з робочого місця користувача здійснюється за його допомогою. Для цього необхідно натиснути на поле «Потрібне налаштування проксі» та виконати певні налаштування, Рис. 32.

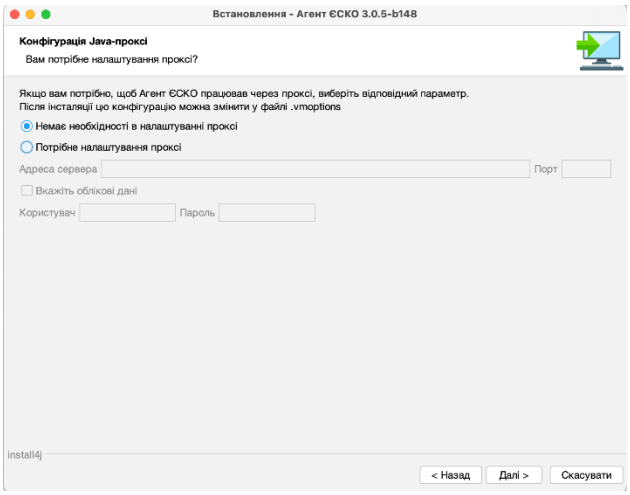

Рис. 32. Налаштування параметрів проксі-сервера

Якщо доступ до мережі Інтернет з робочого місця користувача здійснюється без використання проксі-сервера, необхідно натиснути «Далі».

Вибір каталогу для інсталяції застосунку (Майстром установки запропонований каталог «за замовчуванням», за необхідності його можна змінити, натиснувши кнопку «Перегляд» та обрати необхідний каталог). Після цього натиснути «Далі», Рис. 33.

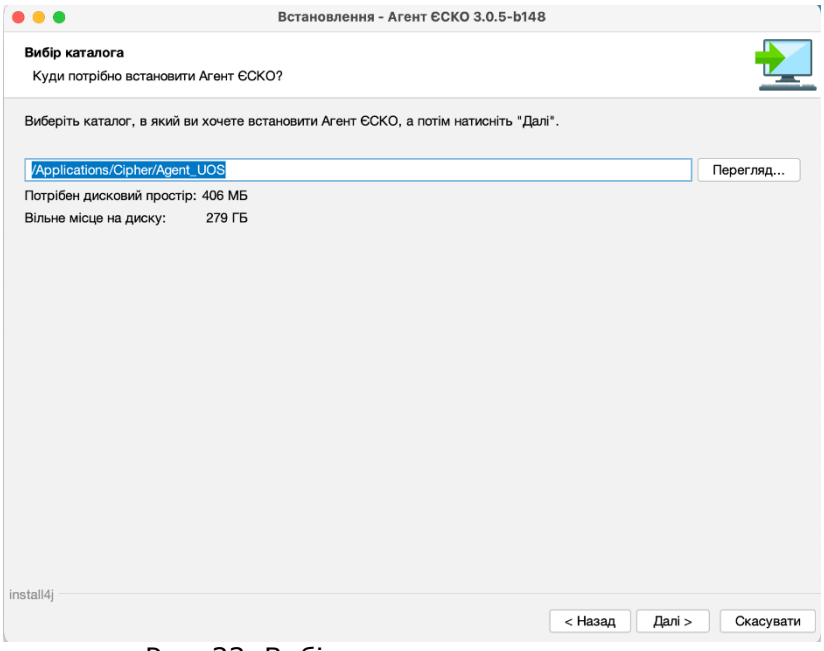

Рис. 33. Вибір шляху для встановлення застосунку

В наступному вікні є можливість не створювати ярлик для застосунку на робочому столі, для цього необхідно зняти відмітку у відповідному полі. За замовчуванням ярлик створюється. Після чого натиснути «Далі», Рис. 34.

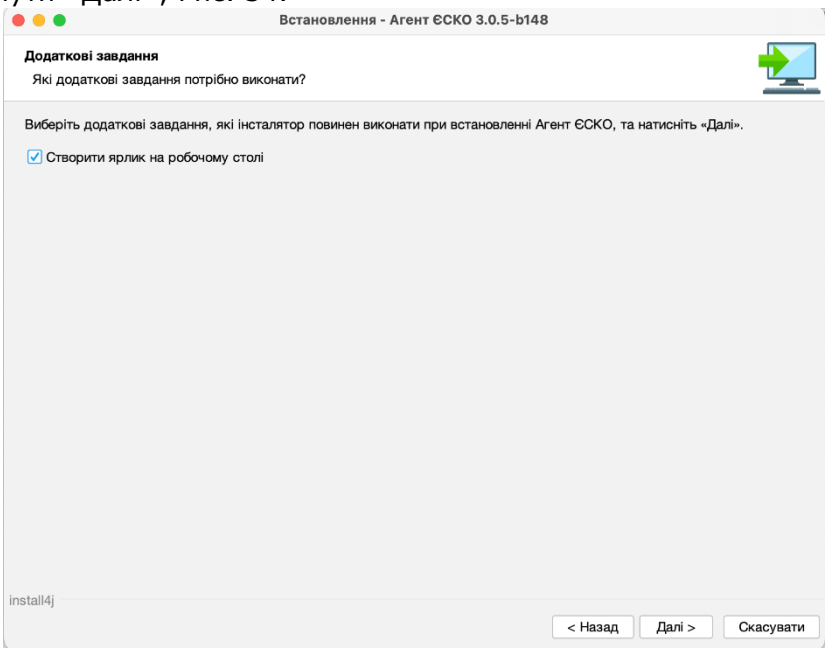

Рис. 34. Налаштування додаткових параметрів ярлика застосунку

Далі починається розпакування та запис файлів застосунку на ПК, Рис. 35.

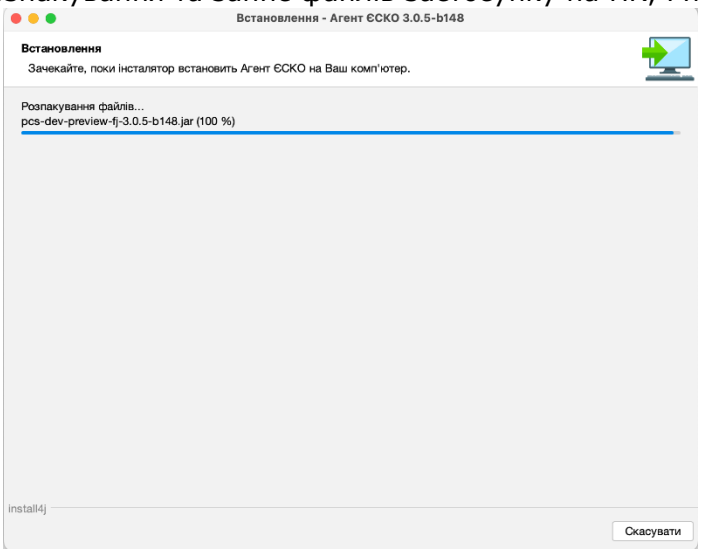

Рис. 35. Процес встановлення застосунку

Після завершення встановлення застосунку є можливість відразу його запустити, для чого необхідно натиснути «Готово», Рис. 36. У разі, коли немає потреби у його запуску необхідно зняти відмітку у відповідному полі.

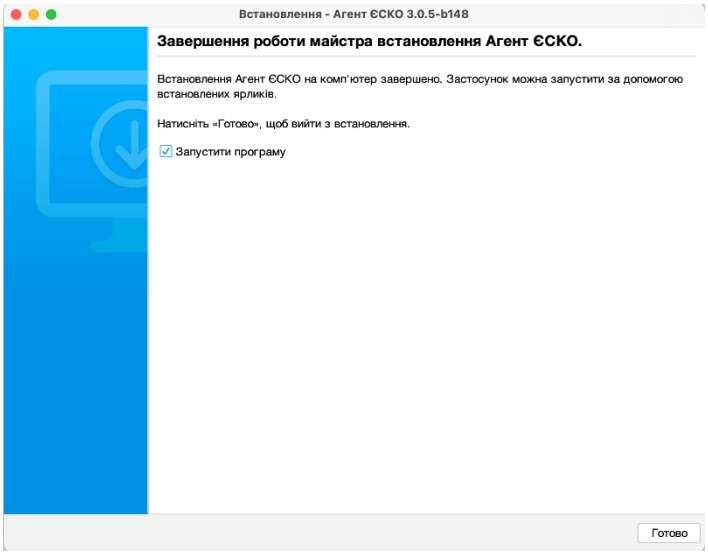

Рис. 36. Завершення процесу встановлення застосунку

Ярлик застосунку буде розміщений у створеному для застосунку каталозі, Рис. 37.

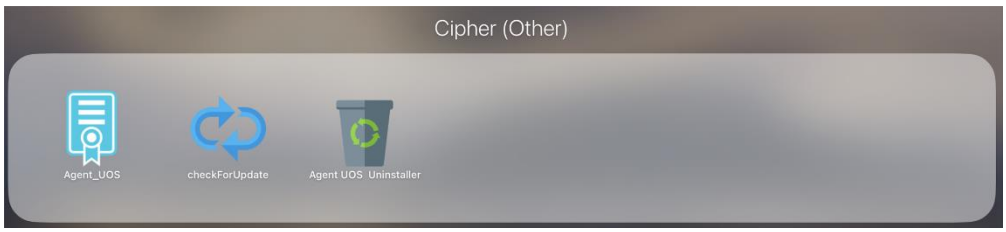

Рис. 37. Розміщення ярлику застосунку

Робота з Агентом Єдиного Криптографічного Центру

Запуск та початок роботи

1. У веб-браузері перейти за посиланням - https://cryptocenter.kredobank.com.ua/ до Клієнту Єдиного Криптографічного Центру. Рис. 1.

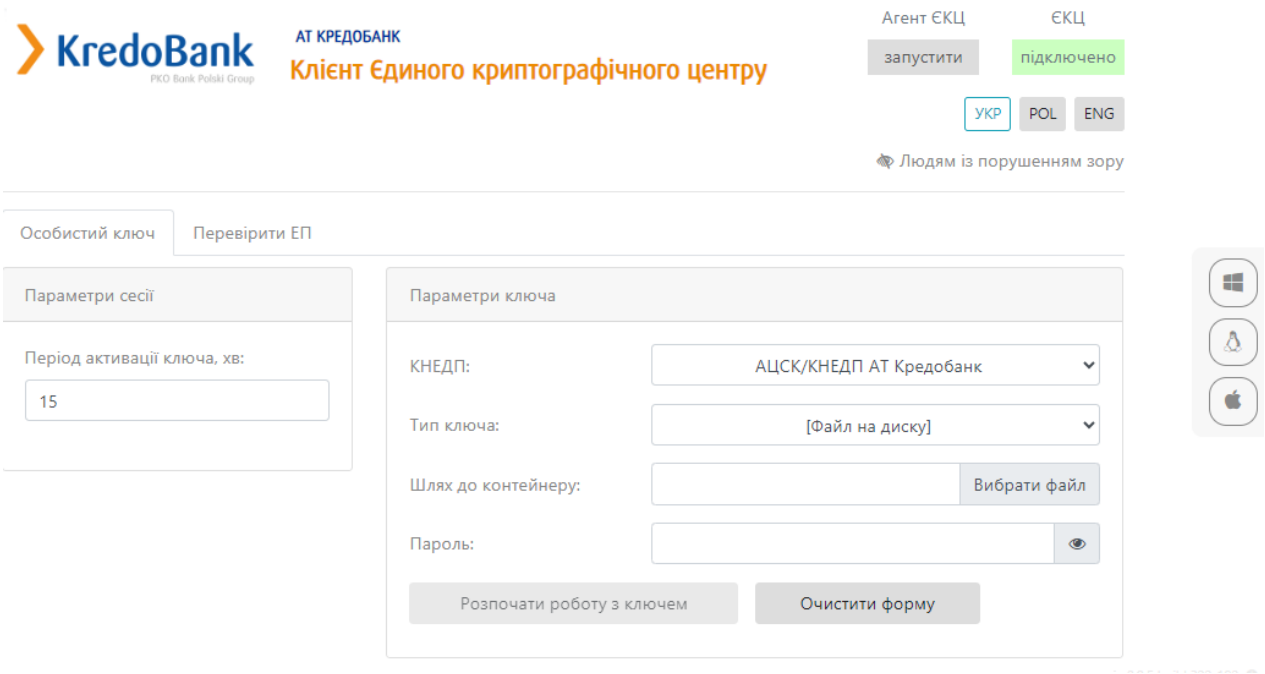

Рис. 1. Стартове вікно ЄКЦ

2. Наступним кроком слід запустити застосунок «Агент ЄСКО», натиснувши на ярлик на робочому столі або запустити його, обравши зі списку встановлених на ПК програм, Рис. 2.

Рис. 2. Запуск Агенту ЄКЦ

3. Далі відкривається вікно Агенту єдиного криптографічного центру, Це означає що Агент запущено, все працює коректно, його слід згорнути та повернутися до веб-браузера, Рис. 3.

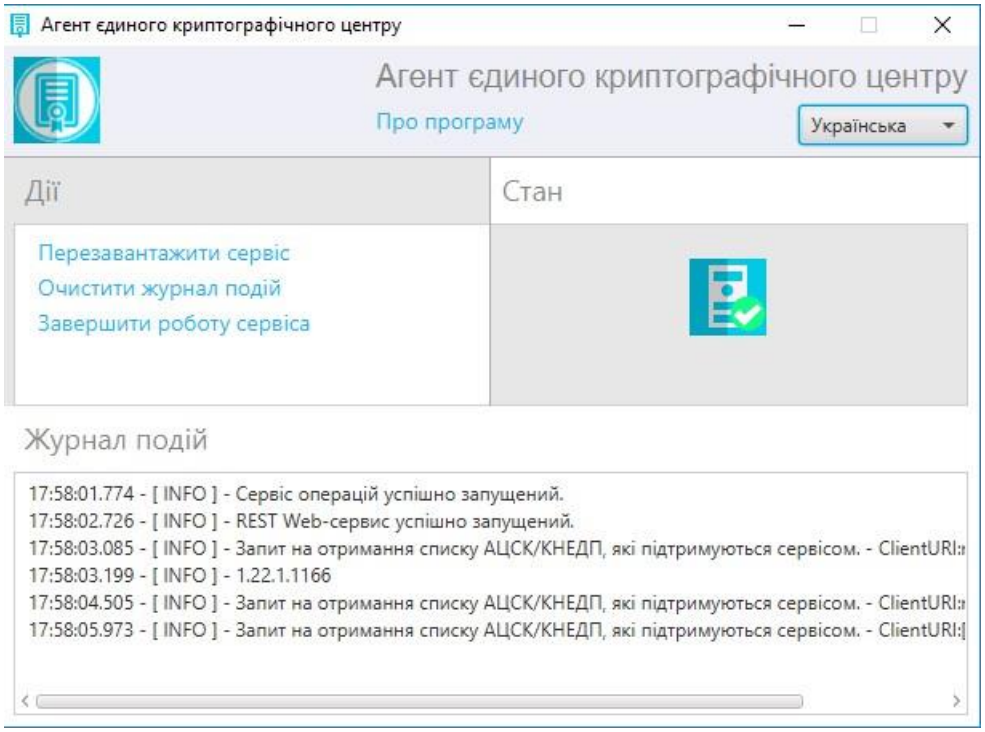

Рис. 3. Вікно «Агенту єдиного криптографічного центру»

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

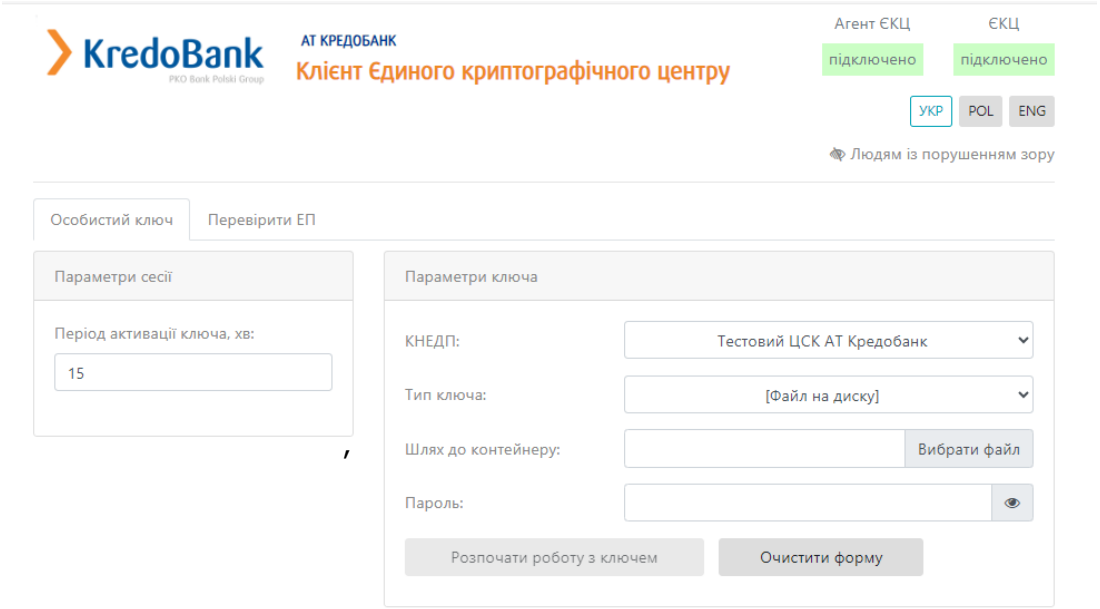

Рис. 4. Стартове вікно Агент ЄКЦ

5. Після виконання вищезазначених дій можна переходити до роботи з Клієнтом Єдиного сервісу криптографічних операцій:

- На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа, за замовчуванням 15 хв.
- На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати ***КНЕДП***, у якому

було отримано ключ.

