Інформаційно-довідковий департамент ДПС

Кваліфікований надавач електронних довірчих послуг

НАСТАНОВА КОРИСТУВАЧА

Засіб кваліфікованого електронного підпису чи печатки «ІІТ Користувач ЦСК-1»

Київ 2020

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

КЕП	–	Кваліфікований електронний підпис;
НКІ	–	Носій ключової інформації;
ПК	–	Персональний комп’ютер;
ПЗ	–	Програмне забезпечення «ІІТ Користувач ЦСК-1»;
СВС	–	Список відкликаних сертифікатів;
Надавач	–	Кваліфікований надавач електронних довірчих послуг Інформаційно-довідковий департамент ДПС;
CMP	–	Certificate Management Protocol (протокол управління обслуговуванням кваліфікованих сертифікатів);
LDAP	–	Lightweight Directory Access Protocol (протокол доступу до каталогу);
OCSP	–	Online Certificate Status Protocol (протокол визначення статусу кваліфікованого сертифіката);
TSP	–	Time Stamp Protocol (протокол фіксування часу);
вебсайт	–	Офіційний інформаційний ресурс Надавача (https://acskidd.gov.ua)
файлове сховище	–	Каталог (папка), призначений для зберігання кваліфікованих сертифікатів та СВС
ПТК	–	Програмно-технічний комплекс

Призначення програми

ПЗ «ІІТ Користувач ЦСК-1» є надійним засобом КЕП, призначеним для застосування на ПК користувача/підписувача Надавача, для реалізації наступних функцій:

- **управління ключами користувача:**
  - генерація ключів користувача Надавача, запис особистого ключа на НКІ та створення запиту на формування кваліфікованого сертифіката;
  - резервне копіювання особистого ключа з одного НКІ на інший;
  - зміна паролю захисту особистого ключа;
  - знищення особистого ключа на НКІ;
  - формування та передача до Надавача запиту на блокування кваліфікованого сертифіката підписувача;
  - формування та передача до Надавача запиту на скасування кваліфікованого сертифіката підписувача;
- **доступ до кваліфікованих сертифікатів Надавача, серверів Надавача, кваліфікованих сертифікатів інших користувачів та СВС:**
  - перегляд кваліфікованих сертифікатів та СВС у файловому сховищі;
  - пошук кваліфікованих сертифікатів у файловому сховищі за допомогою протоколу CMP;
  - визначення статусу кваліфікованих сертифікатів за допомогою СВС та за протоколом OCSP;
  - перевірка чинності та цілісності кваліфікованих сертифікатів та ін.;
- **захист файлів користувача:**
  - підпис файлів;
  - перевірка КЕП;
  - шифрування файлів;
  - розшифрування файлів.

1. Встановлення та обслуговування програмного забезпечення «ІІТ Користувач ЦСК-1»

Увага! Встановивши дане ПЗ Ви зобов'язуєтесь використовувати його виключно за призначенням та в порядку визначеному цією Настановою. Перед використанням обов'язково ознайомтесь з Регламентом Кваліфікованого надавача електронних довірчих послуг Інформаційно-довідкового департаменту ДПС щодо умов обслуговування кваліфікованих сертифікатів.

Для встановлення ПЗ необхідно завантажити архівний файл з інсталяційним пакетом з вебсайту за наступним посиланням https://acskidd.gov.ua/korustyvach_csk

Далі необхідно розпакувати архівний файл, здійснити інсталяцію ПЗ виконавши наступні дії:

1.1. Запускаємо інсталятор ПЗ – EUInstall.exe (рис. 1.1).

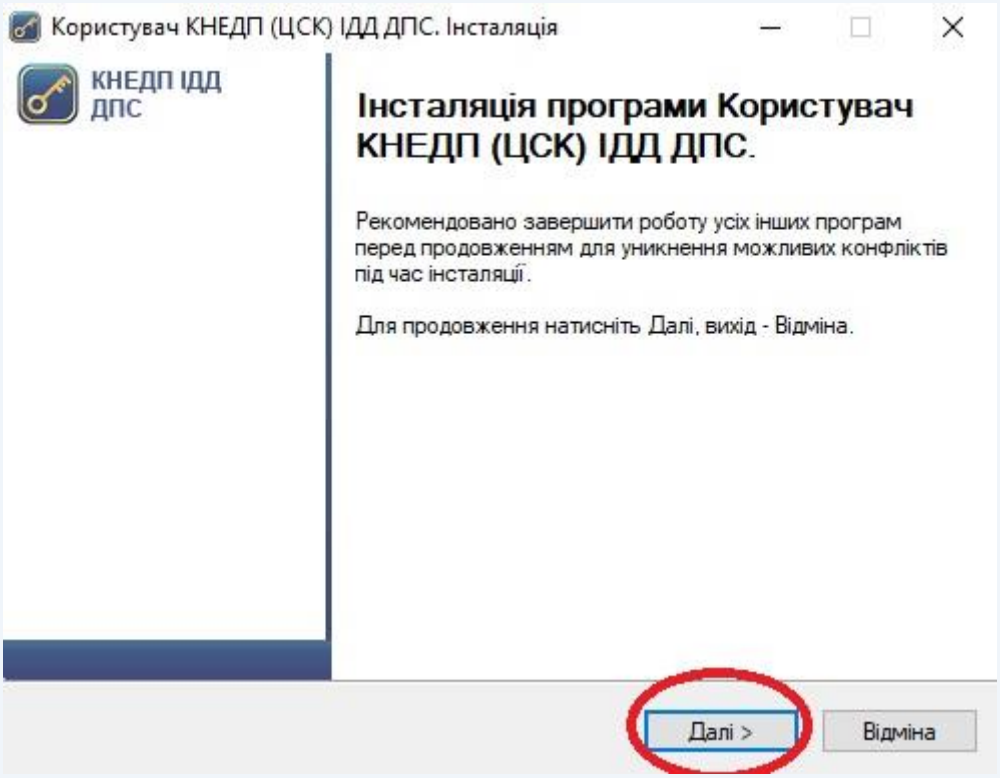


Рисунок 1.1

1.2. Каталог розміщення ПЗ створюється автоматично (за замовчуванням C:\Program Files\Institute of Informational Technologies\Certificate Authority-1.3\End User), змінювати його не рекомендується. Для продовження інсталяції натискаємо кнопку «Далі» (рис. 1.2).

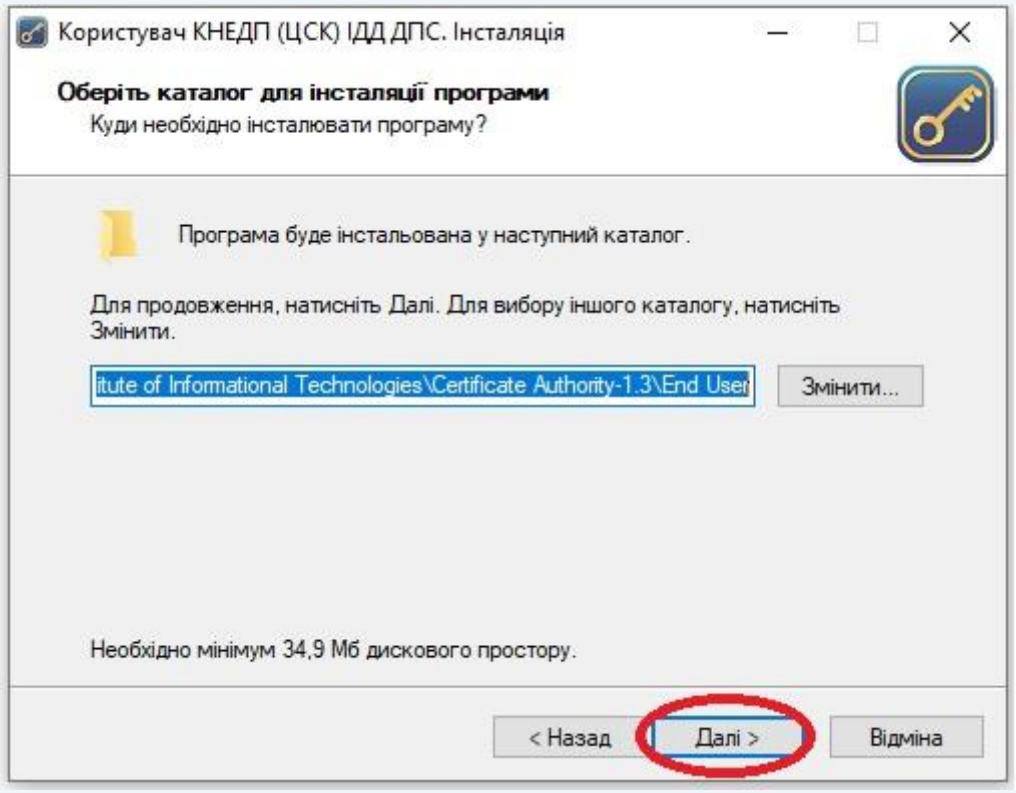


Рисунок 1.2

1.3. Каталог ПЗ у меню «Пуск» створюється автоматично, змінювати його не рекомендується, натискаємо кнопку «Далі» (рис. 1.3).

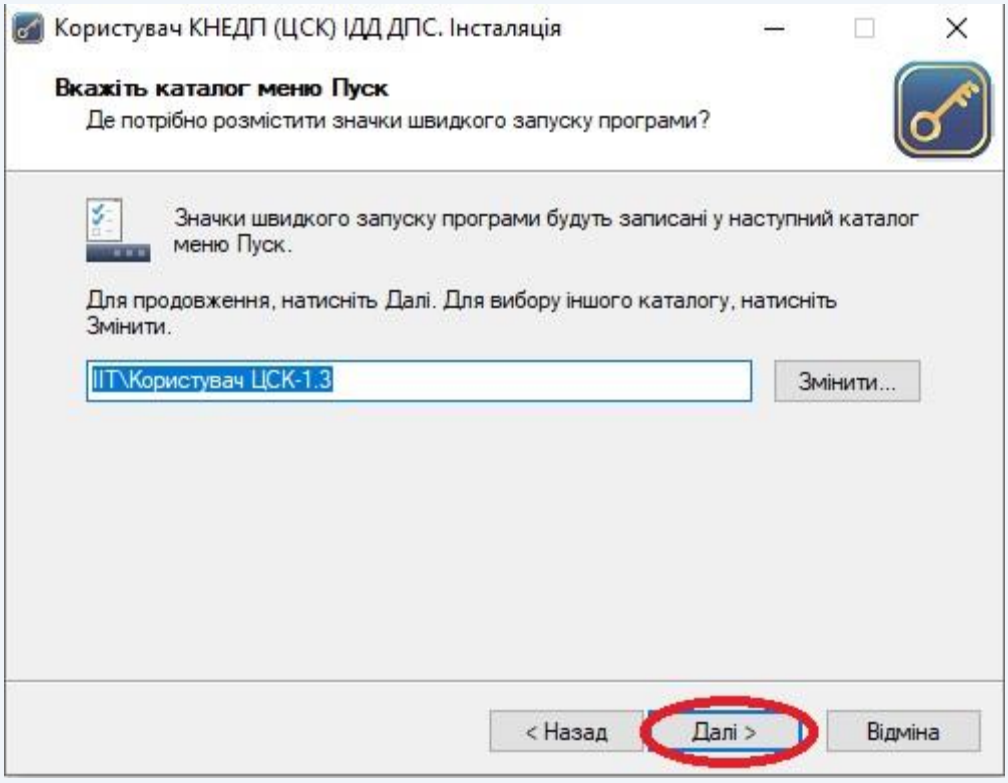


Рисунок 1.3

1.4. Під час встановлення ПЗ файлове сховище для кваліфікованих сертифікатів та СВС створюється автоматично. Для зміни розташування файлового сховища необхідно натиснути кнопку «Змінити» та обрати відповідний каталог. Для продовження інсталяції натискаємо кнопку «Далі» (рис. 1.4).

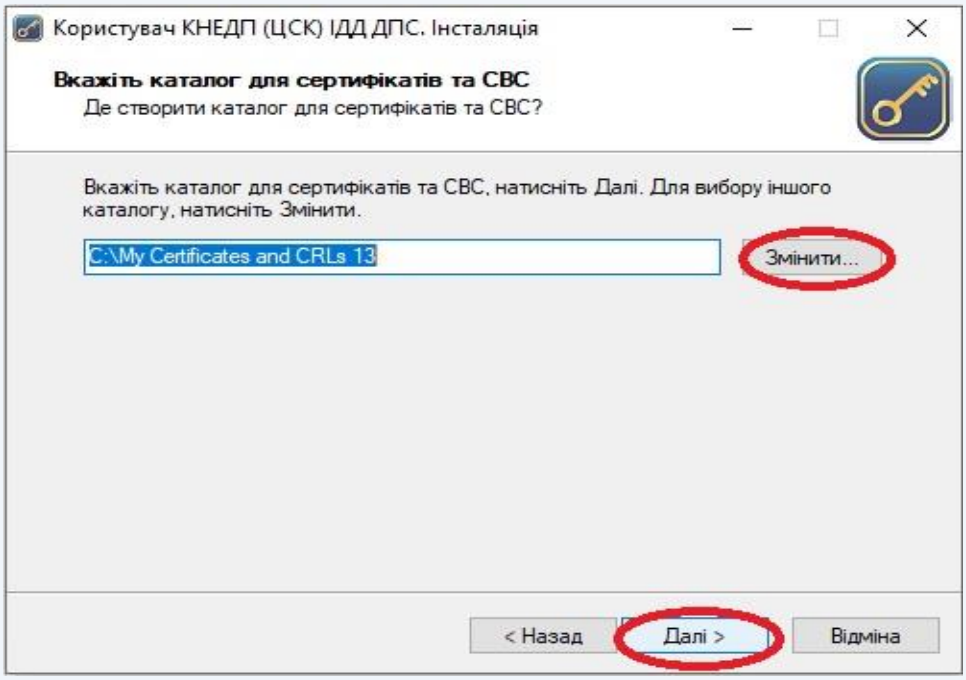


Рисунок 1.4

1.5. За необхідності можна створити ярлик на робочому столі та запустити ПЗ після завершення його інсталяції. Для цього необхідно проставити відповідні позначки (рис. 1.5). Для продовження інсталяції натискаємо кнопку «Далі».

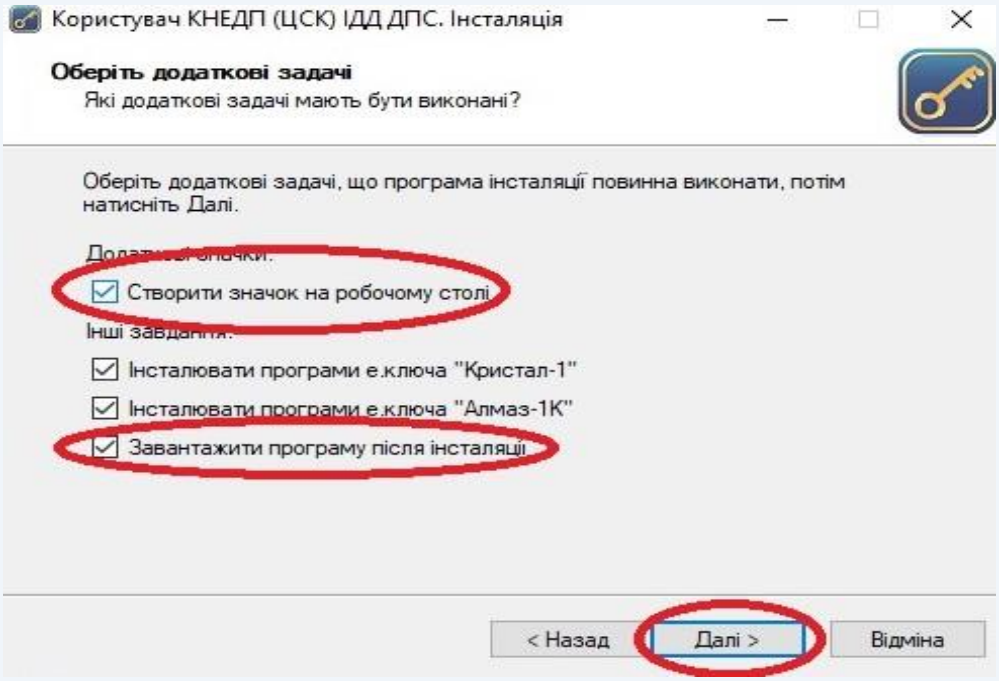


Рисунок 1.5

1.6. У вікні готовності до інсталяції натискаємо кнопку «Встановити» (рис. 1.6). Якщо параметри інсталяції не задовольняють користувача/підписувача, їх можна змінити натиснувши кнопку «Назад». Для виходу з ПЗ необхідно натиснути «Відміна».

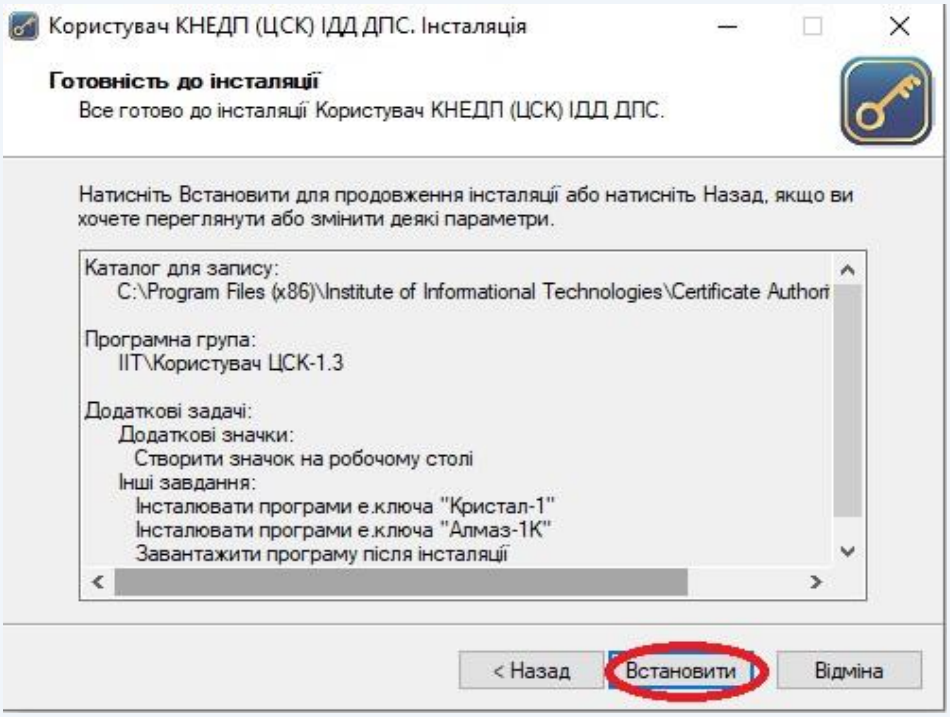


Рисунок 1.6

1.7. Після завершення інсталяції запущене головне вікно ПЗ має такий вигляд (рис. 1.7).

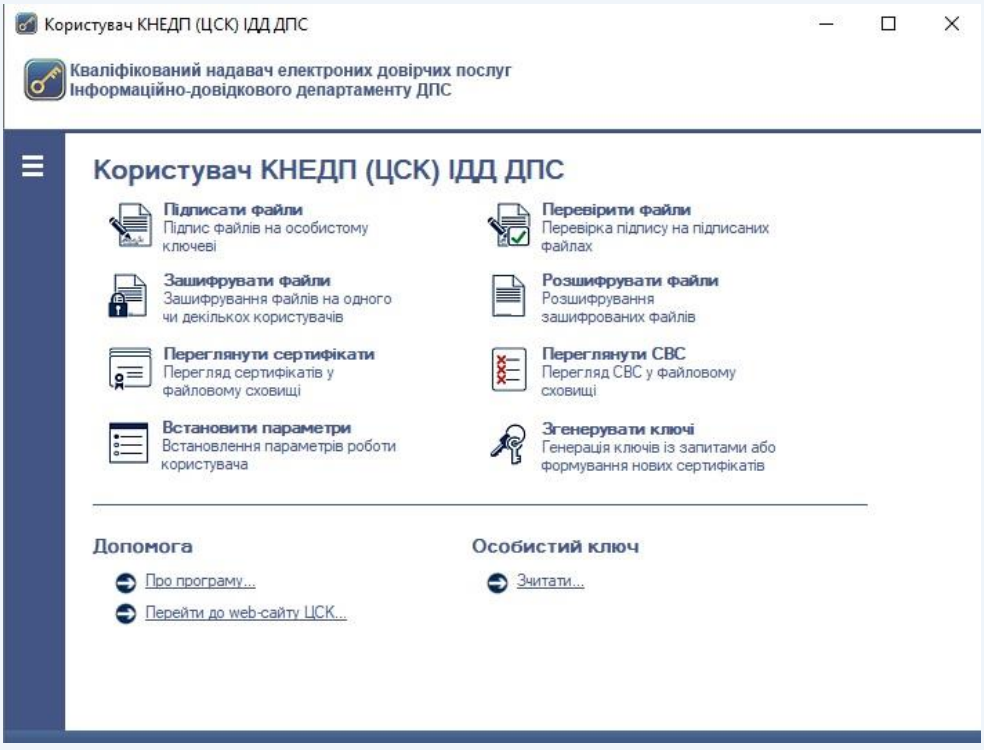


Рисунок 1.7

Перед використанням ПЗ необхідно налаштувати. Кнопка меню знаходиться в верхньому лівому куті (рис. 1.8).

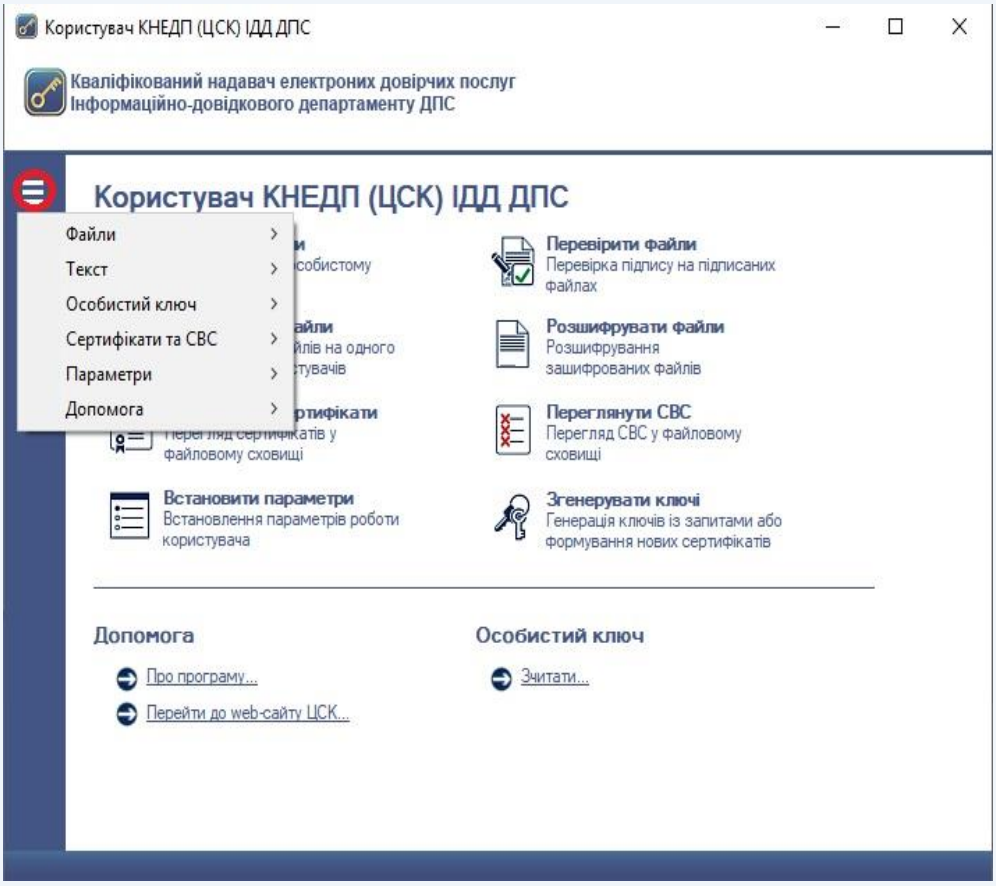


Рисунок 1.8

1.8. У зв’язку з відсутністю в ПЗ функції автоматичного оновлення версій, подальше його обслуговування здійснюватиметься шляхом розміщення на вебсайті (https://acskidd.gov.ua/korustyvach_csk) оновленого архівного файлу з інсталяційним пакетом.

2. Підготовка до роботи програмного забезпечення «ІІТ Користувач ЦСК-1»

Після інсталяції ПЗ, до **файлового сховища** необхідно додати кваліфіковані сертифікати підписувача.

Здійснити перевірку розташування **файлового сховища** можна у головному вікні ПЗ, натиснувши кнопку «**Встановити параметри**», або натиснути комбінацію клавіш **Ctrl+P**. Після чого з’явиться діалогове вікно **«Файлове сховище сертифікатів та СВС».** За необхідності, розташування файлового сховища можна змінити (рис. 2.1.).

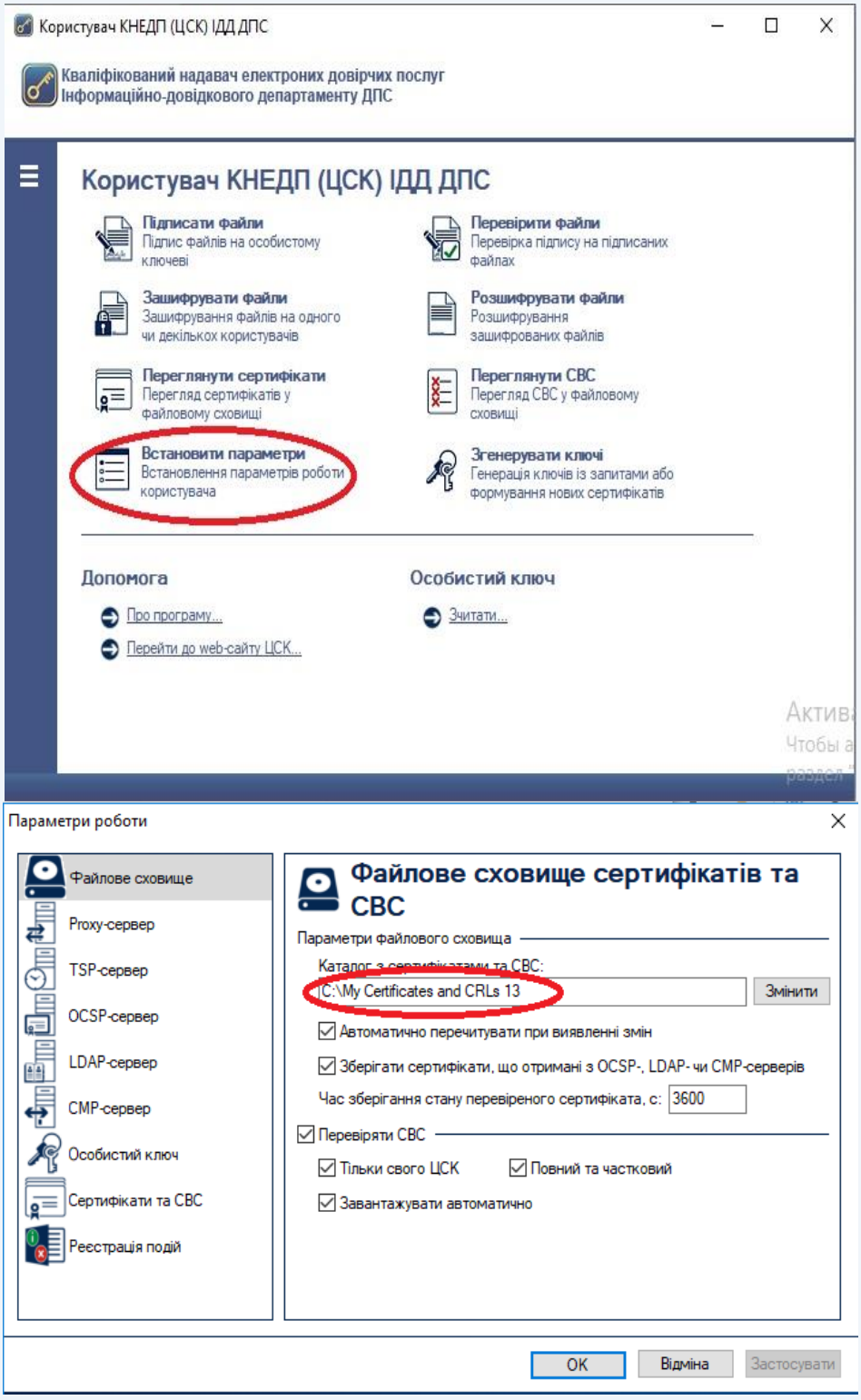


Рисунок 2.1

Виконати пошук кваліфікованого сертифіката можна на вебсайті у розділі «Пошук сертифікатів та СВС», вкладка «Пошук сертифікатів» використовуючи поле «Реєстраційний номер облікової картки платника податків» або поле «Код ЄДРПОУ» (ввівши код платника податків згідно Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань) , або поле «УНЗР ID картки» (зазначивши унікальний номер запису в Єдиному державному демографічному реєстрі) та натиснути кнопку «Пошук» (рис. 2.2).

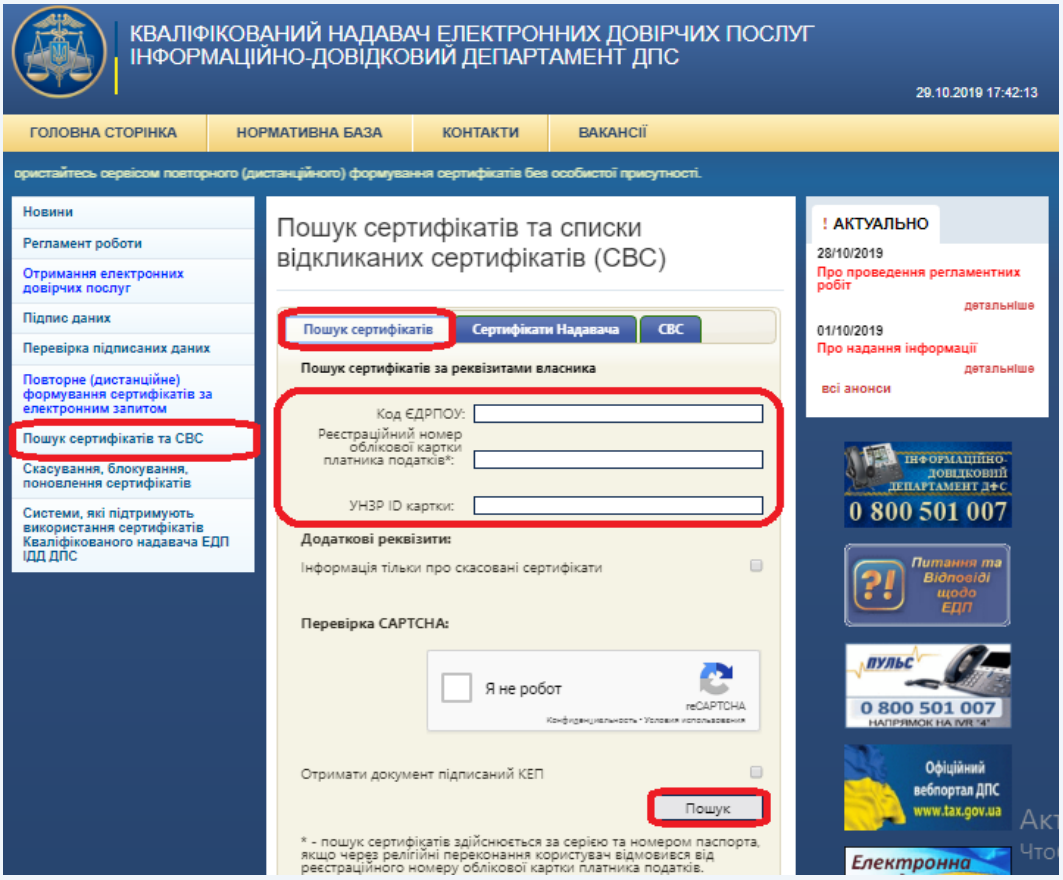


Рисунок 2.2

Якщо ви знайшли кваліфікований сертифікат відповідного підписувача – завантажте його на свій комп'ютер натиснувши кнопки –  (рис. 2.3).

Увага! Для належної роботи ПЗ необхідно завантажити обидва кваліфіковані сертифікати (підпису та шифрування (рис. 2.3) та зберегти їх у файловому сховищі.

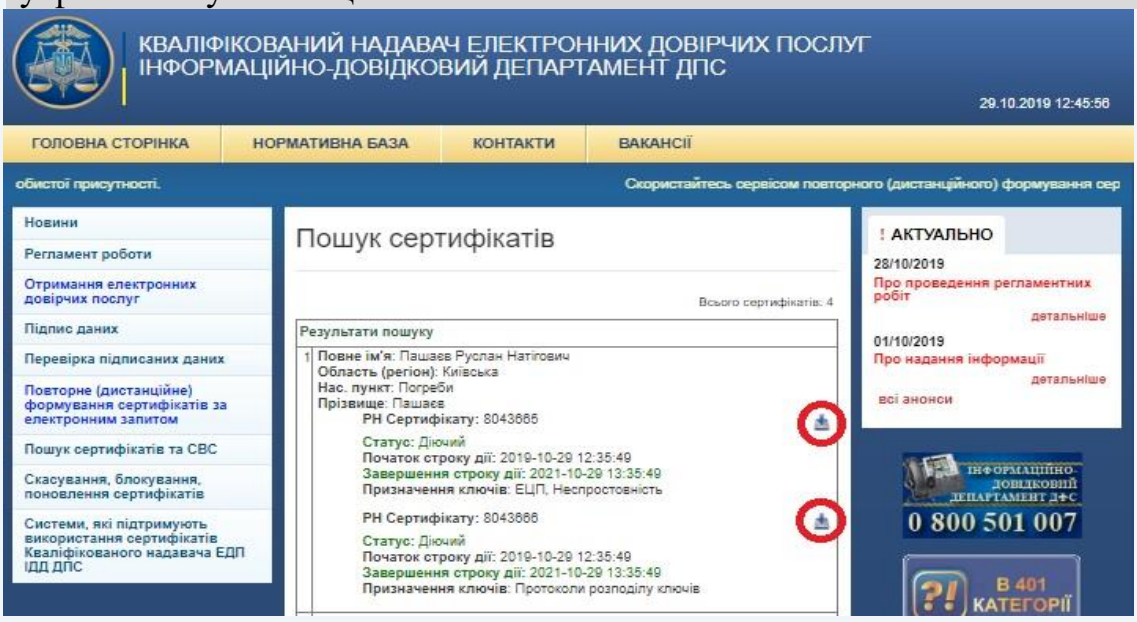


Рисунок 2.3

При використанні браузера «Internet Explorer» збереження кваліфікованого сертифіката необхідно підтвердити натиснувши у спливаючому вікні кнопку «Сохранить» (рис. 2.4).

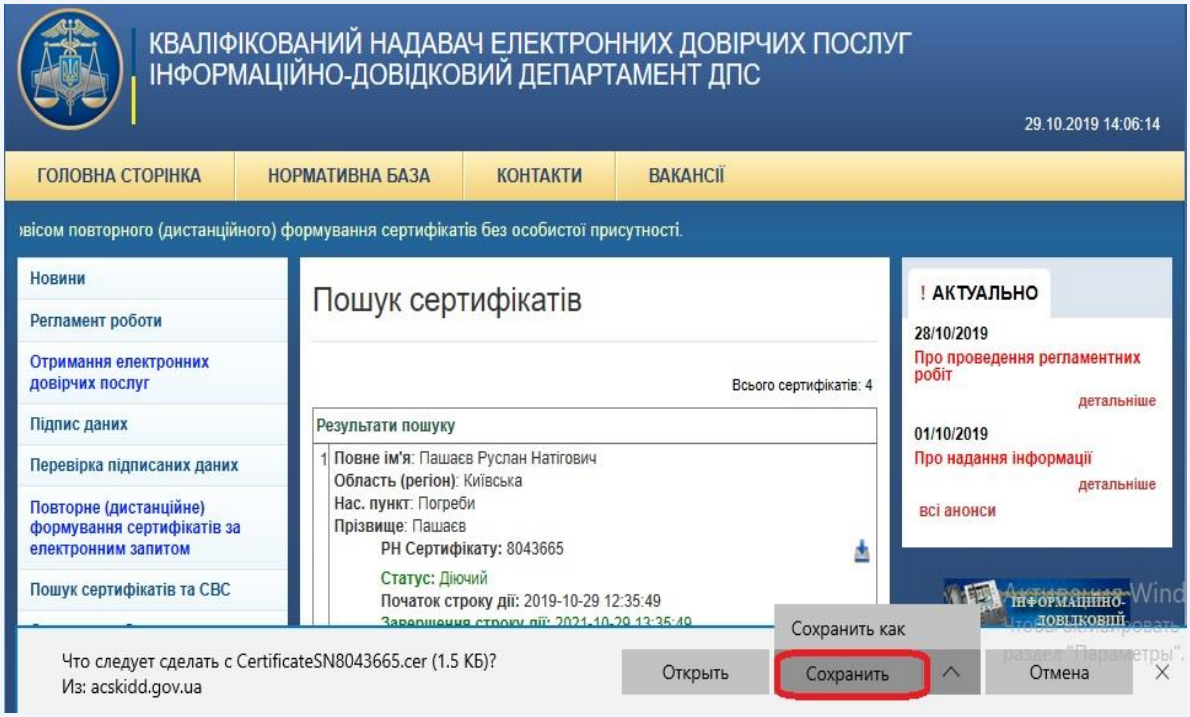


Рисунок 2.4

По завершенні процесу завантаження необхідно натиснути кнопку «Открыть папку» (рис. 2.5).