- На вкладці «***Тип ключа»*** необхідно обрати:

    1. файл на диску;
    2. PKCS#11 пристрої – активний режим (для роботи із захищеним носієм);
    3. PKCS#11 пристрої – пасивний режим (для роботи із захищеним носієм).

- Заповнити поле ***Шлях до контейнеру*** (для роботи з файловим контейнером - обрати шлях до нього; для роботи з захищеним носієм - обрати необхідний носій).
- Ввести ***Пароль*** до ключа чи ***PIN*** до захищеного носія, Рис. 5.

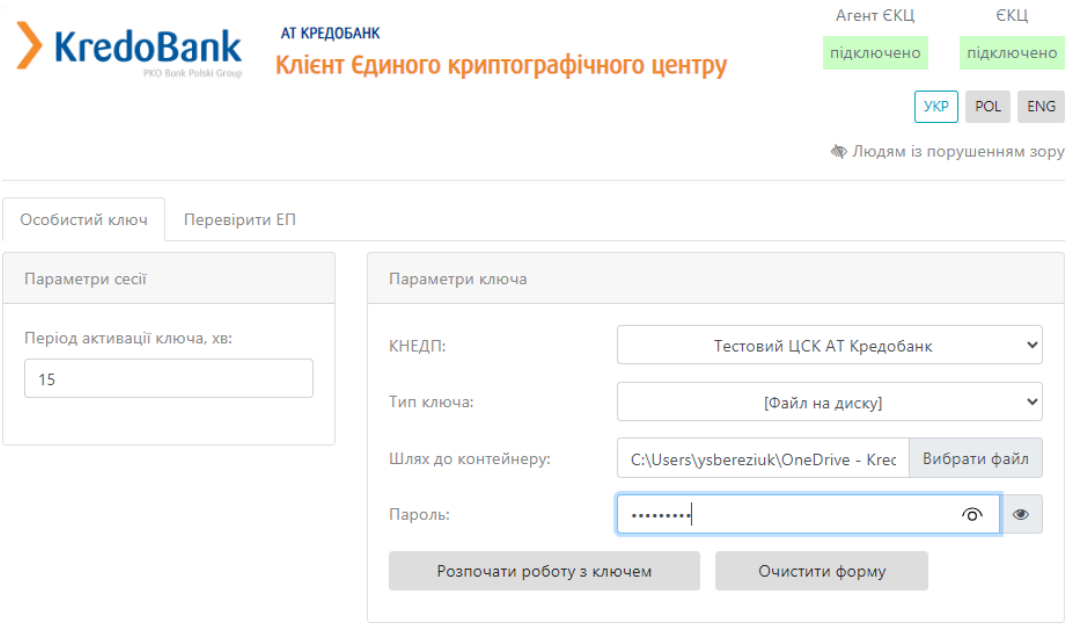

Рис. 5. Заповнення розділу «Параметри ключа»

6. 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 ЄКЦ, Рис. 6.

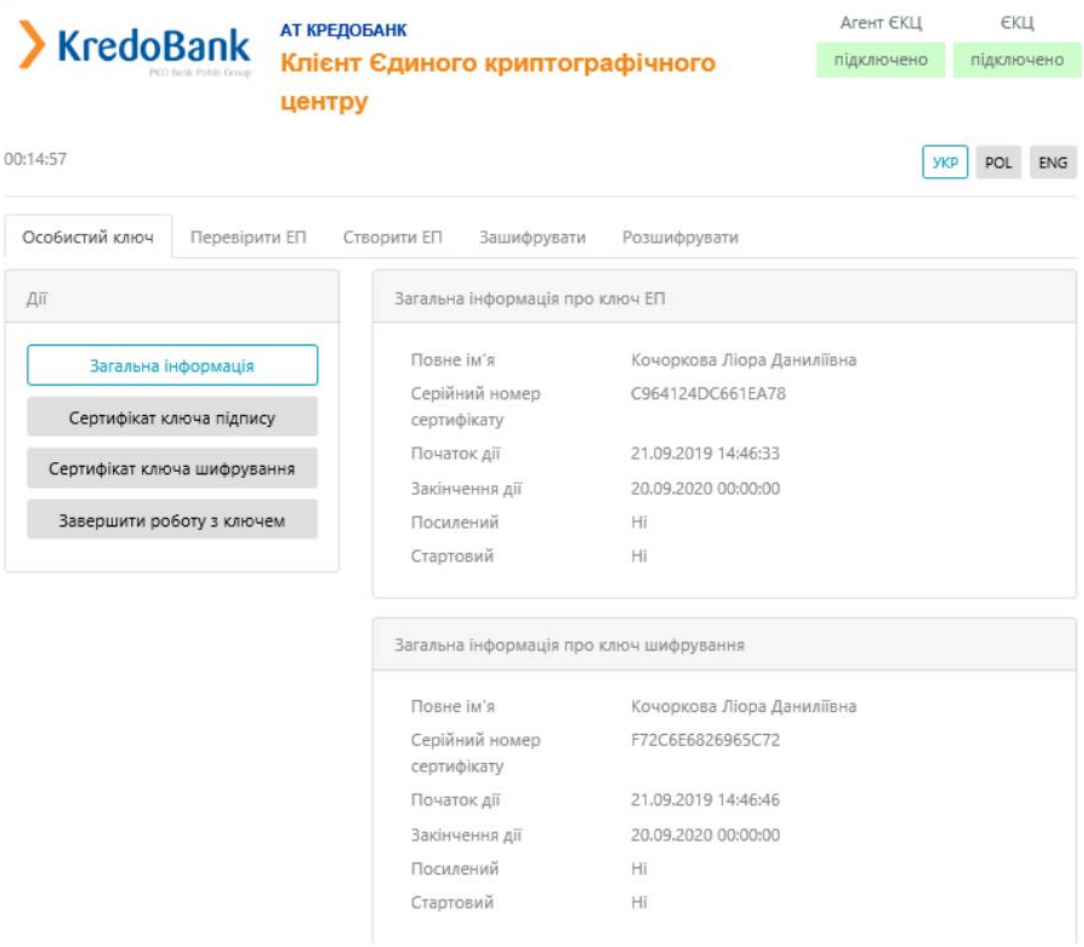

Рис. 6. Робоча область Агенту ЄКЦ

Службові функції та опції ЄКЦ

Після завантаження даних ключового контейнеру у вікні «Клієнту Єдиного Криптографічного Центру» з'являються такі поля та відповідні опції, Рис. 7:

1.Вкладка «Особистий ключ», яка містить кнопки:

- «Загальна інформація» - коротка інформація про ключів.
- «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 (Вбудований чи Відкріплений):
        - Вбудований - можемо завантажувати всі підтримувані типи (вбудований, ASIC-S, ASIC-E), окрім відкріпленого.
        - Відкріплений - підпис розміщується у файлі, зазвичай з розширенням p7s, окремо від даних, що підписуються.
    - 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.
    - Генерація QR.
- «Файл» включає в себе 2 поля:
    - Тип ЕП - Відкріплений: файл для перевірки (файл на який було створено підпис) та файл з підписом (файл, який містить підпис).
    - Тип ЕП – Вбудований: файл з підписом (файл який містить підпис). Також, можна завантажувати ASIC-S, ASIC-E.
- «Текстові дані» включає в себе 2 поля:
    - Кодування UTF-16LE та UTF-8.
    - Тип ЕП - Відкріплений: текстові дані для перевірки (текст на який було створено підпис) та підпис у кодуванні Base64 (текст, який містить підпис).
    - Тип ЕП – Вбудований: підпис у кодуванні Base64 (текст, який містить підпис) та дані з електронного підпису (виведення даних без підпису). Також, можна завантажувати ASIC-S, ASIC-E.

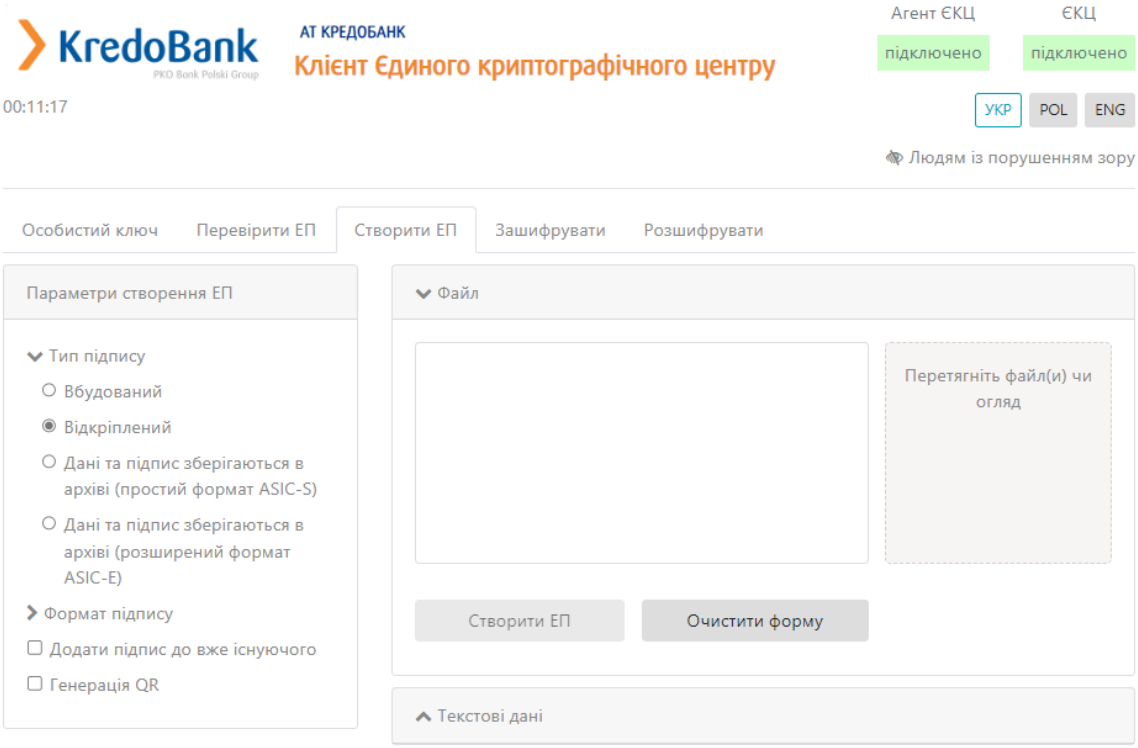

Рис. 7. Робоча область Агенту ЄКЦ

1. Вкладка «Створити ЕП».

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

- «Параметри створення ЕП» включає в себе:
    - Тип ЕП:
        - Вбудована - підпис розміщується у файлі, зазвичай з розширенням p7s, разом з даними, що підписуються
        - Відкріплена - підпис розміщується у файлі, зазвичай з розширенням p7s, окремо від даних, що підписуються
        - Простий формат ASIC-S - дані та підпис зберігаються в архіві. Дозволяє зберігати один файловий об'єкт з пов'язаним е-підписом та в подальшому додавати нові. Також дає можливість додавати файли для захисту е-позначок часу.
        - Розширений формат ASIC-E - дані та підпис зберігаються в архіві. Дозволяє зберігати один або кілька файлових об'єктів з пов'язаними е-підписами та в подальшому додавати файлові об'єкти, файли е-підпису та е-позначки часу.

- Позначка «Додати підпис до вже існуючого» (таким чином, можуть підписувати один файл кілька осіб).
  - Підтримується лише для CAdES
- Формат ЕП:
  - CAdES:
    - Базовий (CAdES-BES) - використовується для автентифікації підписанта та перевірки цілісності електронного документа в період чинності сертифіката відкритого ключа (сертифікат)
    - З повними даними для перевірки (CAdES-X Long) - можливість встановлення дійсності ЕП у довгостроковому періоді (після закінчення строку чинності сертифікату)
  - XAdES:
    - Базовий (XAdES-B-B) - базова перевірка достовірності і цілісності даних
    - З повними даними для перевірки (XAdES-B-LT) - додаються повні дані для перевірки
    - Для тривалого (архівного) зберігання (XAdES-B-LTA) - е-підпис для тривалого (архівного) зберігання
- Генерація QR-коду.

- «Файл». Включає в себе поле:
  - Файл/Файли для підпису (перетягнути файл(и) з Провідника на область «Перетягніть файл(и) чи огляд» або обрати необхідний файл(файли) для підпису, натиснувши на цю область);
  - 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.
  - Кнопка «Видалити» (з'являється кнопка після завантаження файлу/файлів для підпису, дозволяє видалили випадково завантажений файл)
  - Кнопка «Зберегти» (з'являється кнопка після створення ЕП, дозволяє зберегти кожен файл окремо)
- «Текстові дані». Включає в себе 2 поля:
  - 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).

Можливі статуси «Агенту ЄКЦ»:

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

2. Статус роботи програмного комплексу «ЄКЦ» - знаходиться у правій верхній частині вікна.

Можливі статуси ЄКЦ:

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

3. Зміна мови - знаходиться у правій верхній частині вікна можна змінити мову веб-інтерфейсу ЄКЦ. Доступні мови: українська, польська та англійська.
4. Версія Єдиного Криптографічного Центру знаходиться у правому нижньому куті.

Основна форма «Агенту Єдиного Криптографічного Центру» містить такі поля та відповідні опції, Рис. 8.

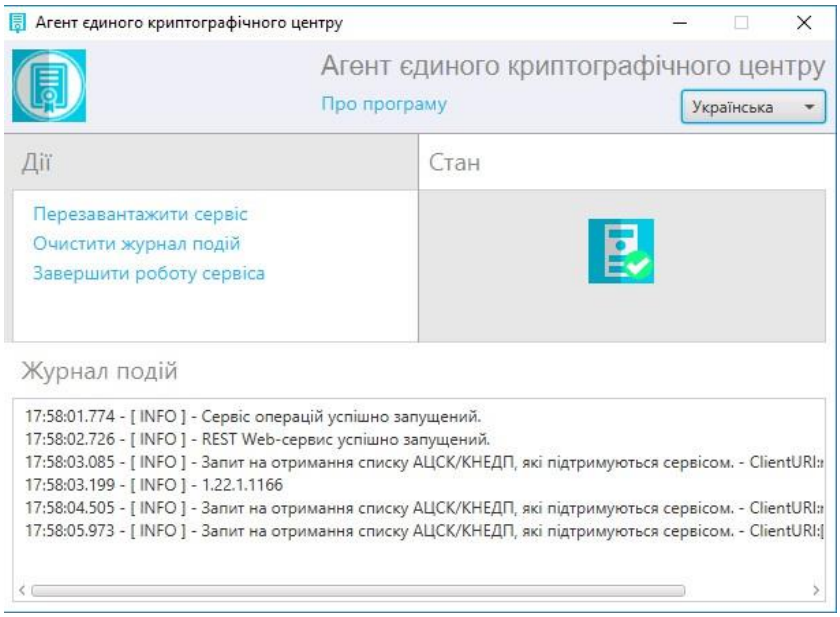

Рис. 8. Агент єдиного криптографічного центру

1. Даний розділ містить:
   - назву Програмного комплексу.
   - гіперпосилання «Про програму», яке відкриває нове вікно з інформацією про розробників, версію продукту, Рис. 9.
   - Випадаючий список зі зміною мови, доступні мови: Українська, Англійська, Польська.

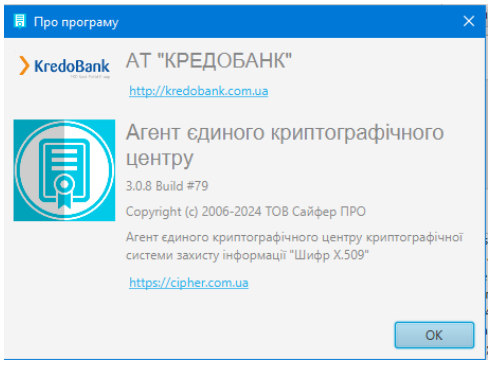

Рис. 9. Вікно «Про програму»

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 ЄКЦ.

Вибір ключа ЕП – файл

1. Стартове вікно Клієнту Єдиного Криптографічного Центру у веб-браузері показано на Рис. 10.

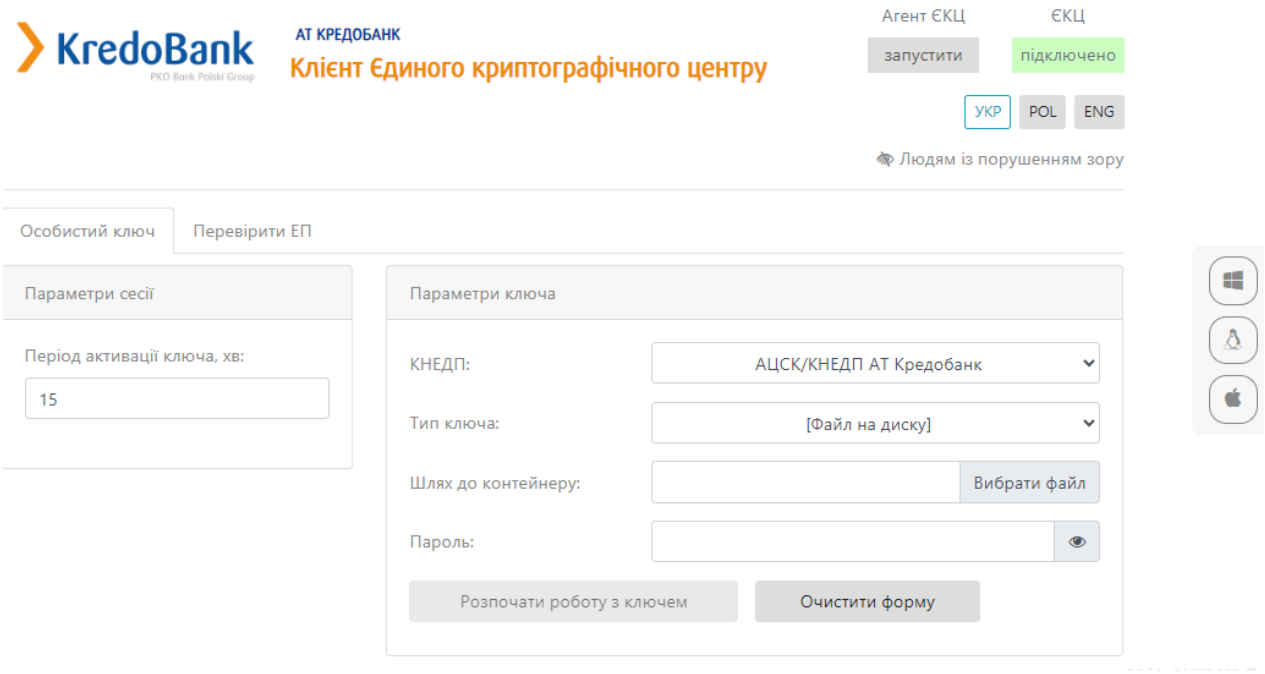

Рис. 10. Стартове вікно ЄКЦ

2. Наступним кроком слід запустити застосунок «Агент ЄСКО», натиснувши на ярлик на робочому столі або запустити його, обравши зі списку встановлених на ПК програм, Рис. 11.