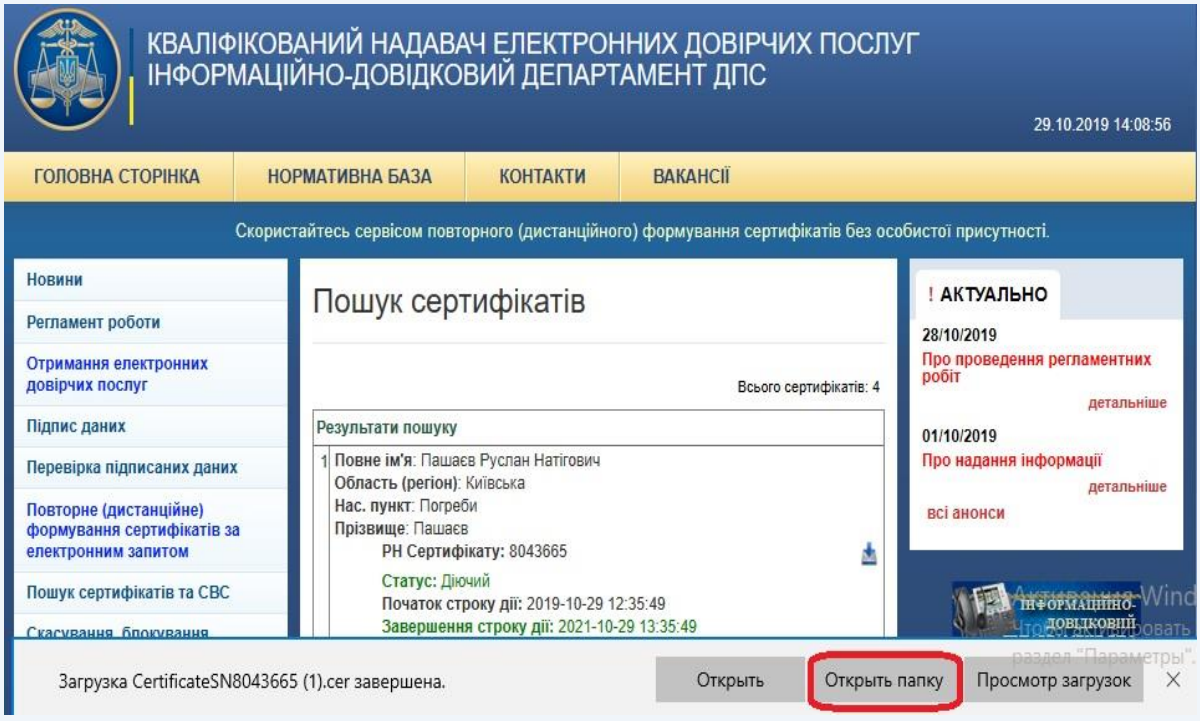


Рисунок 2.5

Якщо ви використовуєте браузер «Mozilla Firefox», з’явиться діалогове вікно, в якому необхідно обрати «Сохранить файл» та натиснути «ОК» (рис. 2.6).

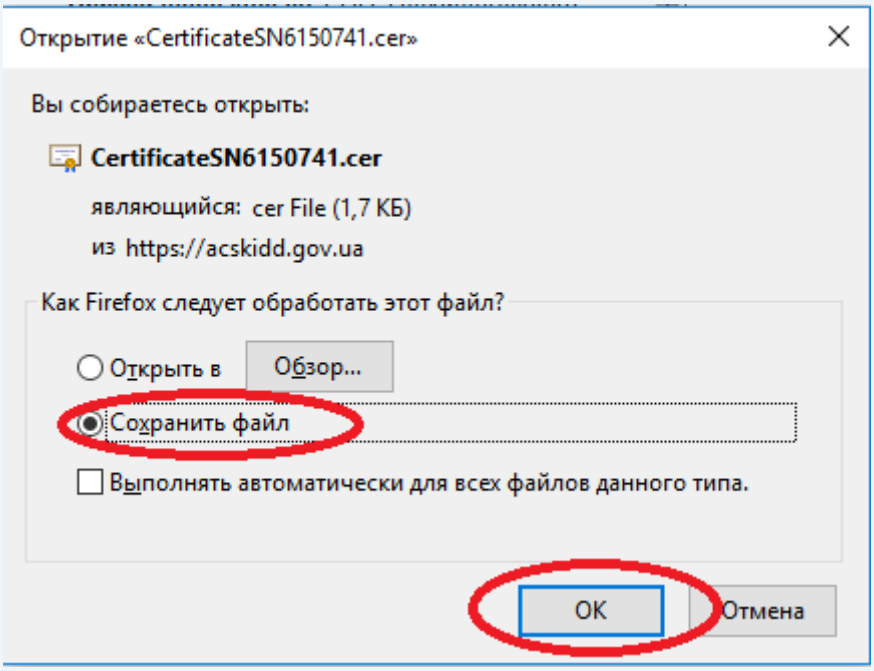


Рисунок 2.6

Далі у випливаючому вікні необхідно натиснути кнопку  навпроти свого кваліфікованого сертифіката (рис. 2.7).

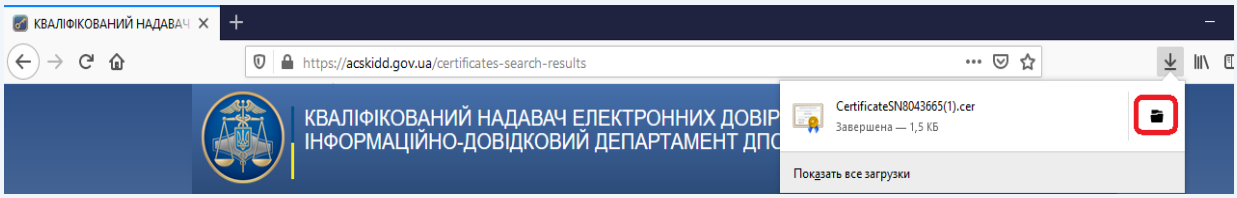


Рисунок 2.7

Якщо ви використовуєте браузер «Google Chrome», після завантаження необхідно натиснути правою кнопкою миші на іконку та обрати в меню «Показати в папці» (рис. 2.8).

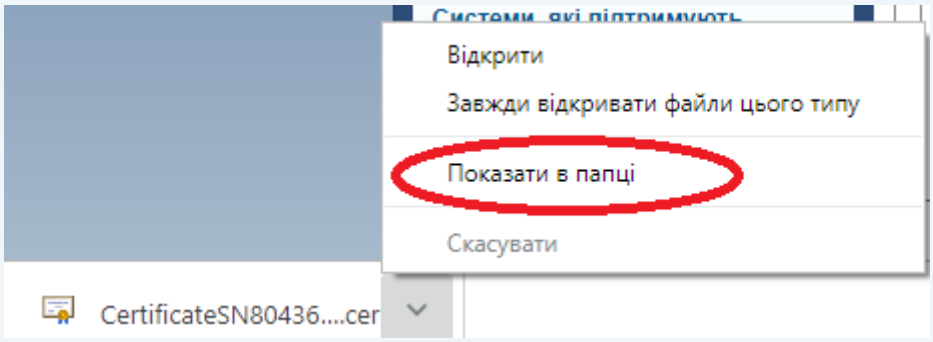


Рисунок 2.8

Завантажені **кваліфіковані сертифікати** (підпису та шифрування) необхідно скопіювати до файлового сховища (за замовчуванням **«C:\My Certificates and CRLs 13»**) (рис. 2.9).

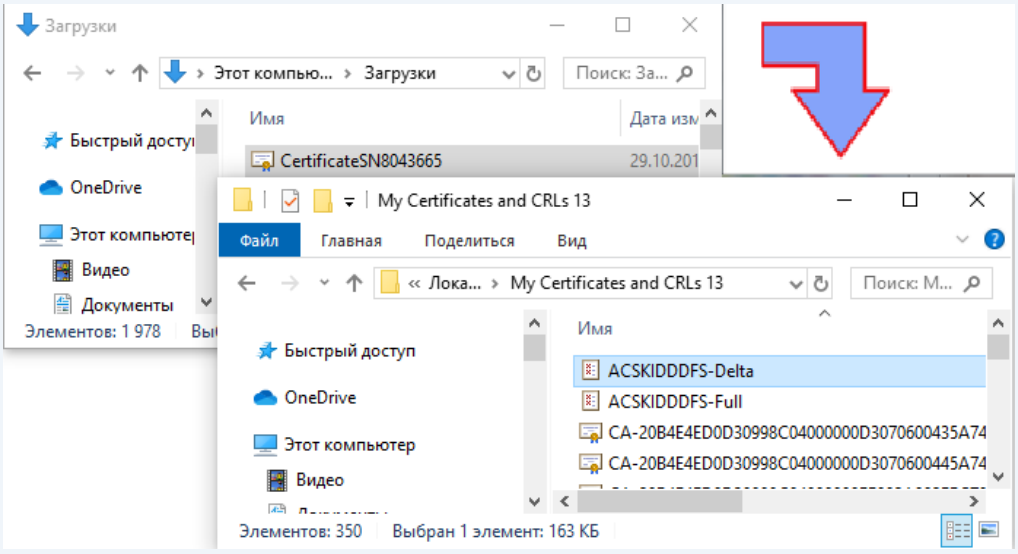


Рисунок 2.9

Окрім кваліфікованих сертифікатів підписувачів у файловому сховищі знаходяться **технологічні сертифікати**, які використовуються при шифруванні/розшифруванні файлів, накладанні/перевірці підпису тощо.

Технологічні сертифікати копіюються до файлового сховища автоматично під час інсталяції ПЗ.

Якщо технологічні сертифікати відсутні у файловому сховищі їх необхідно завантажити з вебсайту (розділ «Пошук сертифікатів та СВС», вкладка Сертифікати Надавача) (рис. 2.10).

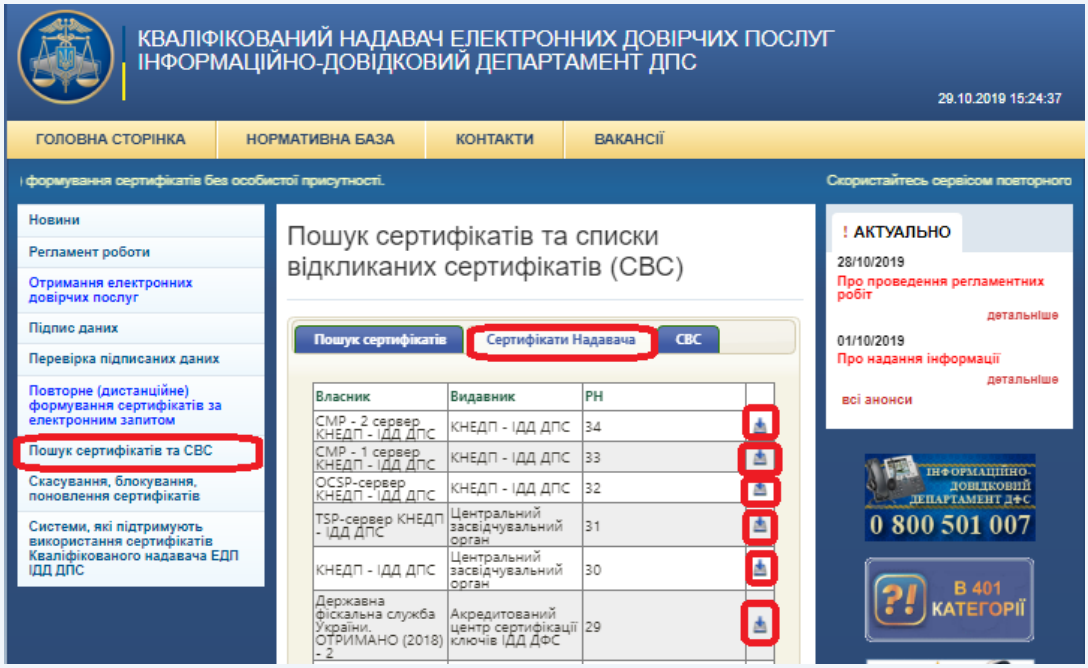


Рисунок 2.10

Також можна виконати автоматичне завантаження усіх кваліфікованих сертифікатів за допомогою запиту до серверу обробки запитів. Запит формується за допомогою особистого ключа підписувача. Для отримання пакету кваліфікованих сертифікатів необхідно обрати підпункт «Отримати з ЦСК…» в пункті меню «Сертифікати та СВС» (рис. 2.11).

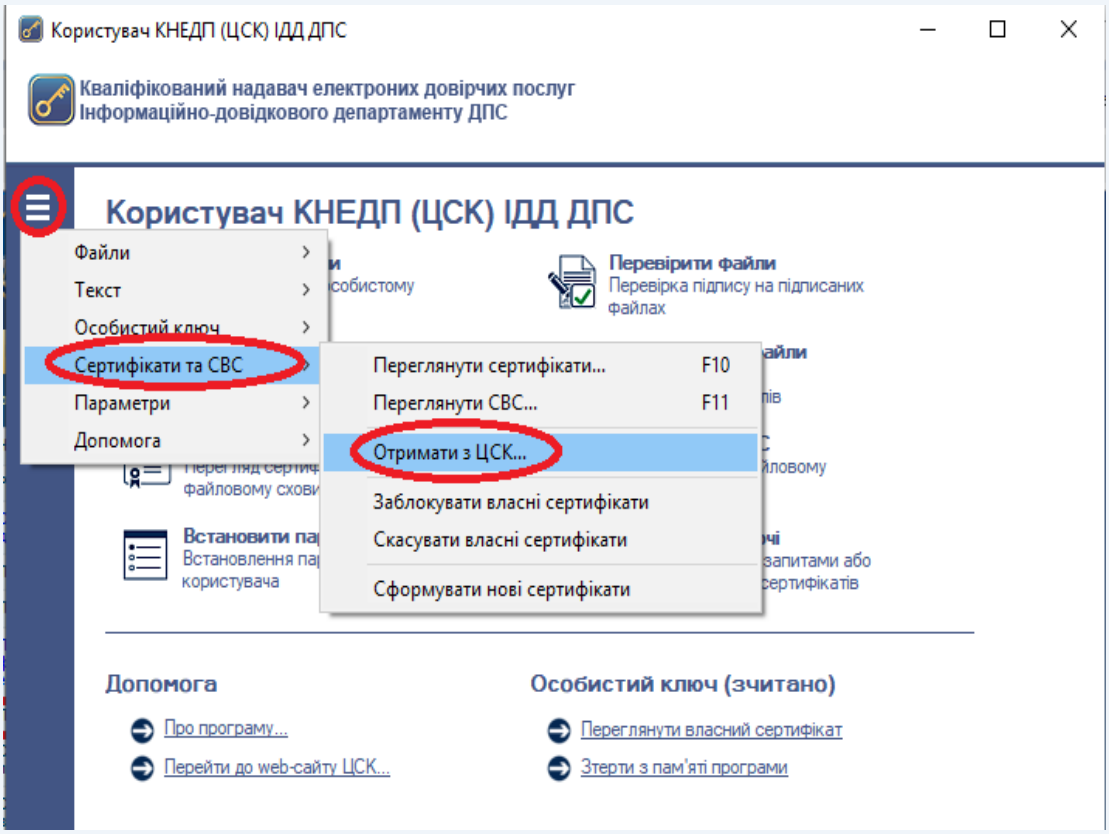


Рисунок 2.11

Після чого буде виведене діалогове вікно (рис. 2.12). Для продовження формування запиту на автоматичне завантаження кваліфікованих сертифікатів натиснути «Да».

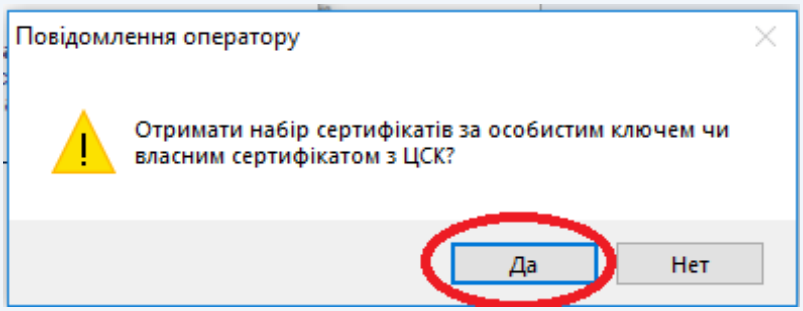


Рисунок 2.12

Після чого з’являється захищений робочий стіл, в якому необхідно обрати НКІ та ввести пароль захисту особистого ключа (рис. 2.13).

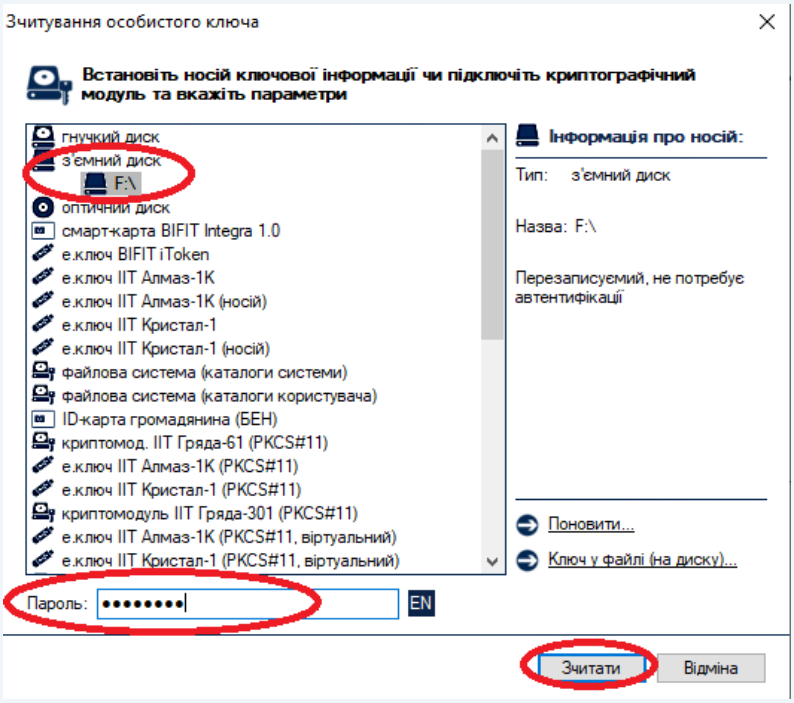


Рисунок 2.13

При відкритті вікна «Завантажені сертифікати» (рис. 2.14), необхідно зберегти їх до файлового сховища натиснувши кнопку «Да».

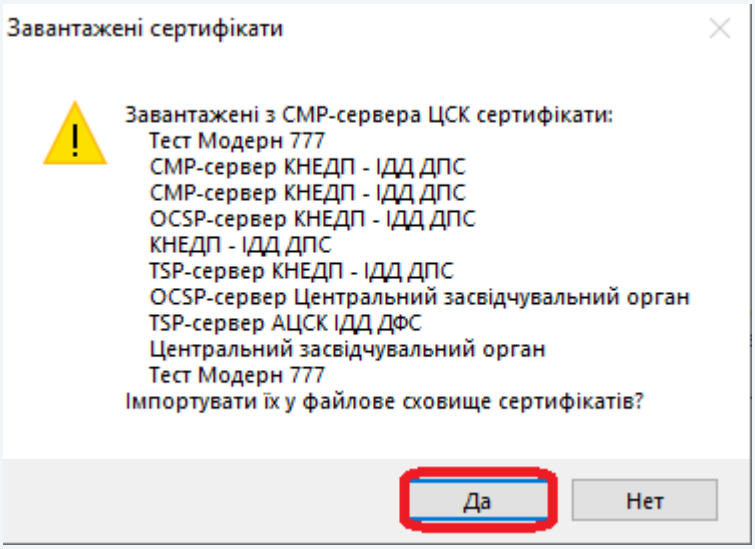


Рисунок 2.14

3. Налаштування програмного забезпечення «ІІТ Користувач ЦСК-1»

Для налаштування ПЗ «ІІТ Користувач ЦСК-1» необхідно встановити відповідні параметри (рис. 3.1 – 3.6).

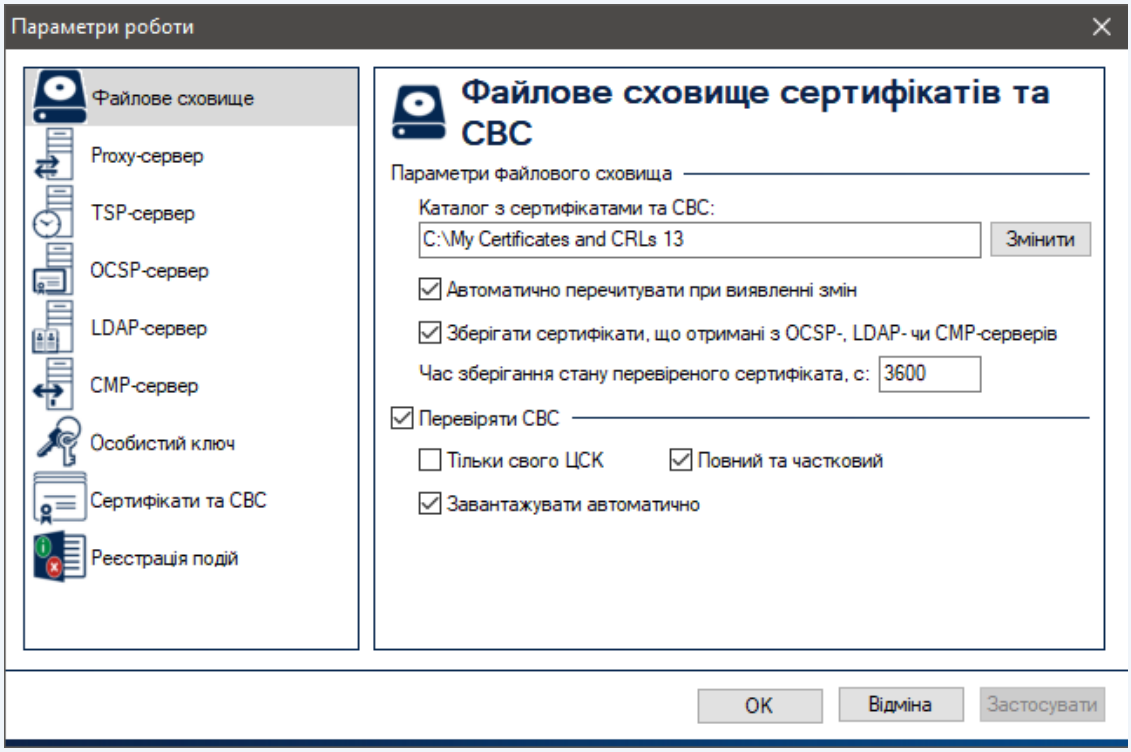


Рисунок 3.1

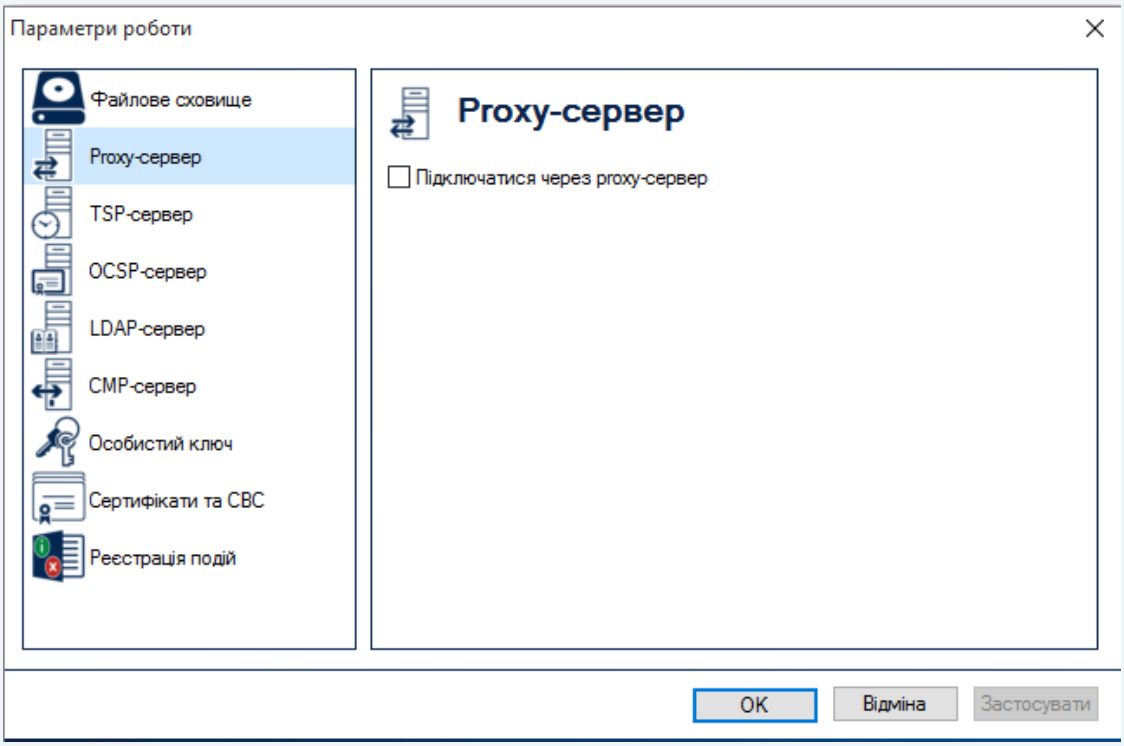


Рисунок 3.2

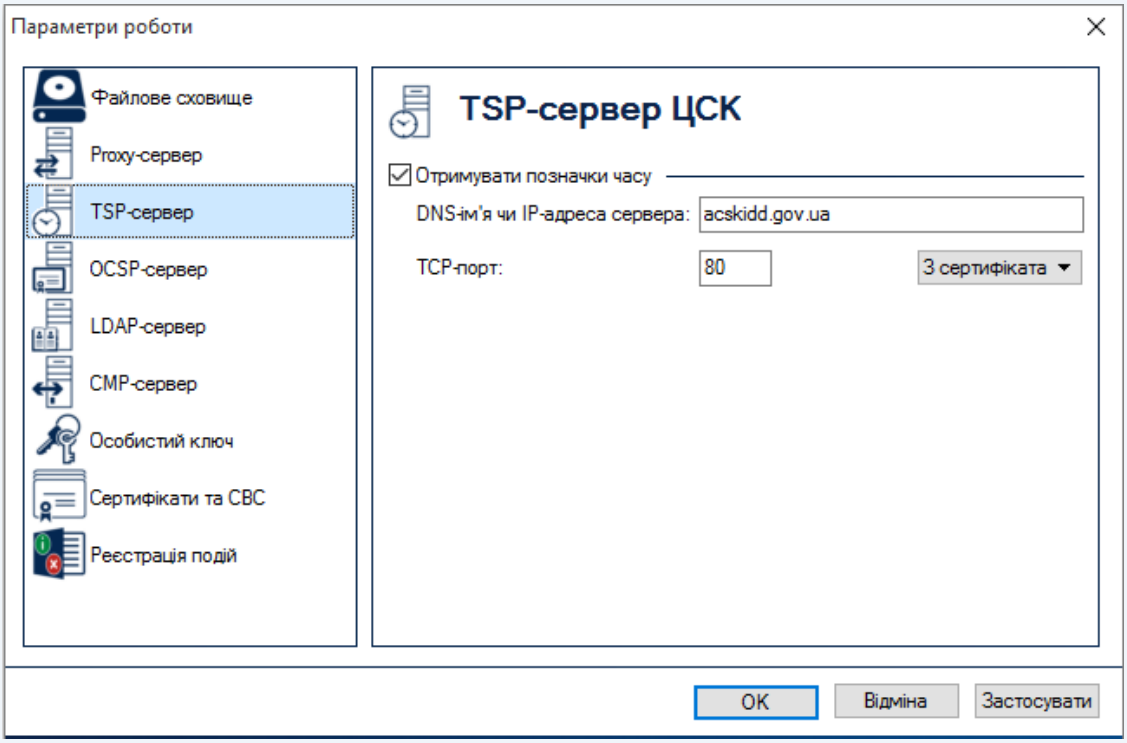


Рисунок 3.3

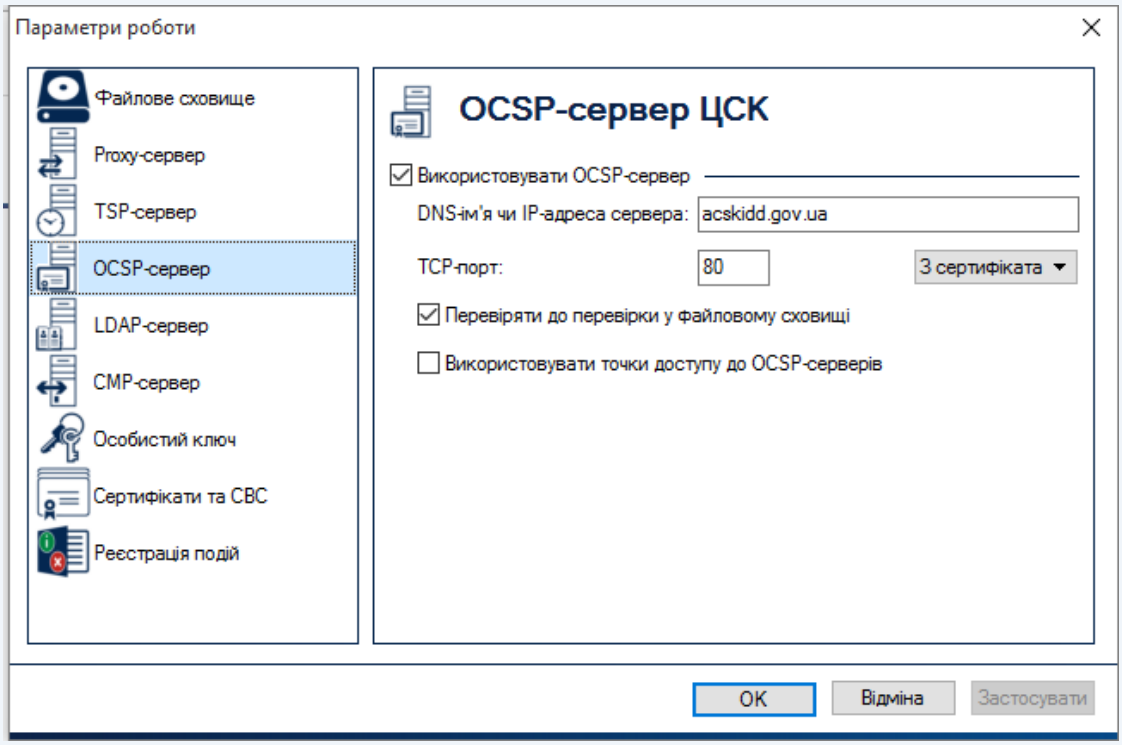


Рисунок 3.4

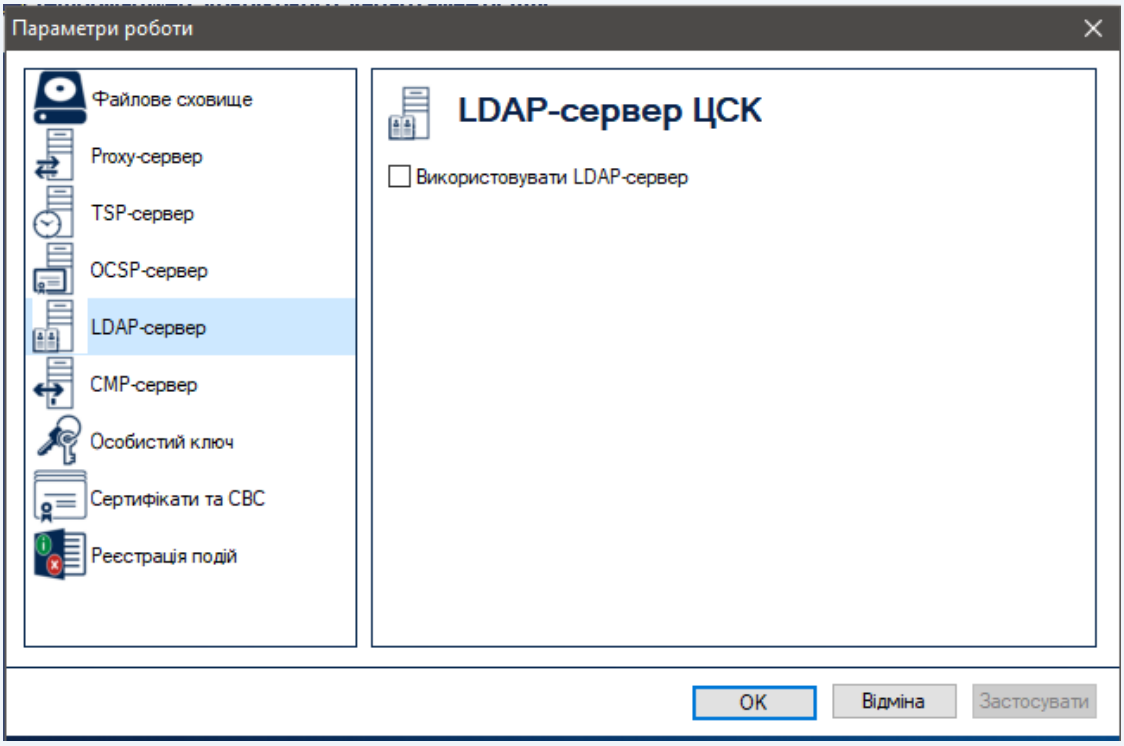


Рисунок 3.5

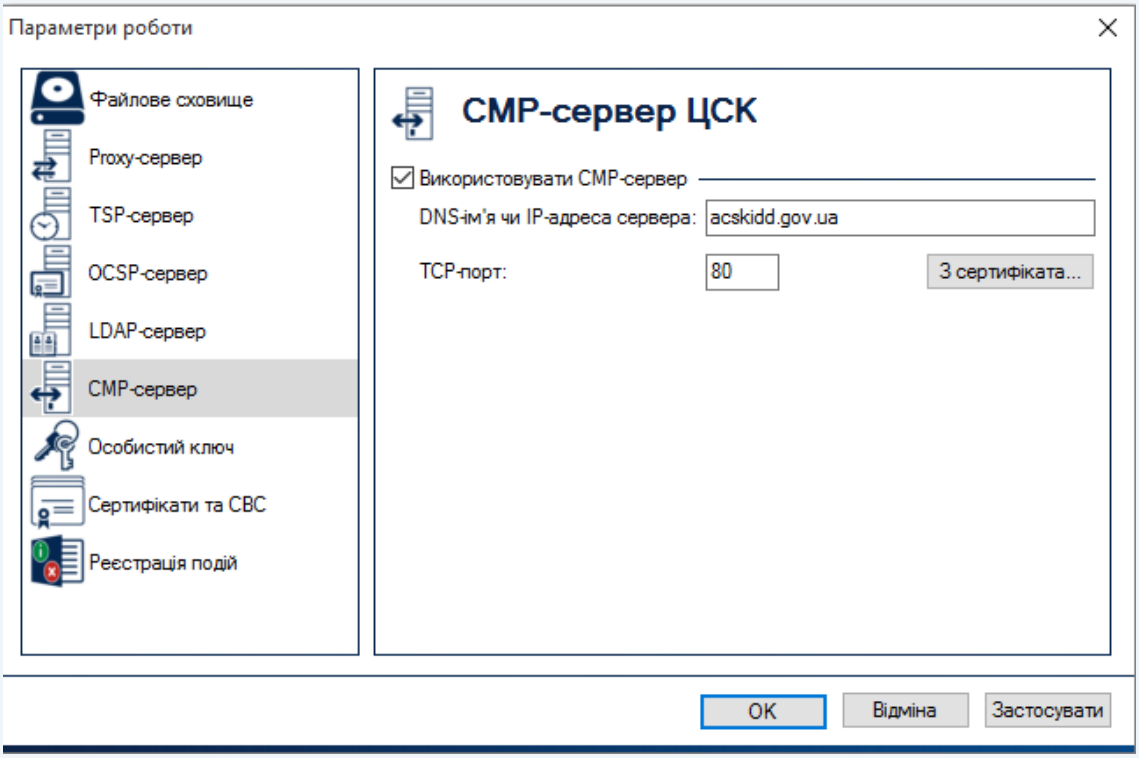


Рисунок 3.6

4. Основні функції програмного забезпечення «ІІТ Користувач ЦСК-1»

4.1 Підписання файлів

Для накладання КЕП на електронний документ необхідно у головному вікні ПЗ натиснути кнопку «Підписати файли» (рис. 4.1).