Рис. 11. Запуск Агенту ЄКЦ

3. Далі відкривається вікно Агенту єдиного криптографічного центру, Це означає що Агент запущено, все працює коректно, його слід згорнути та повернутися до веб-браузера, Рис. 12.

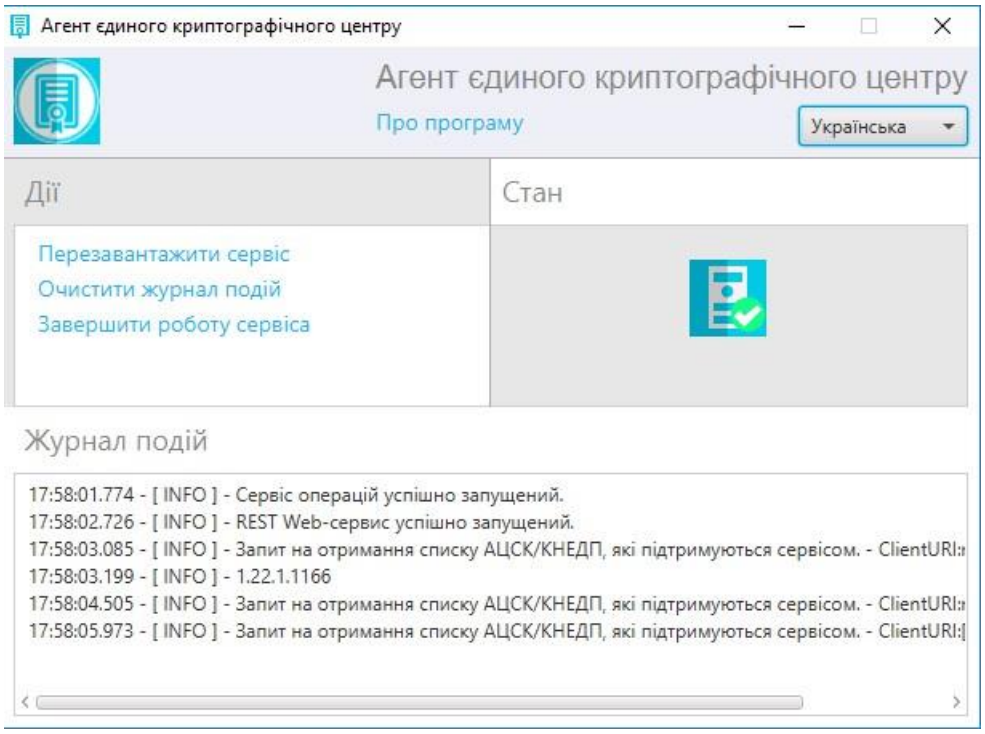

Рис. 12. Агент Єдиного Криптографічного Центру

4. У веб-сторінці одразу помітні зміни. Статус Агенту ЄКЦ змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 13.

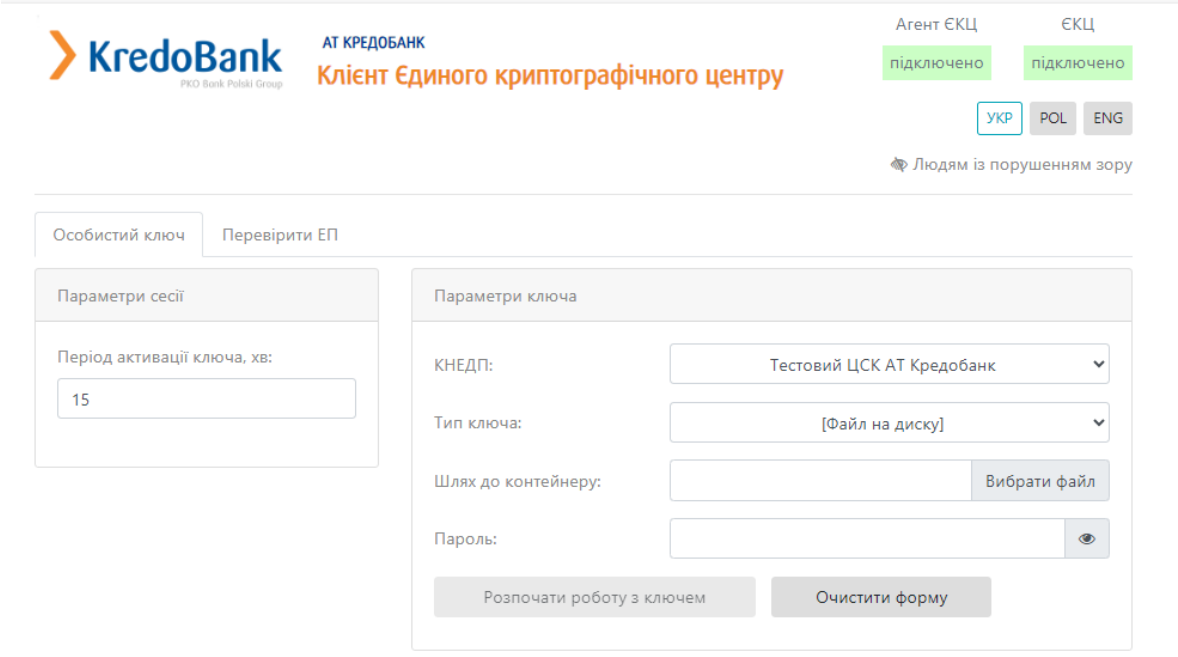

Рис. 13. Стартове вікно Агент ЄКЦ

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. ***КНЕДП***, у якому було отримано ключ;
      - КНЕДП Національного банку України;
      - КНЕДП ІДД ДПС;
      - КНЕДП "ДІЯ";
      - КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
      - КНЕДП АТ «КБ «ПРИВАТБАНК»;
      - КНЕДП АТ «УКРСИББАНК»;
      - КНЕДП «Masterkey»;
      - КНЕДП Збройних Сил України;
      - КНЕДП - АЦСК Міністерства внутрішніх справ України;
      - КНЕДП Державної прикордонної служби України;
      - КНЕДП ЦСК АТ "Укрзалізниці";
      - КНЕДП "АЦСК ринку електричної енергії";
      - КНЕДП ДП «Українські спеціальні системи»;
      - КНЕДП Офіс Генерального прокурора;
      - КНЕДП АТ «Ощадбанк»;
      - КНЕДП Державної казначейської служби України;
      - КНЕДП ТОВ "ДЕПОЗИТ САЙН";
      - КНЕДП АТ "СЕНС БАНК";
      - КНЕДП АТ "КРЕДІ АГРІКОЛЬ БАНК";
      - КНЕДП "eSign" ТОВ "Ілайф";
      - КНЕДП "АЦСК ТОВ "Інтер-Метл";
      - "КНЕДП АТ "ПУМБ";
      - "КНЕДП АТ "БАНК АЛЬЯНС";
      - "КНЕДП АБ "УКРГАЗБАНК";
      - "КНЕДП "Вчасно Сервіс";
      - "КНЕДП АТ "ПРАВЕКС БАНК";
      - "КНЕДП СБ України";
      - "КНЕДП АТ "ТАСКОМБАНК".
   2. ***Тип ключа***:
      - файл на диску (обрати даний пункт з випадаючого списку);
      - PKCS#11 пристрої – активний режим;
      - PKCS#11 пристрої – пасивний режим.
      - Хмарний сервіс Depositsign.
   3. ***Шлях до контейнеру***;
   4. ***Пароль*** до ключа, Рис. 14.

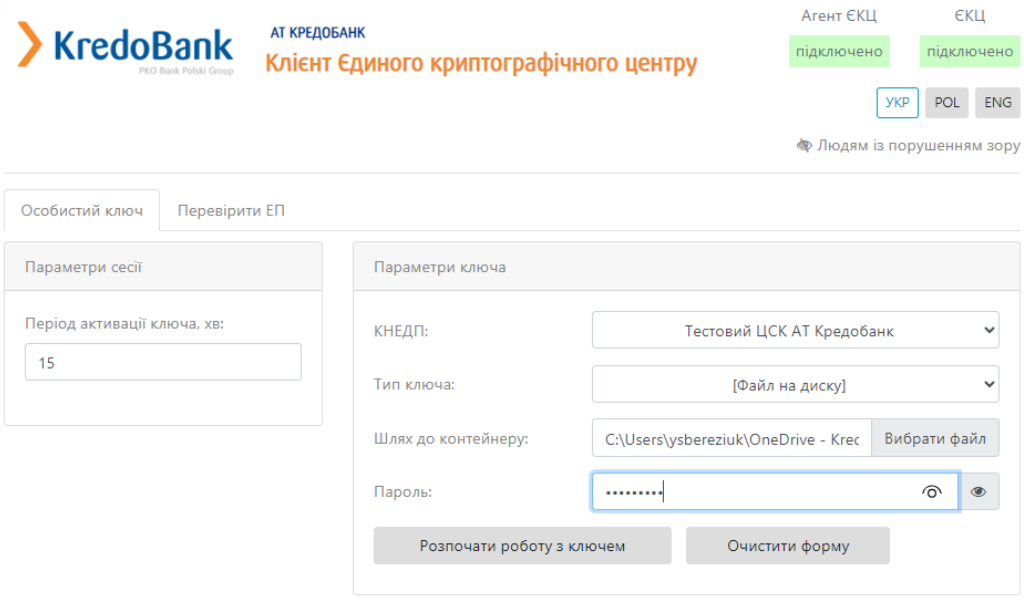

Рис. 14. Заповнення розділу «Параметри ключа»

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 ЄКЦ, Рис. 15.

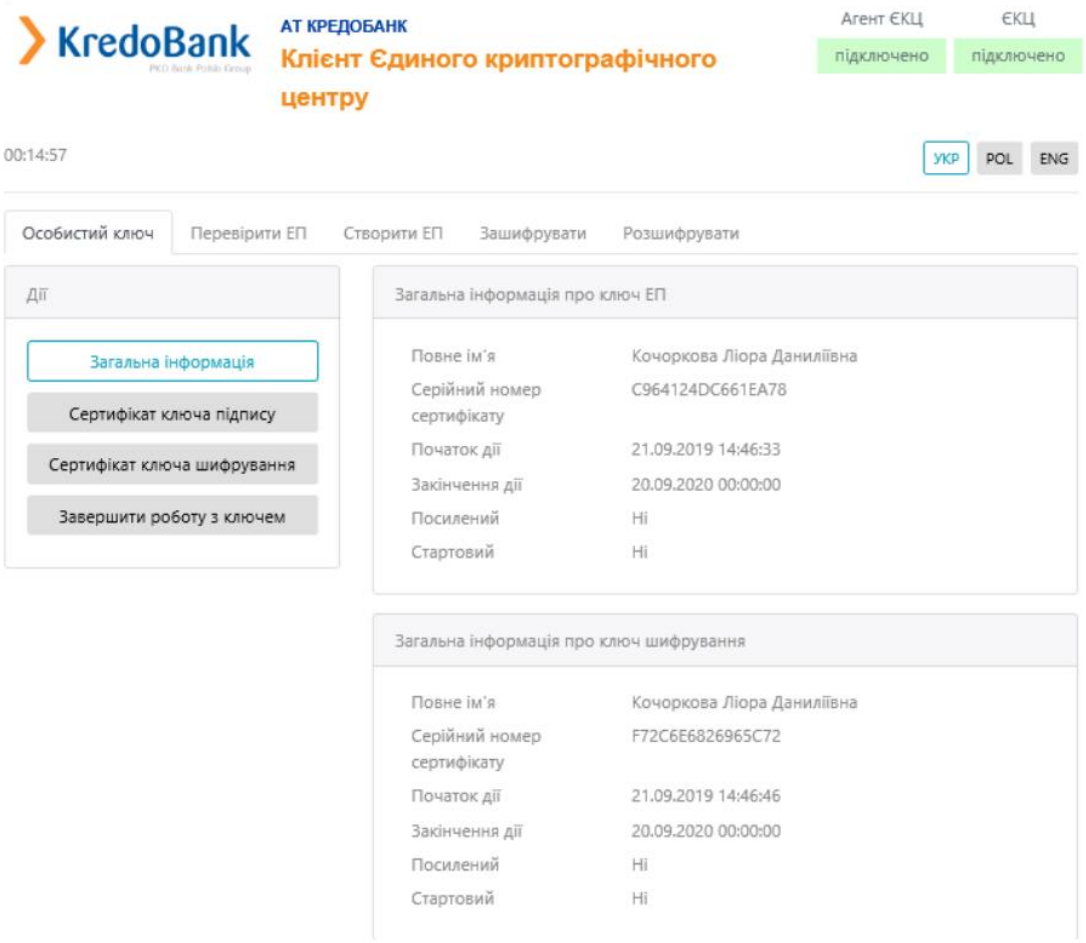

Рис. 15. Робоча область Агенту ЄКЦ

Вибір ключа ЕП – захищений носій

1. Стартове вікно Клієнту Єдиного Криптографічного Центру у веб-браузері показано на Рис. 16.

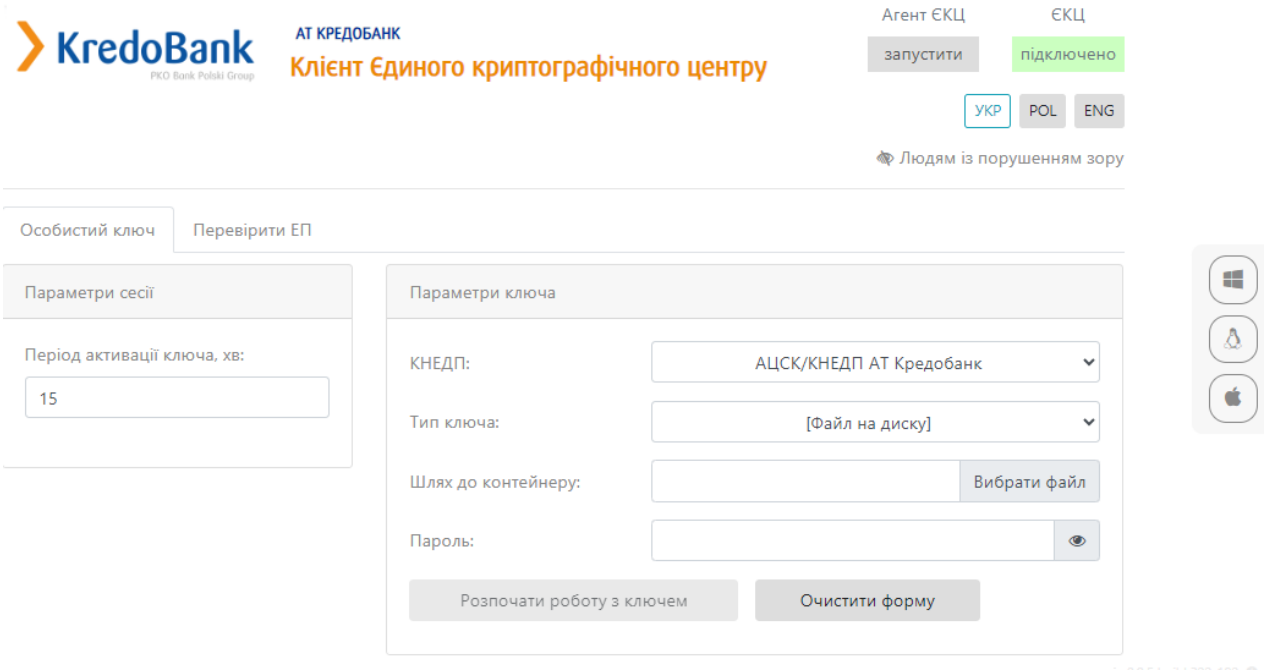

Рис. 16. Стартове вікно ЄКЦ

2. Наступним кроком слід запустити застосунок «Агент ЄСКО», натиснувши на ярлик на робочому столі або запустити його, обравши зі списку встановлених на ПК програм, Рис. 17.

Рис. 17. Запуск Агенту ЄКЦ

3. Далі відкривається вікно Агенту єдиного криптографічного центру, Це означає що Агент запущено, все працює коректно, його слід згорнути та повернутися до веб-браузера, Рис. 18.