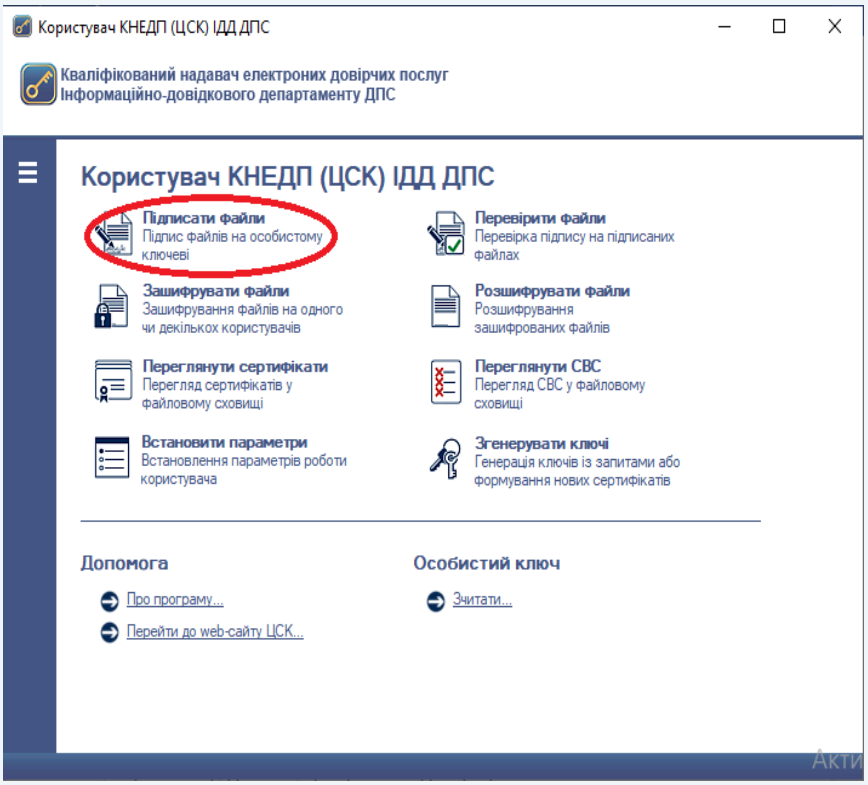


Рисунок 4.1

Після чого з’являється захищений робочий стіл, в якому необхідно обрати НКІ та ввести пароль захисту особистого ключа (рис. 4.2).

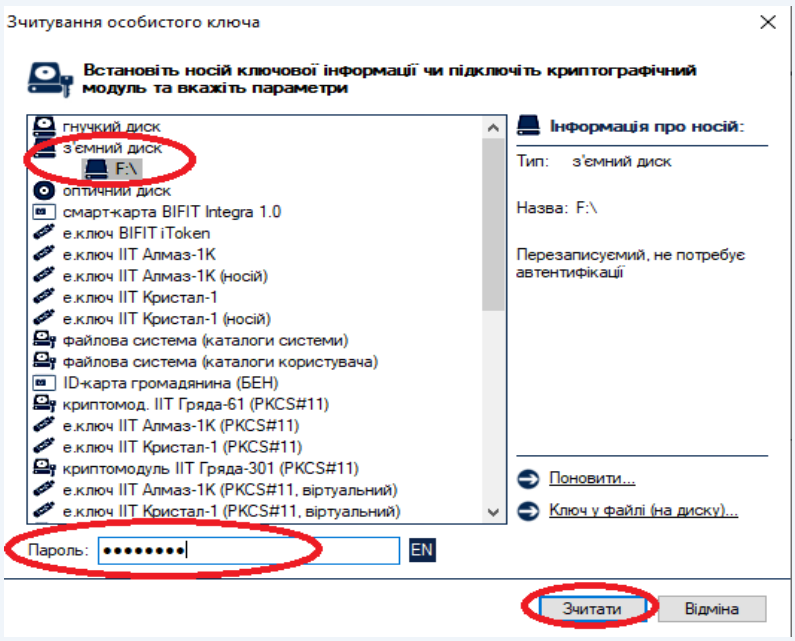


Рисунок 4.2

У випадку відсутності у файловому сховищі власних кваліфікованих сертифікатів підписувача, з’явиться вікно «Повідомлення оператору» (рис. 4.3). Необхідно натиснути кнопку «ОК».

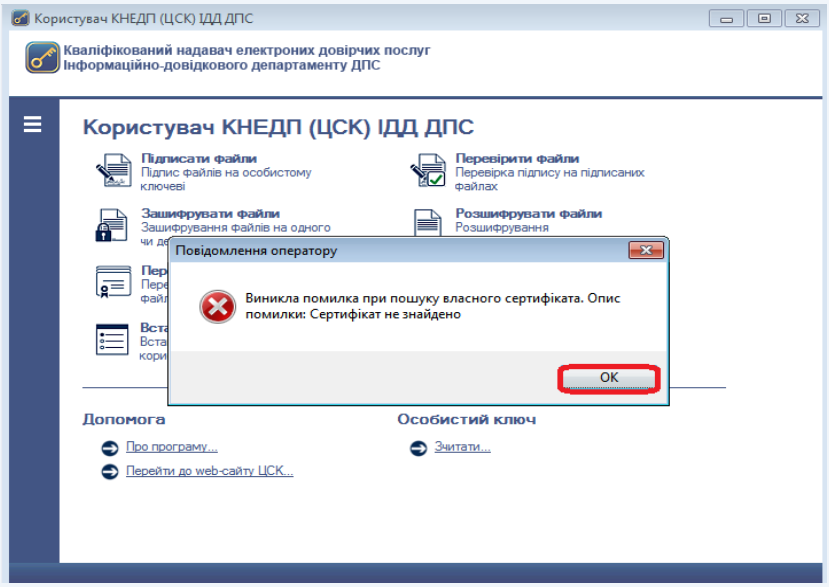


Рисунок 4.3

Після чого буде виведене діалогове вікно (рис. 4.4). Для продовження формування запиту на автоматичне завантаження кваліфікованих сертифікатів відкритого ключа підписувача натиснути «Да».

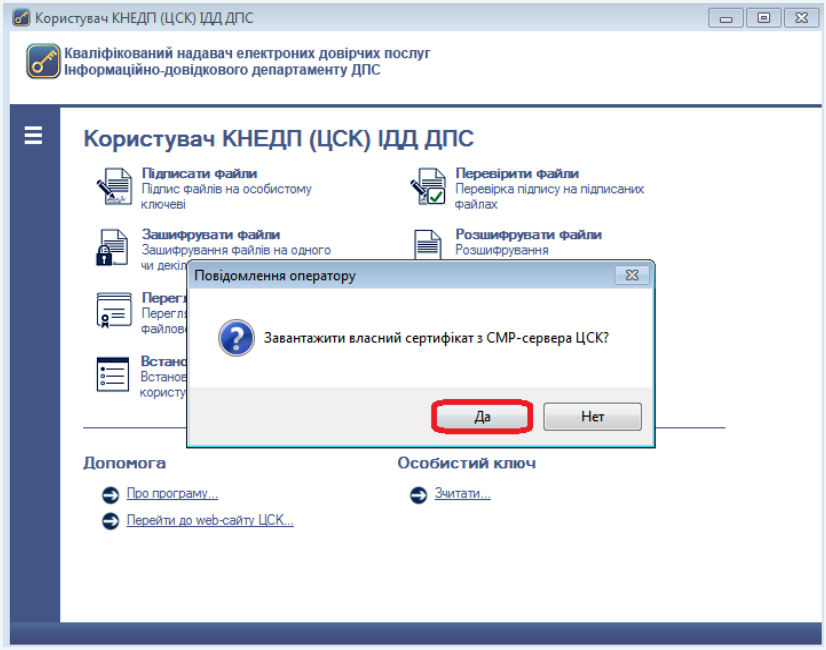


Рисунок 4.4

При відкритті вікна «Завантажені сертифікати» (рис. 4.5), необхідно зберегти їх у файлове сховище натиснувши кнопку «Да».

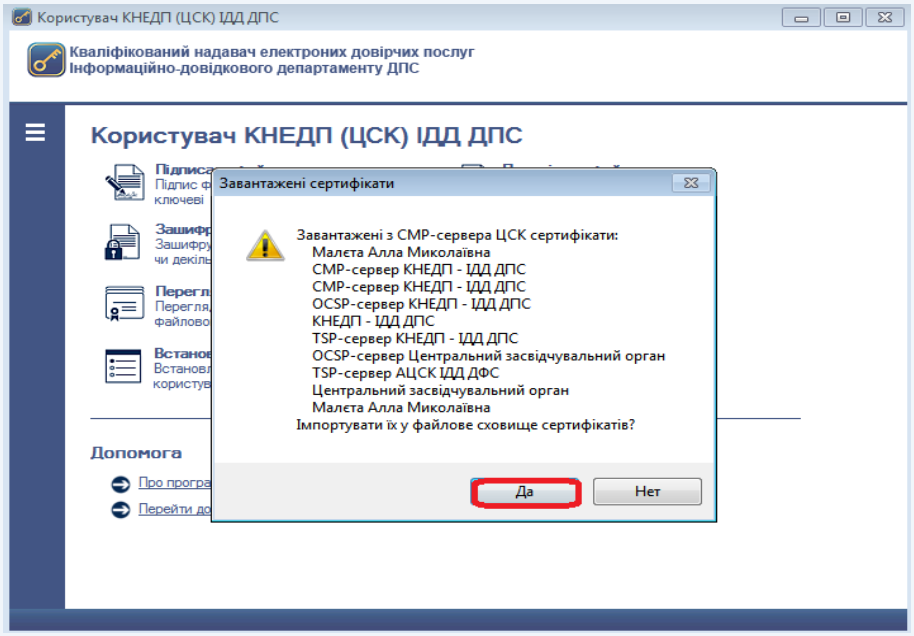


Рисунок 4.5

Після успішного зчитування паролю захисту особистого ключа (успішного завантаження власних кваліфікованих сертифікатів користувача) з'являється вікно «Підпис файлів». Для додавання файлів, які потребують підписання, натискаємо кнопку «Додати» та обираємо розташування файлу (рис. 4.6).

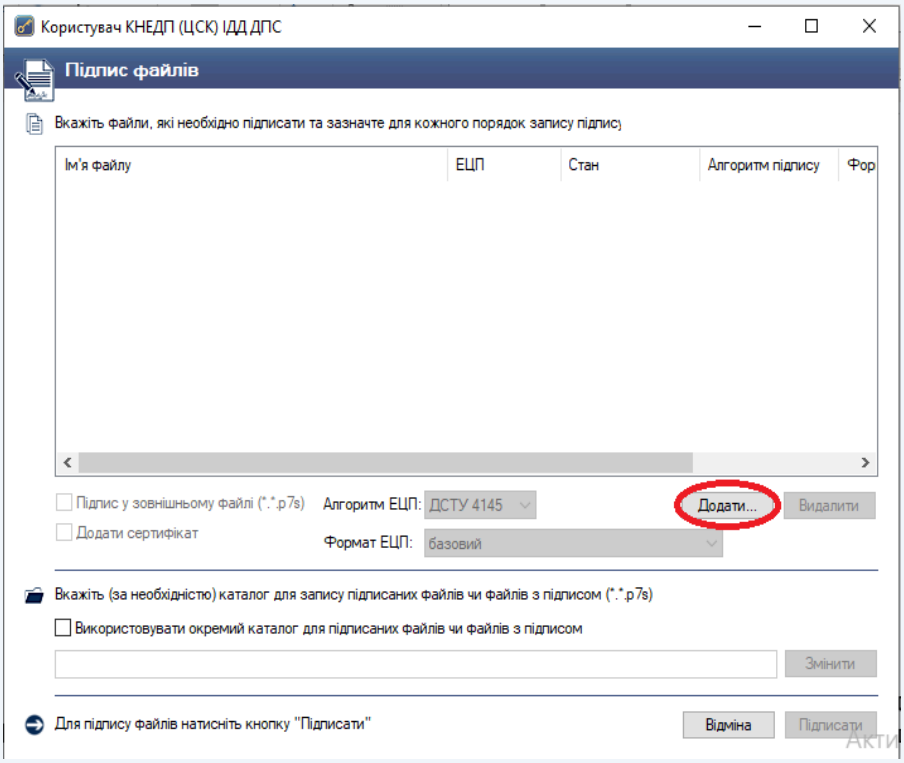


Рисунок 4.6

Додавши необхідний файл, варто звернути увагу на параметри накладання КЕП, оскільки за замовчуванням ПЗ підписує файли внутрішнім КЕП та розміщує підписані файли у тому ж каталозі, в якому розміщується вихідний файл (рис. 4.7).

Також, передбачена можливість додати кваліфікований сертифікат підписувача до файлу, який підписується, що забезпечить ідентифікацію автора за відсутності підключення до мережі Internet та взаємодії з серверами Надавача. Наприклад, якщо файл розташований на робочому столі, підписаний файл буде збережений також на робочому столі. Всі підписані файли мають розширення «.p7s».

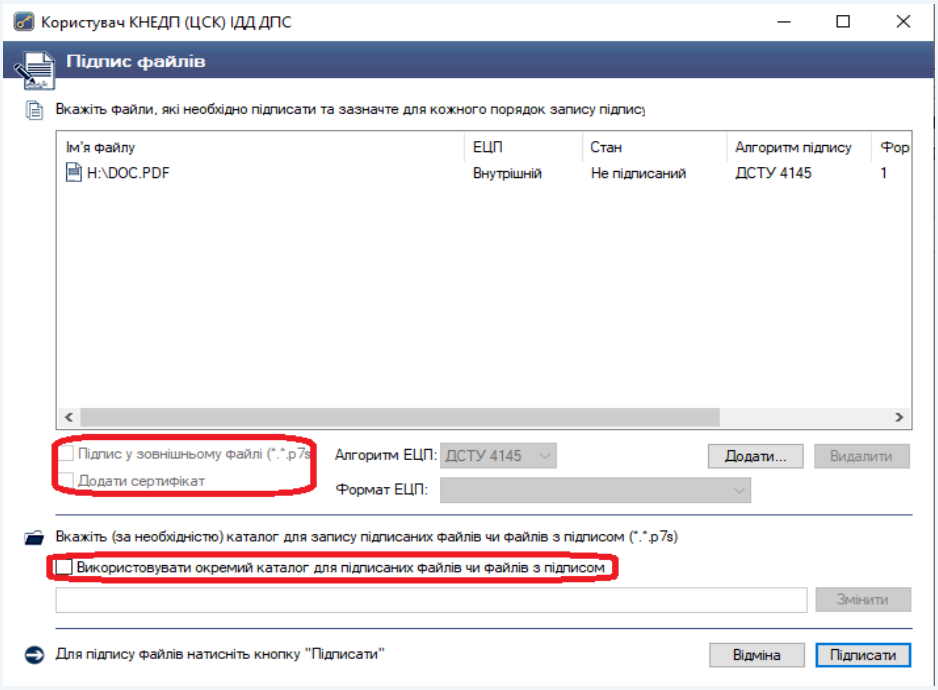


Рисунок 4.7

ПЗ дає можливість одночасно підписати декілька файлів та обрати спосіб накладання КЕП для кожного файлу окремо.

Наприклад, додано три файли, два з яких необхідно підписати зовнішнім КЕП. Для цього у вікні «Підпис файлів» виділяємо необхідні файли та обираємо «ЕЦП у зовнішньому файлі».

4.2 Перевірка КЕП

Для перевірки КЕП у головному вікні ПЗ натискаємо кнопку «Перевірити файли» (рис. 4.5).

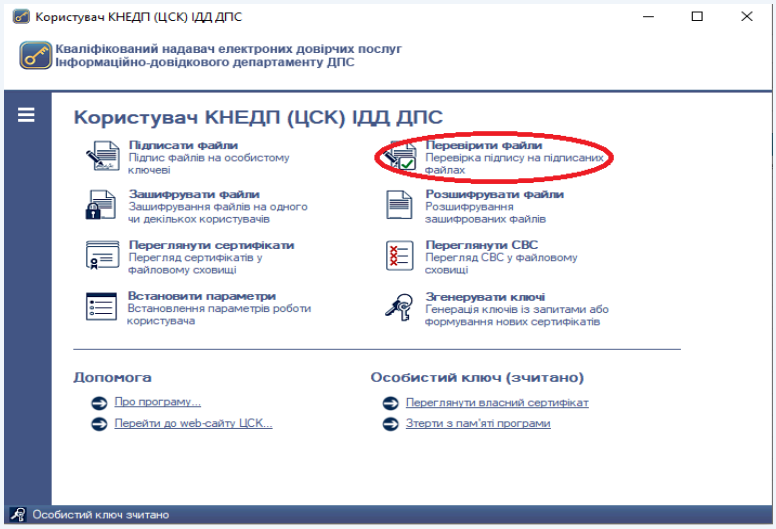


Рисунок 4.5

У вікні «Перевірка підписаних файлів» додати підписані файли (файли з розширенням «.p7s») та натиснути кнопку «Перевірити» (рис. 4.6).

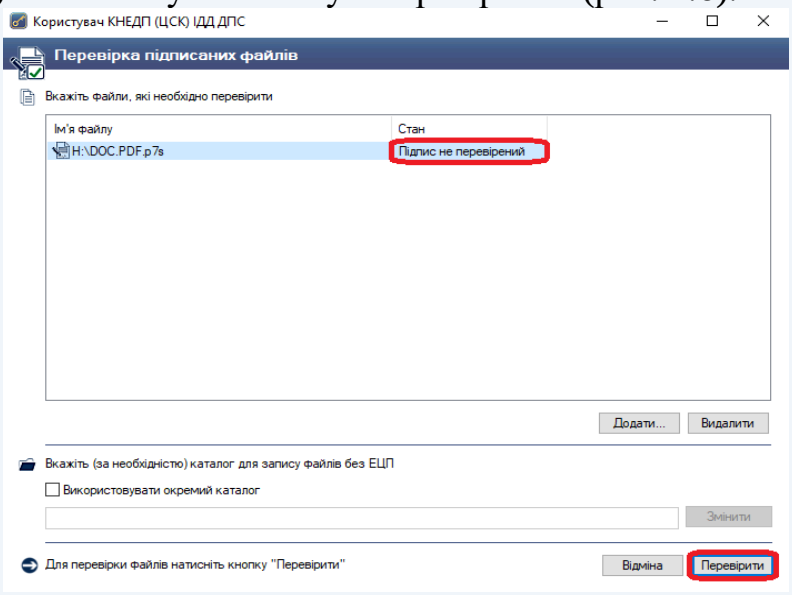


Рисунок 4.6

Результат перевірки КЕП буде відображено у цьому ж вікні (рис. 4.7).

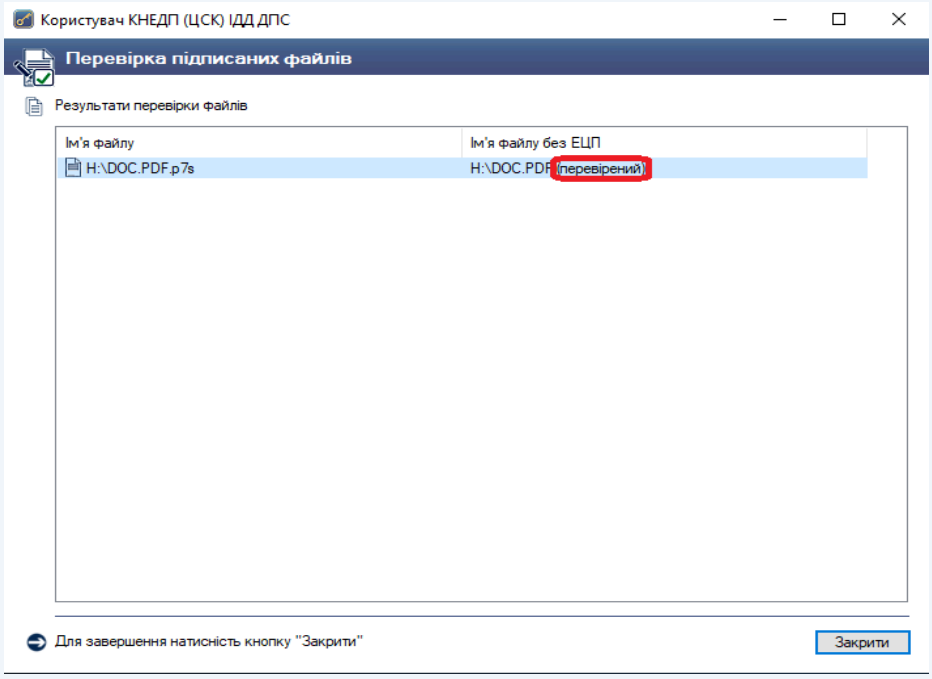


Рисунок 4.7

Для ідентифікації автора, необхідно подвійним кліком миші відкрити посилання на підписаний файл (рис. 4.8).

У вікні «Підписані дані» можна переглянути детальну інформацію про автора документа.

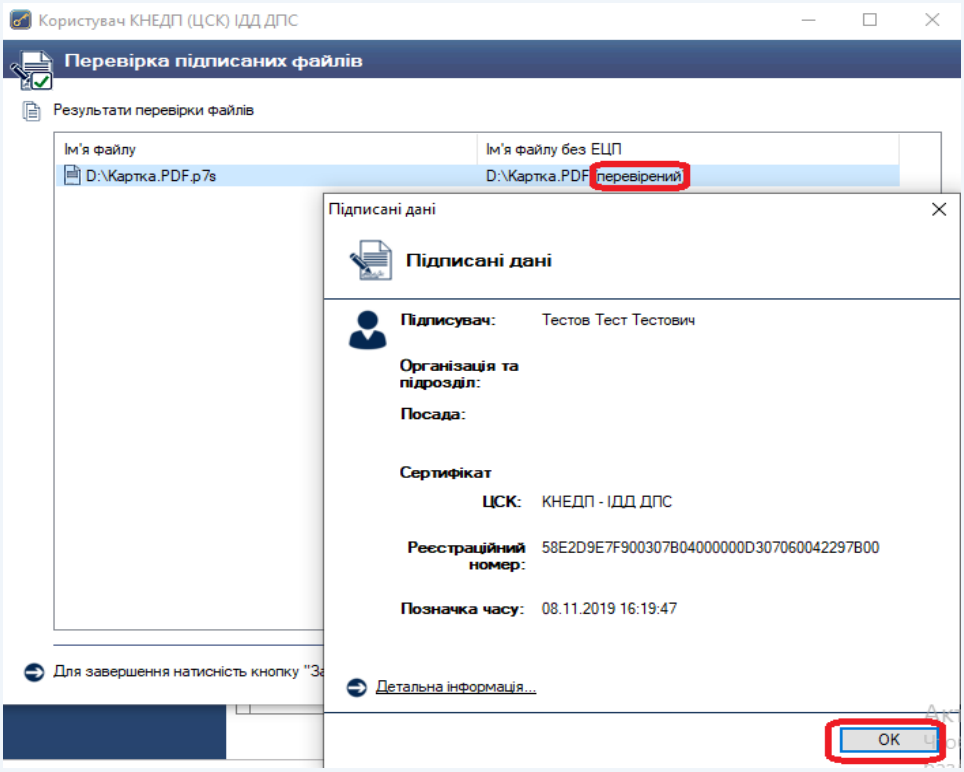


Рисунок 4.8

4.3 Шифрування файлів

У ПЗ реалізовано функцію криптографічного захисту інформації шляхом її направленого шифрування, що дає змогу підписувачу зашифровувати необхідні файли на кваліфікованих сертифікатів конкретного адресата.

Для шифрування файлів необхідно у головному вікні ПЗ натиснути кнопку «Зашифрувати файли» (рис. 4.9).

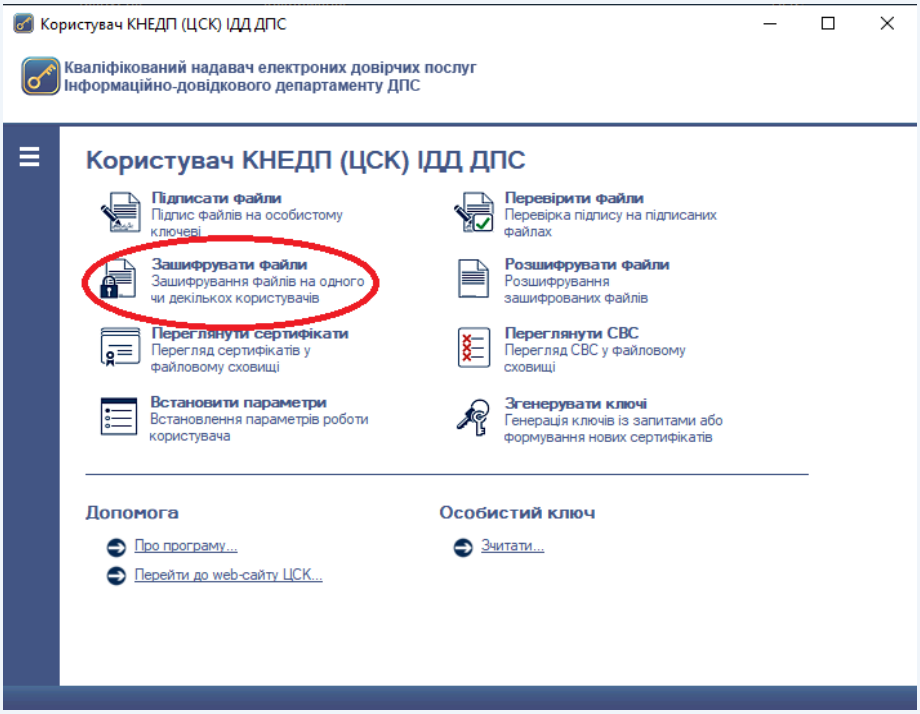


Рисунок 4.9

Наступним кроком є поява захищеного робочого столу, в якому необхідно обрати з’ємний НКІ та ввести пароль захисту особистого ключа (рис. 4.10).

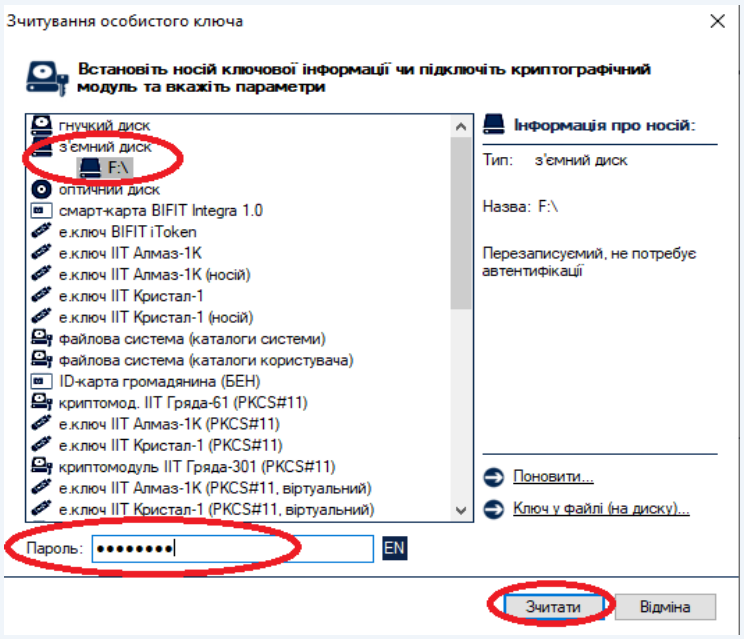


Рисунок 4.10

У новому вікні «Зашифрування файлів» підписувачу надається можливість одночасно з шифруванням файлів додатково їх підписати та додати власний кваліфікований сертифікат, що забезпечить ідентифікацію автора за відсутності підключення до мережі Internet та взаємодії з серверами Надавача (рис. 4.11).

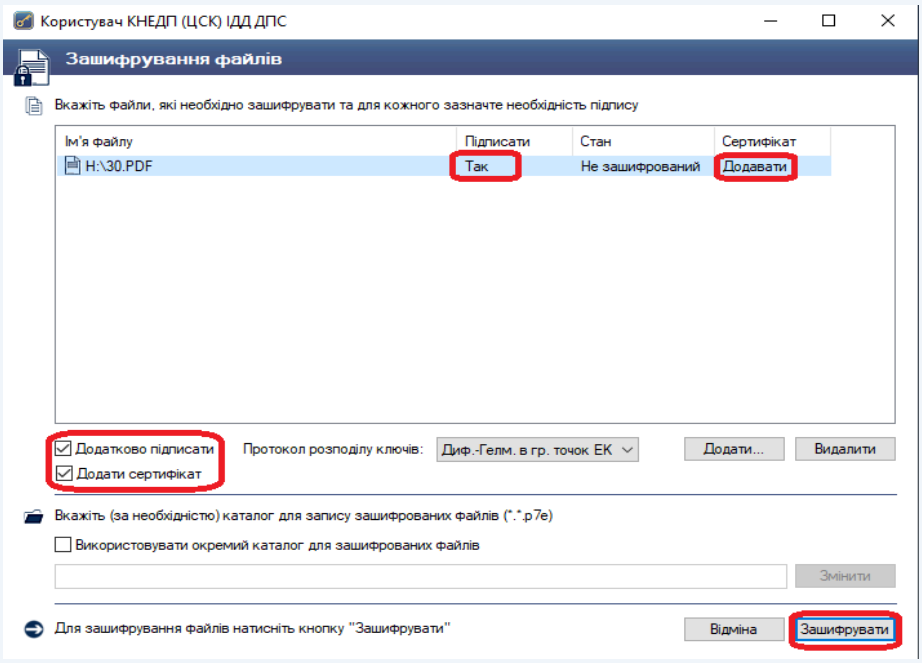


Рисунок 4.11

Після налаштування способу шифрування натискаємо кнопку «Зашифрувати» та у вікні «Сертифікати користувачів-отримувачів» обираємо кваліфікований сертифікат отримувача або кваліфіковані сертифікати декількох отримувачів. Розшифрувати файл зможуть лише власники кваліфікованих сертифікатів обрані у цьому вікні (рис. 4.12).

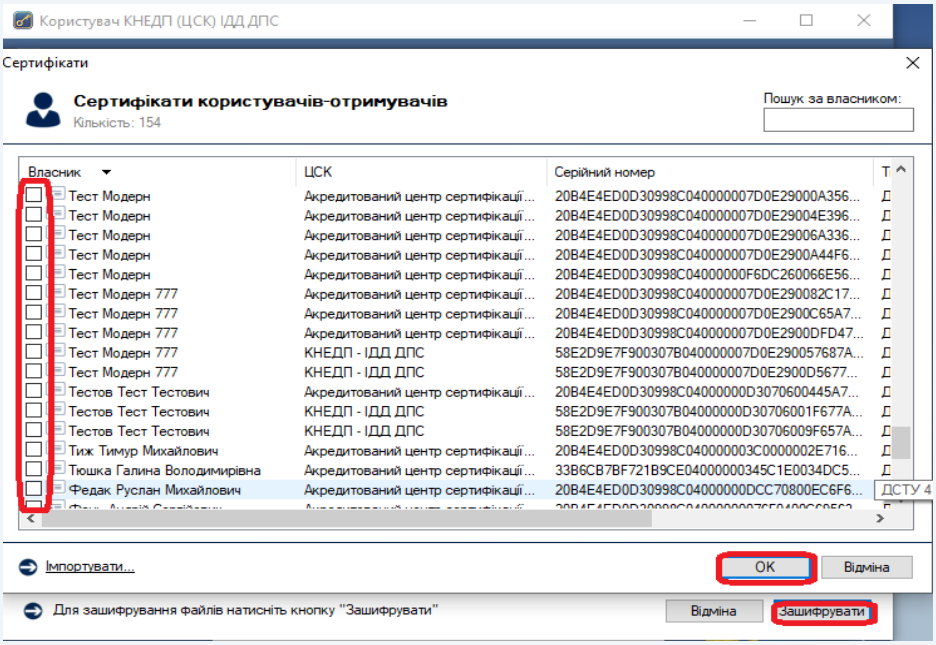


Рисунок 4.12

Шифрування файлів завершується появою вікна (рис. 4.13) із зазначенням ім’я зашифрованого файлу. Всі зашифровані файли мають розширення «.p7e».

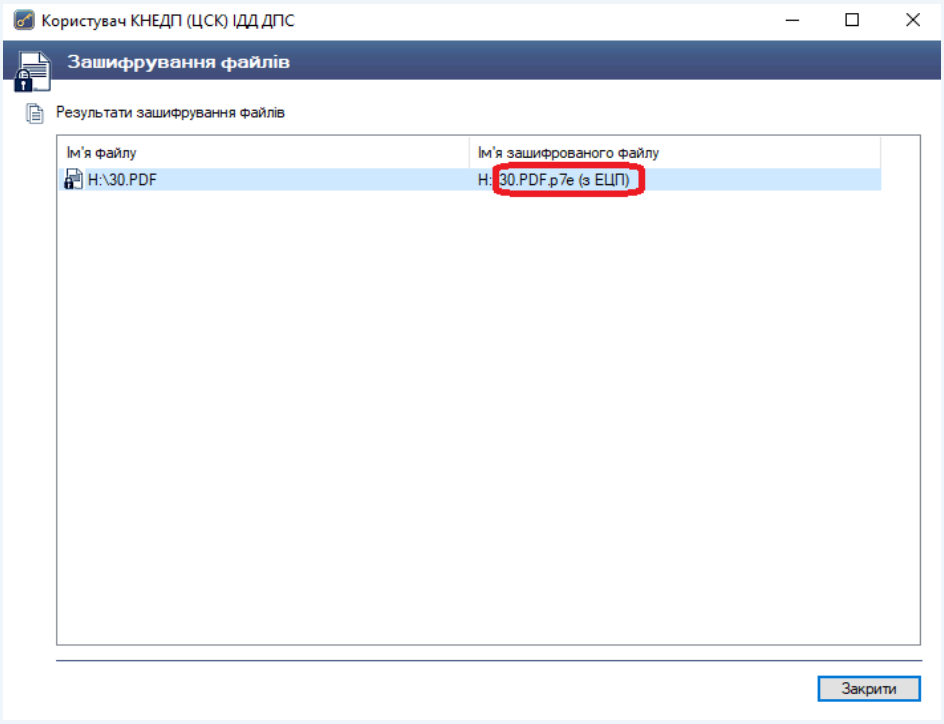


Рисунок 4.13

4.4 Розшифрування файлів

Для розшифрування файлів необхідно обрати у головному вікні ПЗ кнопку «Розшифрувати файли» (рис. 4.14).

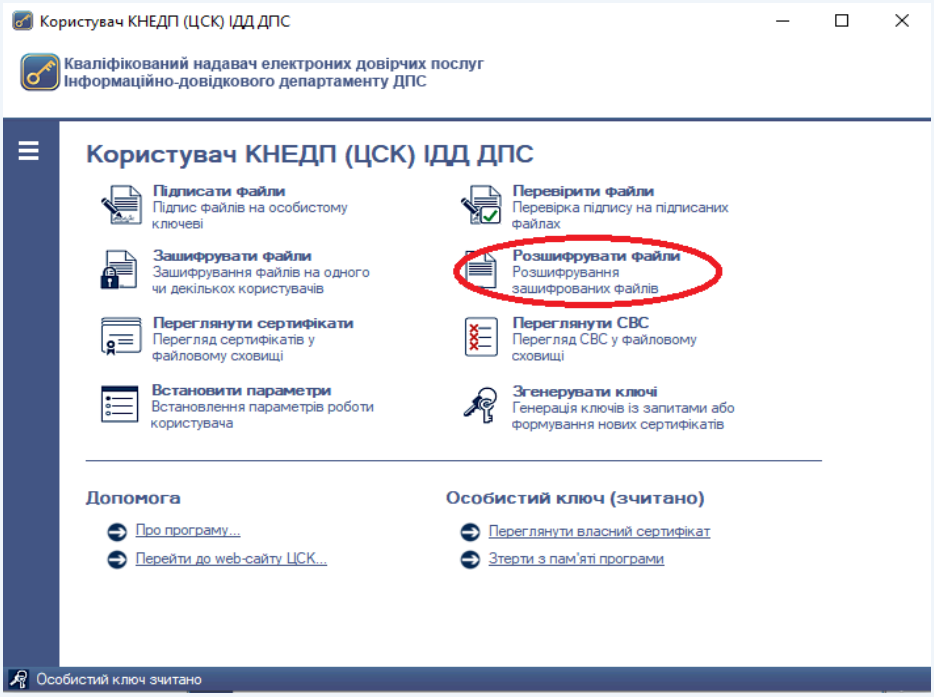


Рисунок 4.14

Після появи захищеного робочого столу, необхідно обрати з’ємний НКІ та ввести пароль захисту особистого ключа (рис. 4.15).

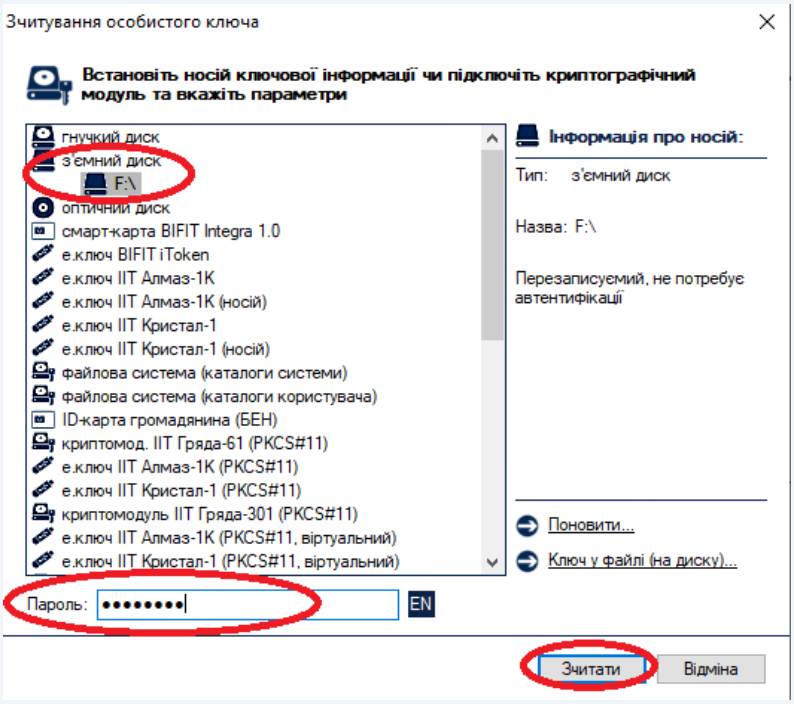


Рисунок 4.15

У вікні «Розшифрування зашифрованих файлів» необхідно додати необхідні документи та натиснути кнопку «Розшифрувати» (рис. 4.16).

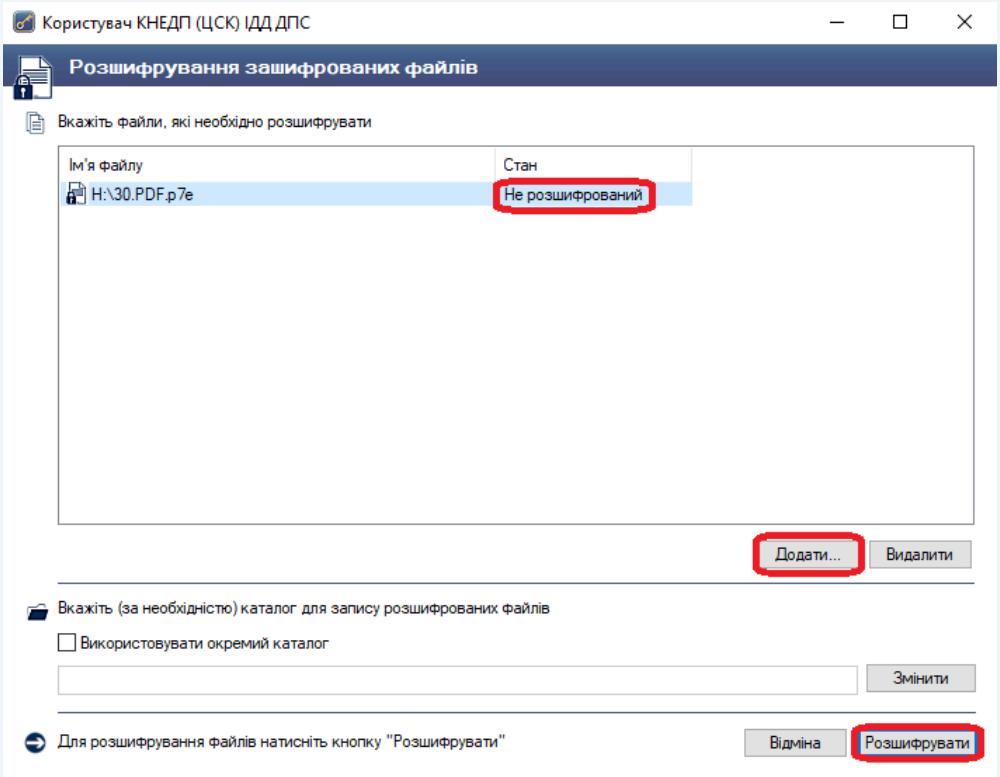


Рисунок 4.16

Файл можна переглянути одразу після його розшифрування.

У випадку відсутності у підписувача прав доступу до зашифрованого файлу з’явиться вікно «Повідомлення оператору» (рис. 4.17).

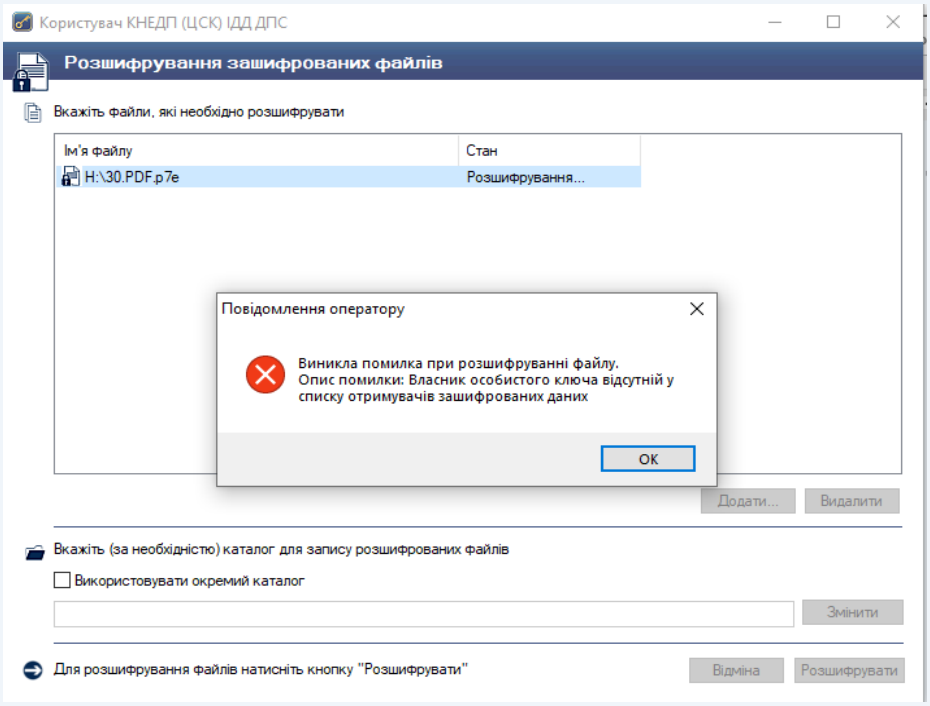


Рисунок 4.17

4.5 Шифрування тексту

Для шифрування тексту необхідно в пункті меню «Текст» обрати підпункт «Зашифрувати» (рис. 4.18).

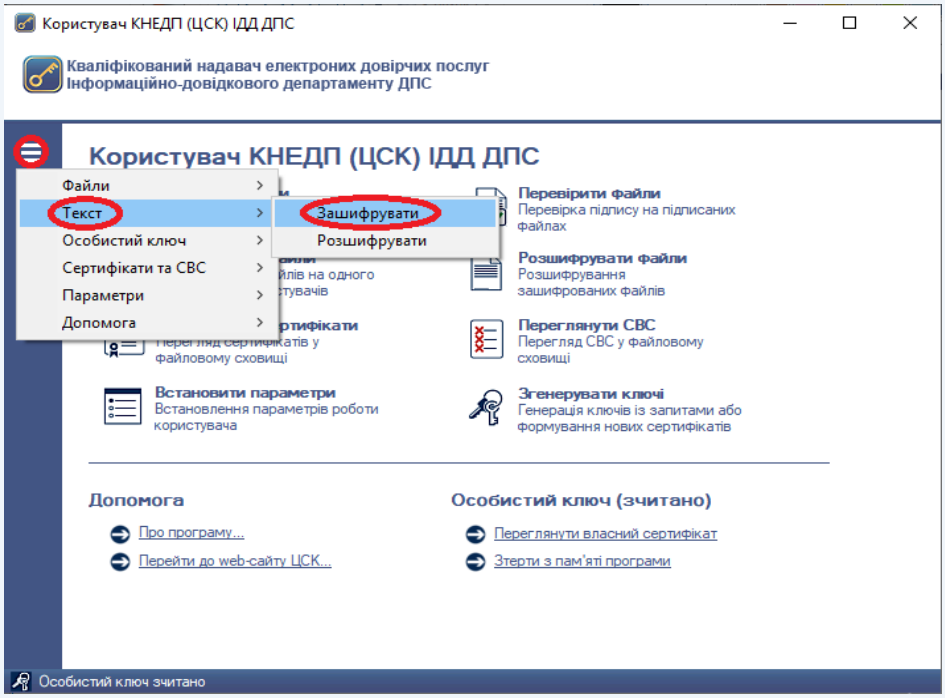


Рисунок 4.18

Після появи захищеного робочого столу, необхідно обрати з'ємний НКІ, ввести пароль захисту особистого ключа та натиснути кнопку «Зчитати» (рис. 4.19).

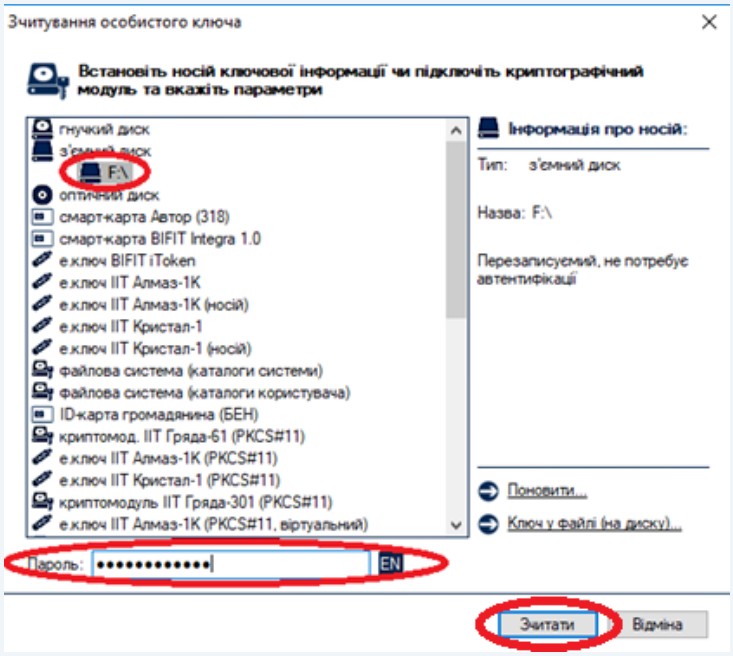


Рисунок 4.19

У новому вікні «Зашифрування тексту» підписувачу надається можливість ввести текст, який необхідно зашифрувати. Текст можна ввести в два способи:

1. методом прямого введення тексту в спеціальне вікно ПЗ (рис. 4.20).

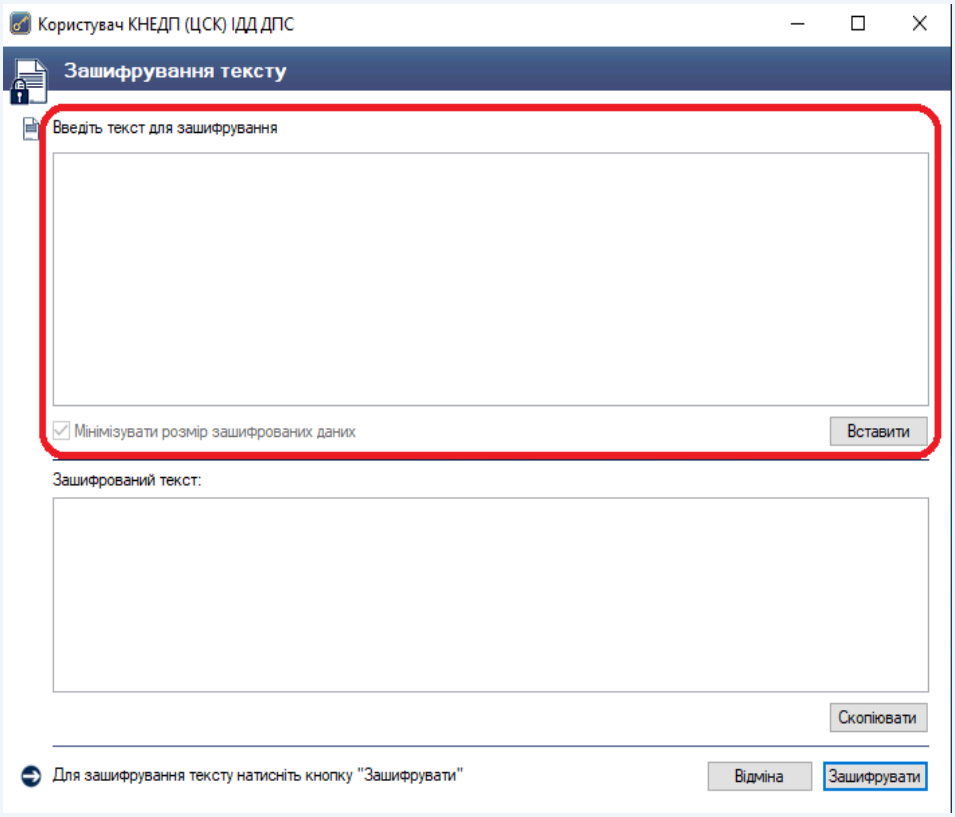


Рисунок 4.20

2. скопіювати необхідний текс та додати його за допомогою кнопки «Вставити» (рис. 4.21).

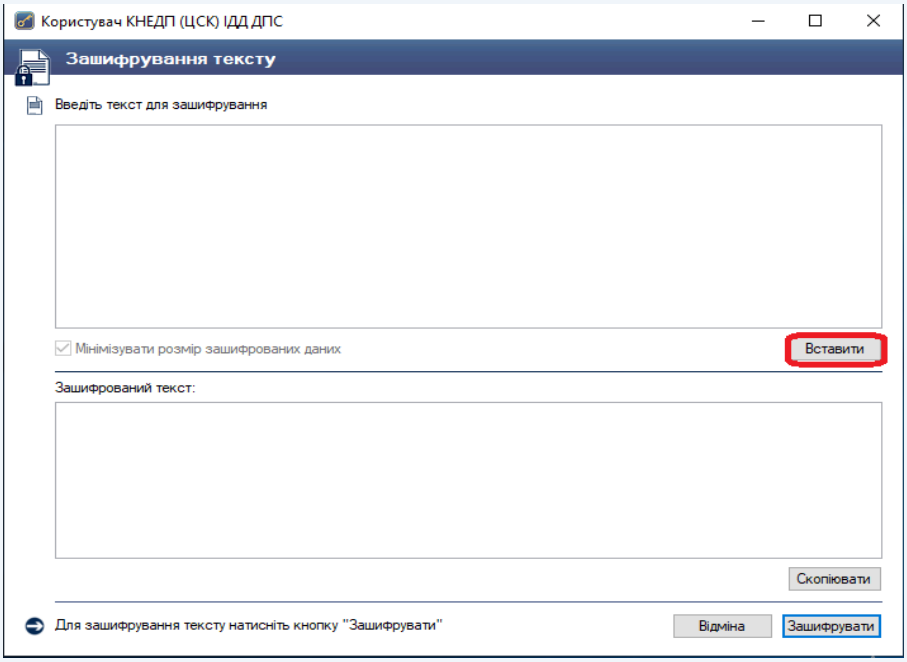


Рисунок 4.21

Після введення тексту необхідно натиснути кнопку «Зашифрувати» (рис. 4.22)

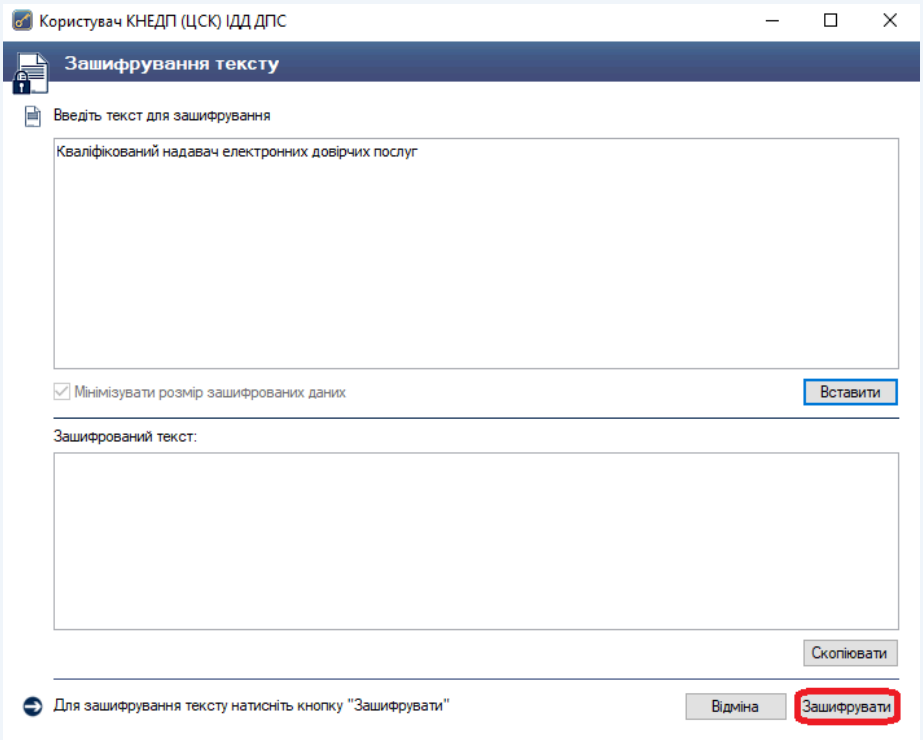


Рисунок 4.22

Після налаштування способу шифрування натискаємо кнопку «Зашифрувати» та у вікні «Сертифікати користувачів-отримувачів» обираємо кваліфікований сертифікат отримувача або кваліфіковані сертифікати декількох отримувачів. Розшифрувати файл зможуть лише власники кваліфікованих сертифікатів обрані у цьому вікні (рис. 4.23).

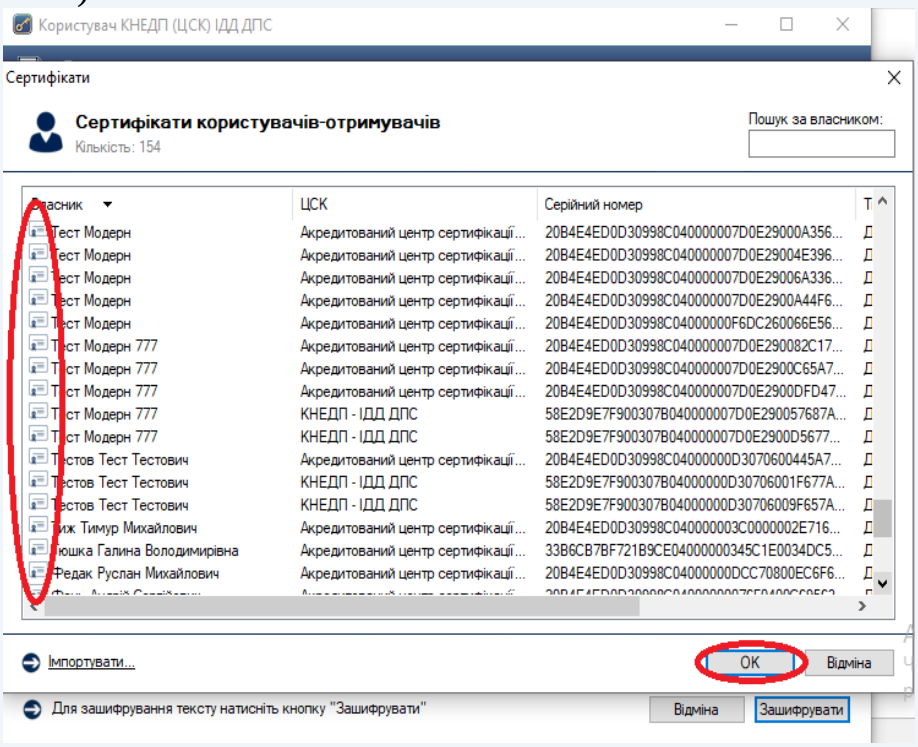


Рисунок 4.23

Шифрування тексту завершується появою зашифрованого тексту у вікні «Зашифрований текст», який можна скопіювати за допомогою кнопки «Скопіювати» (рис. 4.24).

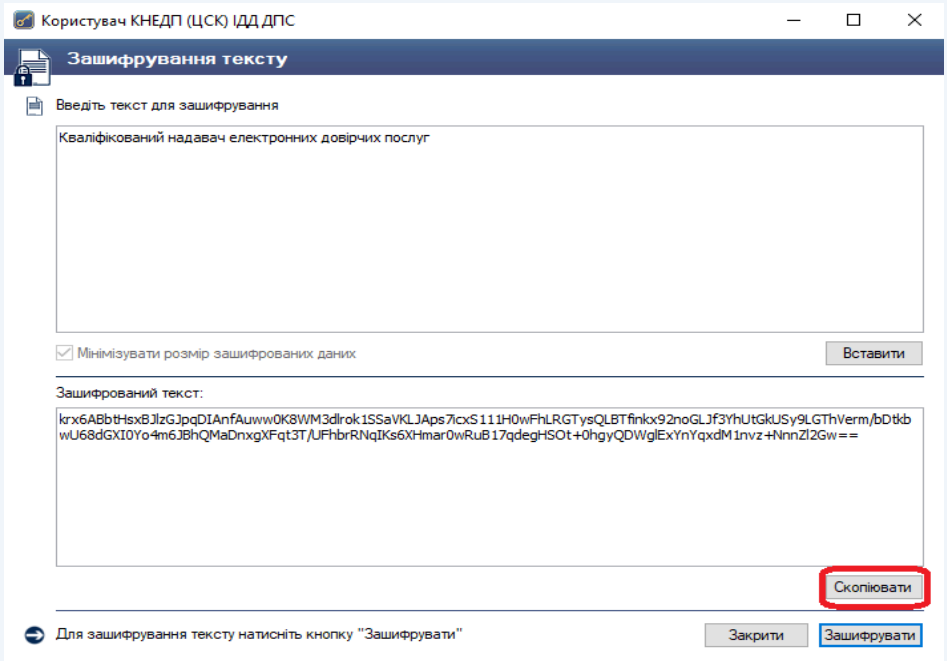


Рисунок 4.24

4.6 Розшифрування тексту

Для розшифрування тексту необхідно в пункті меню «Текст» обрати підпункт «Розшифрувати» (рис. 4.25).

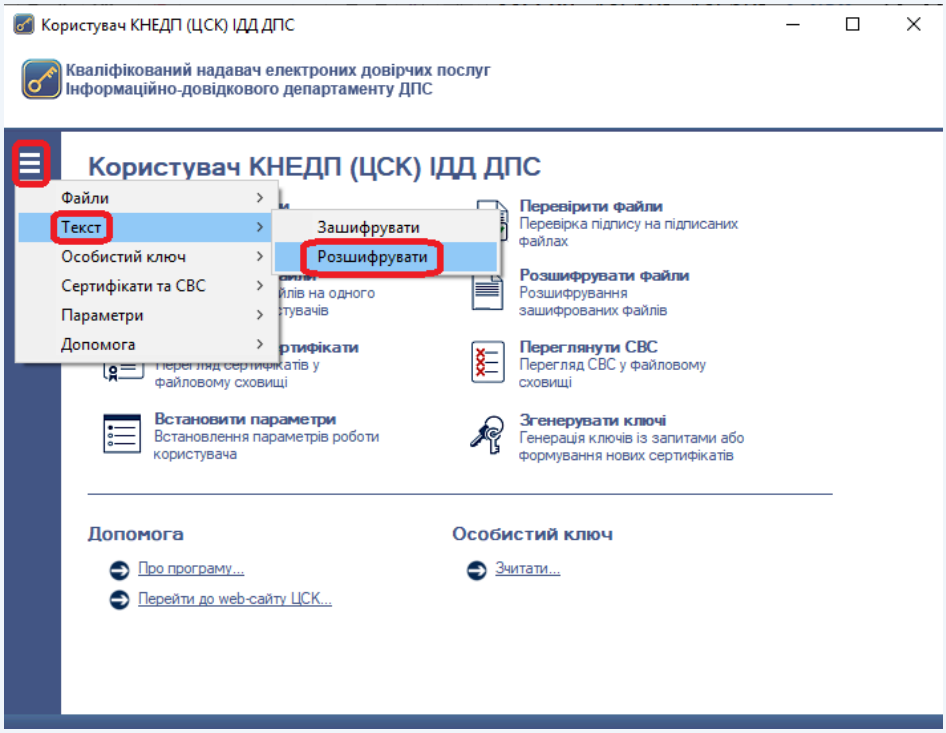


Рисунок 4.25

Після появи захищеного робочого столу, необхідно обрати з'ємний НКІ, ввести пароль захисту особистого ключа та натиснути кнопку «Зчитати» (рис. 4.26).

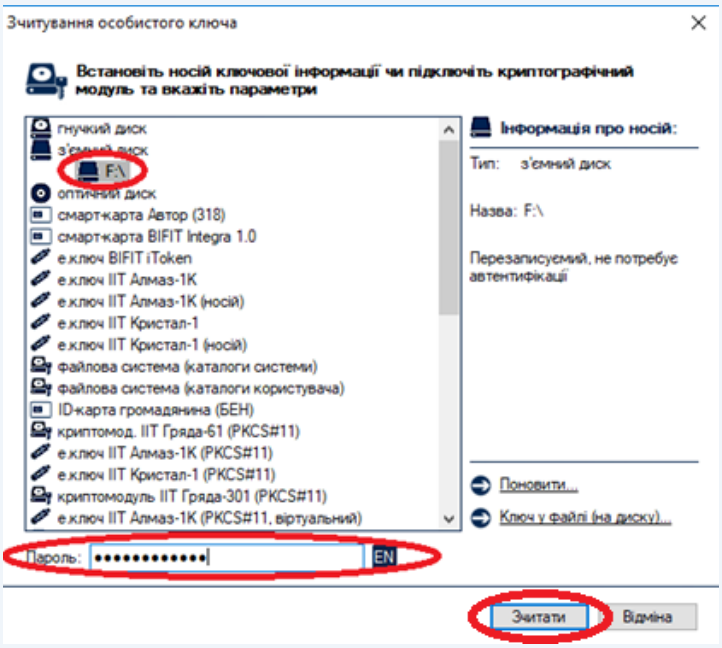


Рисунок 4.26

У вікні «Розшифрування тексту» необхідно додати скопійований зашифрований текст за допомогою кнопки «Вставити» та натиснути кнопку «Розшифрувати» (рис. 4.27).

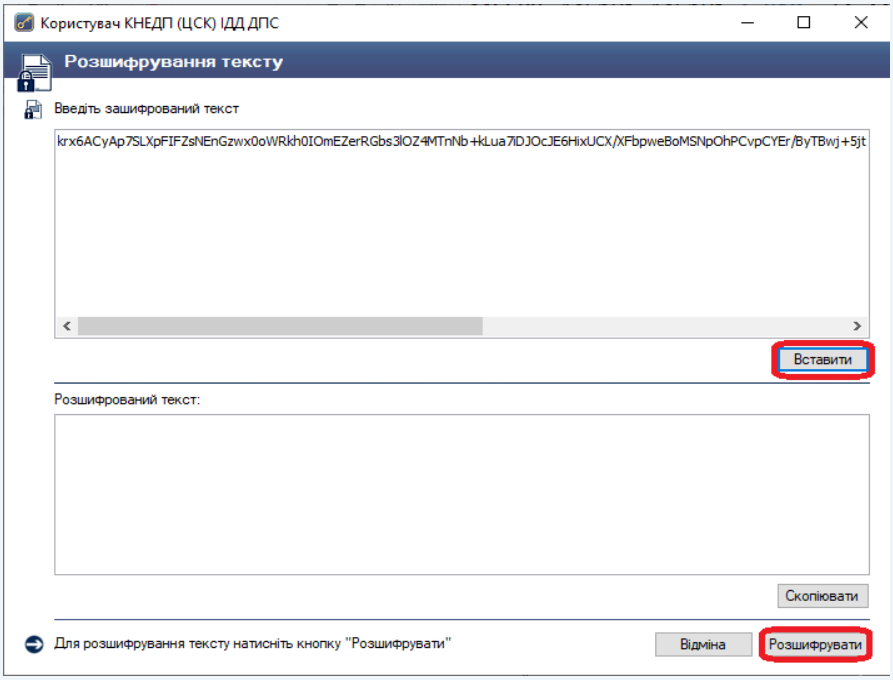


Рисунок 4.27

Текст можна переглянути одразу після його розшифрування у вікні «Розшифрований текст» та скопіювати його за допомогою кнопки «Скопіювати» (рис. 4.28).

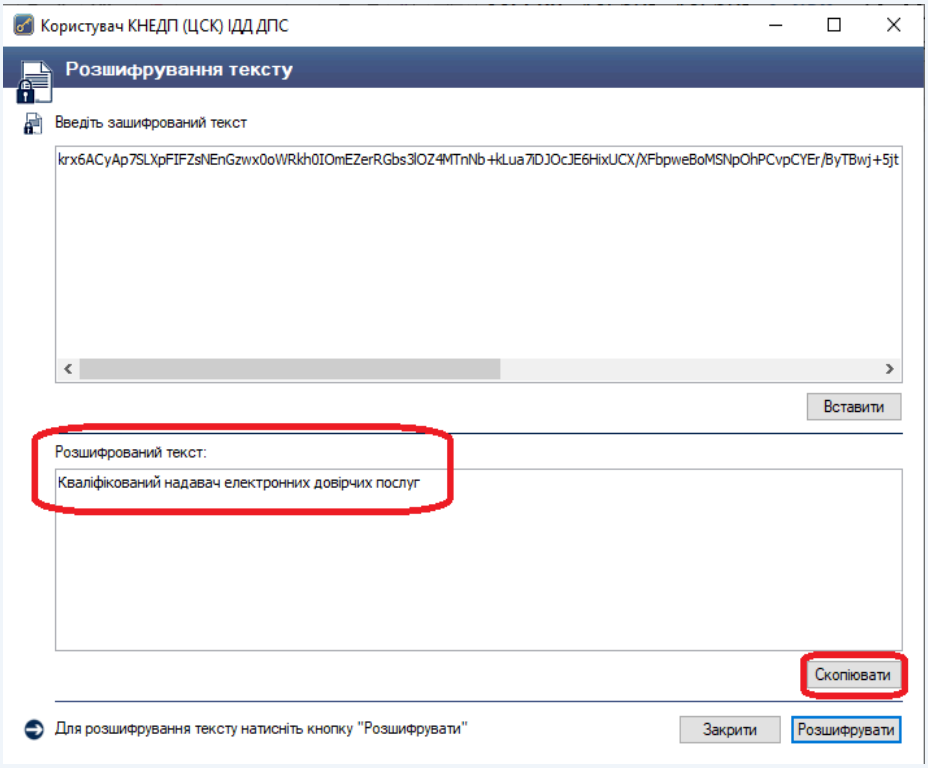


Рисунок 4.28

У випадку відсутності у підписувача прав доступу до зашифрованого тексту з’явиться вікно «Повідомлення оператору» (рис. 4.29).

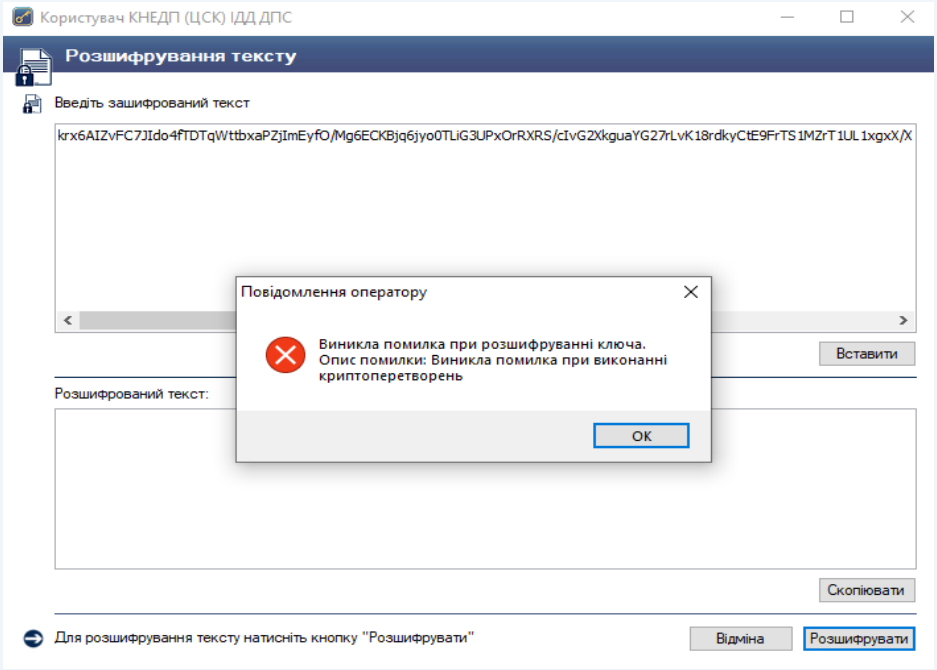


Рисунок 4.29

4.7 Перегляд та друк кваліфікованих сертифікатів

Для перегляду кваліфікованих сертифікатів, що містяться у файловому сховищі необхідно натиснути кнопку «Переглянути сертифікати» у головному вікні ПЗ або натиснути клавішу F10 (рис. 4.30).

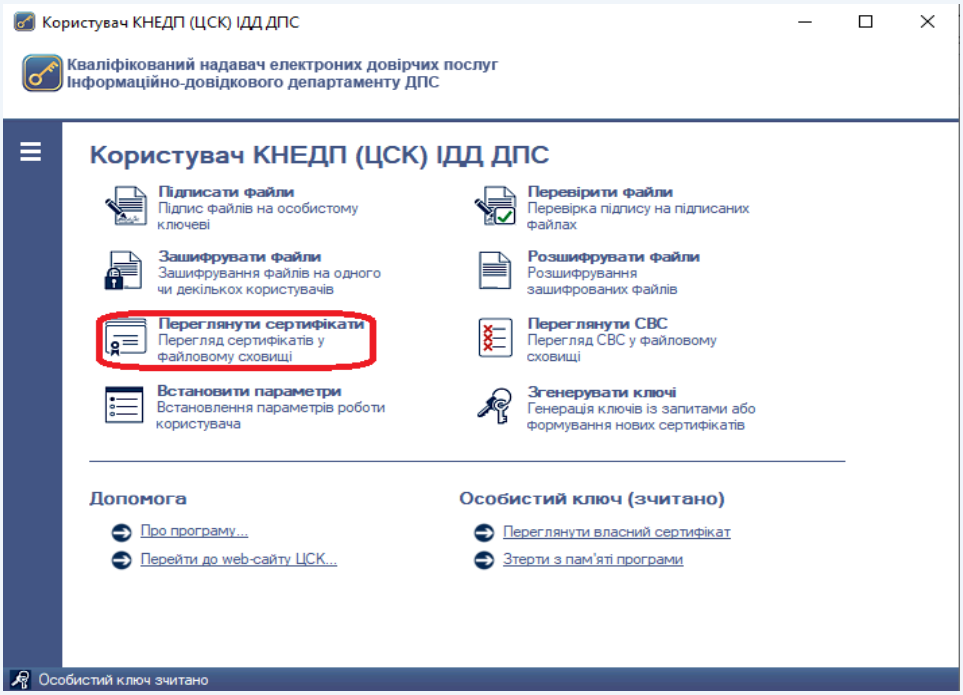


Рисунок 4.30

У вікні перегляду кваліфікованих сертифікатів (рис. 4.31) можна імпортувати, експортувати, переглянути, перевірити та видалити обраний кваліфікований сертифікат.

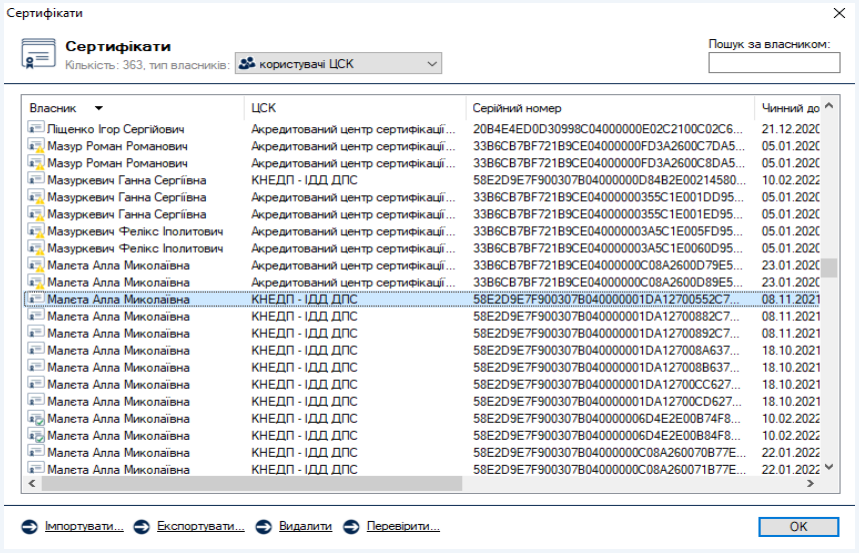


Рисунок 4.31

Кваліфіковані сертифікати у вікні відображаються за типами власників (тип власника обирається у верхній частині вікна):

- всі сертифікати;
- сертифікати Надавача;
- сертифікати серверів Надавача;
- сертифікати CMP-серверів;
- сертифікати TSP-серверів;
- сертифікати OCSP-серверів;
- сертифікати користувачів Надавача.

Для перегляду даних про власника кваліфікованого сертифіката необхідно натиснути на відповідному записі про кваліфікований сертифікат у списку, після чого будуть відображені дані кваліфікованого сертифіката (рис. 4.32 та 4.33).