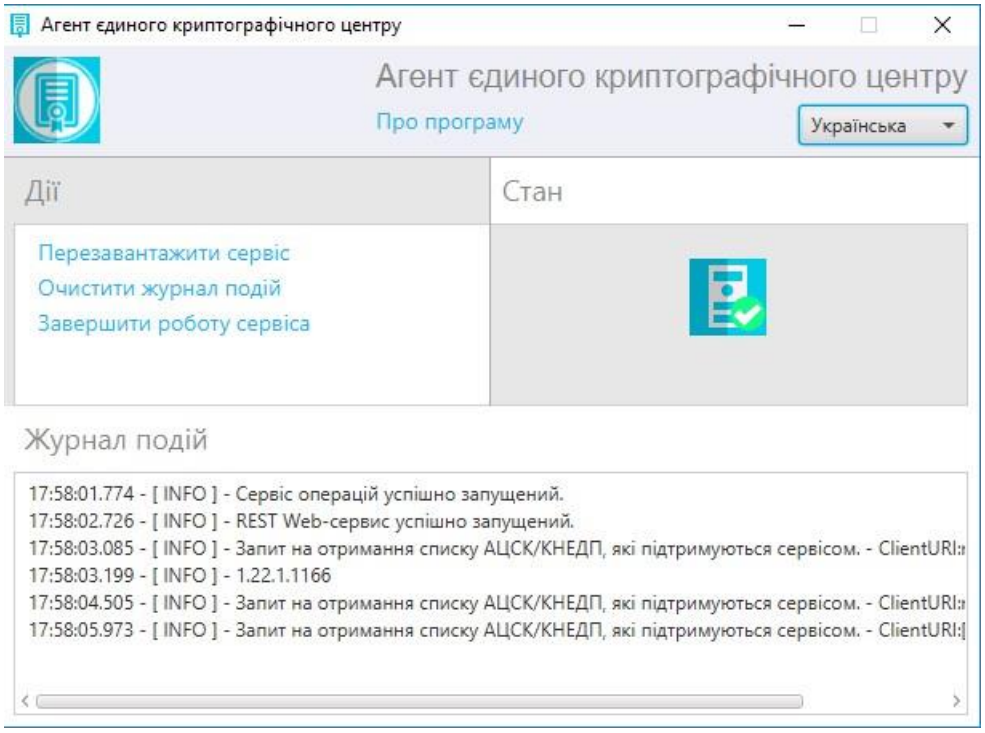

Рис. 18. Агент Єдиного Криптографічного Центру

4. У веб-сторінці одразу помітні зміни. Статус Агенту ЄКЦ змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 19.

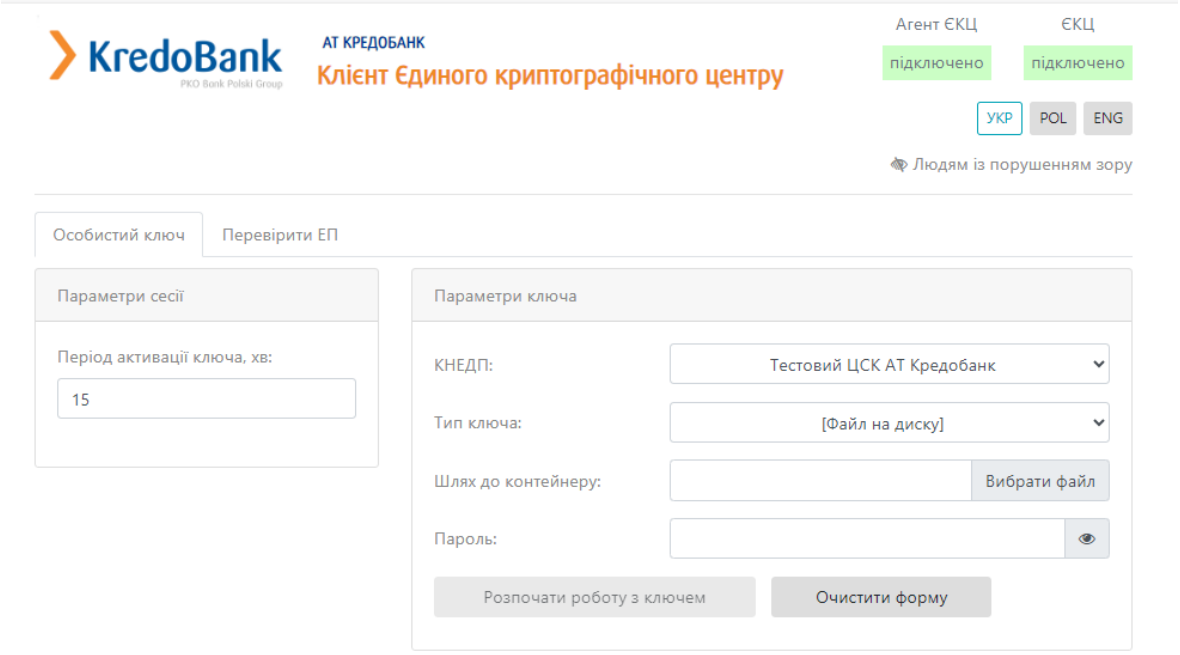

Рис. 19. Стартове вікно Агент ЄКЦ

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. ***КНЕДП***, у якому було отримано ключ;

- КНЕДП Національного банку України;
- КНЕДП ІДД ДПС;
- КНЕДП "ДІЯ";
- КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- КНЕДП АТ «КБ «ПРИВАТБАНК»;
- КНЕДП АТ «УКРСИББАНК»;
- КНЕДП «Masterkey»;
- КНЕДП Збройних Сил України;
- КНЕДП - АЦСК Міністерства внутрішніх справ України;
- КНЕДП Державної прикордонної служби України;
- КНЕДП ЦСК АТ "Укрзалізниці";
- КНЕДП "АЦСК ринку електричної енергії";
- КНЕДП ДП «Українські спеціальні системи»;
- КНЕДП Офіс Генерального прокурора;
- КНЕДП АТ «Ощадбанк»;
- КНЕДП Державної казначейської служби України;
- КНЕДП ТОВ "ДЕПОЗИТ САЙН";
- КНЕДП АТ "СЕНС БАНК";
- КНЕДП АТ "КРЕДІ АГРІКОЛЬ БАНК";
- КНЕДП "eSign" ТОВ "Ілайф";
- КНЕДП "АЦСК ТОВ "Інтер-Метл";
- "КНЕДП АТ "ПУМБ";
- "КНЕДП АТ "БАНК АЛЬЯНС";
- "КНЕДП АБ "УКРГАЗБАНК";
- "КНЕДП "Вчасно Сервіс";
- "КНЕДП АТ "ПРАВЕКС БАНК";
- "КНЕДП СБ України";
- "КНЕДП АТ "ТАСКОМБАНК".

   2. ***Тип ключа***:
      - файл на диску (обрати даний пункт з випадаючого списку);
      - PKCS#11 пристрої – активний режим;
      - PKCS#11 пристрої – пасивний режим.
      - Хмарний сервіс Depositsign.

   3. ***Шлях до контейнеру,*** *Рис. 20;*

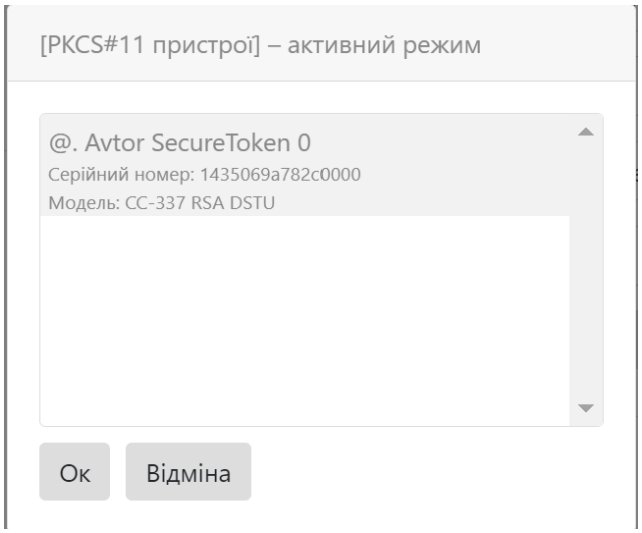

Рис. 20. Вказівка «Шлях до контейнера»

   4. ***PIN*** до захищеного носія, Рис. 21.

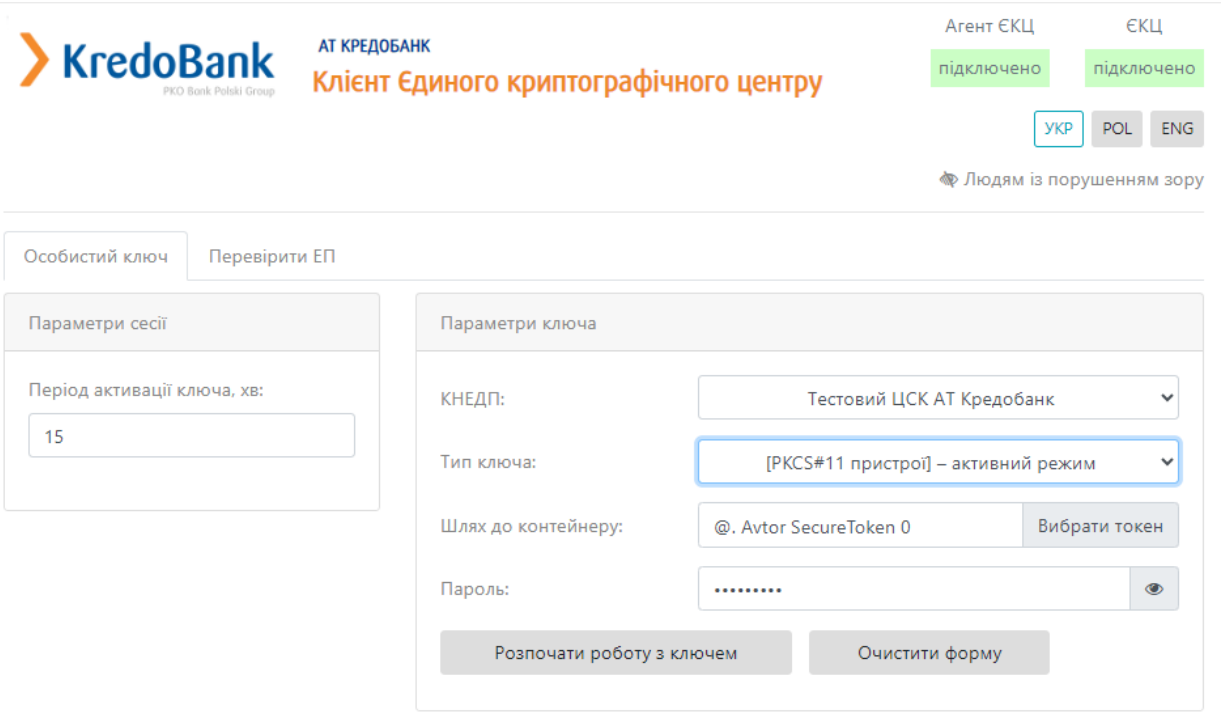

Рис. 21. Форма «Агент ЄКЦ»

1. Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу з’являється повідомлення з інформацією, що дані ключового контейнеру успішно завантажені, Рис. 22.

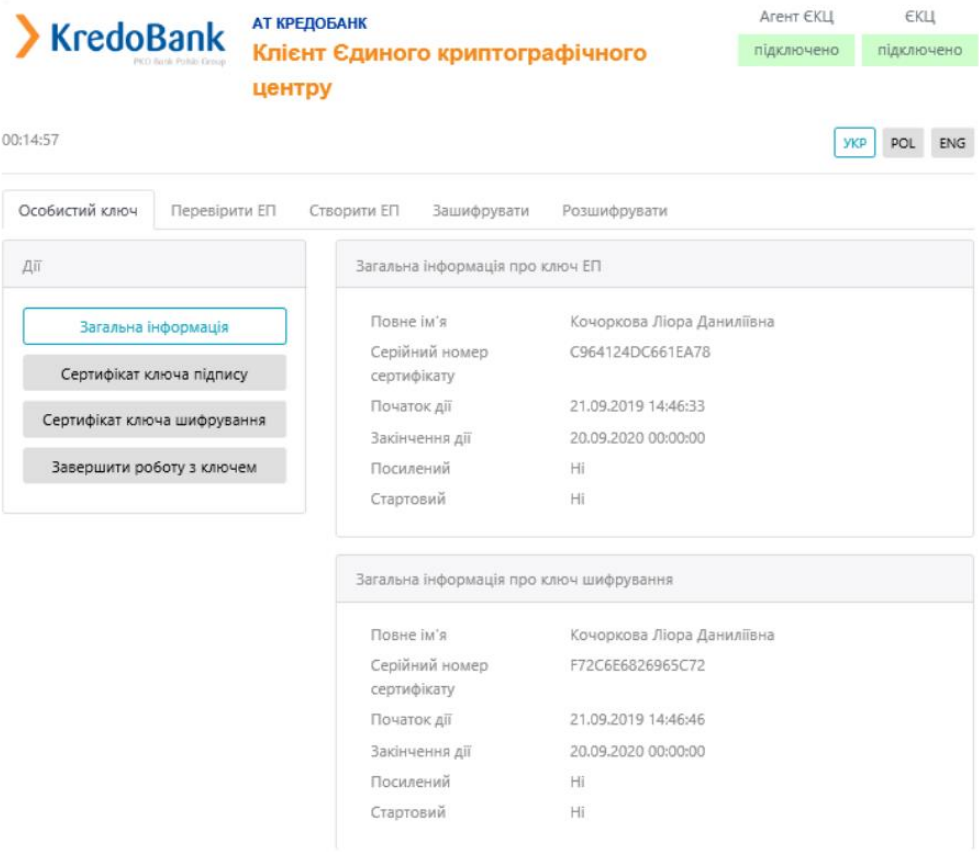

Рис. 22. Робоча область Агенту ЄКЦ

Створення ЕП

Вкладка «Створити ЕП» містить розділи: Параметри створення ЕП, Текстові дані та Файл, Рис. 23.

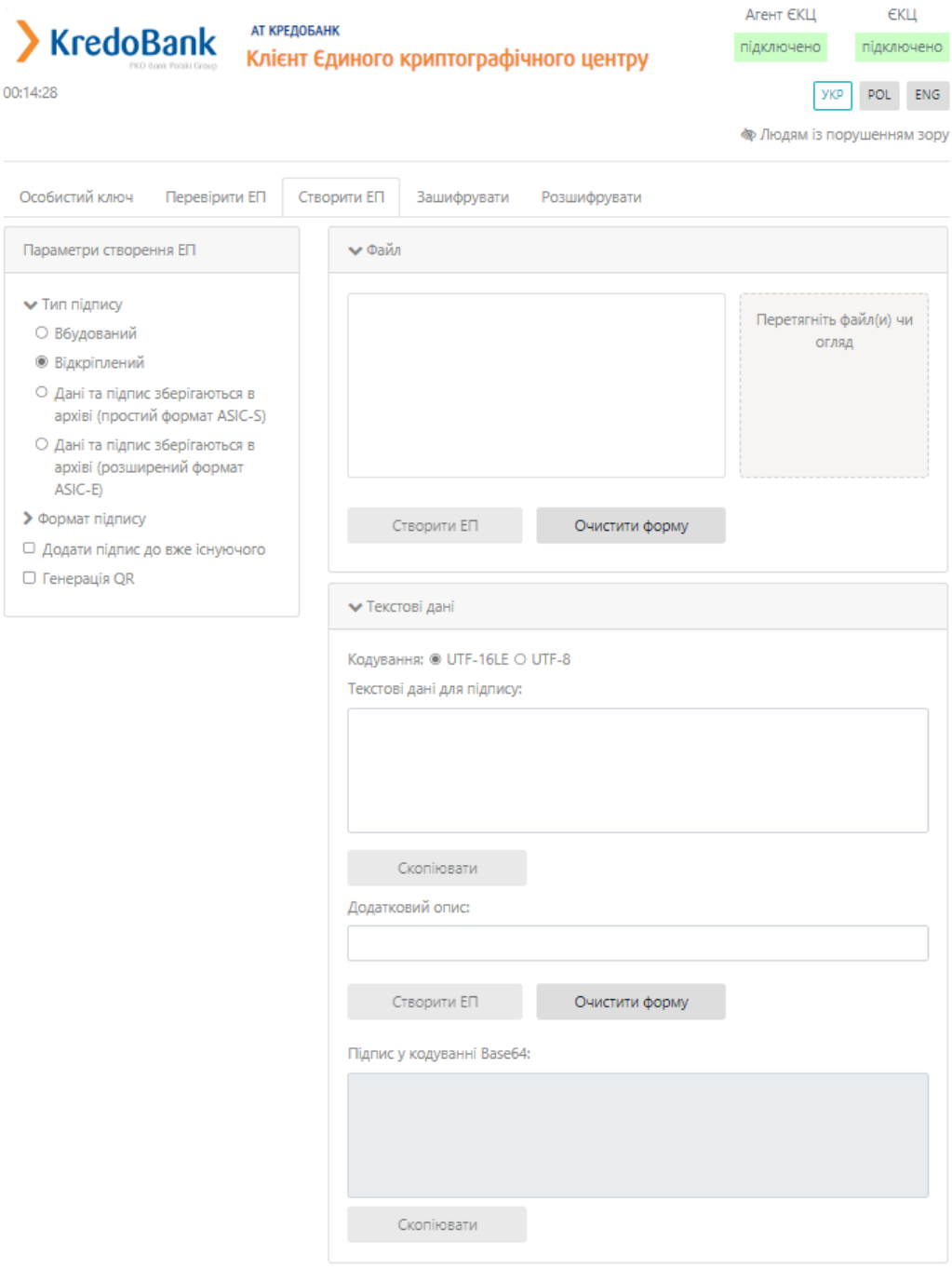

Рис. 23. Вкладка «Створити ЕП»

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

- «Параметри створення ЕП» включає в себе:
  - Тип ЕП:
    - Вбудована - підпис розміщується у файлі, зазвичай з розширенням p7s,

разом з даними, що підписуються
        - Відкріплена - підпис розміщується у файлі, зазвичай з розширенням p7s, окремо від даних, що підписуються
        - Простий формат ASIC-S - дані та підпис зберігаються в архіві. Дозволяє зберігати один файловий об'єкт з пов'язаним е-підписом та в подальшому додавати нові. Також дає можливість додавати файли для захисту е-позначок часу.
        - Розширений формат ASIC-E - дані та підпис зберігаються в архіві. Дозволяє зберігати один або кілька файлових об'єктів з пов'язаними е-підписами та в подальшому додавати файлові об'єкти, файли е-підпису та е-позначки часу.
    - Позначка «Додати підпис до вже існуючого» (таким чином, можуть підписувати один файл кілька осіб).
    - Формат ЕП:
        - CAdES:
            - Базовий (CAdES-BES) - використовується для автентифікації підписанта та перевірки цілісності електронного документа в період чинності сертифіката відкритого ключа (сертифікат)
            - З повними даними для перевірки (CAdES-X Long) - можливість встановлення дійсності ЕП у довгостроковому періоді (після закінчення строку чинності сертифікату)
        - XAdES:
            - Базовий (XAdES-B-B) - базова перевірка достовірності і цілісності даних
            - З повними даними для перевірки (XAdES-B-LT) - додаються повні дані для перевірки
            - Для тривалого (архівного) зберігання (XAdES-B-LTA) - е-підпис для тривалого (архівного) зберігання
    - Генерація QR-коду.
- «Файл». Включає в себе поле:
    - Файл/Файли для підпису (перетягнути файл(и) з Провідника на область «Перетягніть файл(и) чи огляд» або обрати необхідний файл(файли) для підпису, натиснувши на цю область);
    - 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.
    - Кнопка «Видалити» (з'являється кнока після завантаження файлу/файлів для підпису, дозволяє видалили випадково завантажений файл)
    - Кнопка «Зберегти» (з'являється кнопка після створення ЕП, дозволяє зберегти кожен файл окремо)
    - Кнопка «Зберегти ZIP» (з'являється кнопка після створення ЕП, дозволяє зберегти підписаний файл/файли в одному архіві)
- «Текстові дані». Включає в себе 2 поля:
    - 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 «Вбудований» на файл

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП»: Тип ЕП, Формат ЕП та обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 24. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об'єм всіх файлів не повинен перевищувати 100Мб.

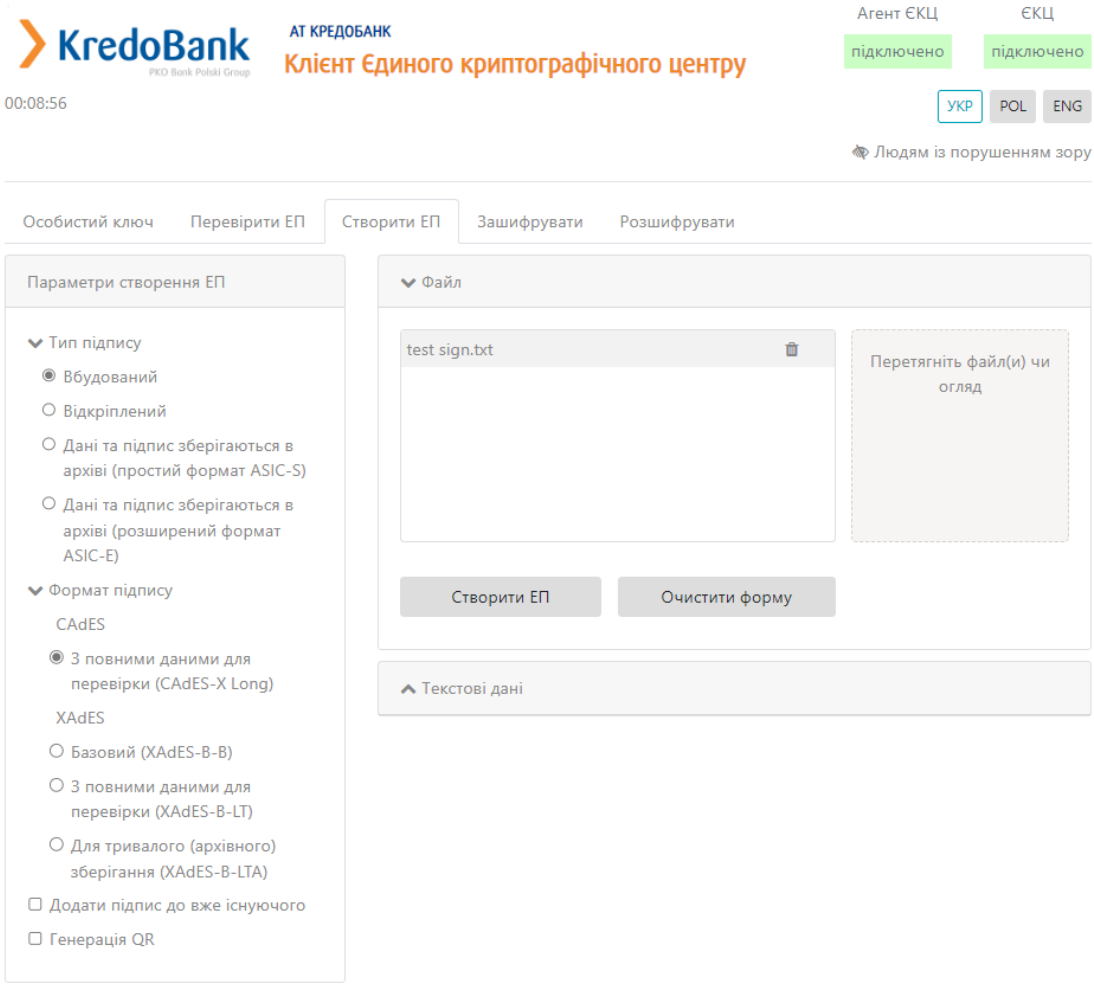

Рис. 24. Створення ЕП

Після натискання кнопки «Створити ЕП» з’являється інформування про успішне створення електронного підпису, Рис. 25.

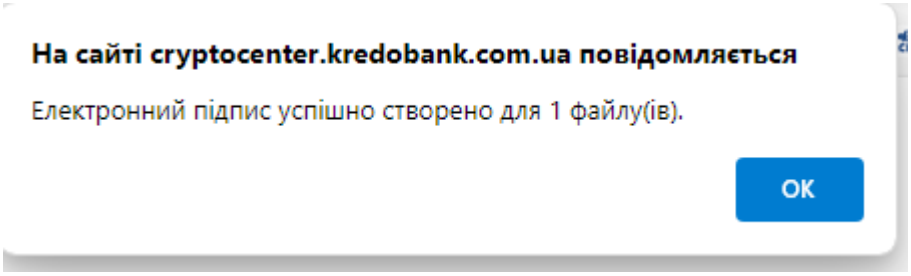

Рис. 25. Повідомлення про створення електронного підпису

Далі зберігається файл з підписом за допомогою кнопки «стрілки вниз», яка з’являється біля кожного файлу на який накладено підпис, Рис. 26.

За необхідності вказуємо шлях для збереження та очищаємо форму.

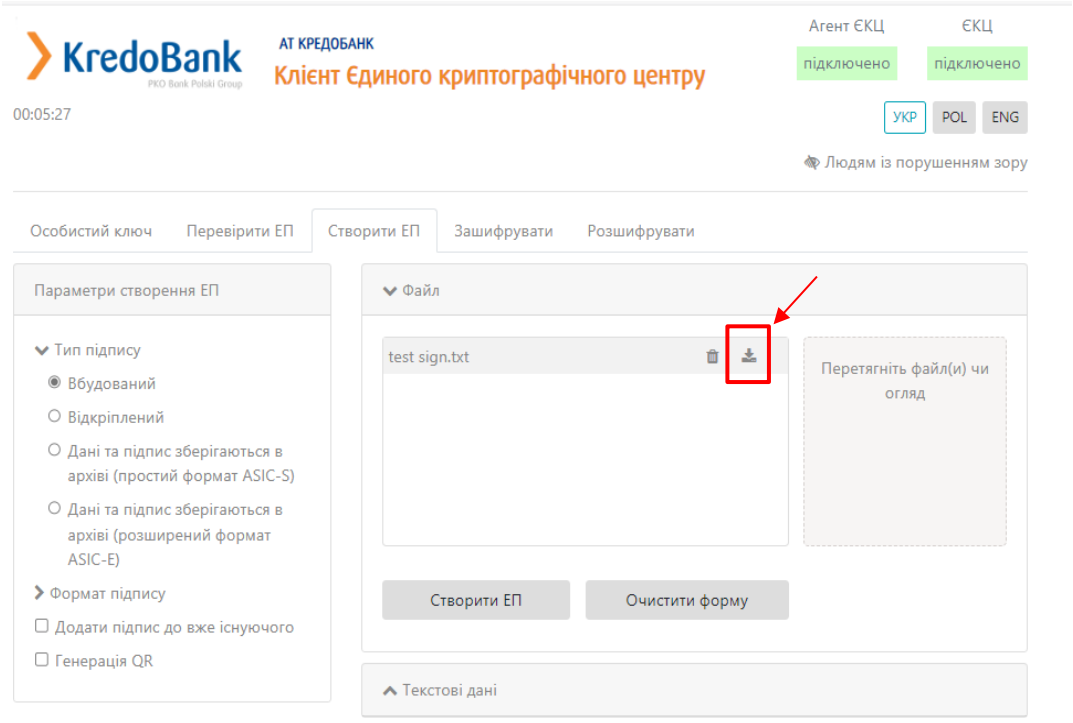

Рис. 26. Збереження підпису у файл

Створення ЕП за типом «Відкріплений» на файл

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП»: Тип ЕП, Формат ЕП та обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 27. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об'єм всіх файлів не повинен перевищувати 100Мб.

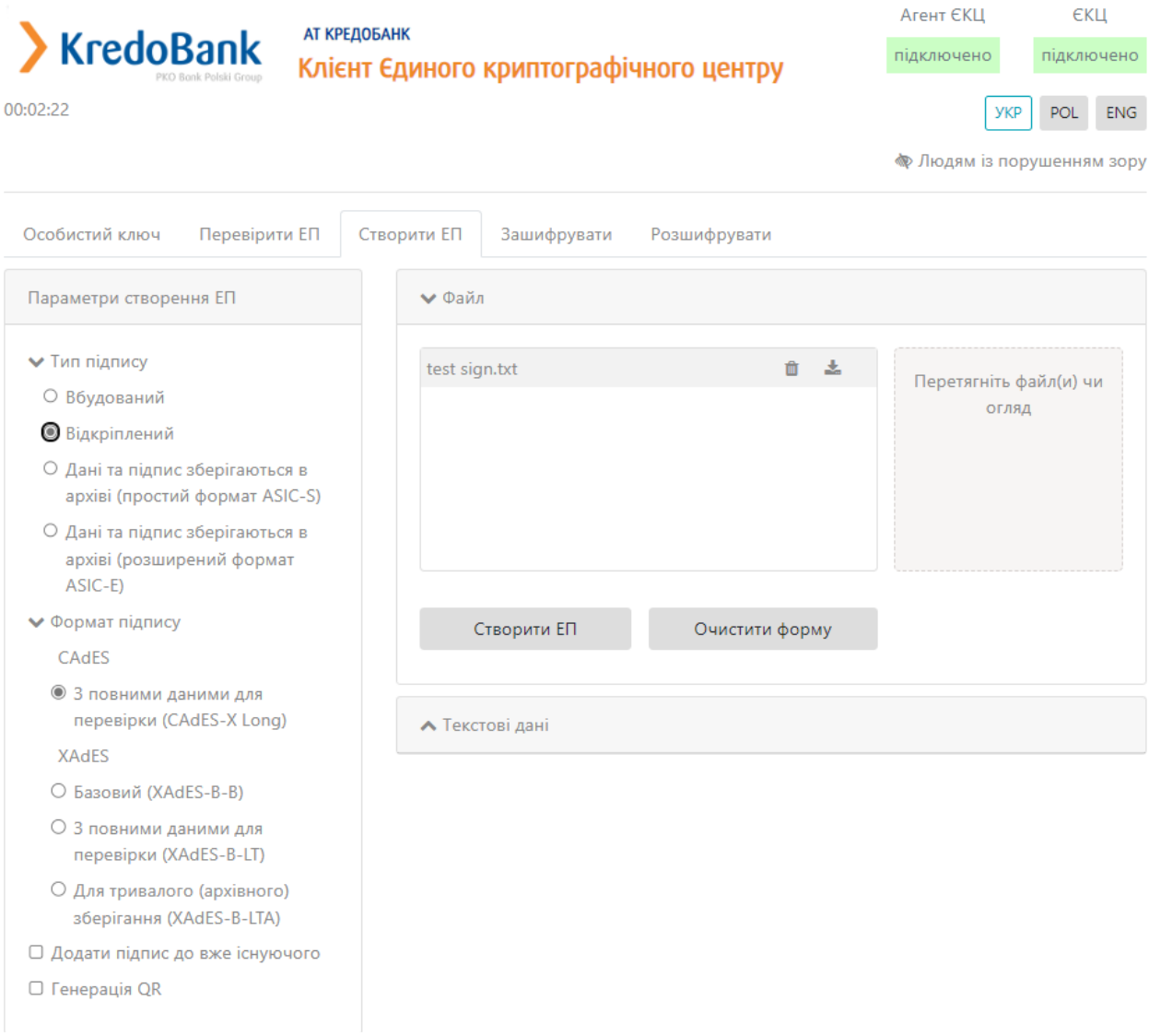

Рис. 27. Створення ЕП

Після натискання кнопки «Створити ЕП» з’являється вікно про успішне створення електронного підпису, Рис. 28.

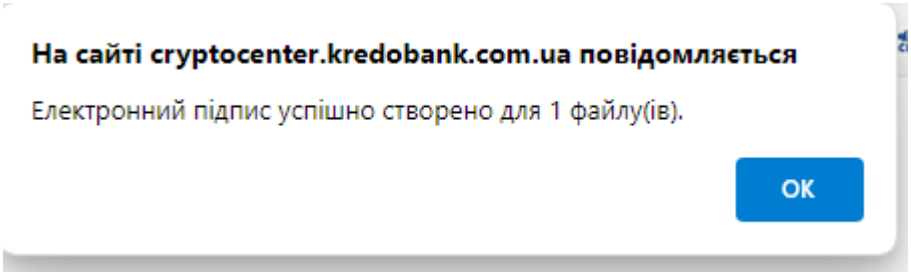

Рис. 28. Повідомлення про створення електронного підпису

Далі зберігається файл з підписом за допомогою кнопки «стрілки вниз», яка з’являється біля кожного файлу на який накладено підпис, Рис. 29.

За необхідності вказуємо шлях для збереження та очищаємо форму.

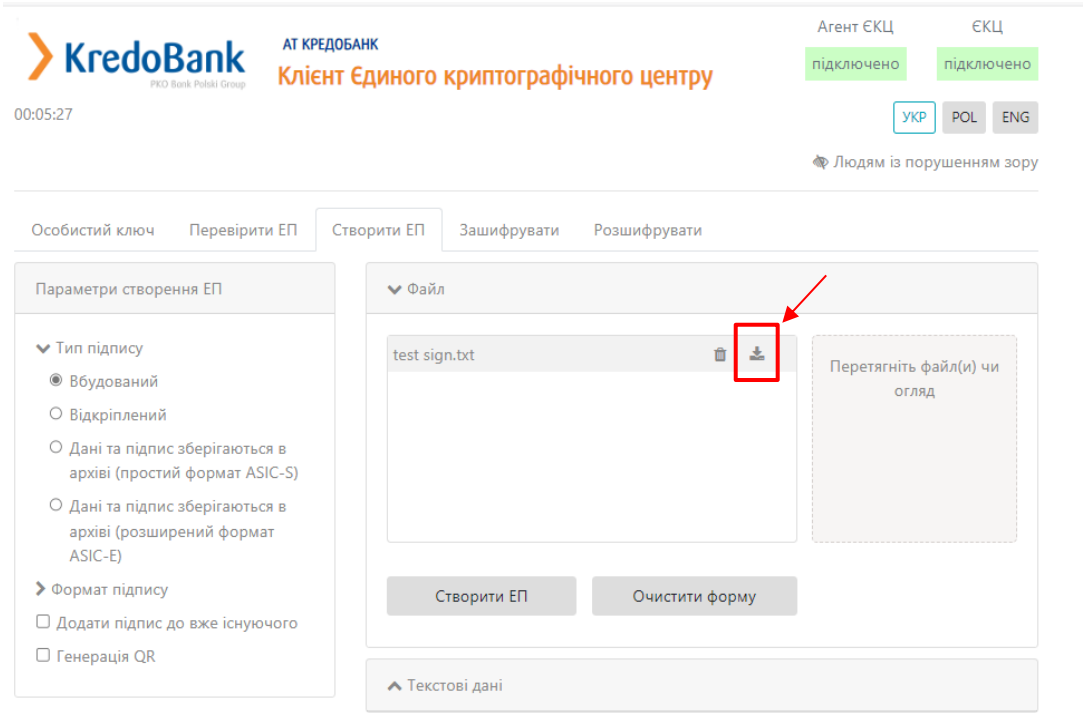

Рис. 29. Збереження підпису у файл

Перевірка ЕП

Дана функція є доступною і без ключа.

Варто зазначити! Кваліфікований електронний підпис вважається тоді, якщо сертифікат отриманий у Кваліфікованого надавача електронних довірчих послуг та ключ згенеровано на захищеному носії чи мережному криптомодулі чи у "хмарі". Якщо, хоча б одна умова не виконується, то підпис не є Кваліфікованим.