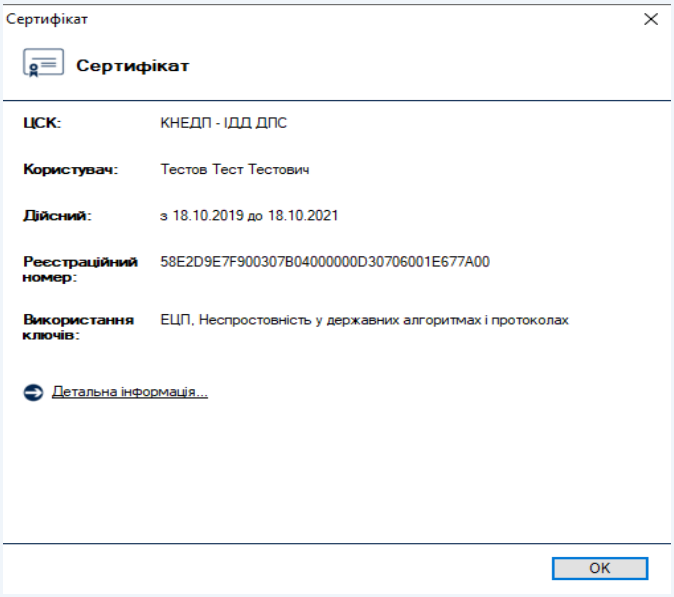


Рисунок 4.32

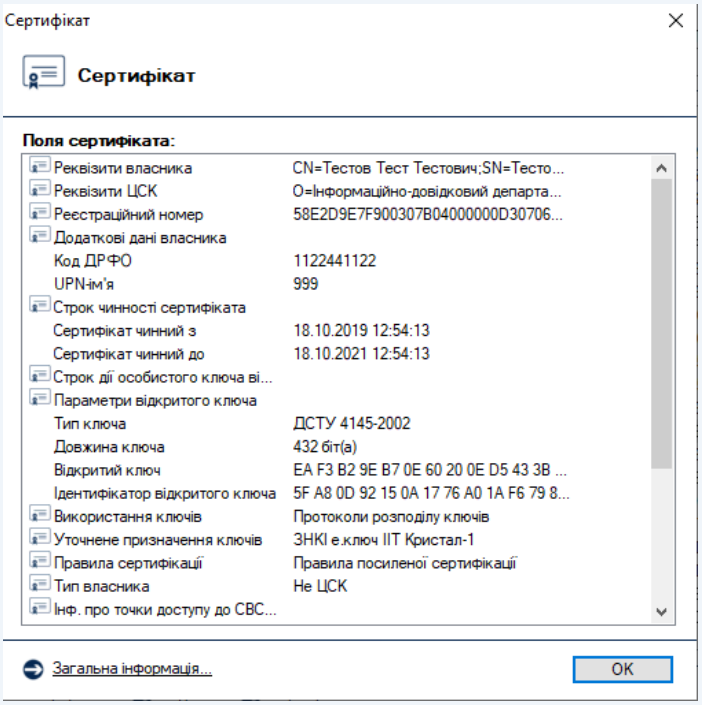


Рисунок 4.33

Для друкування кваліфікованого сертифікату відкритого ключа необхідно обрати пункт «Детальна інформація» (рис. 4.34) та у вікні, яке з’явилось, натиснути праву кнопку миші та обрати пункт «Друкувати» (рис. 4.35).

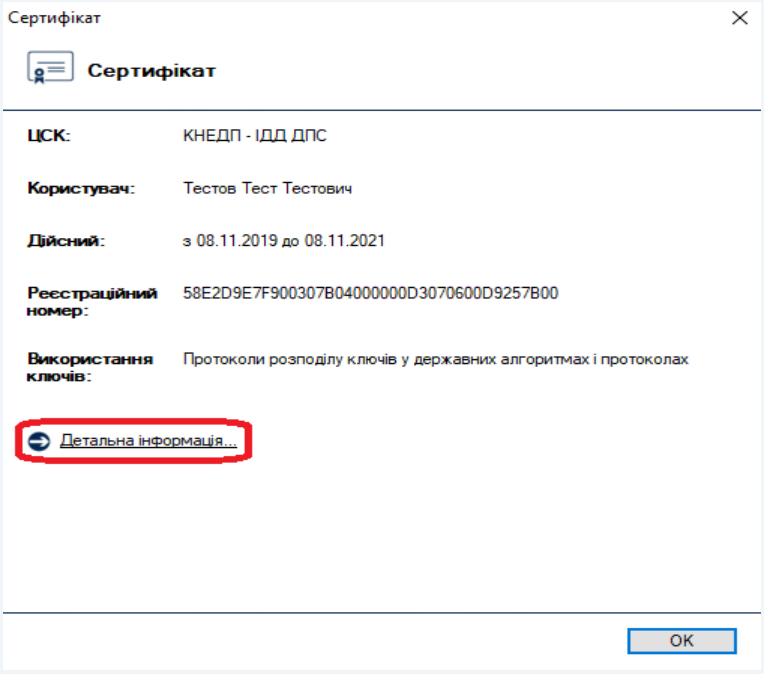


Рисунок 4.34

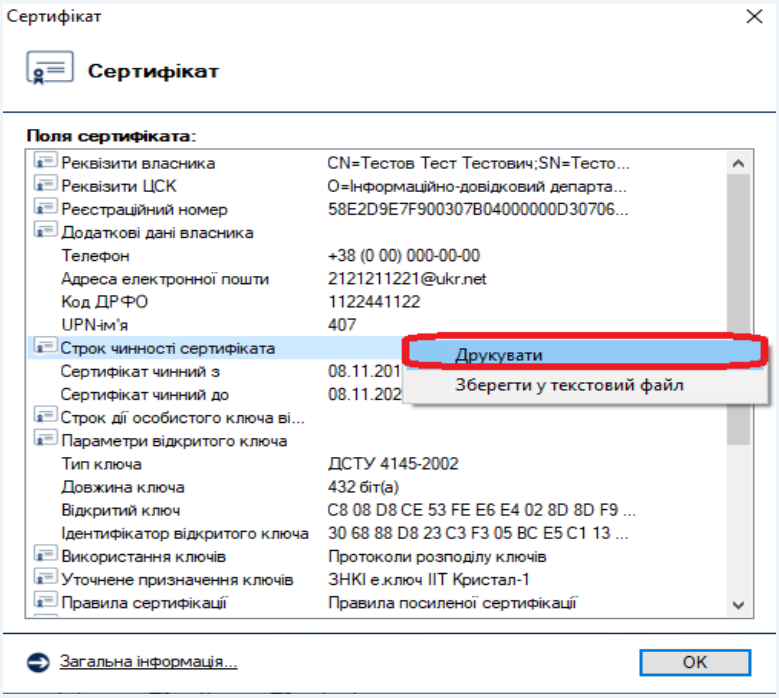


Рисунок 4.35

Для видалення кваліфікованих сертифікатів з файлового сховища необхідно відмітити у списку (рис. 4.31) відповідні записи та натиснути кнопку «Видалити».

Для перевірки кваліфікованого сертифіката необхідно відмітити відповідний запис про кваліфікований сертифікат у списку та натиснути кнопку «Перевірити». Перевірка кваліфікованого сертифіката здійснюється відповідно до встановлених параметрів роботи ПЗ, за допомогою СВС чи OCSP-протоколу. Появою вікна «Пошук та визначення статусу сертифіката» (рис. 4.36) закінчується перевірка кваліфікованого сертифіката. Детальну інформацію про кваліфікований сертифікат можна переглянути обравши пункт «Сертифікат».

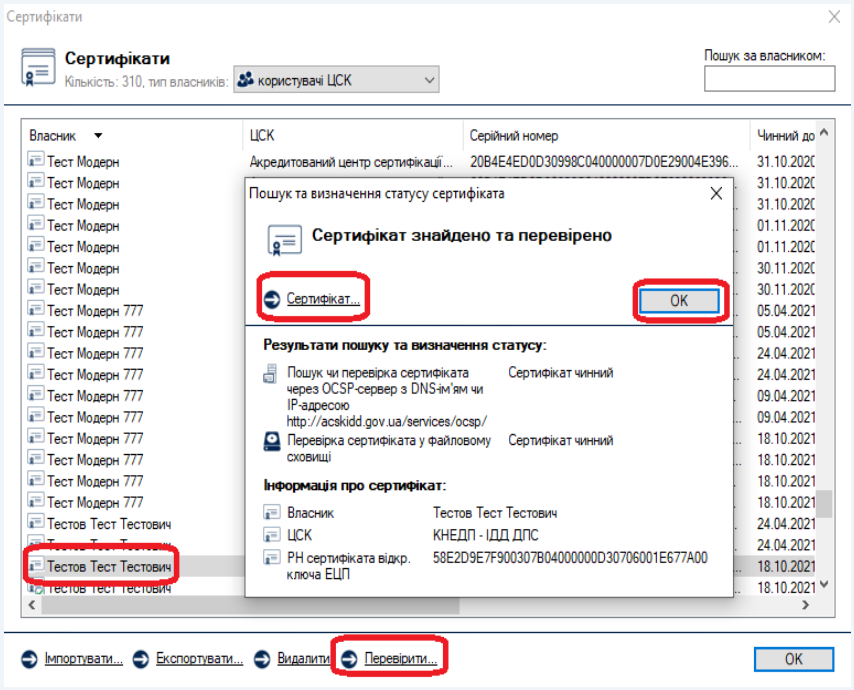


Рисунок 4.36

Для експорту кваліфікованого сертифіката з файлового сховища в інше місце (носій інформації тощо), необхідно натиснути «Експортувати», та обрати інше місце розташування.

4.8 Перегляд СВС

Для перегляду СВС необхідно натиснути підпункт «Переглянути СВС» у головному меню або натиснути клавішу F11 (рис. 4.37). Вікно перегляду СВС наведене на рис. 4.38.

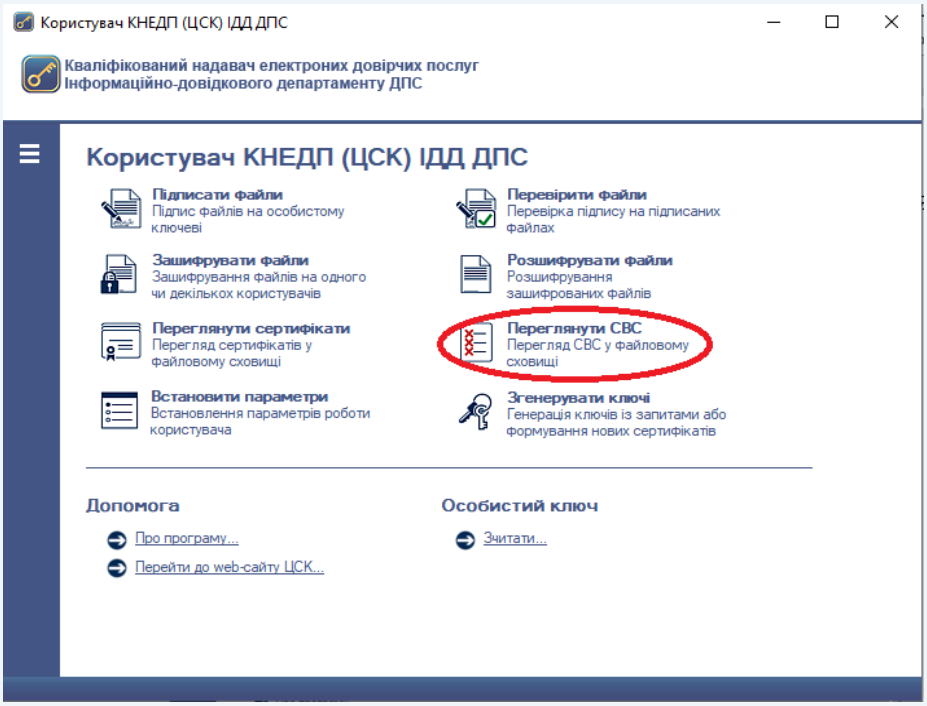


Рисунок 4.37

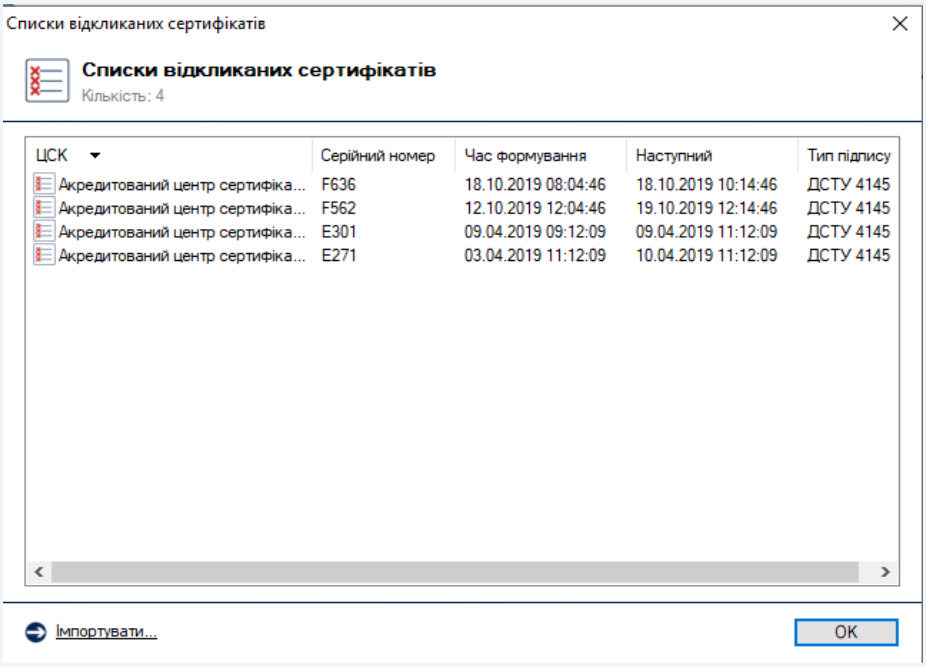


Рисунок 4.38

Вікно перегляду СВС дозволяє імпортувати, видаляти чи переглядати СВС, що завантажені з вебсайту.

Самостійно завантажити СВС можна у розділі «Пошук сертифікатів та СВС» вкладка «СВС» вебсайту (рис. 4.39) та імпортувати до ПЗ.

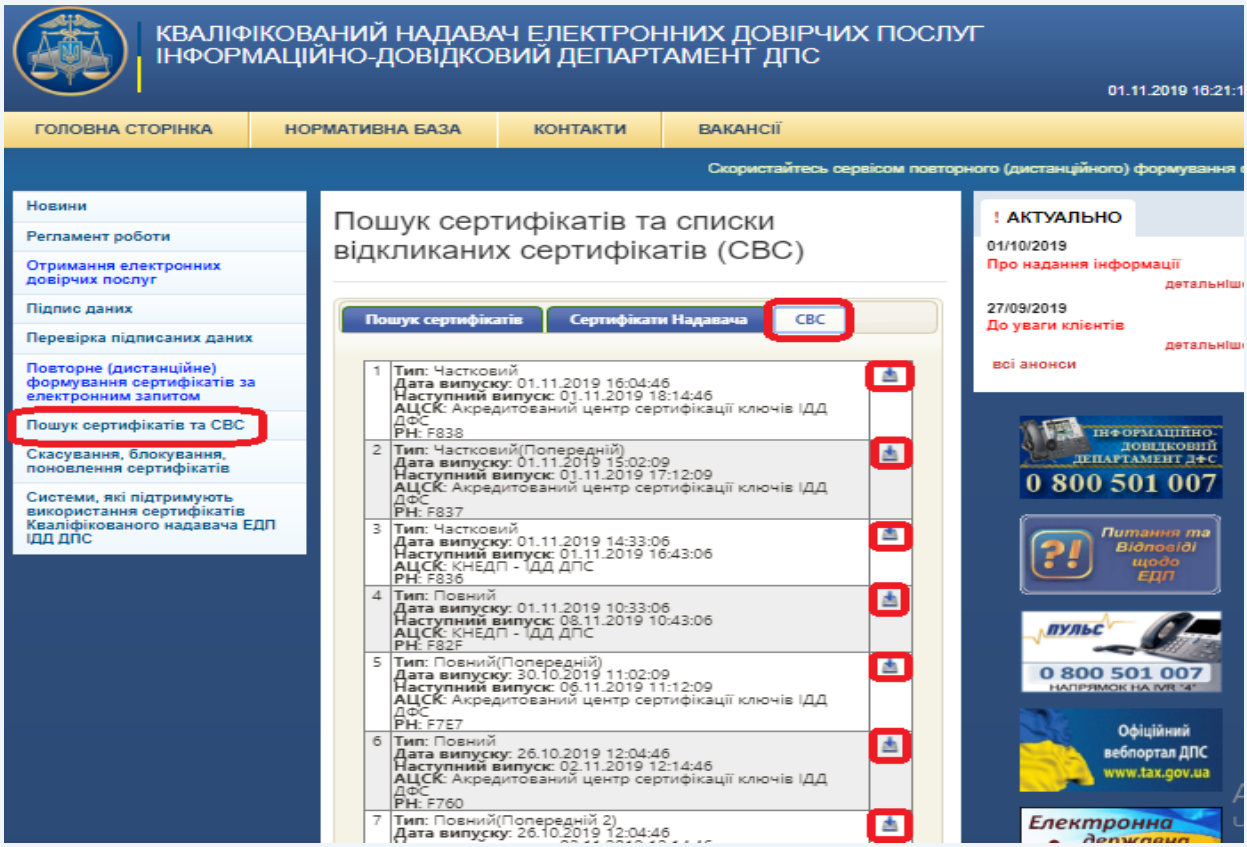


Рисунок 4.39

Для імпорту СВС до файлового сховища необхідно натиснути «Імпортувати» та обрати попередньо завантажений СВС.

Для перегляду СВС необхідно натиснути на відповідному записі про СВС у списку (рис. 4.40-4.42).

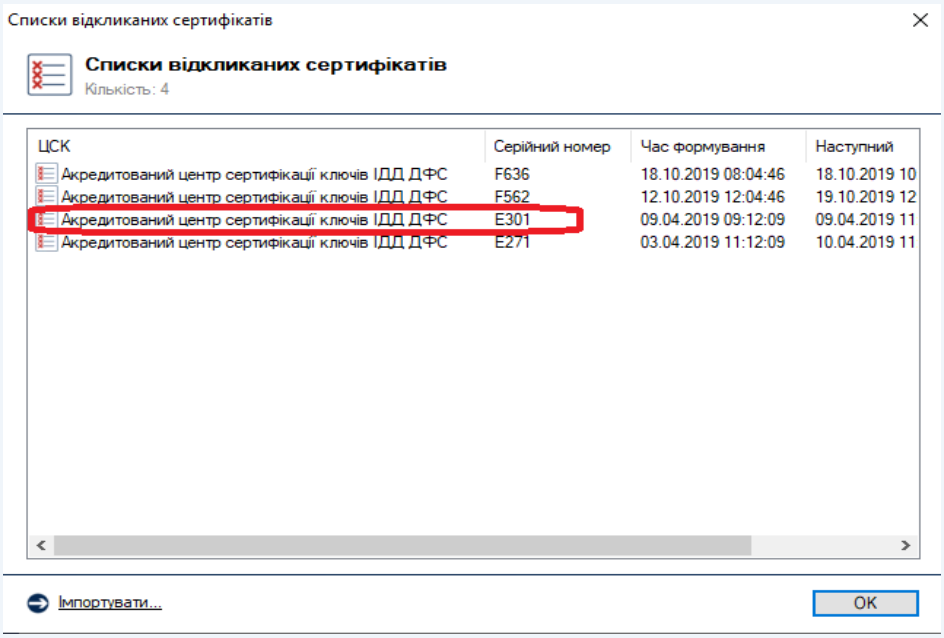


Рисунок 4.40

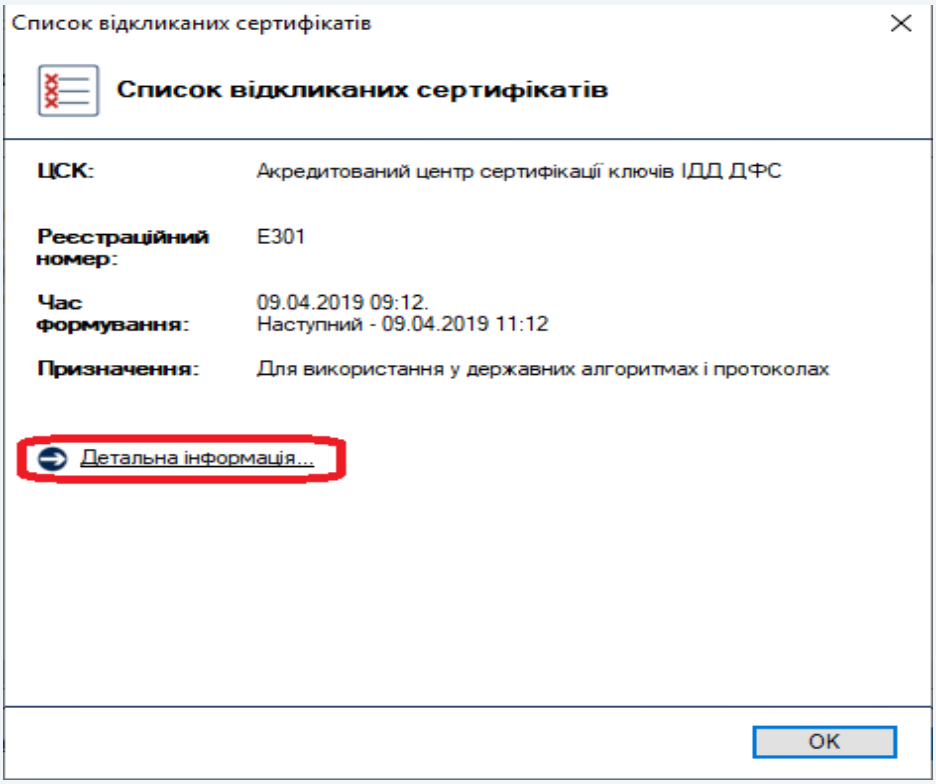


Рисунок 4.41

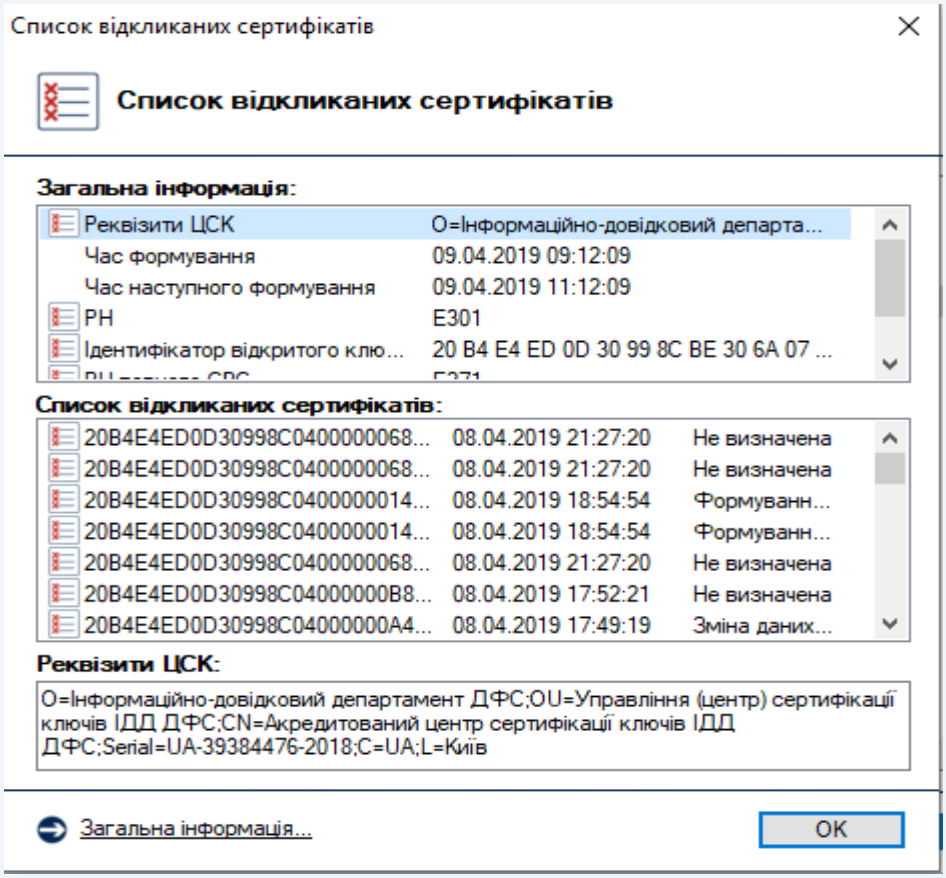


Рисунок 4.42

Для видалення файлу СВС з файлового сховища необхідно відмітити відповідний запис про СВС у списку та натиснути кнопку «Видалити».

5. Додаткові функції програмного забезпечення «ІІТ Користувач ЦСК-1»

5.1 Генерація особистого ключа

Для генерації особистого ключа на робочому місці підписувача застосовується надійний засіб КЕП – ПЗ. Згенерований особистий ключ захищається паролем та записується на НКІ.

Увага! Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе підписувач. Особисті ключі підписувачів та паролі захисту до них у Надавача не зберігаються.
Сервіс самостійної генерації ключів доступний лише для посадових осіб органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій державної форми власності.

Разом з цим створюються запити на формування кваліфікованих сертифікатів, що містять відкритий ключ підписувача та додаткову інформацію, які разом з комплектом реєстраційних документів передаються до пункту реєстрації користувачів Надавача для формування кваліфікованих сертифікатів.

Для генерації особистого ключа необхідно обрати у головному вікні ПЗ кнопку «Згенерувати ключі», після чого з'явиться вікно «Повідомлення оператору»,

в якому необхідно обрати пункт «Згенерувати ключі та сформувати запити на сертифікати» (рис. 5.1)

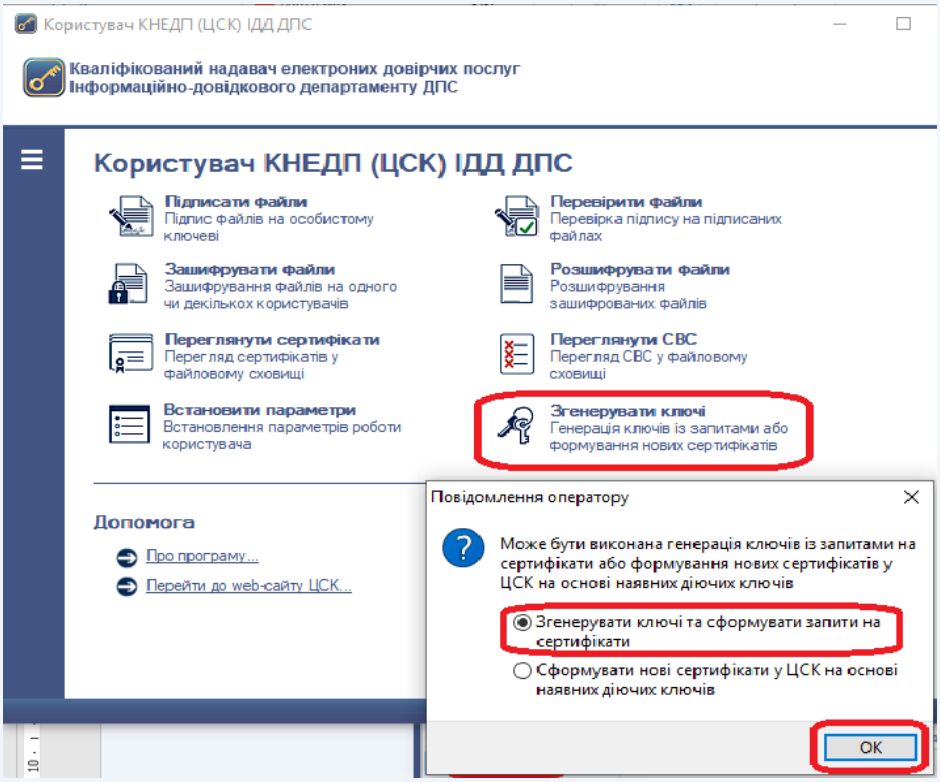


Рисунок 5.1

У вікні генерації ключів необхідно встановити параметр «Використовувати окремий ключ для протоколу розподілу», при цьому буде згенеровано дві ключові пари, одна з яких буде використовуватись для підписання даних, а друга (ключ протоколу розподілу) буде використовуватись для шифрування даних.

Для продовження генерації ключа необхідно натиснути кнопку «Далі» (рис.5.2).

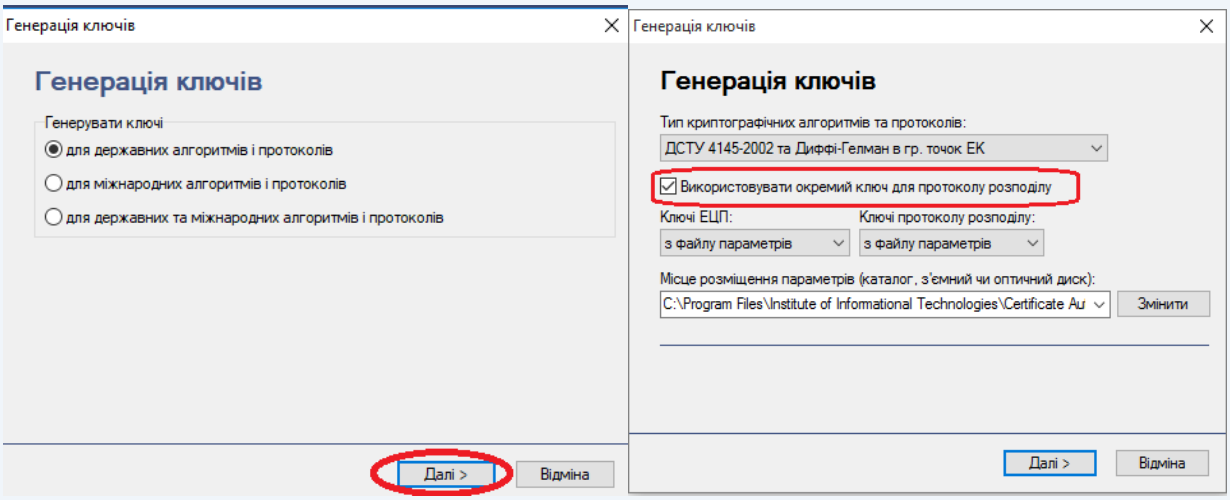


Рисунок 5.2

Після появи захищеного робочого столу, необхідно обрати з’ємний носій, на який буде записано особистий ключ, ввести пароль захисту до нього та натиснути кнопку «Записати» (рис.5.3).

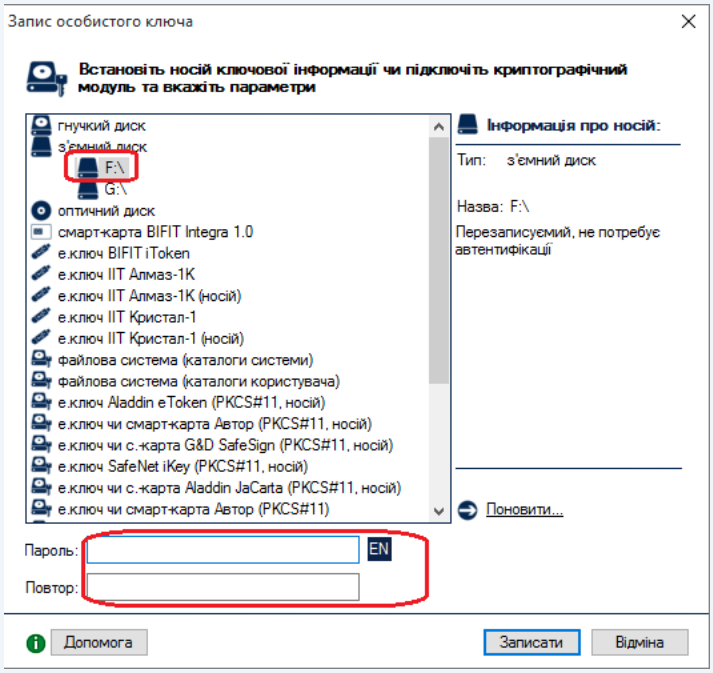


Рисунок 5.3

Обидва особистих ключа (для підпису та шифрування) будуть записані у вигляді одного файлу особистого ключа – «Key-6.dat».

На окремі носії інформації під час генерації особистих ключів програмно-технічний комплекс Кваліфікованого надавача ЕДП ІДД ДПС автоматично записує файл «Key-11.dat», що містить службову інформацію та не є особистим ключем.

Увага! Якщо в якості засобу зберігання особистого ключа використовується електронний ключ “Кристал-1” або “Алмаз-1К”, для відображення інформації у кваліфікованому сертифікаті, що особистий ключ збережений на захищеному носії ключової інформації (ЗНКІ) (рис.5.4) необхідно обирати “Кристал-1” в апаратному режимі роботи (рис.5.5)

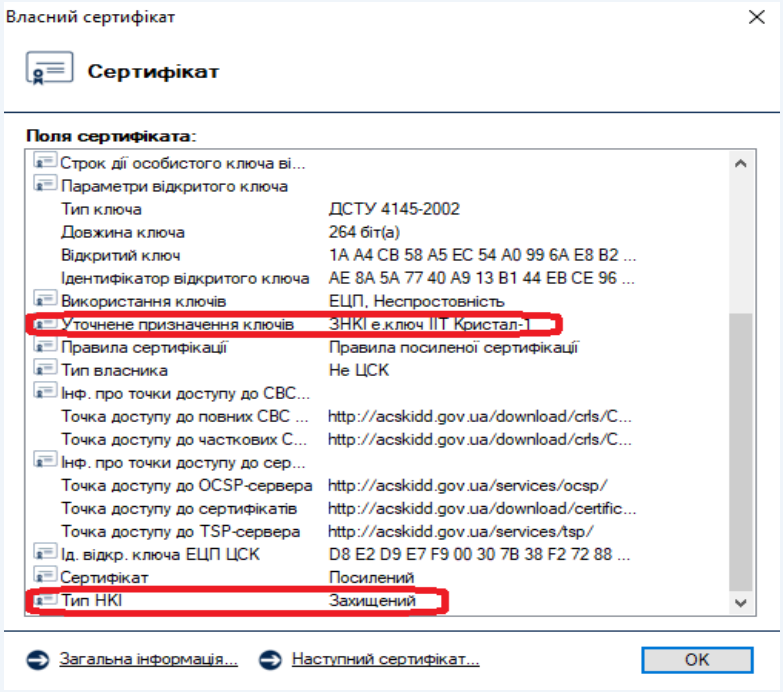


Рисунок 5.4

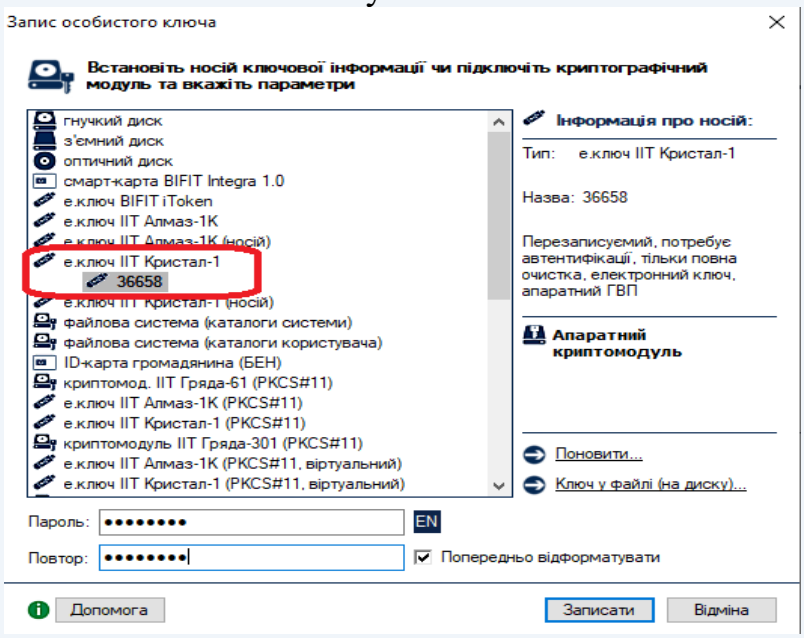


Рисунок 5.5

Після запису особистого ключа на з'ємний носій буде виведено вміст запиту на формування кваліфікованого сертифіката з відкритим ключем КЕП та запиту на формування кваліфікованого сертифіката з відкритим ключем протоколу розподілу. Для продовження генерації натискаємо кнопку «ОК» (рис. 5.6, 5.7).