Вкладка «Перевірити ЕП» містить розділи: Параметри перевірки ЕП, Текстові дані та Файл, Рис. 30-Рис. 31.

Розділ «Параметри перевірки ЕП», який у свою чергу включає:
1.Поле «Тип ЕП», яке містить:

- Вбудований (завантажуються за типом: Вбудований, ASIC-S, ASIC-E);
- Відкріплений;

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.
4.Позначка «Розширити ЕП».
5.Генерація QR-коду.

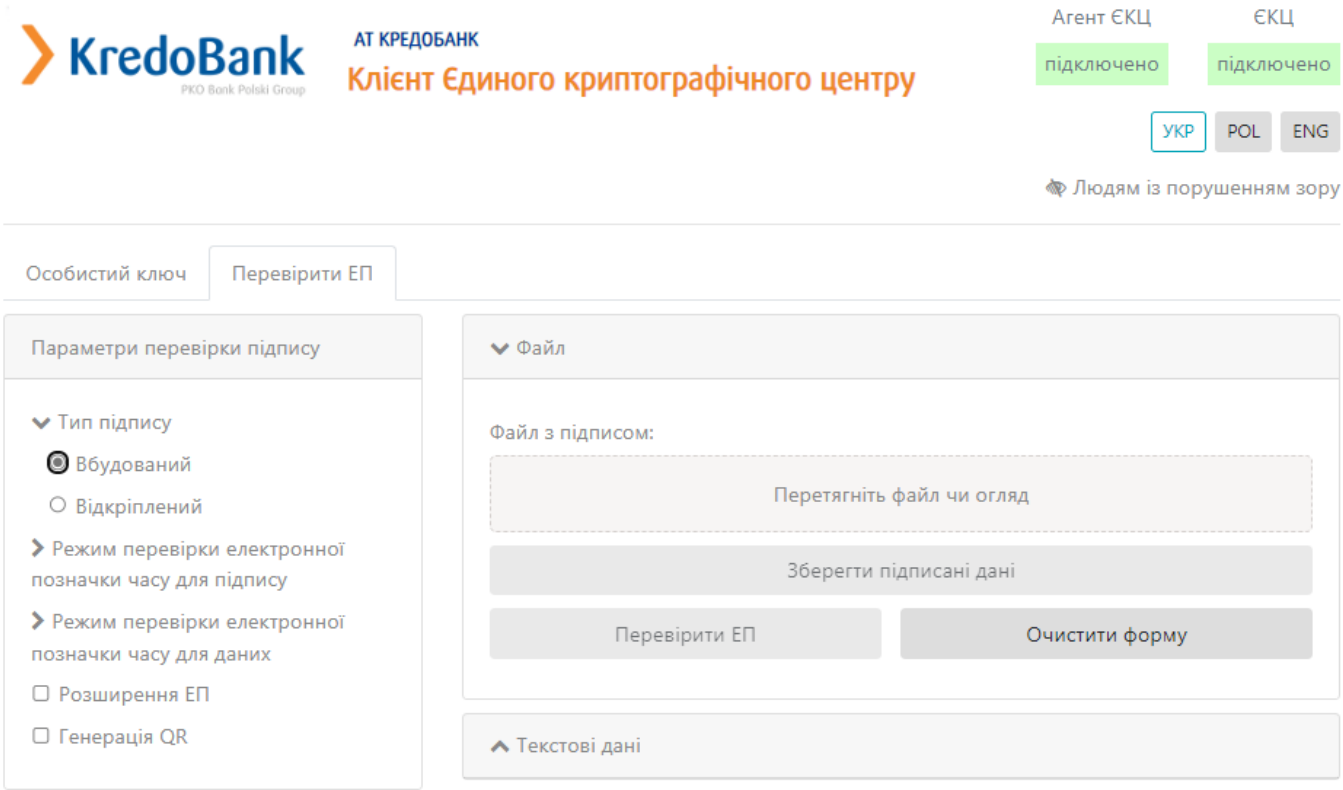

Рис. 30. Вкладка «Перевірити ЕП»

Розділ «Файл», який у свою чергу включає:

Якщо перевіряється файл за типом ЕП – **Вбудований (завантажуються за типом: Вбудований, ASIC-S, ASIC-E)**.

1. Поле «Файл з підписом» (обирається файл, який містить підпис за типом ЕП Вбудований, ASIC-S, ASIC-E).
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.

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

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 Відкріплений);
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.

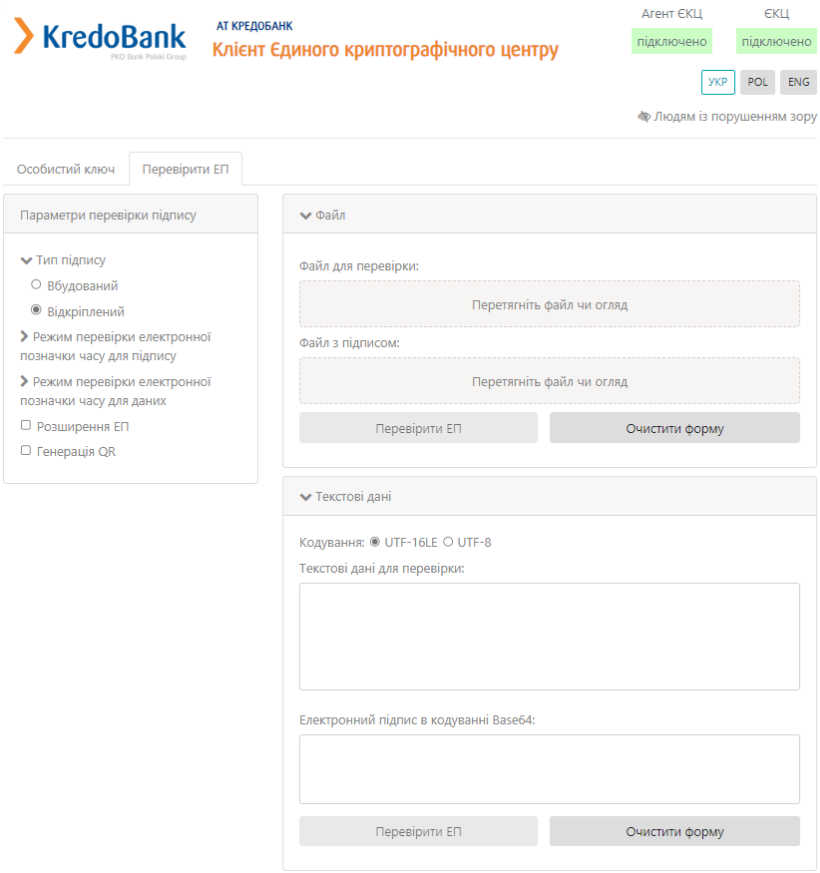

Рис. 31. Вкладка «Перевірити ЕП» зі вказівкою позначки «Розширення ЕП»

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 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.

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/текстові дані з підписом, натискаємо кнопку «Перевірити ЕП». За необхідності можна змінити файл/дані.

Перевірка ЕП за типом «Вбудований», файл

Для перевірки ЕП за типом «Вбудований» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Вбудований, 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. 32.

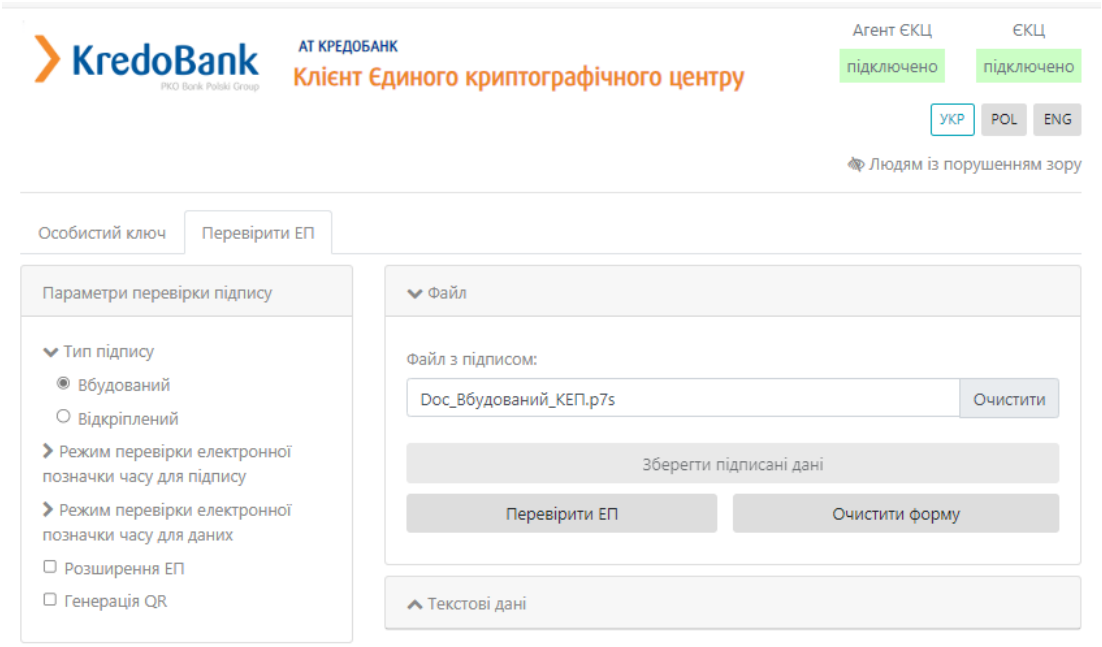

Рис. 32. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 33.

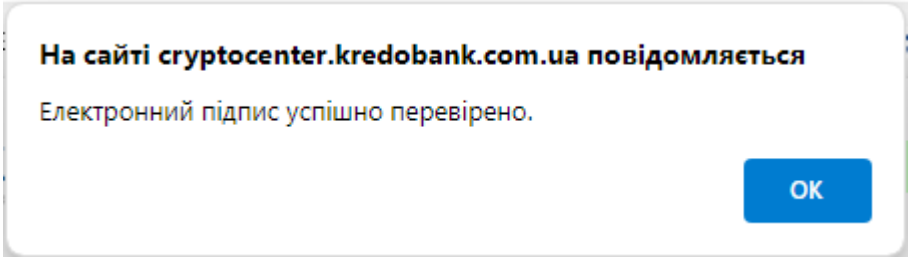

Рис. 33. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дату підпису, Рис. 34. За необхідності зберегти первинні дані (без підпису), натиснувши на кнопку «Зберегти підписані дані». Після чого, натискаємо кнопку «Очистити форму».

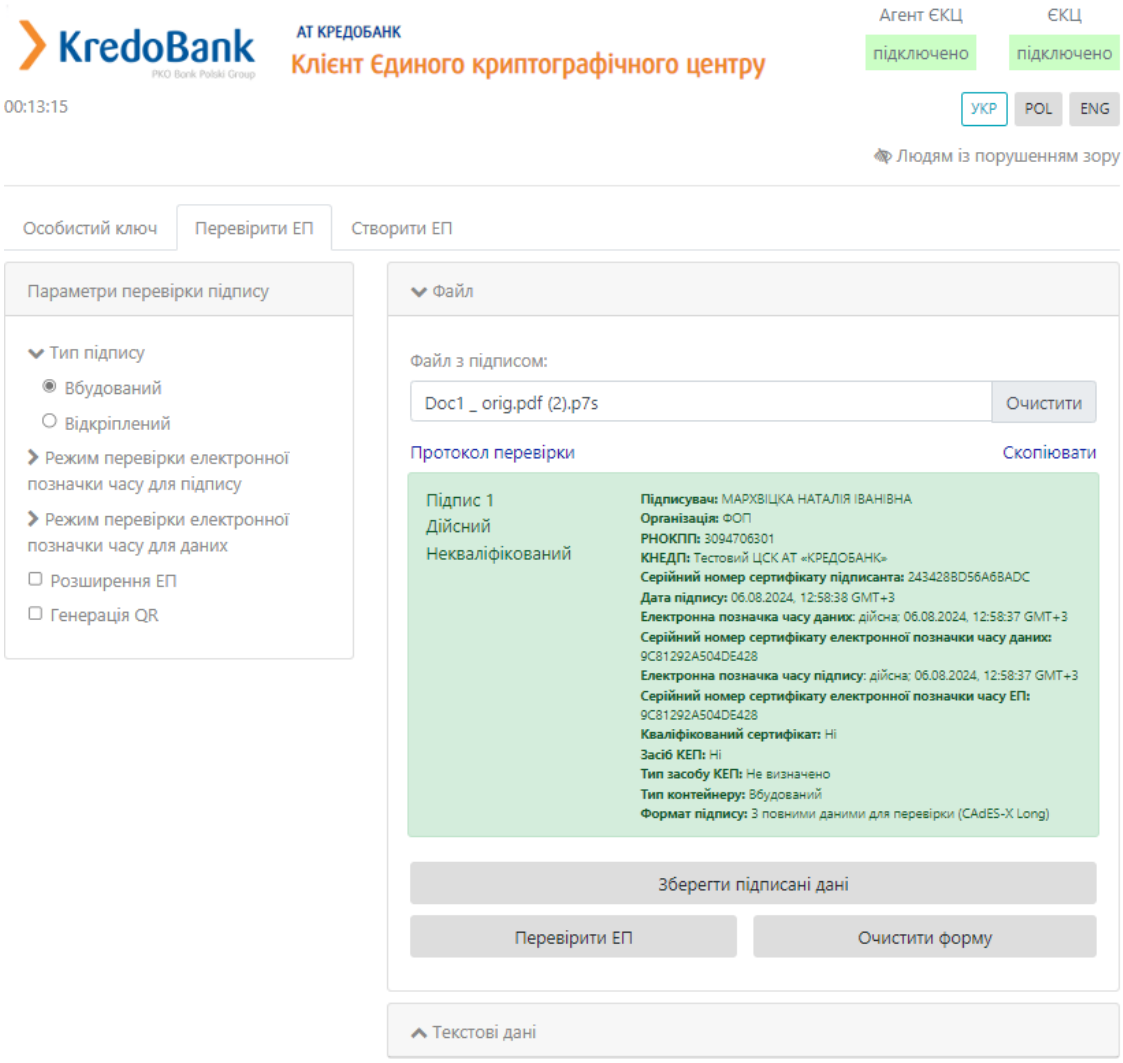

Рис. 34. Результат перевірки

Перевірка ЕП за типом «Відкріплений», файл

Для перевірки ЕП за типом «Відкріплений» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Відкріплений, 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. 35.

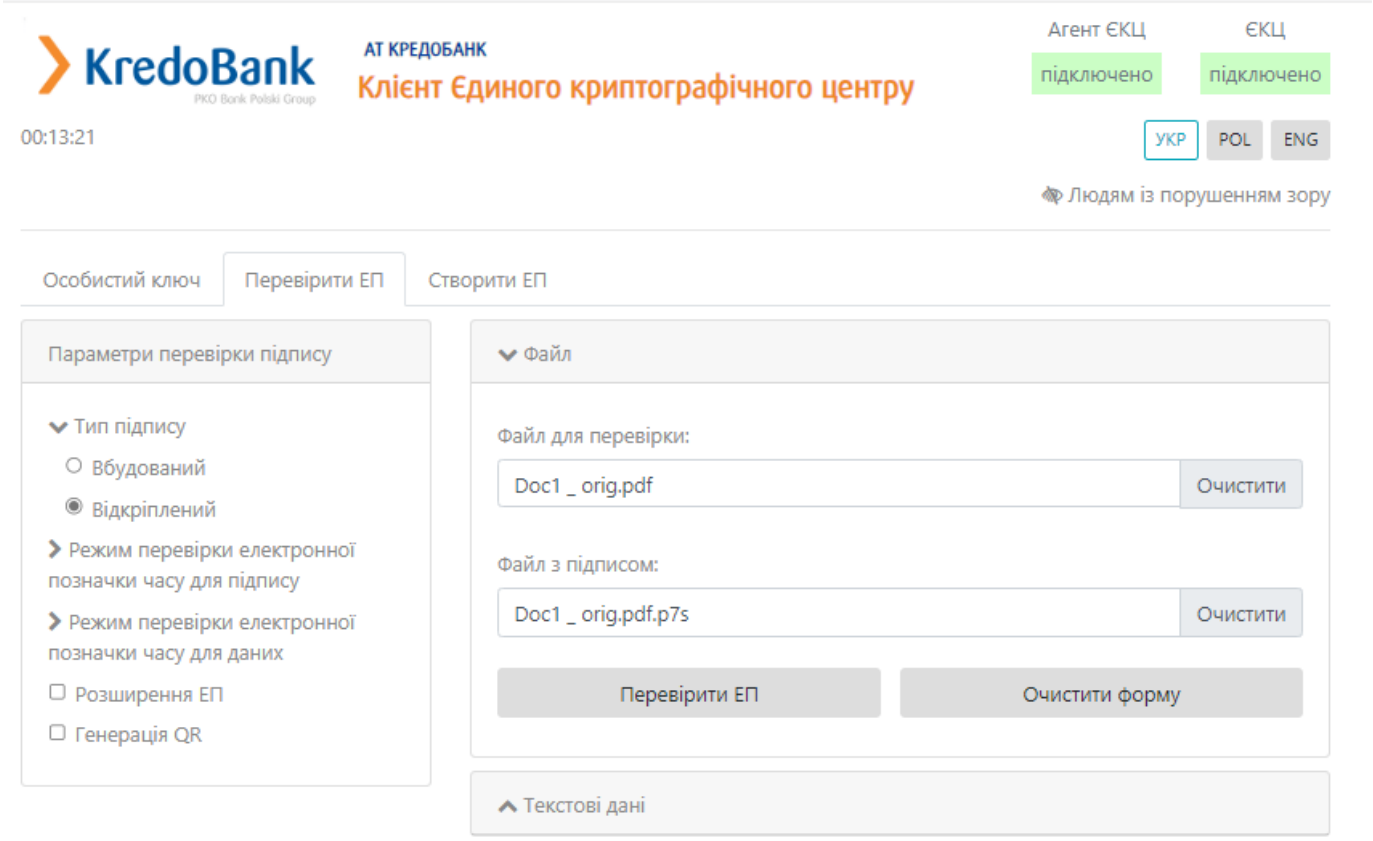

Рис. 35. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з’являється повідомлення з результатами перевірки електронного підпису, Рис. 36.

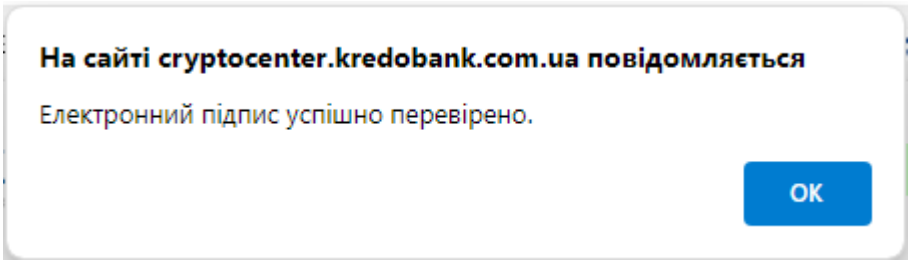

Рис. 36. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з’являється інформація про дійсність підпису, вказується інформація про підписанта та дата підпису, Рис. 37. Після чого, натискаємо кнопку «Очистити форму».

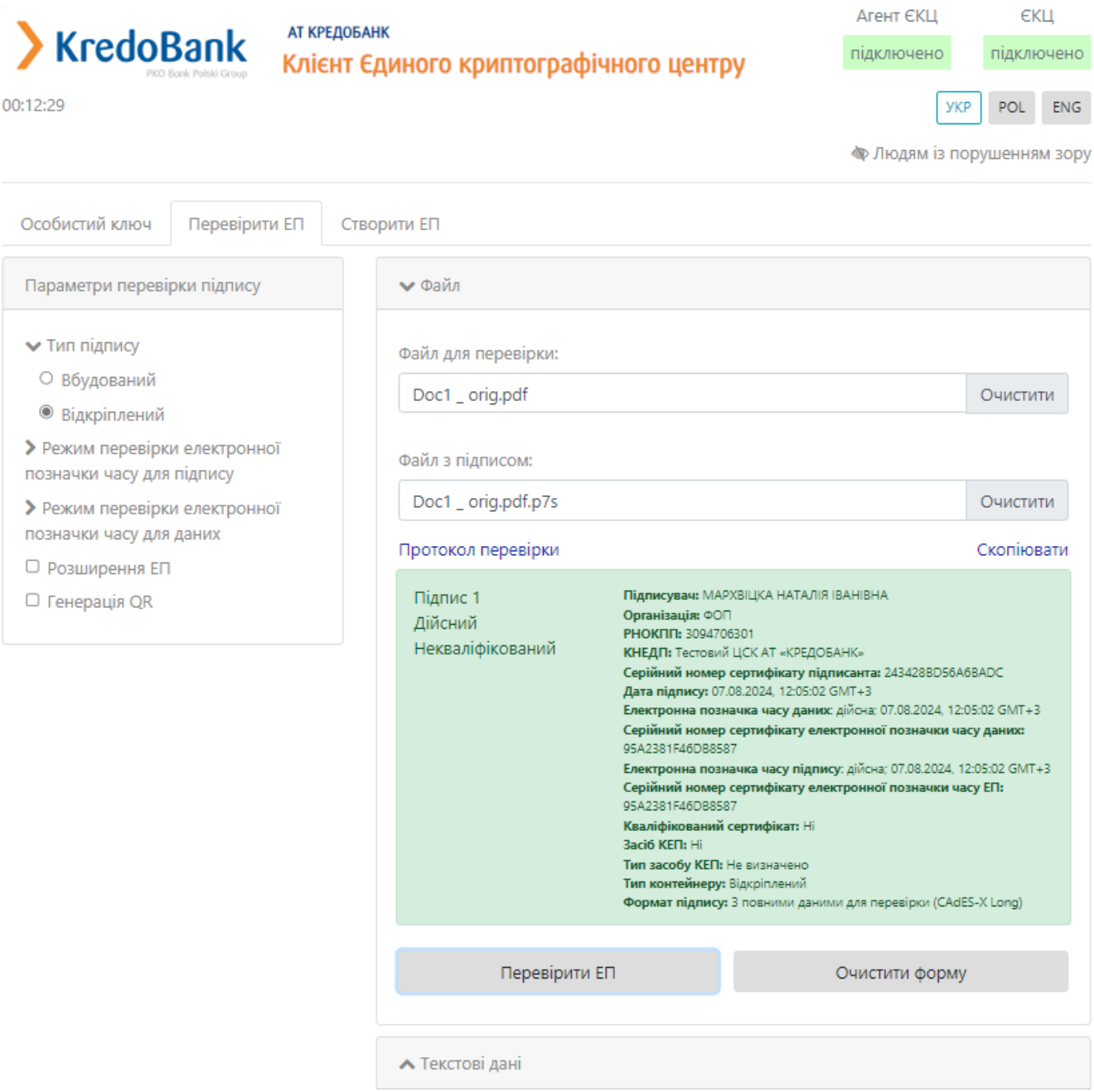

Рис. 37. Результат перевірки

Перевірка базового ЕП

Для перевірки ЕП за типом «Вбудований», формат ЕП «Базовий» 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.38.

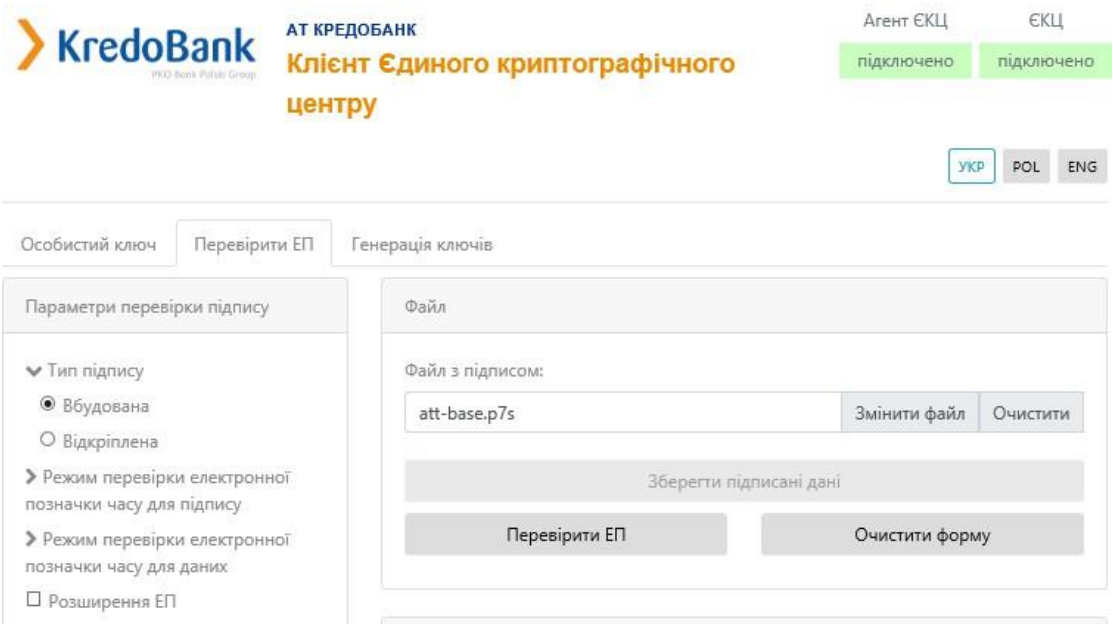

Рис. 38. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис.39.

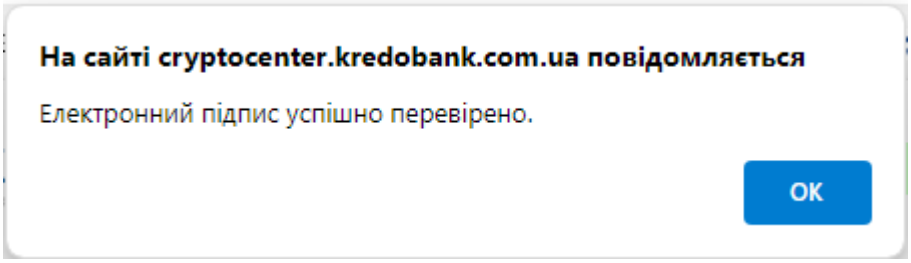

Рис. 39. Повідомлення про перевірку електронного підпису

Після натискання «ОК», з'являється інформація про перевірку підпису, вказується інформація про підписанта, дату підпису та повідомлення, що підпис є Базовий, Рис. 40. За необхідності зберегти первинні дані (без підпису), натиснувши на кнопку «Зберегти підписані дані». Після чого, натискаємо кнопку «Очистити форму».

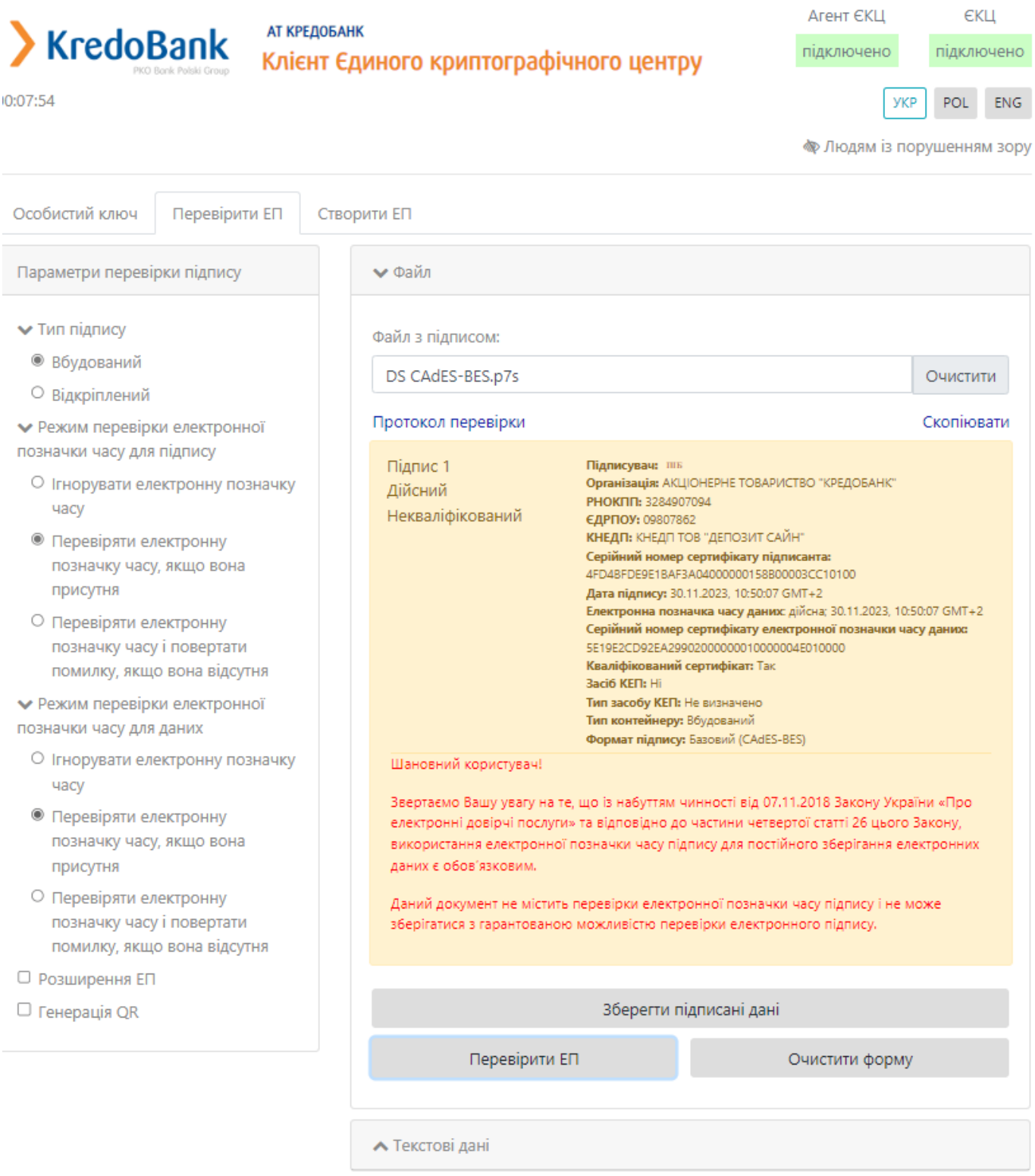

Рис. 40. Результат перевірки

Розширення ЕП

Вкладка «Перевірити ЕП» містить додаткову позначку «Розширити ЕП».

На прикладі вбудованого електронного підпису, який отримано раніше. Слід обрати файл та натиснути кнопку «Перевірити ЕП». Отримаємо результат перевірки електронного підпису, Рис. 41.

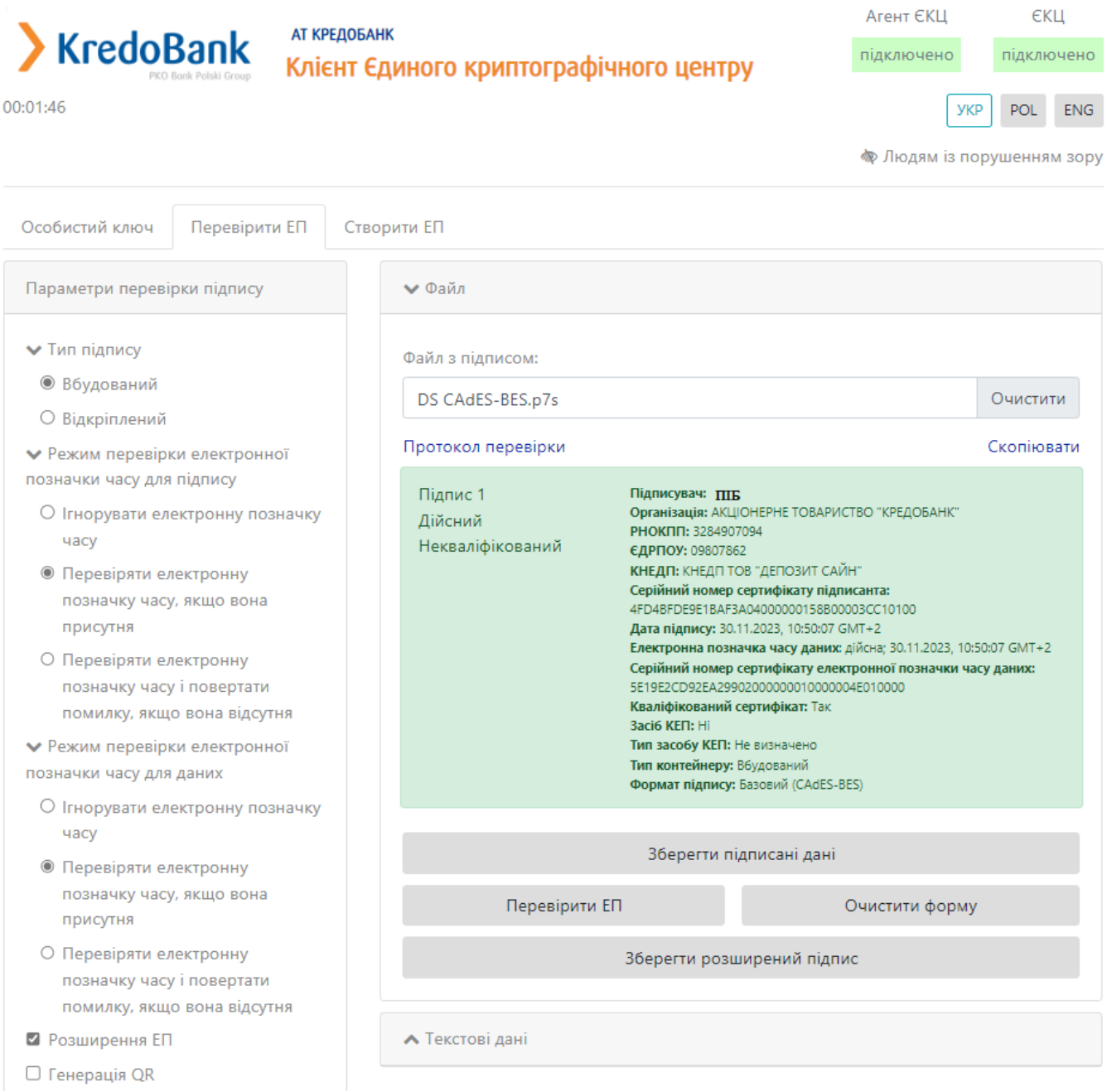

Рис. 41. Розширення вбудованого ЕП

Зашифрувати

Процес зашифрування здійснюється із застосуванням захищеного носія чи файлового ключового контейнеру.

Вкладка «Зашифрувати» містить такі розділи: Параметри шифрування, Сертифікат отримувача, Текстові дані та Файл, Рис. 42.