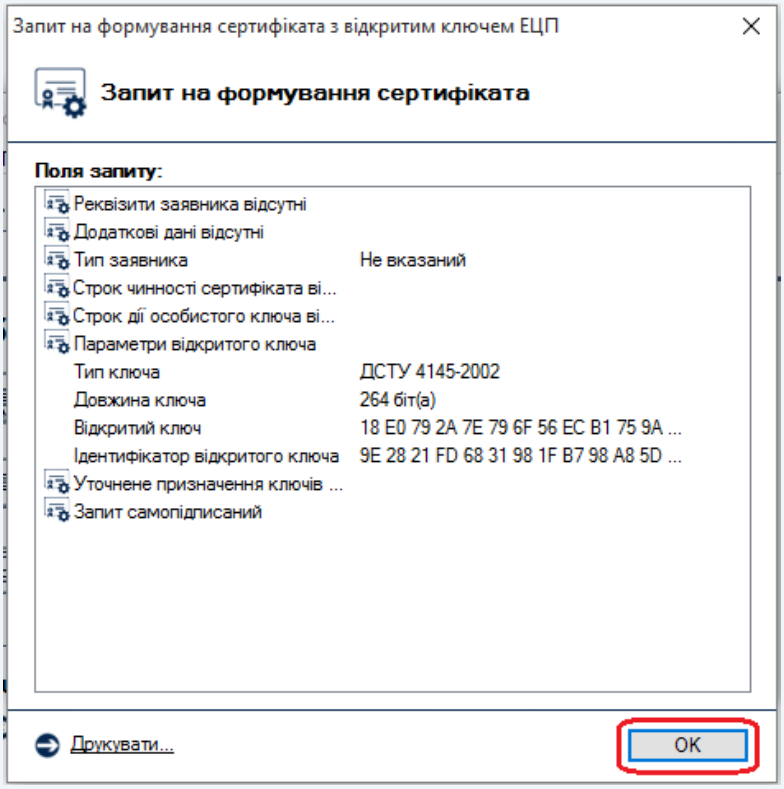


Рисунок 5.6

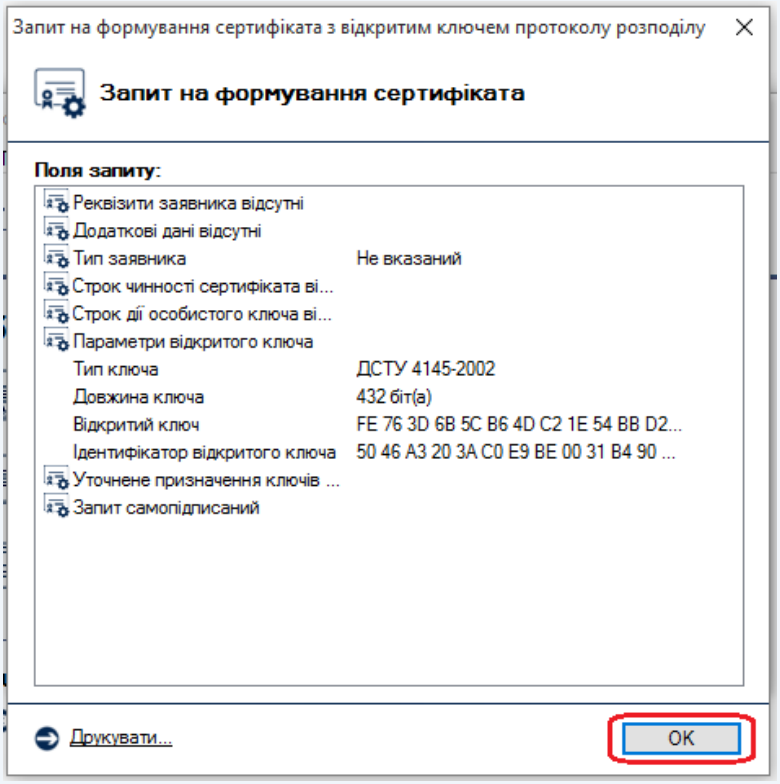


Рисунок 5.7

Для передачі запитів на формування кваліфікованих сертифікатів до Надавача необхідно зберегти їх у файл (рис. 5.8). Для цього встановити параметр «Зберегти у файл» та натиснути кнопку «Далі».

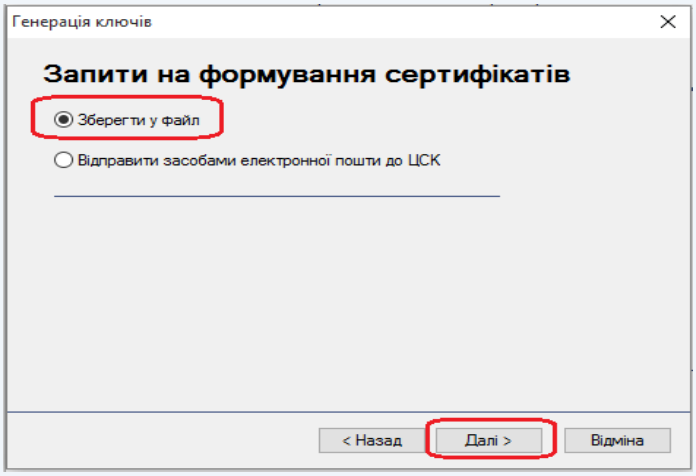


Рисунок 5.8

Запити повинні бути записані на носій інформації чи на жорсткий диск. Для цього необхідно натиснути кнопку «Змінити» (рис. 5.9) та вказати необхідний носій інформації та ім’я запитів на формування кваліфікованих сертифікатів у файл.

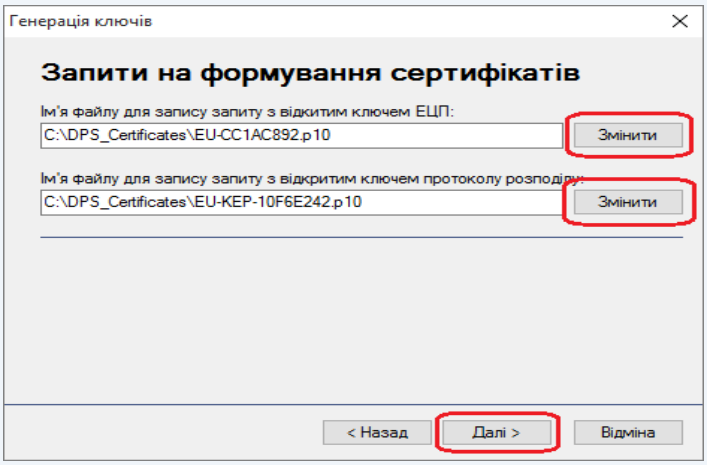


Рисунок 5.9

Увага! Для коректної ідентифікації запитів з відкритим ключем КЕП та протоколом розподілу користувача файл запиту на формування кваліфікованого сертифіката повинен обов’язково зберігатись з ім’ям у наступному форматі:
«ПІБ EU-XXXXXXXX.p10» та **«ПІБ EU-KEPXXXXXXXX.p10»**, де:
ПІБ – прізвище ім’я по батькові підписувача;
EU-XXXXXXXX.p10 та EU-KEP-XXXXXXXX.p10 – унікальне ім’я файлу запиту, що формується програмним забезпеченням за замовчуванням та повинно залишатись без змін.

Наприклад: **Ждан Олег Тарасович EU-69PH0S9W.p10;**
Ждан Олег Тарасович EU-KEP-KB50S67Z.p10.

Для завершення генерації необхідно натиснути кнопку «Завершити» (рис. 5.10).

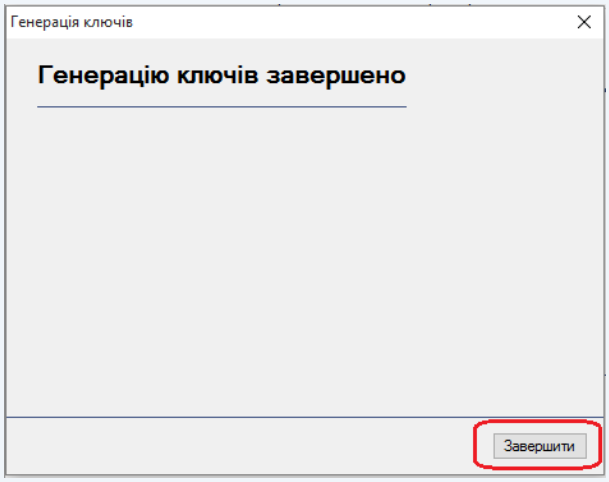


Рисунок 5.10

Після цього, запити разом з комплектом реєстраційних документів можуть бути передані до пункту реєстрації користувачів Надавача для формування кваліфікованих сертифікатів.

5.2 Зчитування особистого ключа та завантаження відповідних йому власних сертифікатів

Для роботи з більшістю функцій (захист файлів та ін.) ПЗ потребує попереднього зчитування особистого ключа підписувача.

Ініціювання зчитування особистого ключа може бути виконано автоматично при виборі певної функції ПЗ або шляхом вибору підпункту «Зчитати ...» в пункті «Особистий ключ» у головному вікні ПЗ або шляхом натискання комбінації клавіш **Ctrl+K** (рис. 5.9).

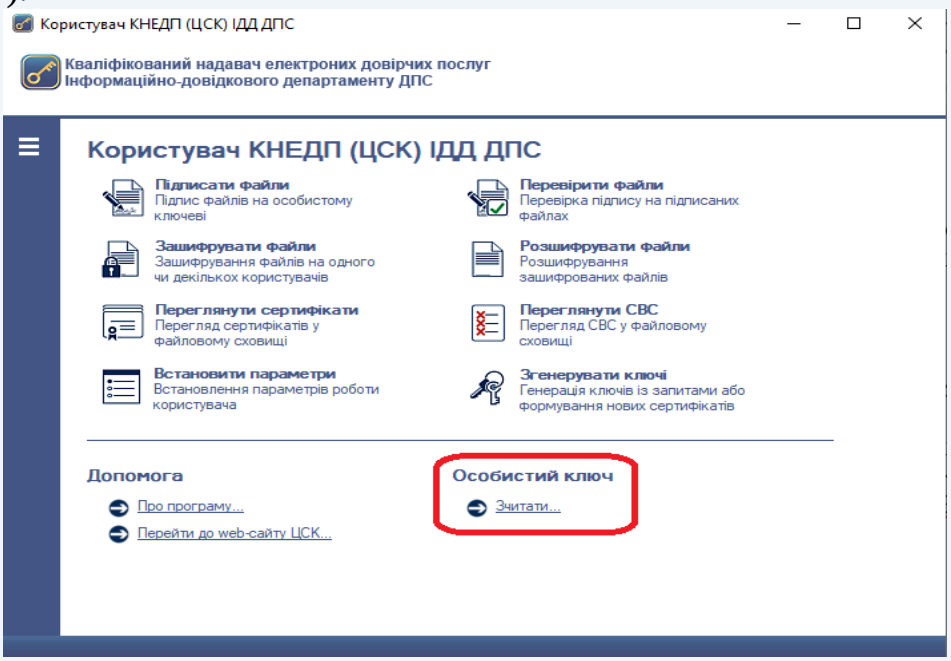


Рисунок 5.9

Після появи захищеного робочого столу (рис. 5.10), необхідно обрати з’ємний НКІ, ввести пароль захисту особистого ключа та натиснути кнопку «Зчитати»

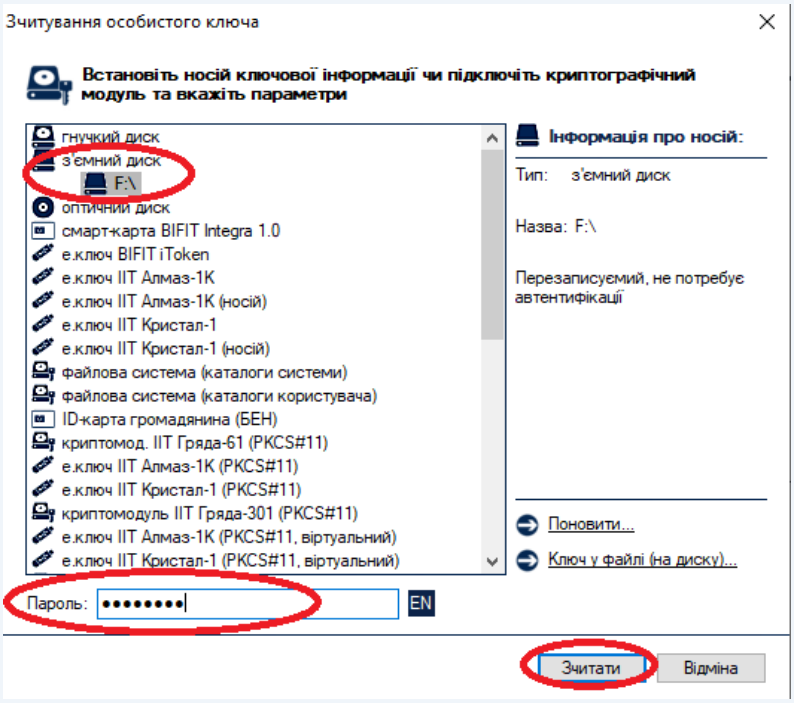


Рисунок 5.10

У випадку відсутності у файловому сховищі власних кваліфікованих сертифікатів підписувача, з'явиться вікно «Повідомлення оператору» (рис. 5.11). Необхідно натиснути кнопку «ОК».

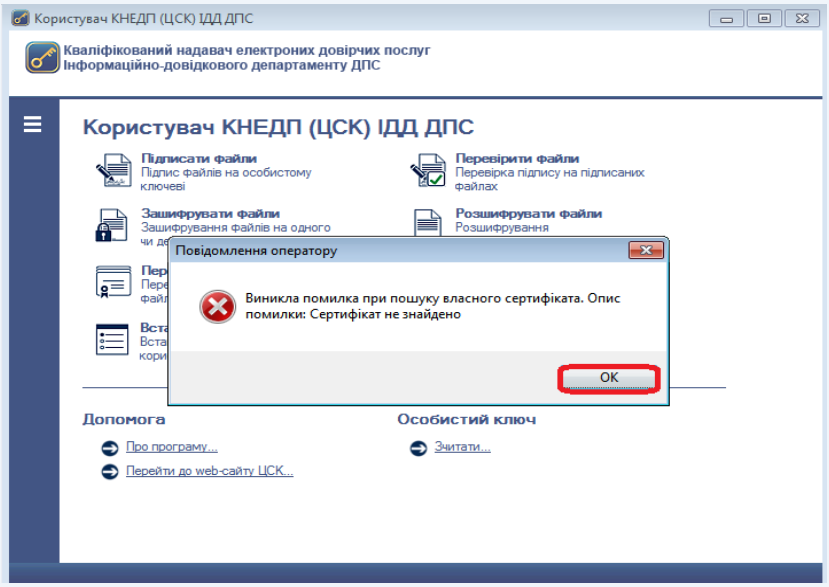


Рисунок 5.11

Після чого буде виведене діалогове вікно (рис. 5.12). Для продовження формування запиту на автоматичне завантаження кваліфікованих сертифікатів відкритого ключа підписувача натиснути «Да».

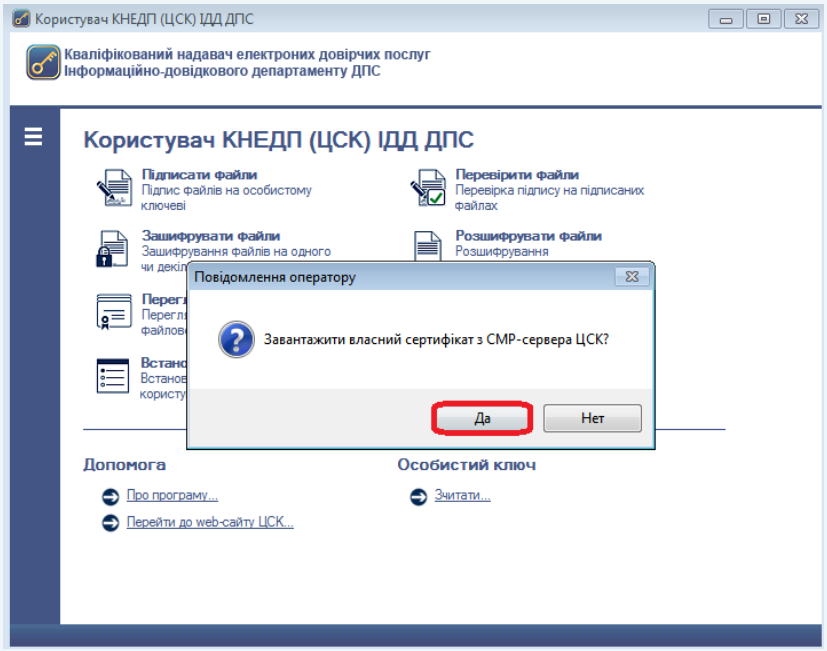


Рисунок 5.12

При відкритті вікна «Завантажені сертифікати» (рис. 5.13), необхідно зберегти їх у файлове сховище, натиснувши кнопку «Да».

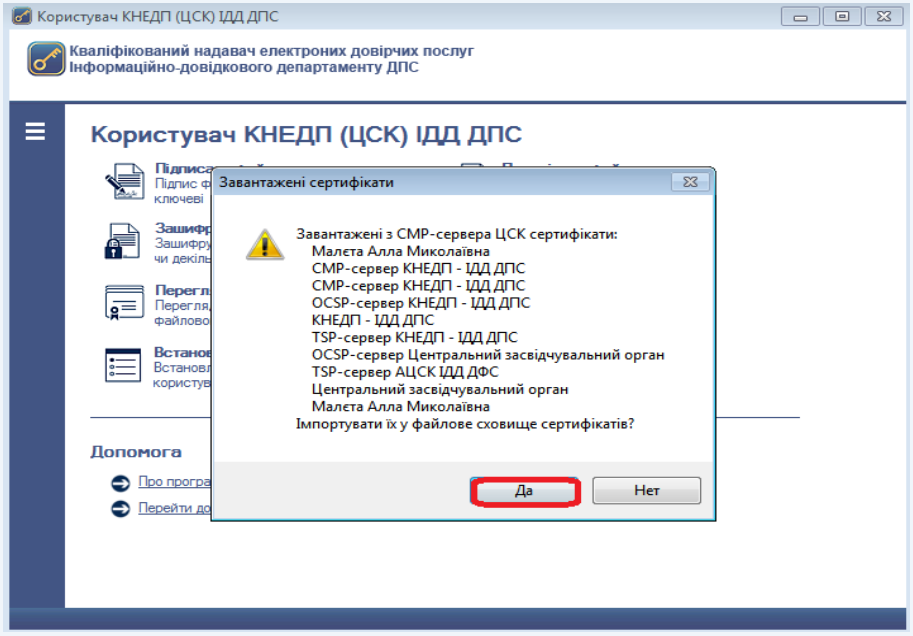


Рисунок 5.13

Для експорту кваліфікованого сертифіката з файлового сховища в інше місце (носій інформації тощо), необхідно натиснути кнопку «Переглянути сертифікати» у головному вікні ПЗ або натиснути клавішу F10 (рис. 5.14).

Далі відмітити у списку відповідні записи, натиснути кнопку «Експортувати», та обрати інше місце розташування (рис. 5.15).

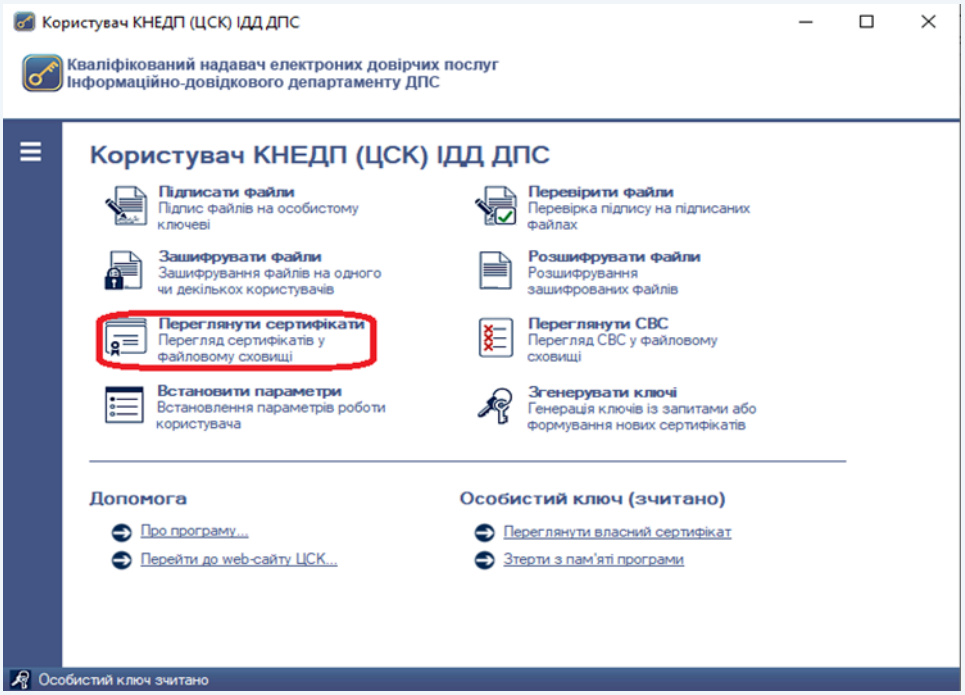


Рисунок 5.14

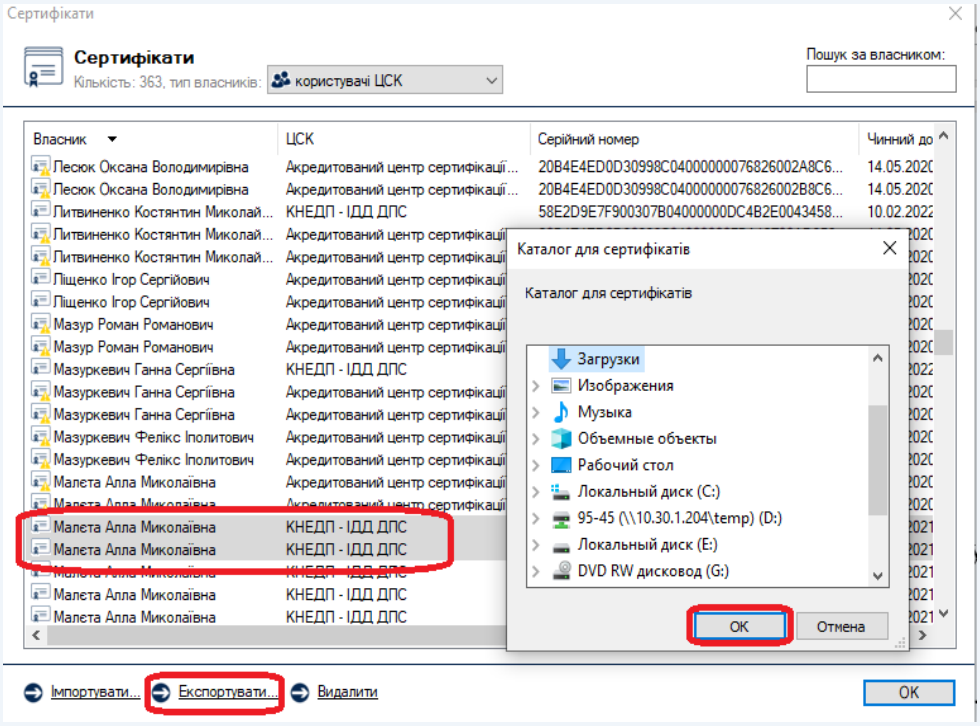


Рисунок 5.15

Інформація про те, що особистий ключ зчитаний та знаходиться в пам’яті ПК відображається у панелі стану вікна (рис. 5.16).

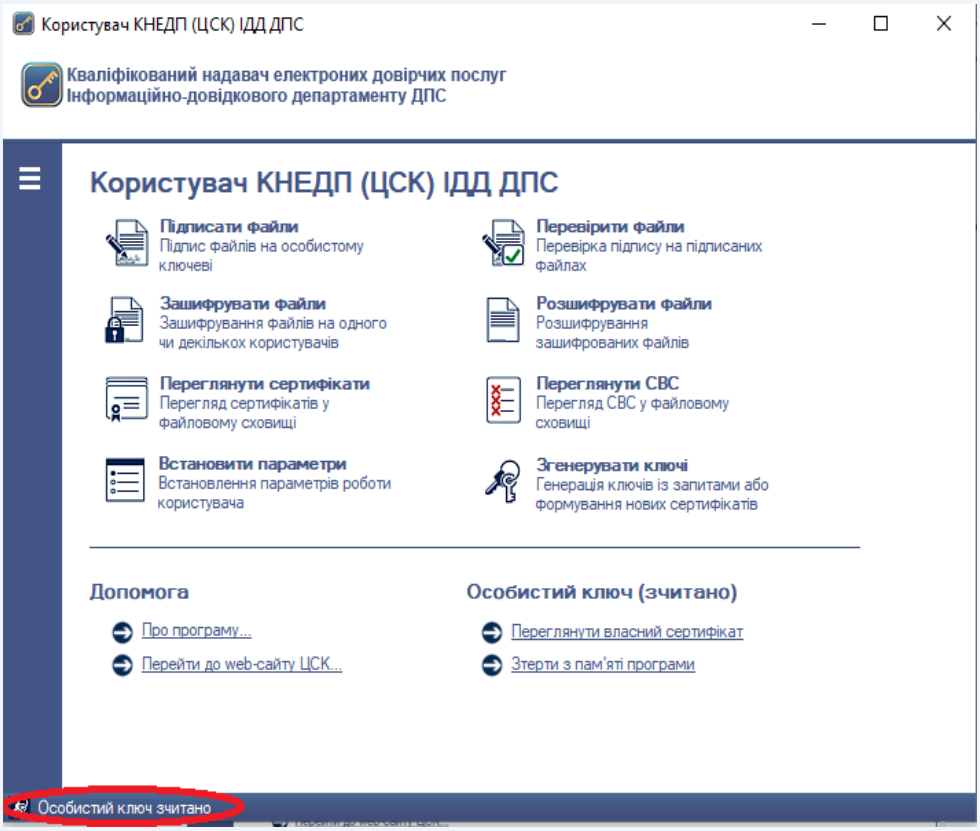


Рисунок 5.16

5.3 Зміна паролю захисту особистого ключа

Для зміни паролю захисту особистого ключа необхідно обрати підпункт «Змінити пароль захисту особистого ключа» у пункті меню «Особистий ключ» (рис. 5.17).

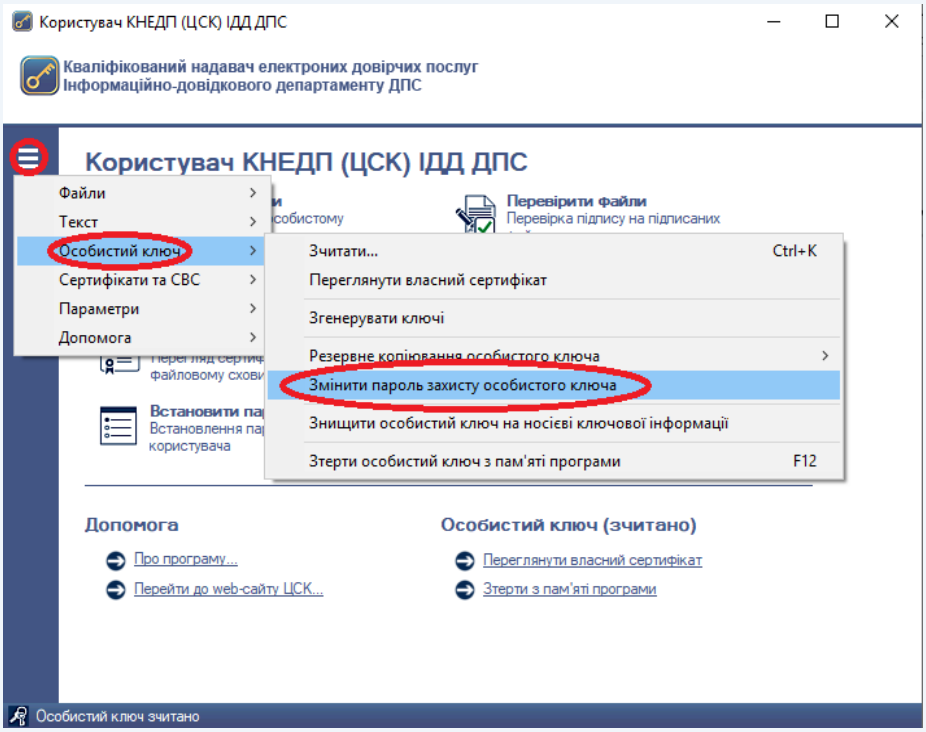


Рисунок 5.17

Після появи захищеного робочого столу (рис. 5.18), необхідно вказати:

- тип НКІ;
- назву носія;
- пароль захисту особистого ключа;
- новий пароль захисту особистого ключа (з підтвердженням).

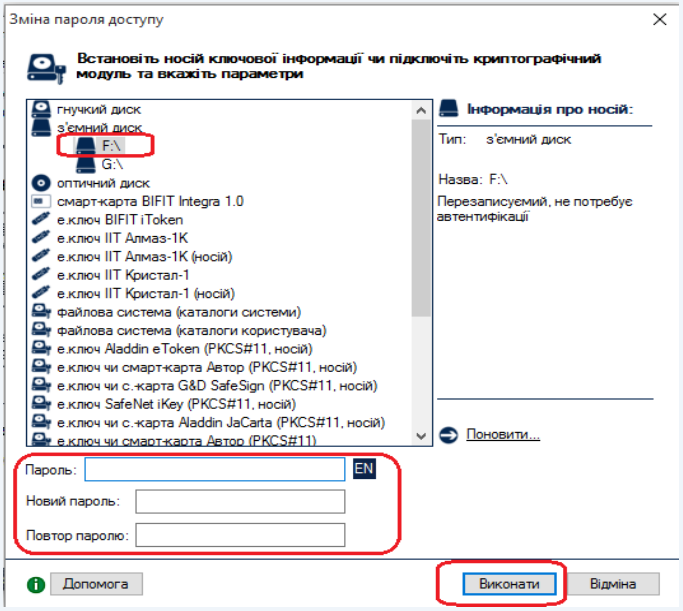


Рисунок 5.18

5.4 Знищення особистого ключа на носієві

Для знищення особистого ключа необхідно обрати підпункт «Знищити особистий ключ на носієві ключової інформації» в пункті меню «Особистий ключ» (рис. 5.19).

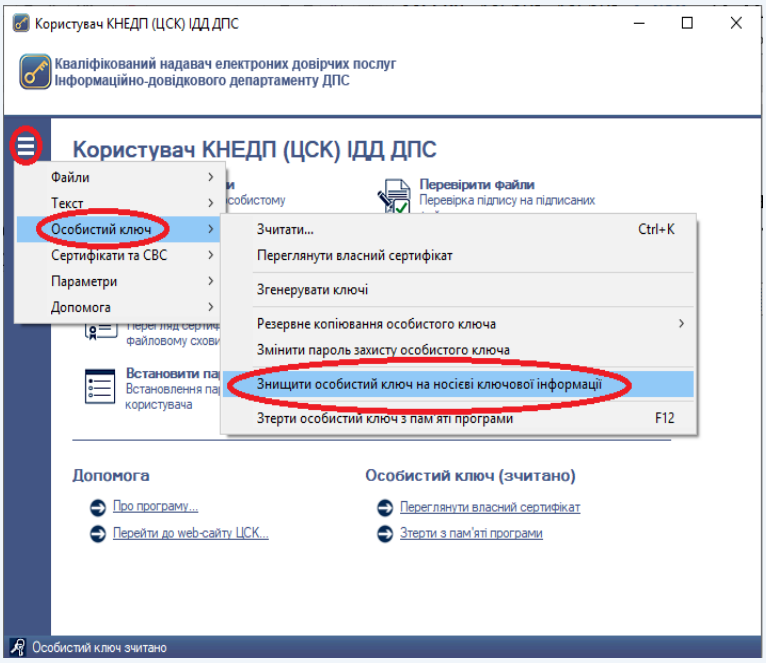


Рисунок 5.19

Після появи захищеного робочого столу необхідно вказати тип та назву НКІ, ввести пароль захисту особистого ключа та натиснути кнопку «Знищити» (рис. 5.20).

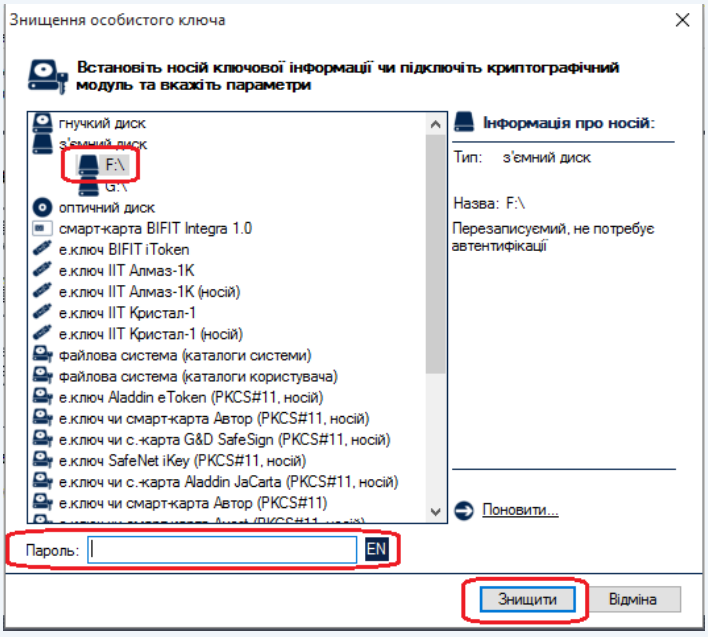


Рисунок 5.20

5.5 Знищення особистого ключа з пам’яті ПК

ПЗ передбачає можливість знищення особистого ключа з пам’яті ПК після кожної операції. Для встановлення зазначеної опції необхідно обрати параметр «Зтирати після кожної операції» підпункту «Зтирання особистого ключа з пам’яті програми» пункту меню «Параметри».

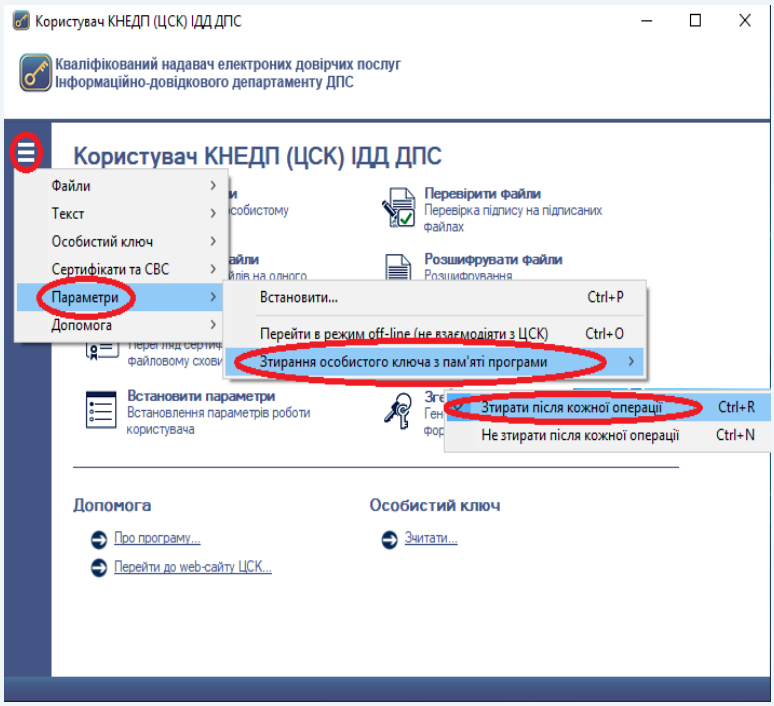


Рисунок 5.21

Якщо необхідно знищити ключ з пам’яті не виходячи з ПЗ необхідно обрати пункт «Зтерти» у головному вікні ПЗ або натиснути клавішу F12 (рис. 5.22).

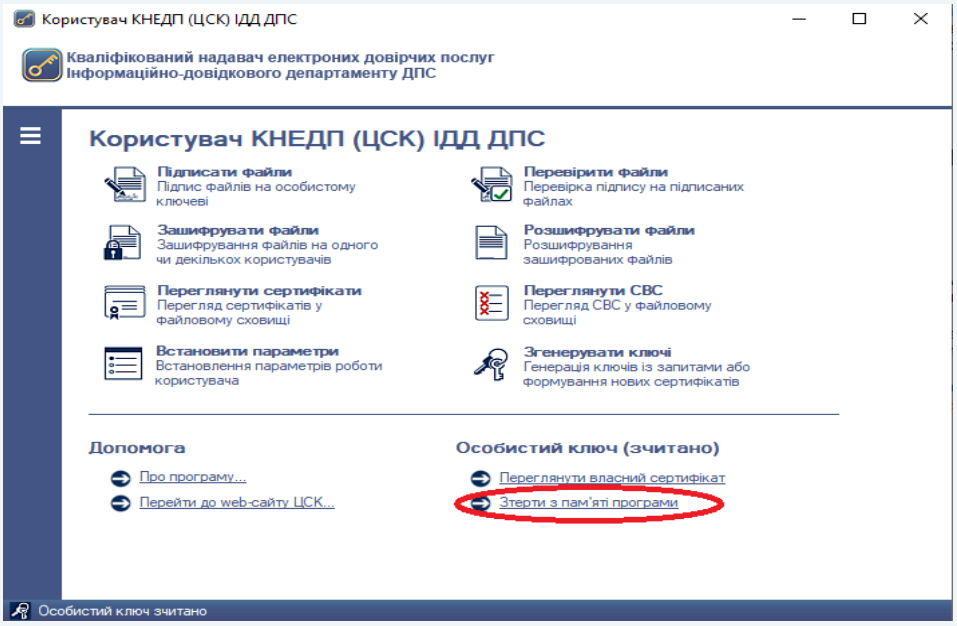


Рисунок 5.22

5.6 Резервне копіювання особистого ключа з носія ключа на носій

Для резервного копіювання особистого ключа з одного НКІ на інший необхідно обрати підпункт «Резервне копіювання особистого ключа» в пункті меню «Особистий ключ» та встановити параметр «з носія ключа на носій» (рис. 5.23).