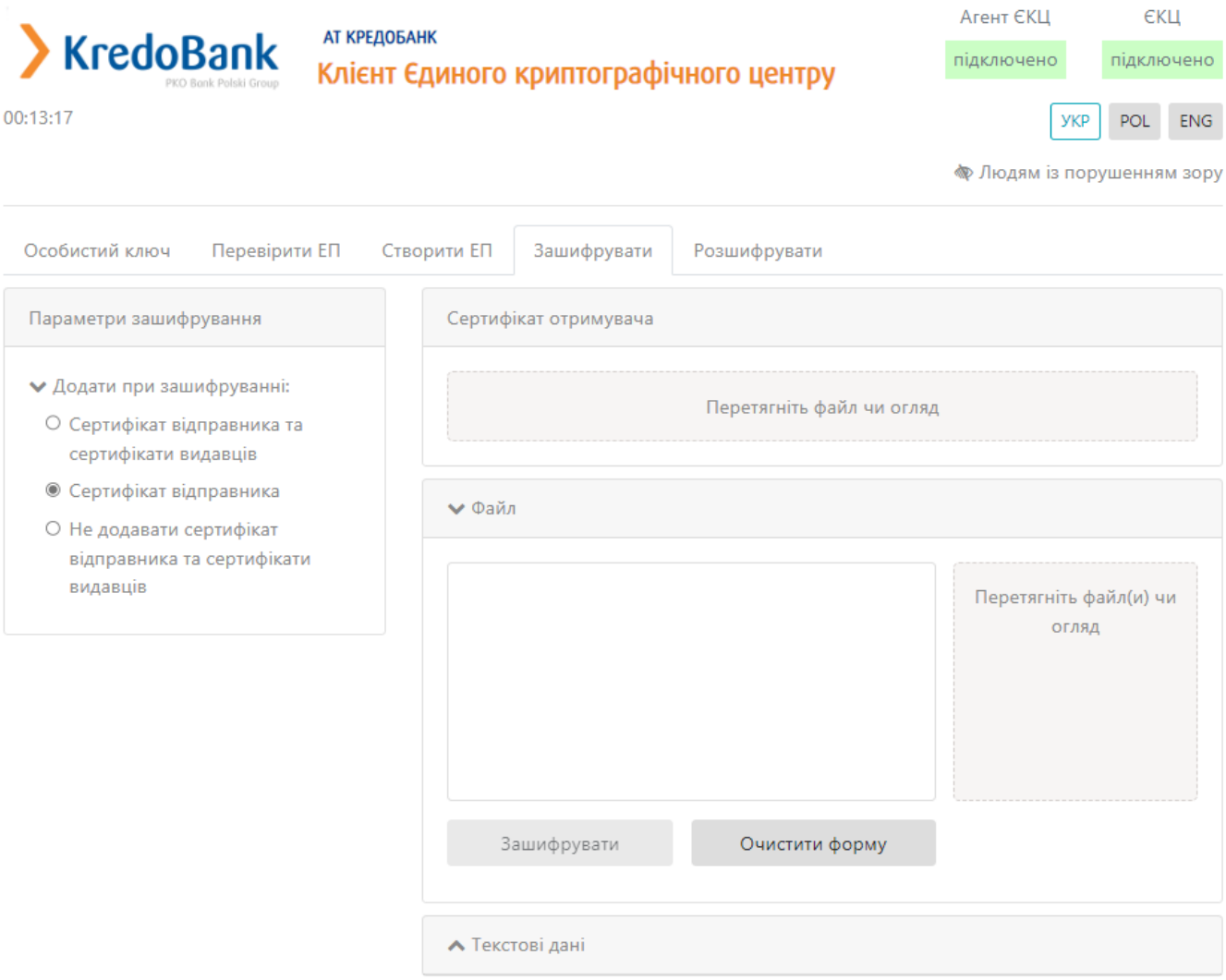

Рис. 42. Вкладка «Зашифрувати»

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:

2. Поле «Сертифікат отримувача» (завантажуємо файл-сертифікат отримувача).

Розділ «Файл», який включає:

1. Поле «Файл» для додавання файлу/файлів для шифрування;
2. Кнопка «Зашифрувати» (здійснює зашифрування файлу);
3. 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».

Операція зашифрування файлу

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. 43.

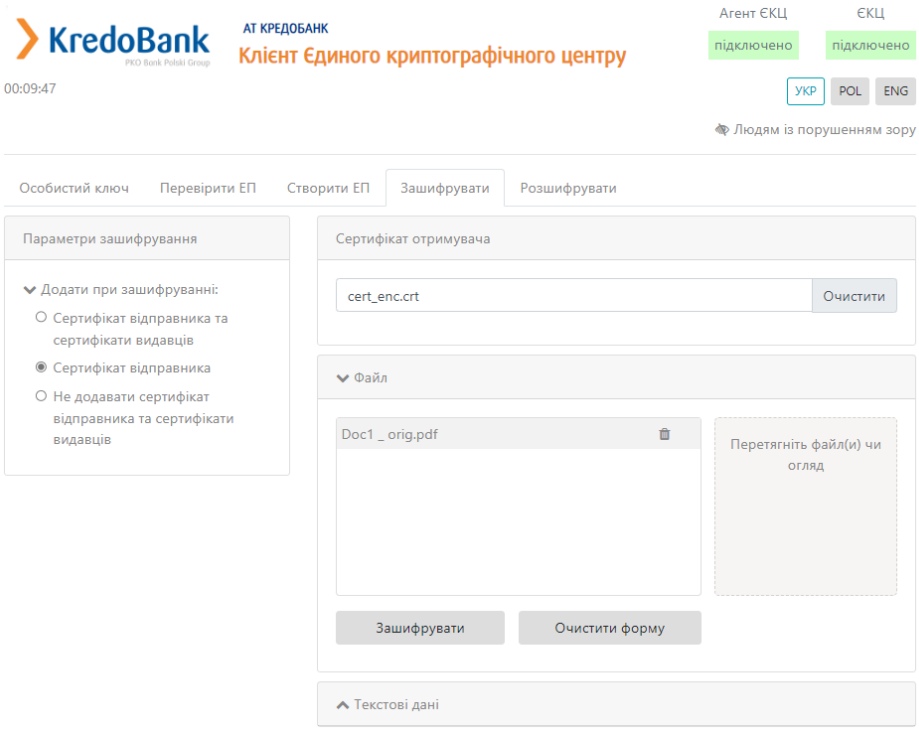

Рис. 43. Процес зашифрування

Після натискання на кнопку «Зашифрувати» з’являється вікно з повідомленням з результатом зашифрування, Рис. 44.

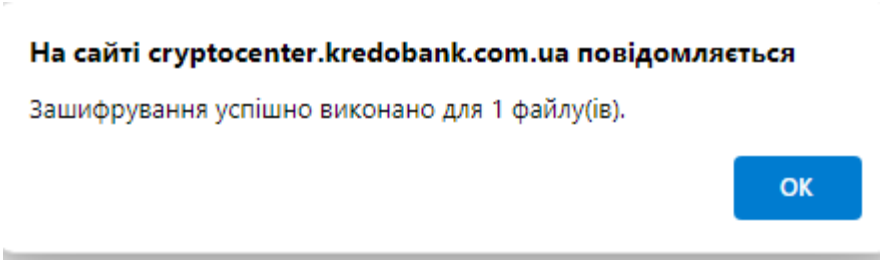

Рис. 44. Повідомлення про успішне зашифрування даних

Після, за допомогою відповідної кнопки «стрілка вниз» можна зберегти зашифрований файл та очищаємо форму, Рис. 45.

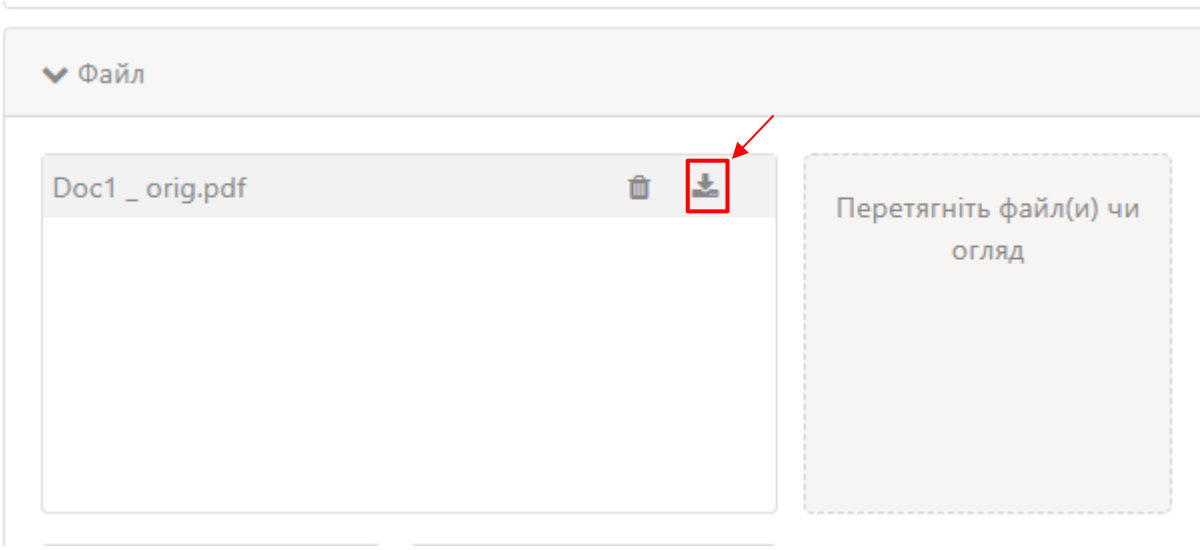

Рис. 45. Збереження зашифрованого файлу

Розшифрувати

Дана вкладка містить розділ Файл.

Розділ «Файл», який включає, Рис. 46:

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

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.

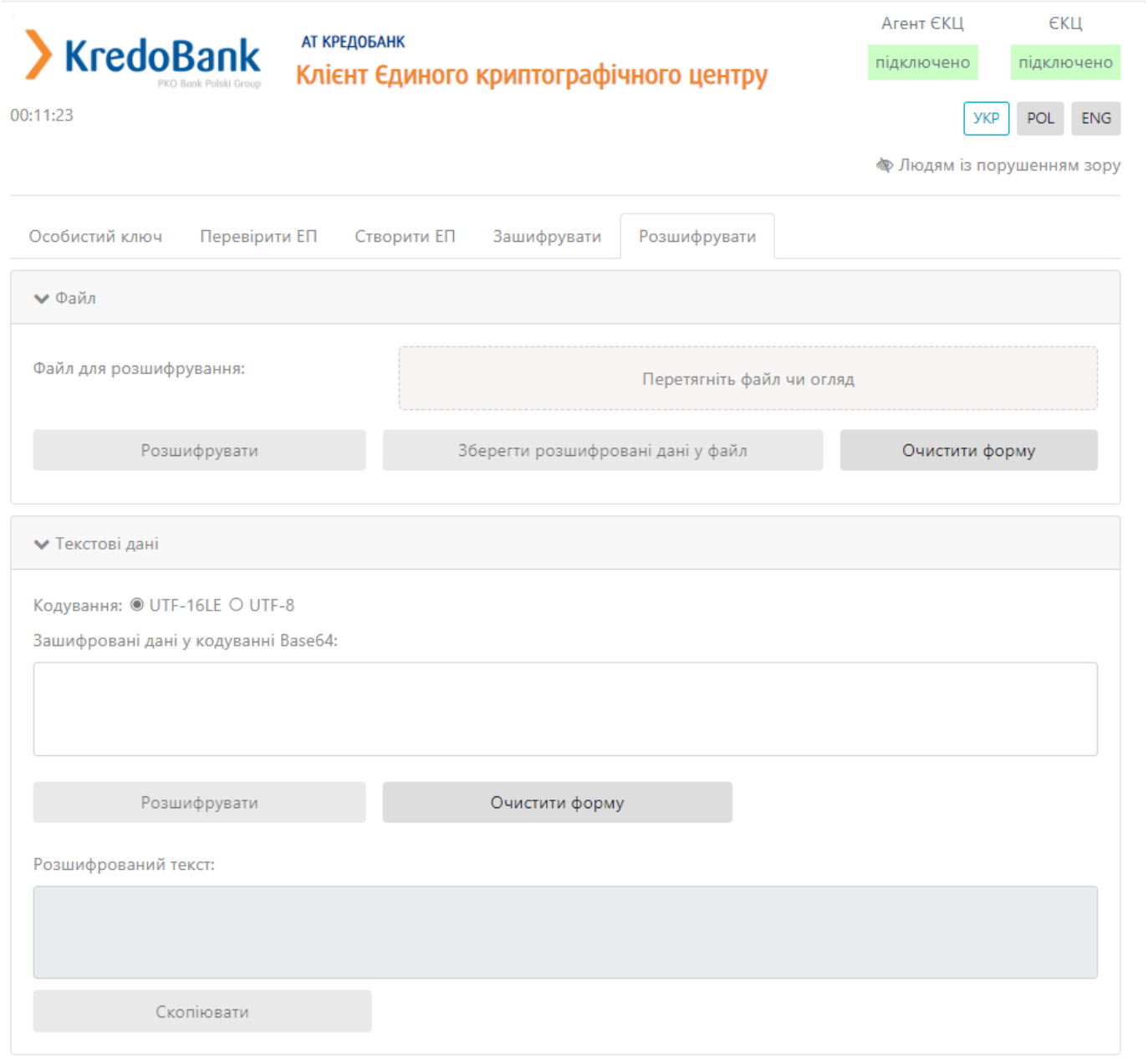

Рис. 46. Вкладка «Розшифрувати»

Операція розшифрування файлу

Для того, щоб розшифрувати файл, у розділі «Файл», необхідно вказати файл для розшифрування та натиснути кнопку «Розшифрувати», Рис. 47.

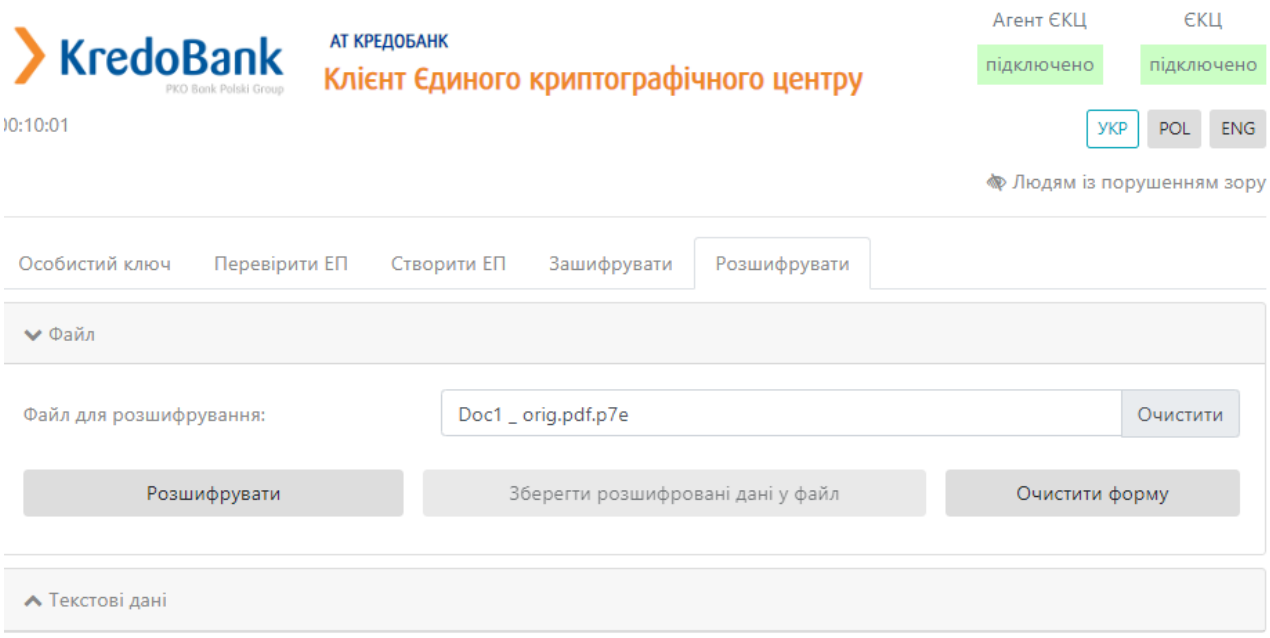

Рис. 47. Процес розшифрування

Після натискання на кнопку «Розшифрувати» з’являється вікно з повідомленням з результатом зашифрування, Рис. 48, де слід натиснути кнопку «ОК» та для збереження розшифрованих даних необхідно натиснути кнопку «Зберегти розшифровані дані у файл», Рис. 49 та очистити форму.

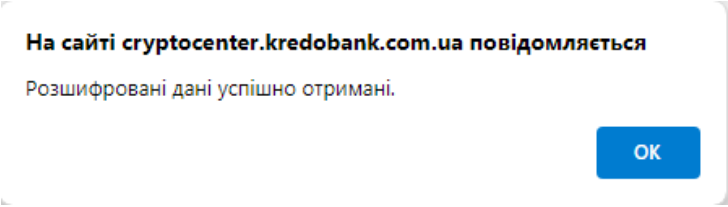

Рис. 48. Повідомлення про успішне розшифрування даних

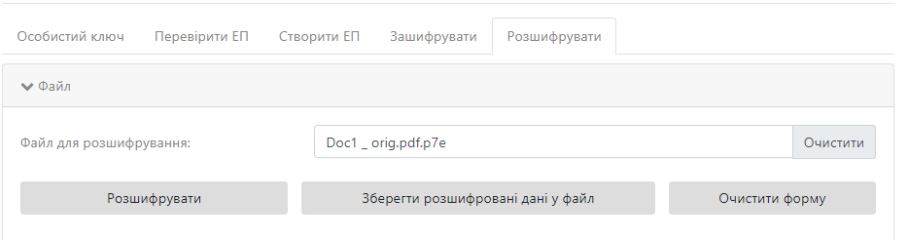

Рис. 49. Збереження розшифрованих даних