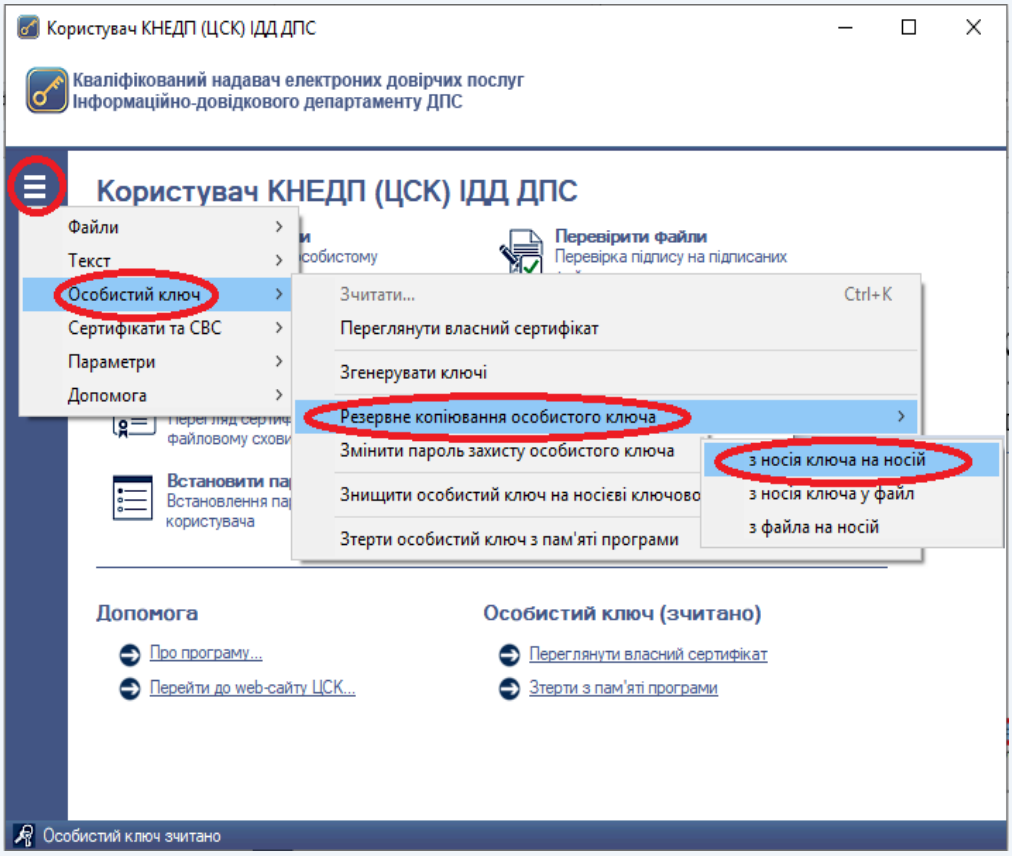


Рисунок 5.23

Після появи захищеного робочого столу необхідно обрати з’ємний НКІ, з якого буде знята копія, та ввести пароль захисту особистого ключа (рис. 5.24).

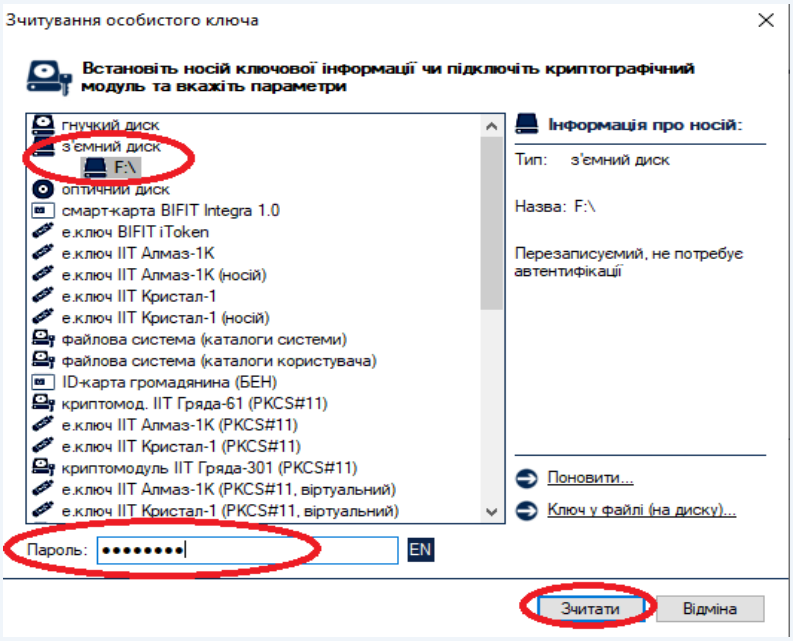


Рисунок 5.24

Далі, необхідно обрати з’ємний НКІ, на який буде записана копія особистого ключа та ввести пароль захисту до нього (рис. 5.25).

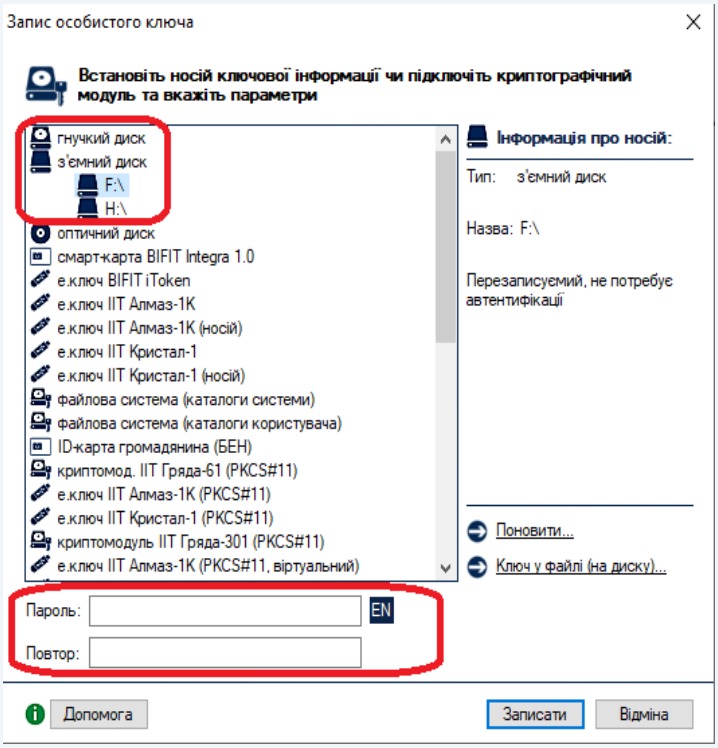


Рисунок 5.25

5.7 Резервне копіювання особистого ключа з носія ключа у файл

Для резервного копіювання особистого ключа з НКІ на жорсткий диск ПК необхідно обрати підпункт «Резервне копіювання особистого ключа» пункту меню «Особистий ключ» та обрати параметр «з носія ключа у файл» (рис. 5.26).

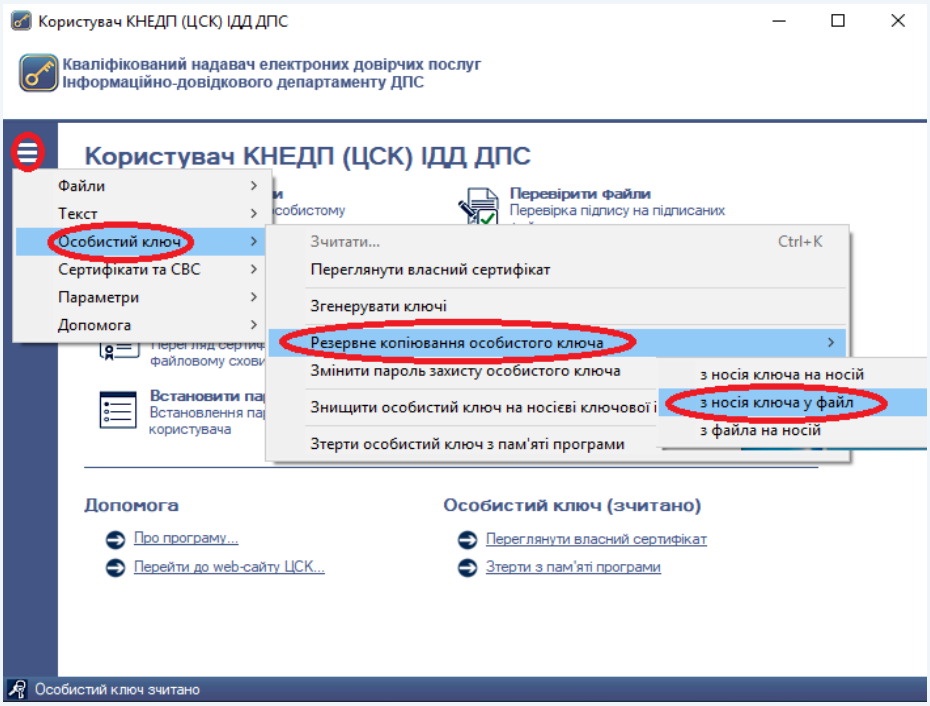


Рисунок 5.26

Після появи захищеного робочого столу необхідно обрати з’ємний НКІ, з якого буде знята копія, та ввести пароль захисту особистого ключа (рис. 5.27).

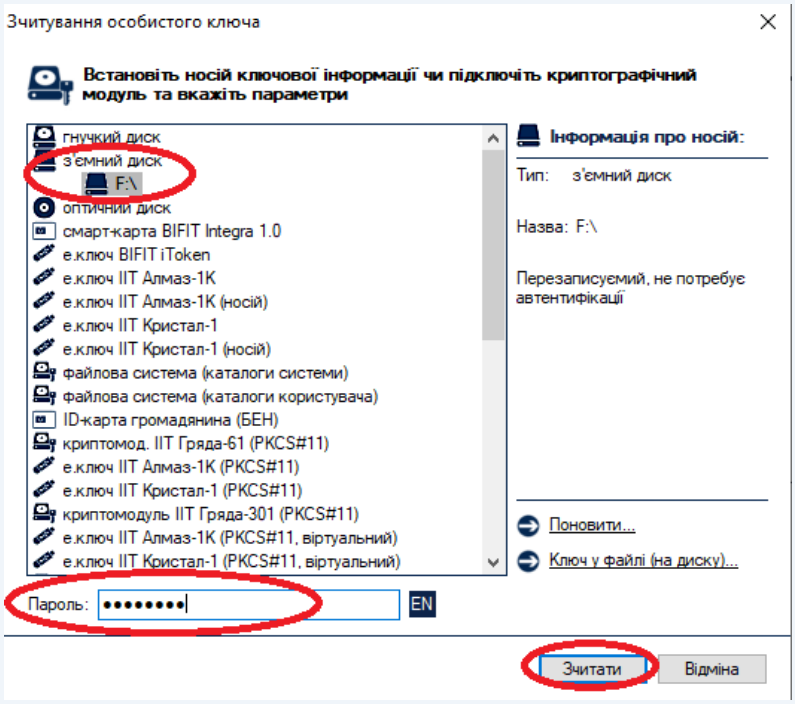


Рисунок 5.27

В наступному вікні необхідно обрати місце на жорсткому диску ПК, де буде записана копія особистого ключа (рис. 5.28).

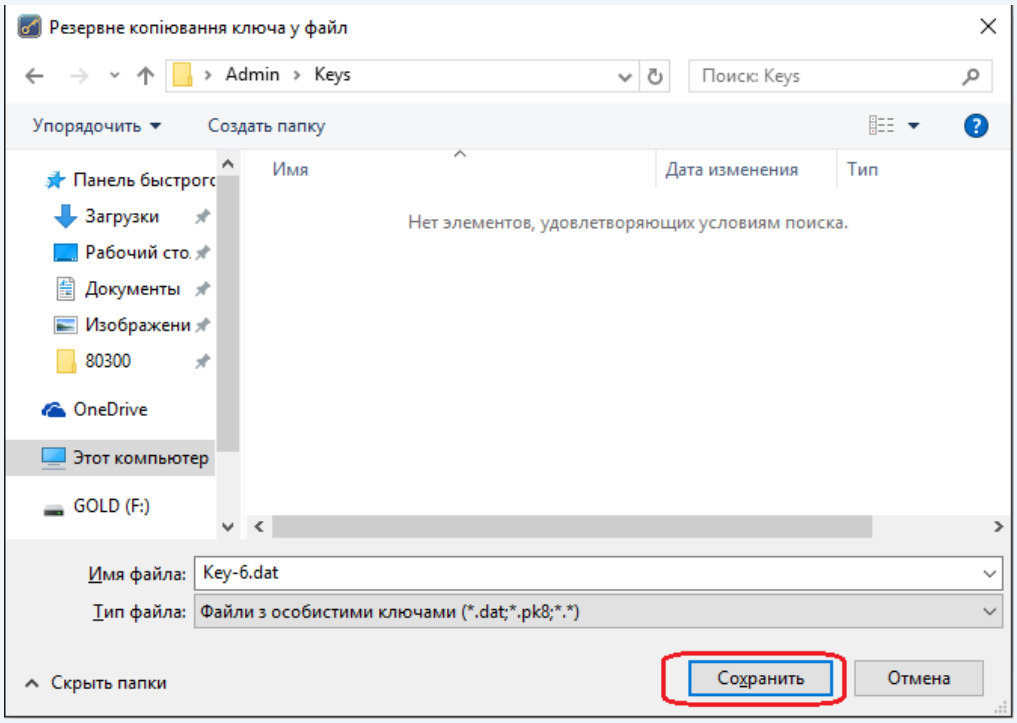


Рисунок 5.28

Увага! Для належної роботи особистого ключа змінювати ім’я файлу **«Key-6.dat» забороняється.**

Після завершення резервного копіювання необхідно натиснути кнопку «ОК» (рис. 5.29).

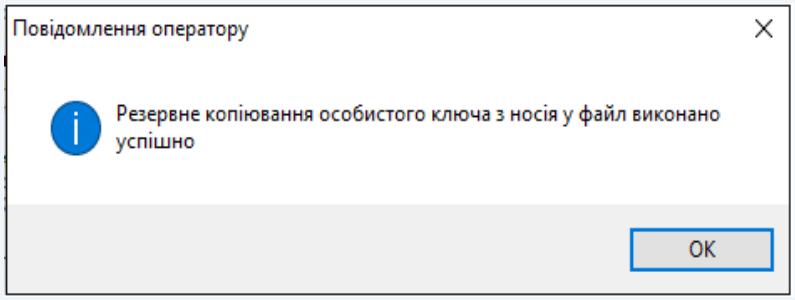


Рисунок 5.29

5.8 Резервне копіювання особистого ключа з файла на носій

Для резервного копіювання особистого ключа з жорсткого диску ПК на НКІ необхідно обрати підпункт «Резервне копіювання особистого ключа» в пункті меню «Особистий ключ» та встановити параметр «з файла на носій» (рис. 5.30).

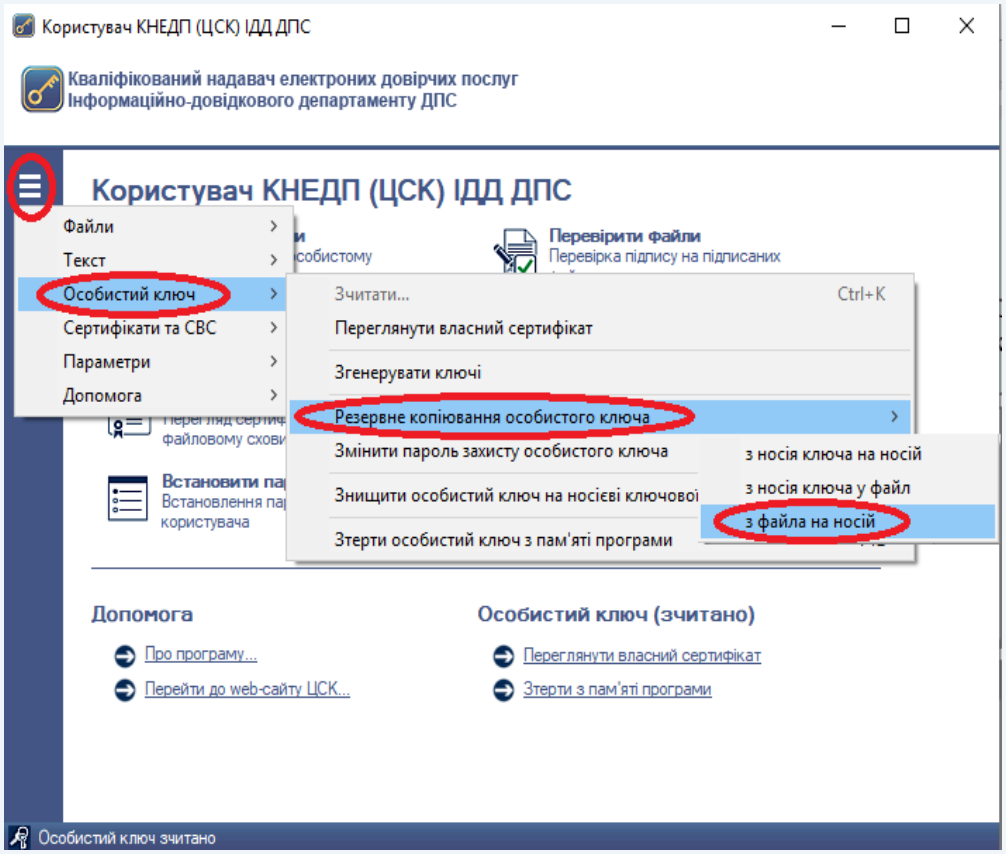


Рисунок 5.30

В наступному вікні необхідно обрати копію особистого ключа «Key-6.dat», розміщену на жорсткому диску ПК (рис. 5.31).

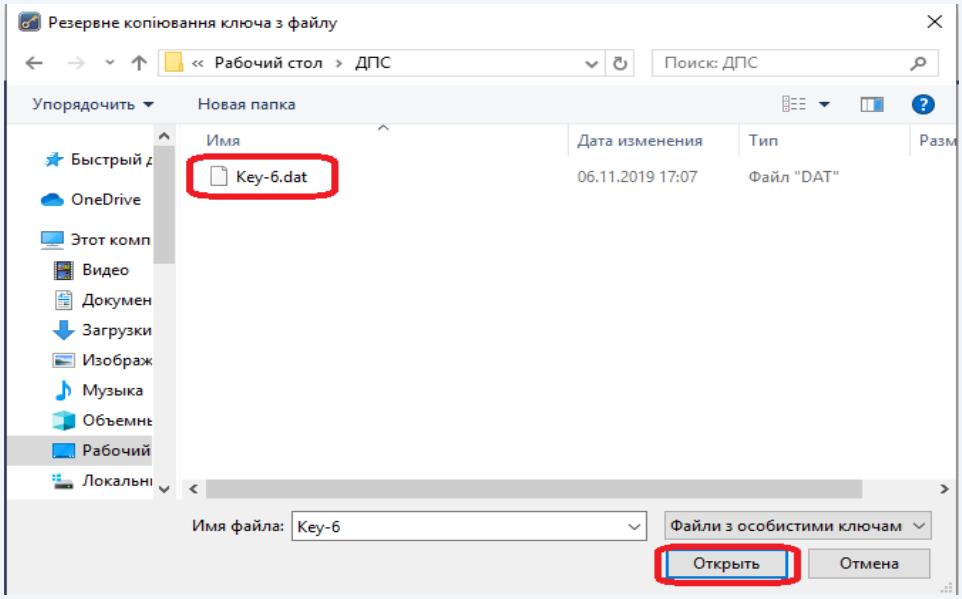


Рисунок 5.31

Після появи захищеного робочого столу необхідно обрати НКІ, на який буде записана копія особистого ключа та ввести пароль захисту особистого ключа (рис. 5.32).

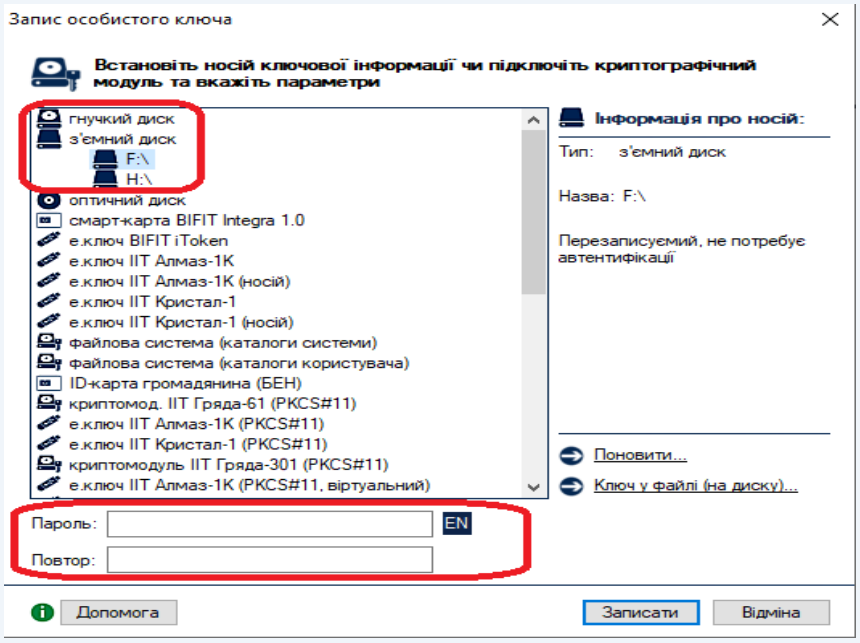


Рисунок 5.32

Після завершення резервного копіювання необхідно натиснути кнопку «ОК» (рис. 5.33).

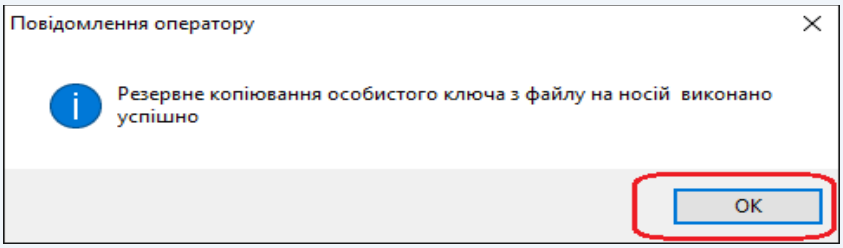


Рисунок 5.33

5.9 Експорт особистого ключа

Для експорту особистого ключа необхідно в головному вікні програми натиснути кнопку «Встановити параметри» (рис. 5.34).

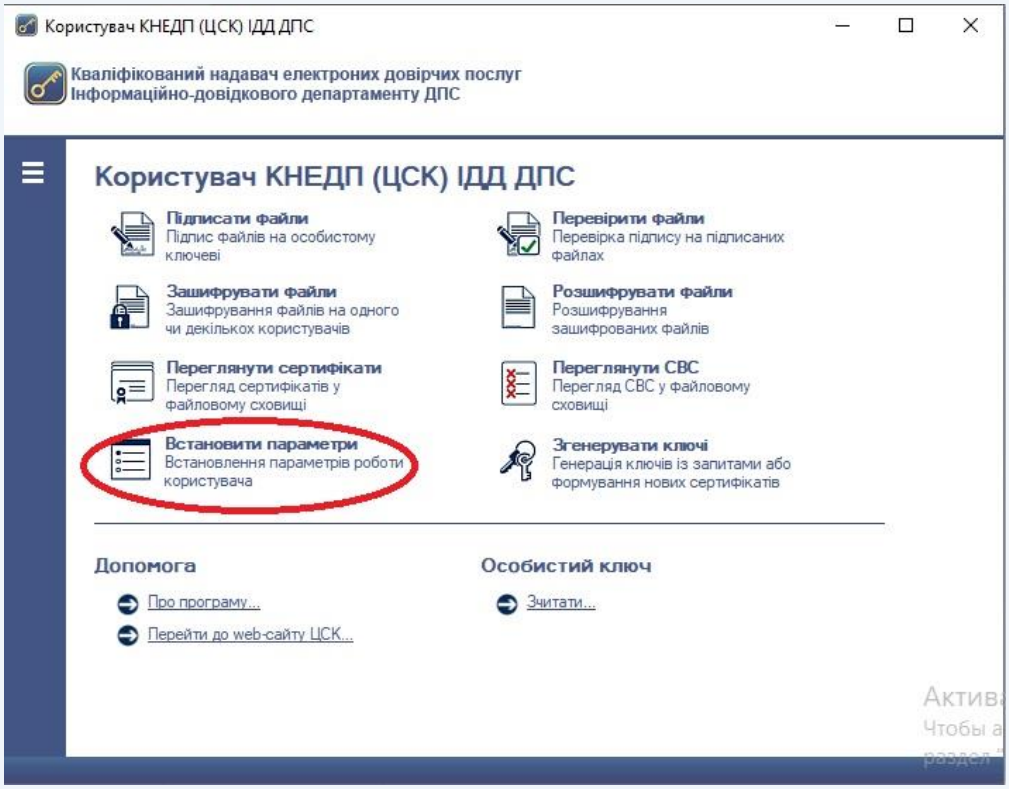


Рисунок 5.34

У наступному вікні необхідно обрати підпункт «Особистий ключ» та натиснути кнопку «Експортувати» (рис. 5.35)

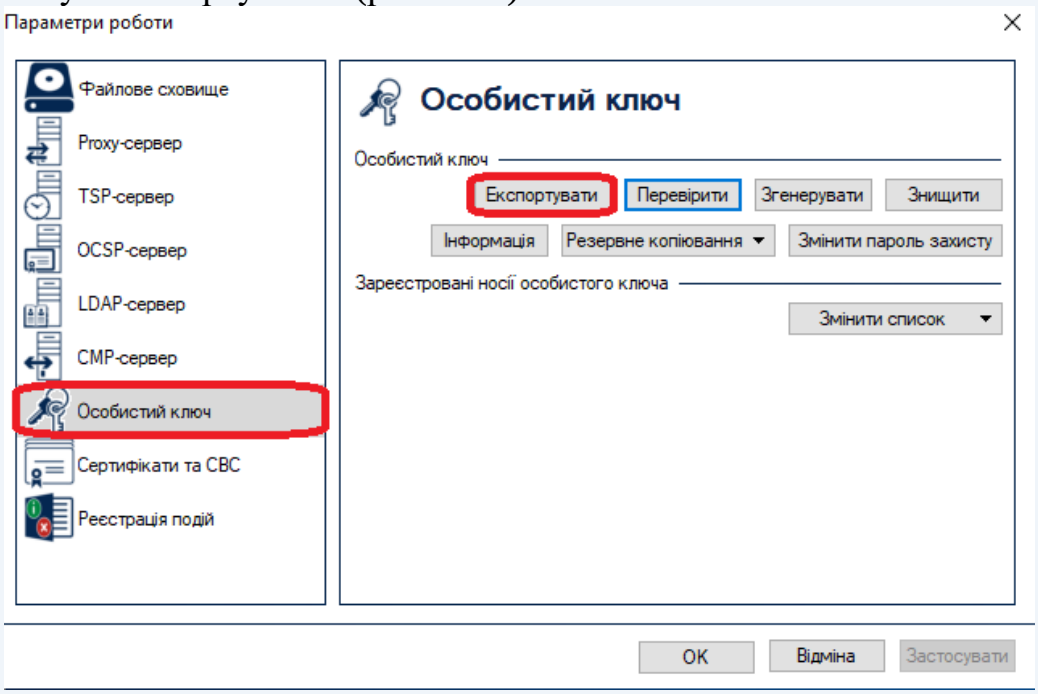


Рисунок 5.35

Під час експорту здійснюється зчитування особистого ключа (рис. 5.36)

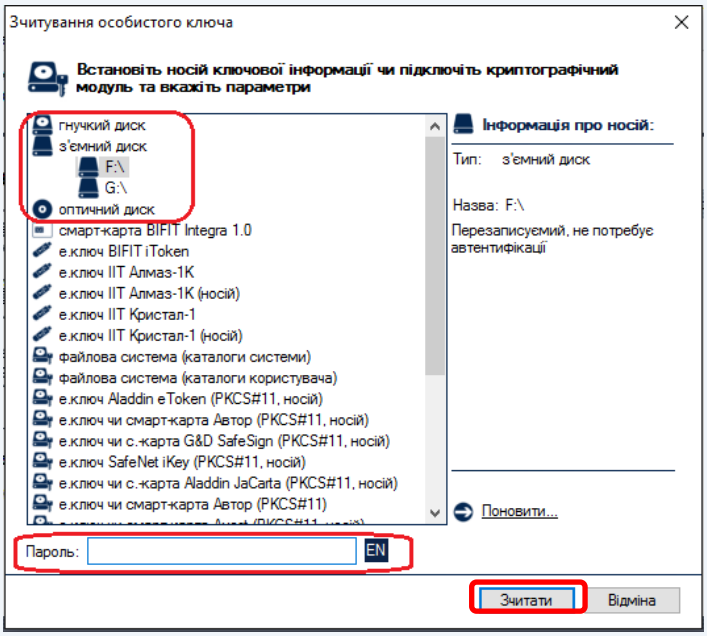


Рисунок 5.36

Після зчитування особистого ключа необхідно обрати типи особистих ключів для експорту, а також вказати параметри експорту (рис. 5.37). Підписувачу надається можливість експорту у **<u>контейнер особистих ключів і сертифікатів</u>** (*.pfx) та у **<u>контейнер особистих ключів</u>** (*.pk8)

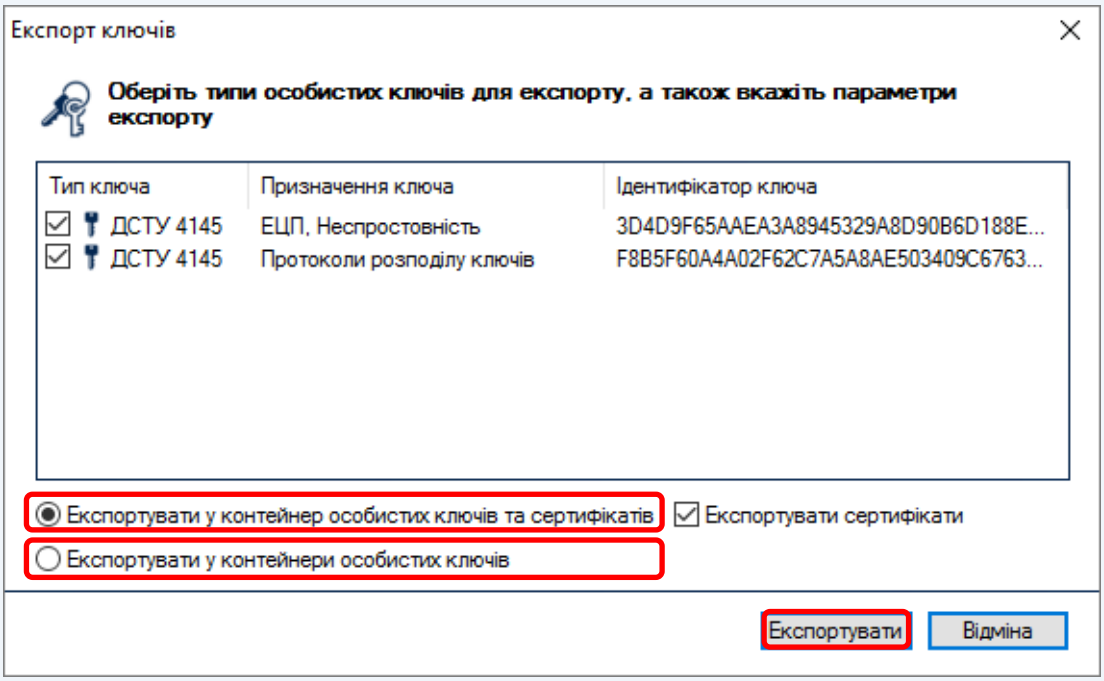


Рисунок 5.37

Після вибору параметрів експорту необхідно вказати пароль доступу до контейнеру особистих ключів (рис. 5.38), вказати назву та розміщення файлу-контейнеру особистих ключів (рис. 5.39).

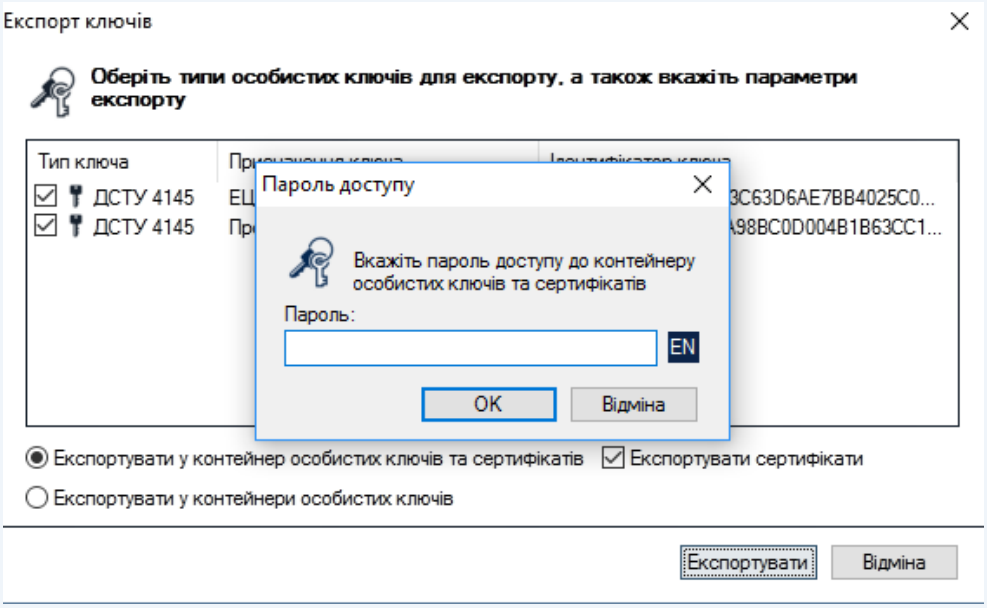


Рисунок 5.38

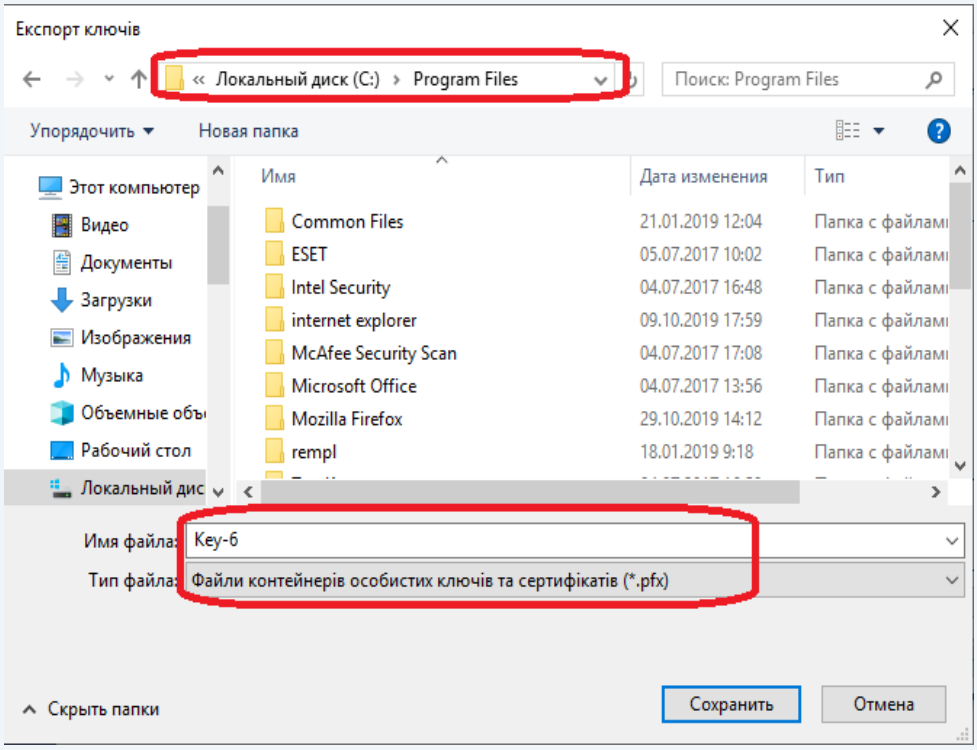


Рисунок 5.39

Увага! Пароль доступу до контейнеру особистих ключів може співпадати з паролем захисту особистого ключа, що знаходиться на носієві ключової інформації, з якого проводиться експорт.

Додатково підписувачу надається можливість вказати будь-яке розміщення та назву файлу-контейнеру особистого ключа.

5.10 Блокування власного кваліфікованого сертифіката

Під блокуванням кваліфікованого сертифіката розуміється тимчасове припинення чинності кваліфікованого сертифіката.

Після блокування кваліфікованого сертифіката, підписувач може протягом тридцяти календарних днів поновити строк чинності кваліфікованого сертифіката. Блокований кваліфікований сертифікат буде автоматично скасований Надавачем, якщо протягом зазначеного строку клієнт не поновить його чинність.

Для блокування власного кваліфікованого сертифіката у ПЗ необхідно обрати підпункт «Заблокувати власний сертифікат» в пункті меню «Сертифікати та СВС» (рис. 5.40).

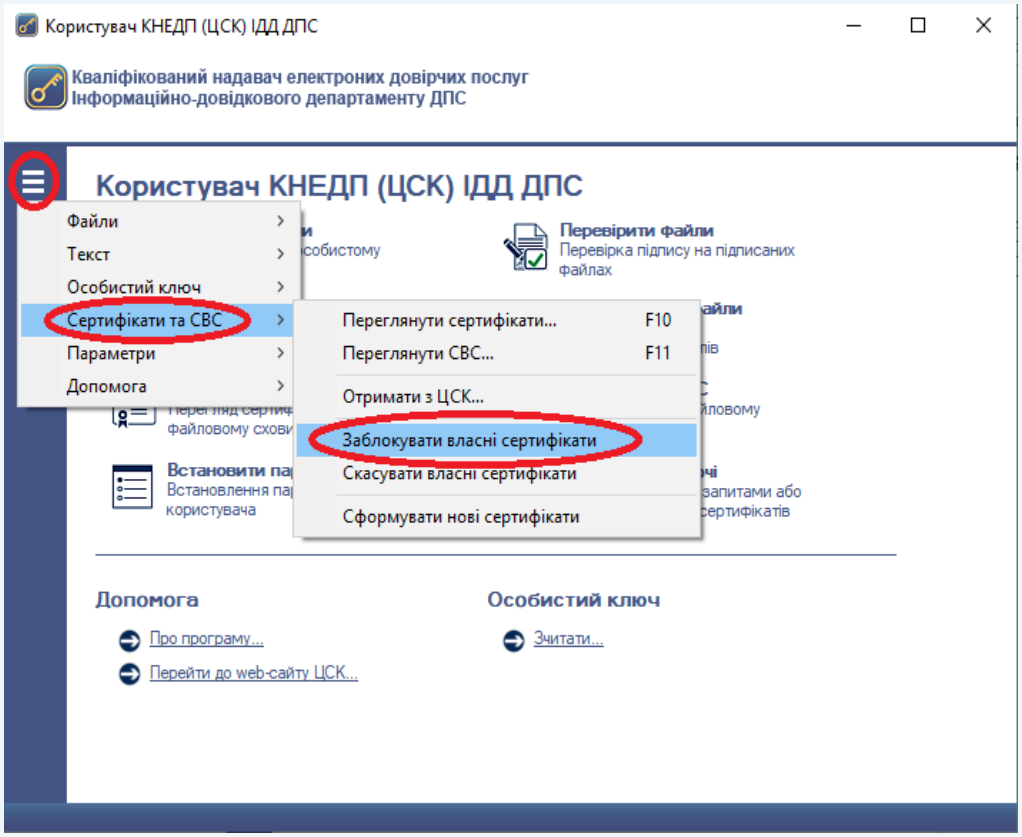


Рисунок 5.40

Далі з’являється повідомлення щодо блокування кваліфікованого сертифіката, для підтвердження блокування натискаємо кнопку «Да» (рис. 5.41).

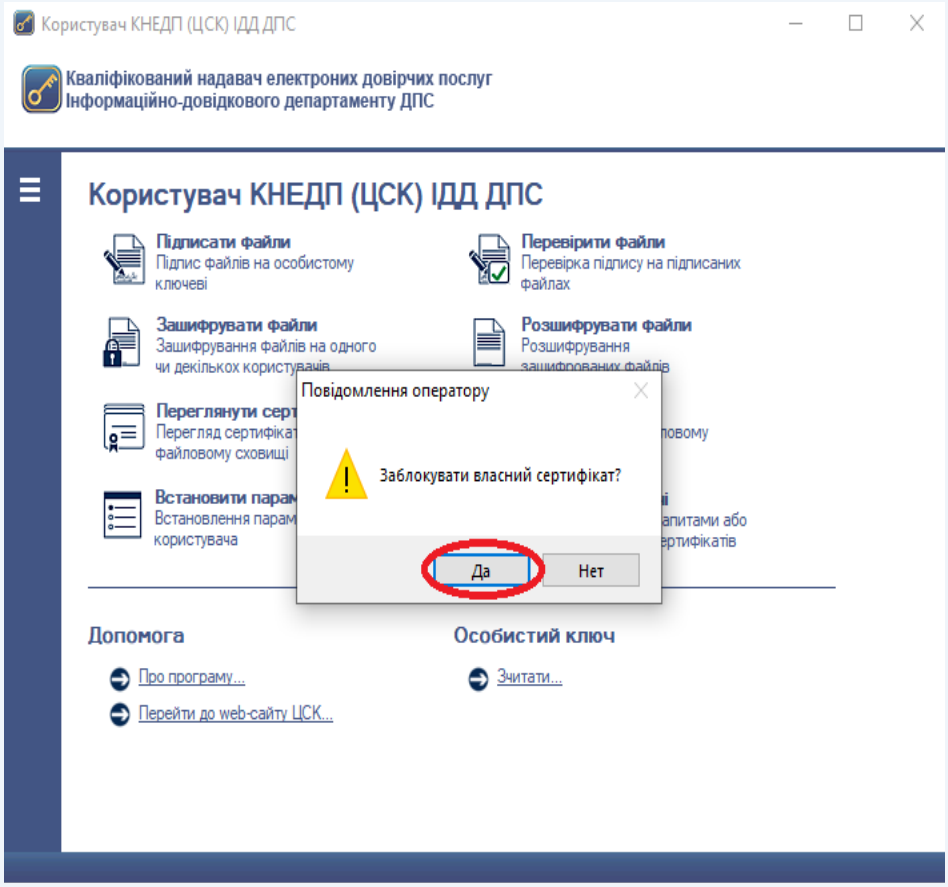


Рисунок 5.41

Після появи захищеного робочого столу необхідно обрати НКІ та ввести пароль захисту особистого ключа (рис. 5.42).

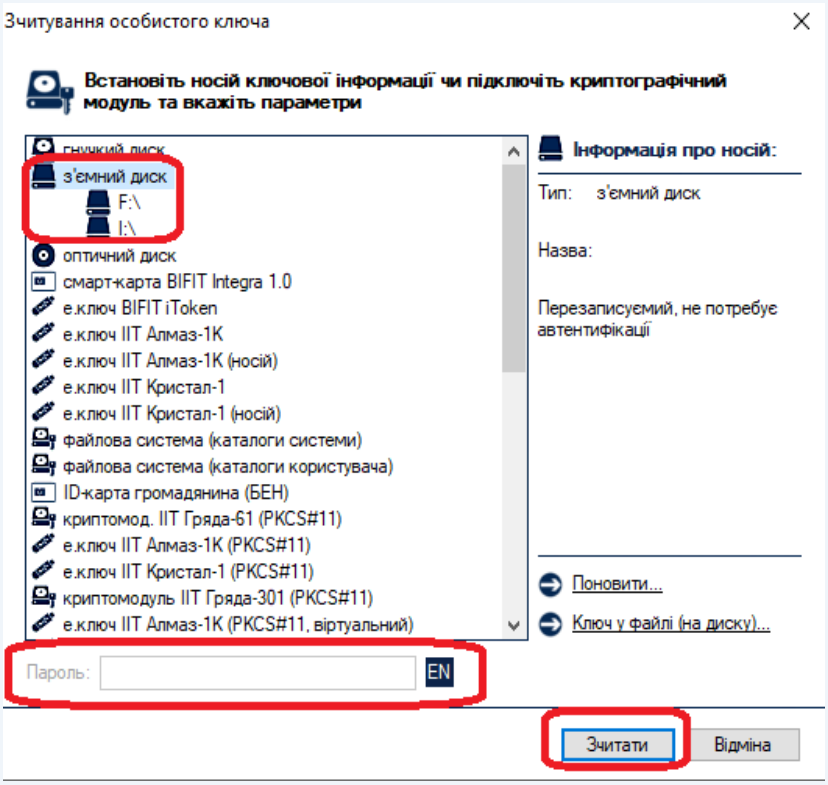


Рисунок 5.42

Після зчитування особистого ключа підписувачу необхідно підтвердити наміри щодо блокування кваліфікованого сертифіката.

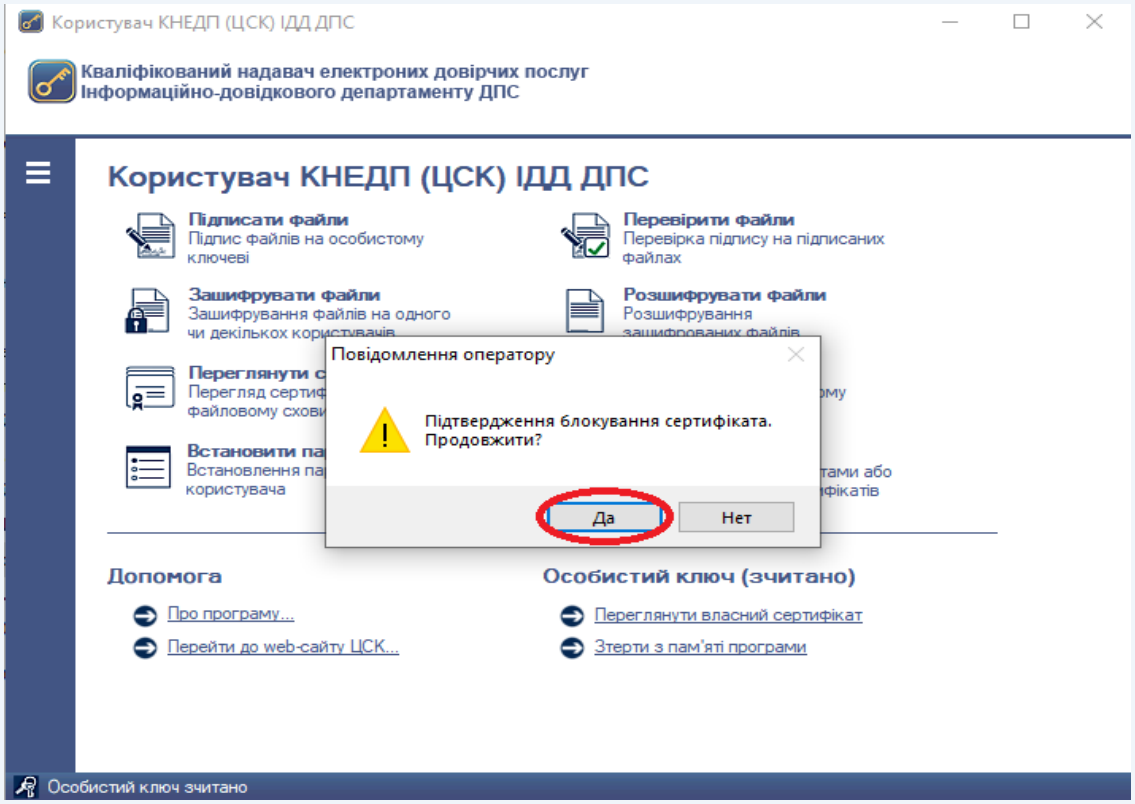


Рисунок 5.43

Після відправки запиту на блокування кваліфікованого сертифіката з’явиться вікно «Результат обробки запиту» (рис. 5.44).

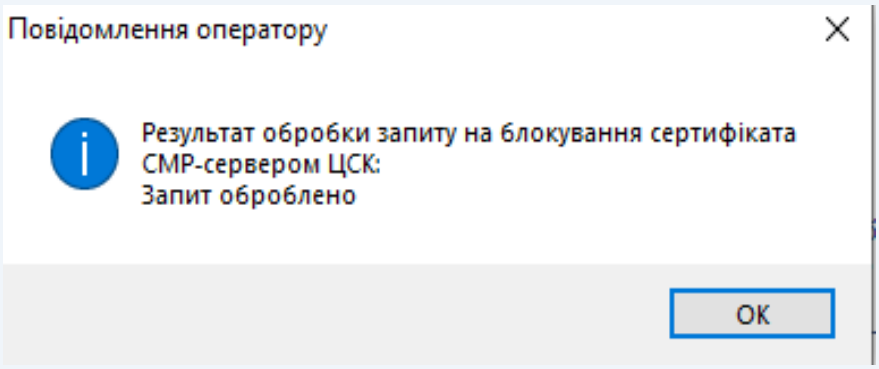


Рисунок 5.44

Поява даного вікна свідчить про успішне блокування кваліфікованого сертифіката.

5.11 Скасування власного кваліфікованого сертифіката

Скасування кваліфікованого сертифіката – це дострокове припинення чинності кваліфікованого сертифіката. Скасовані кваліфіковані сертифікати поновленню не підлягають.

Для скасування власного кваліфікованого сертифіката у ПЗ необхідно обрати підпункт «Скасувати власний сертифікат» в пункті меню «Сертифікати та СВС» (рис. 5.45).

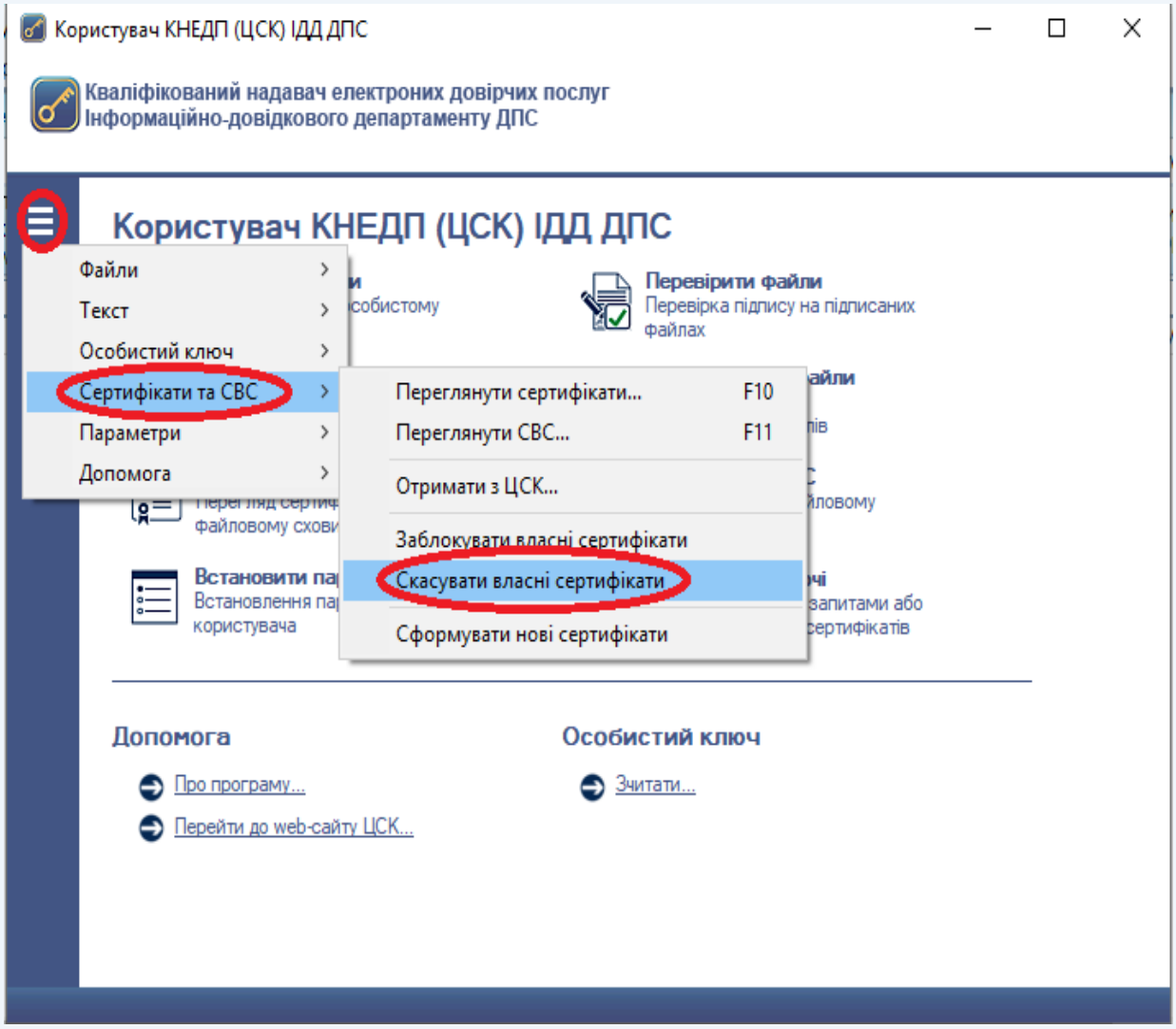


Рисунок 5.45

Далі з’являється повідомлення щодо скасування кваліфікованого сертифіката. Для підтвердження скасування натискаємо кнопку «Да» (рис. 5.46).

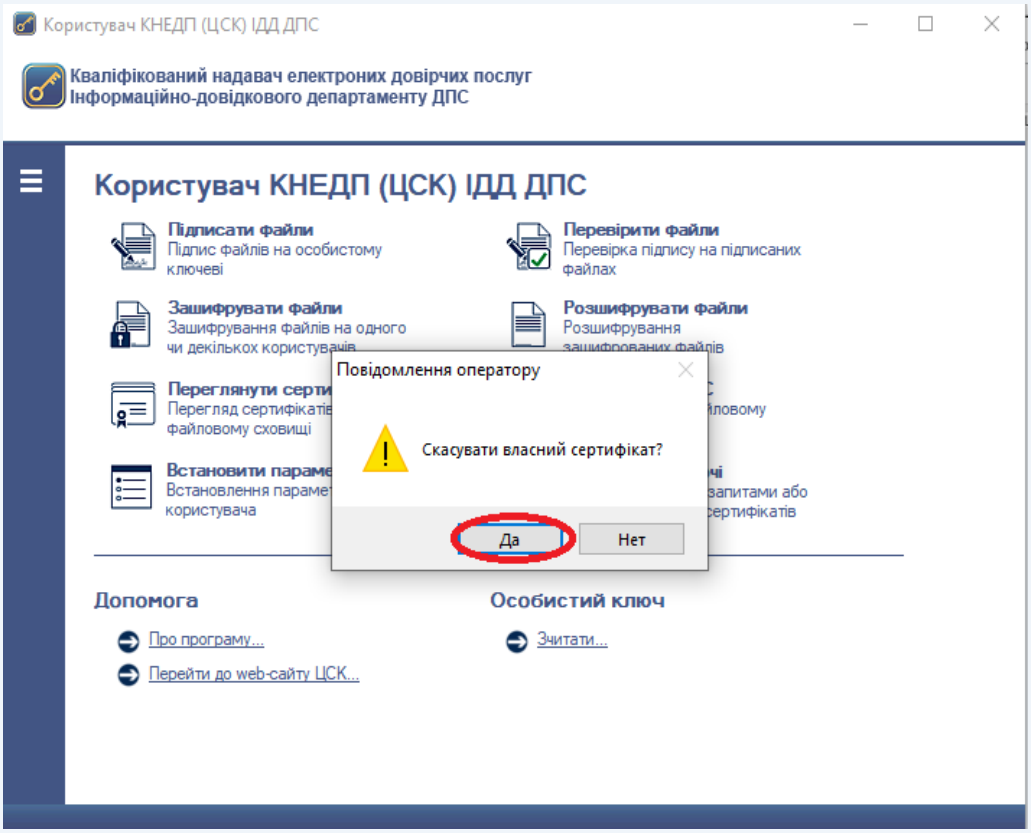


Рисунок 5.46

Після появи захищеного робочого столу необхідно обрати НКІ та ввести пароль захисту особистого ключа (рис. 5.47).

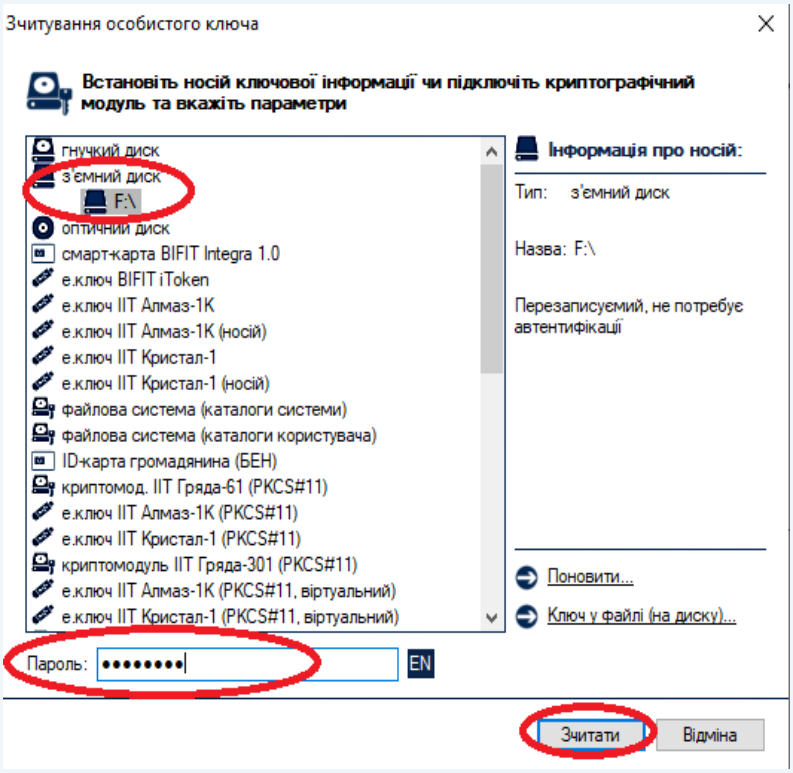


Рисунок 5.47

Після зчитування особистого ключа підписувачу необхідно підтвердити наміри щодо скасування кваліфікованого сертифіката (рис. 5.48).

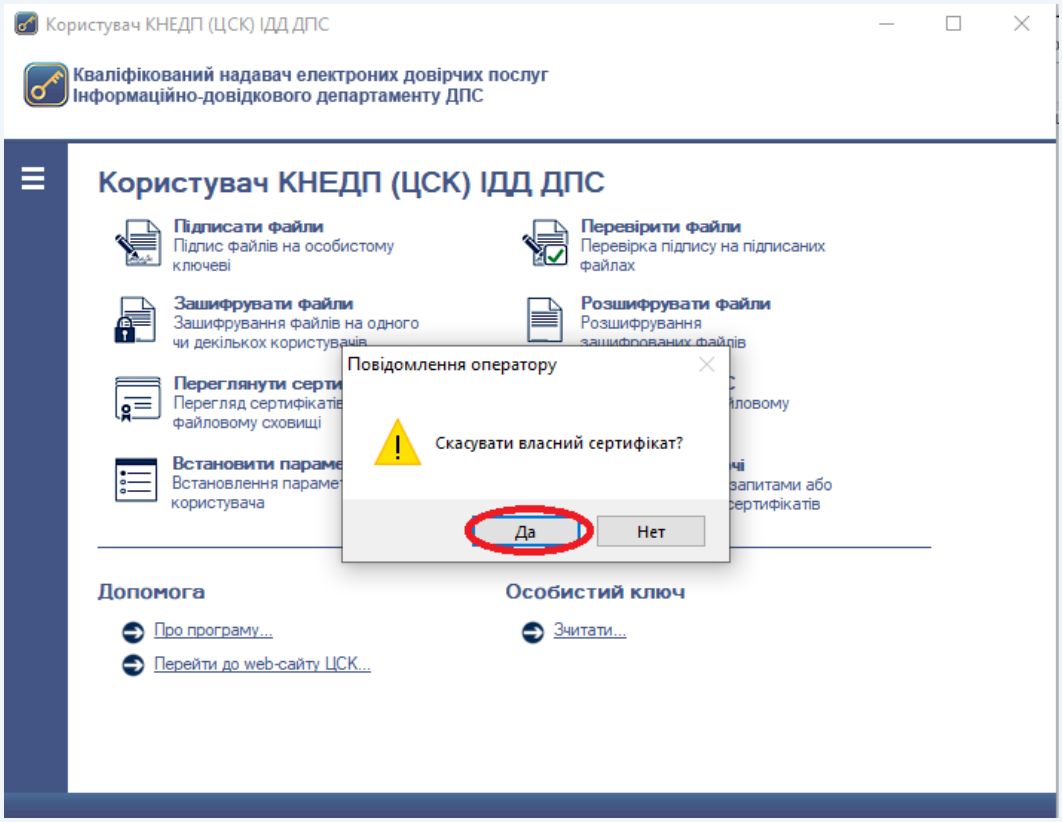


Рисунок 5.48

Після відправки запиту на скасування кваліфікованого сертифіката з’явиться вікно «Результат обробки запиту» (рис. 5.49).

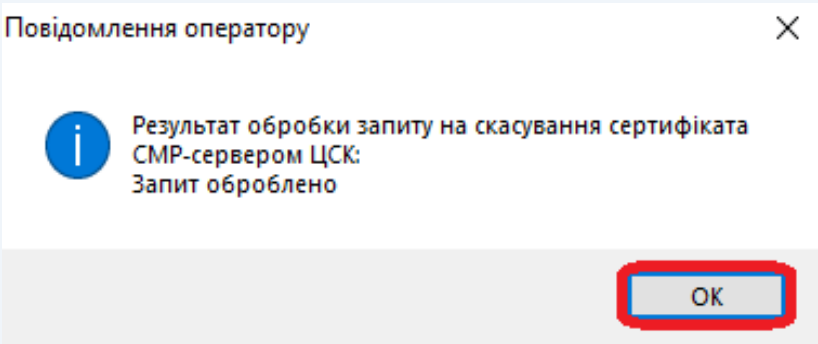


Рисунок 5.49

Поява даного вікна свідчить про успішне скасування кваліфікованого сертифіката.

5.12 Off-line режим роботи програми

Режим off-line передбачений для роботи ПЗ за відсутності доступу до мережі Internet.

В off-line режимі ПЗ не взаємодіє з ПТК Надавача, тому on-line перевірка статусу кваліфікованого сертифіката та позначка часу будуть недоступні.

Для перевірки статусу кваліфікованих сертифікатів в off-line режимі необхідно використовувати СВС. Для цього необхідно виконати завантаження СВС (більш детально див. п. 4.6) та в налаштуваннях ПЗ увімкнути параметр «Перевіряти СВС» (рис. 5.50).

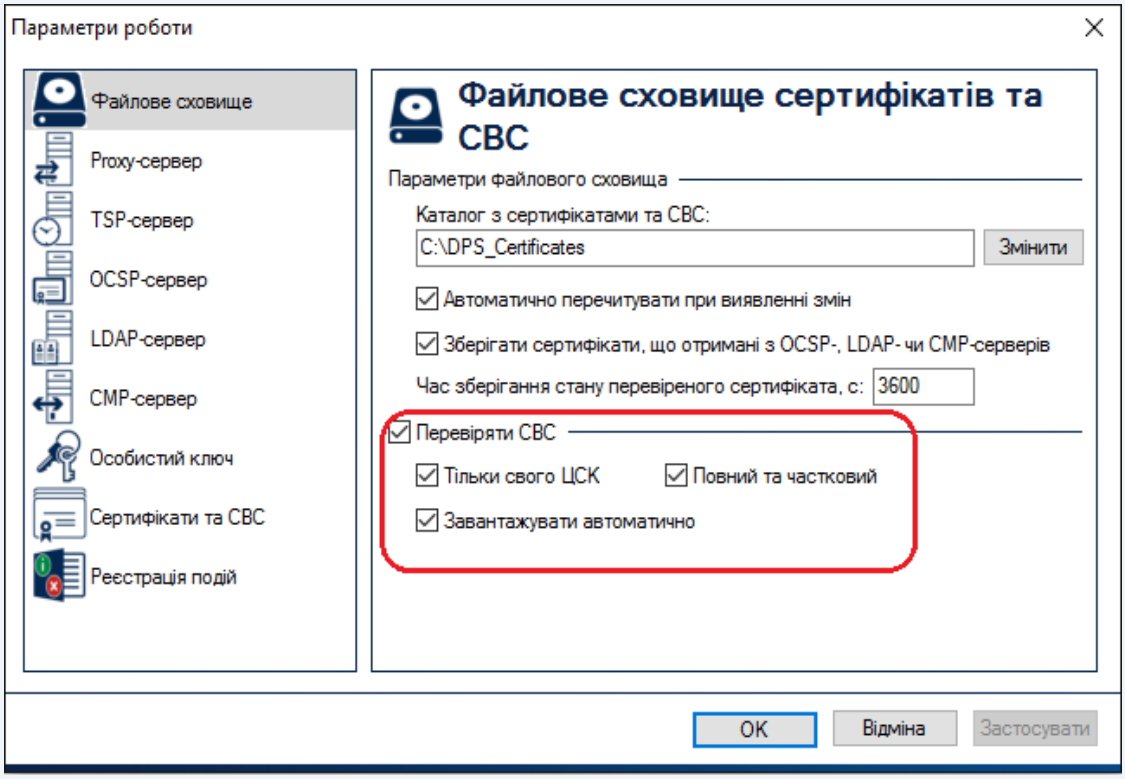


Рисунок 5.50

Для переходу в режим off-line необхідно обрати підпункт «Перейти в режим off-line (не взаємодіяти з ЦСК)» в пункті меню «Параметри» або натиснути **Ctrl+O** (рис. 5.51-5.53).

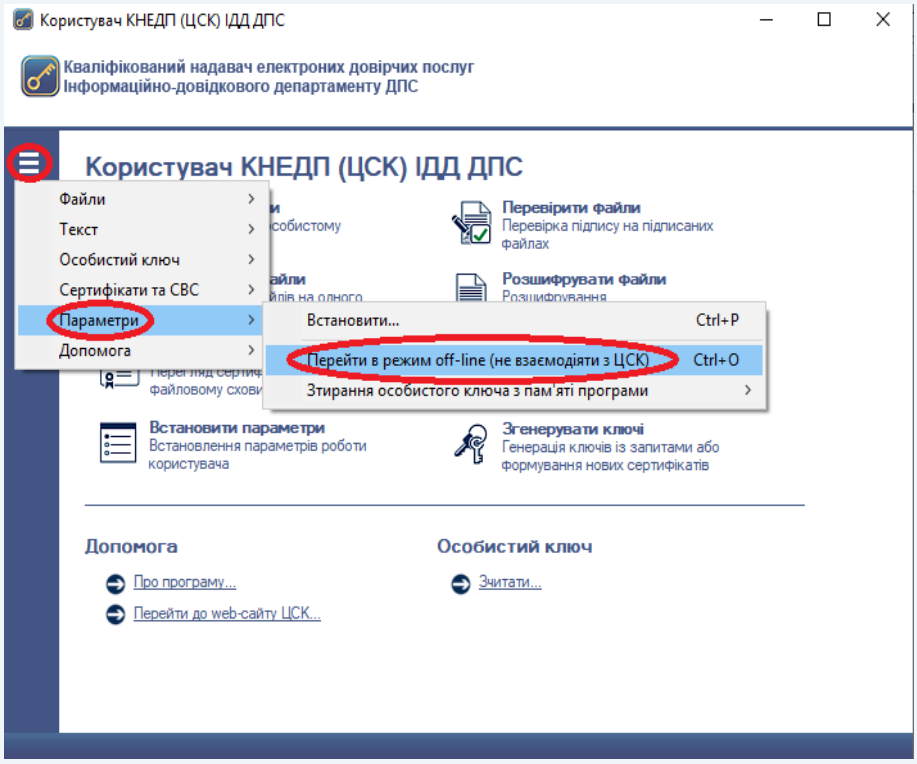


Рисунок 5.51

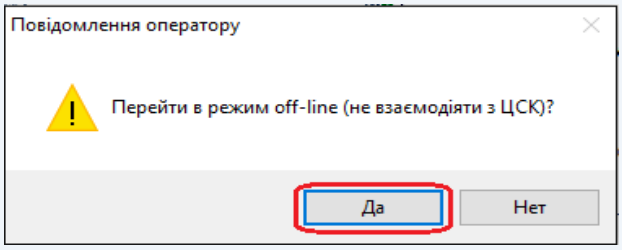


Рисунок 5.52

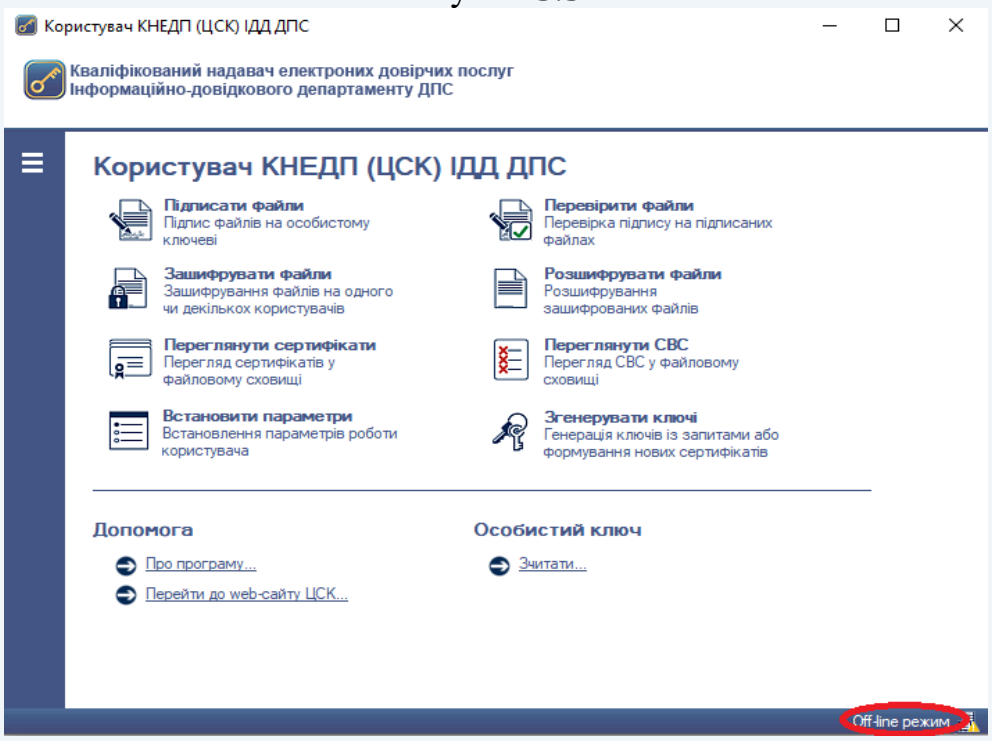


Рисунок 5.53

6. Повторне (дистанційне) формування сертифікатів за електронним запитом

Сформувати нові сертифікати за допомогою електронного запиту можуть діючі клієнти Надавача, реєстраційні дані яких не змінилися.

Увага! Якщо особистий ключ пошкоджено або втрачено пароль захисту до нього, сформувати новий сертифікат за допомогою електронного запиту неможливо.

Після формування нових сертифікатів, старі автоматично скасовуються.

Для формування нових сертифікатів необхідно обрати у головному вікні ПЗ кнопку «Згенерувати ключі», після чого з'явиться вікно «Повідомлення оператору», в якому необхідно обрати пункт «Сформувати нові сертифікати у ЦСК на основі наявних діючих ключів» та додатково підтверджуємо формування, натиснувши на кнопку «да» (рис. 6.1-6.2).

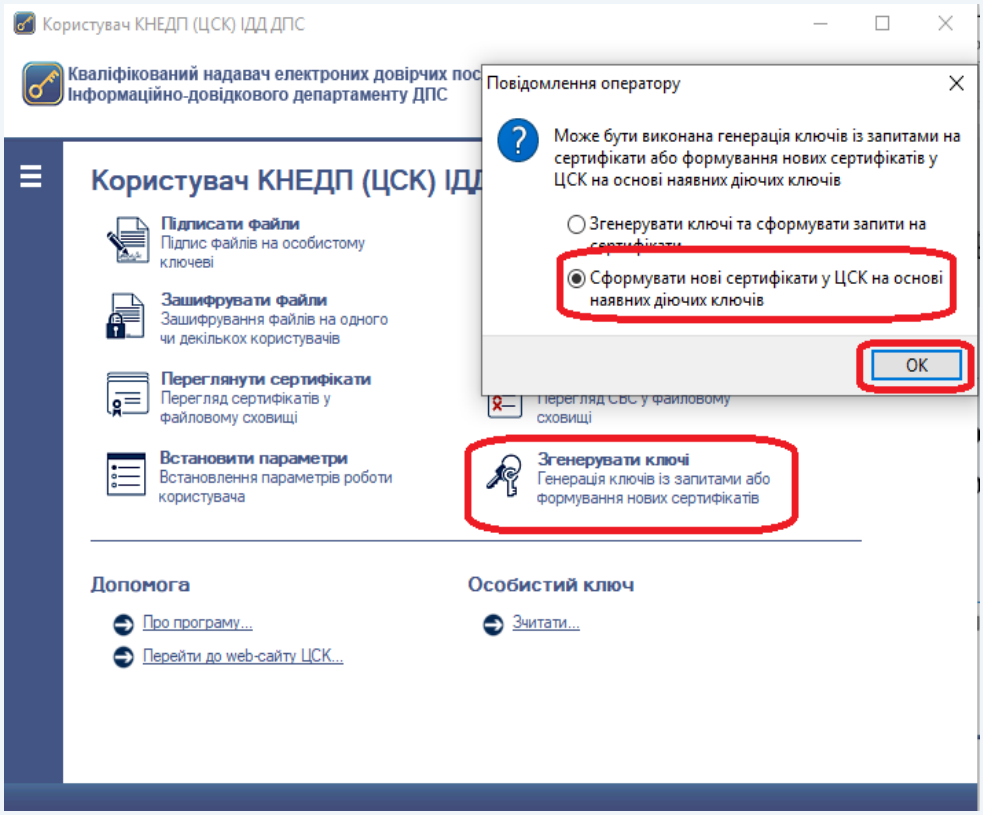


Рисунок 6.1

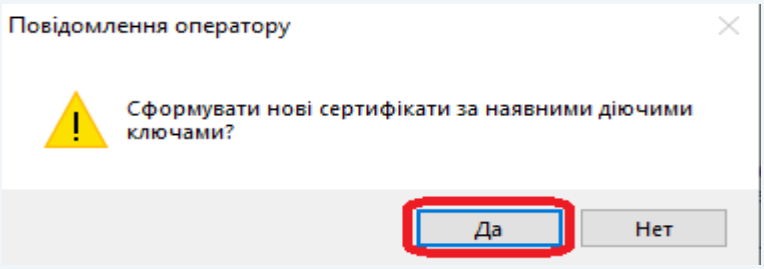


Рисунок 6.2

Після появи захищеного робочого столу необхідно обрати з'ємний НКІ, на якому записаний діючий особистий ключ, та ввести пароль захисту особистого ключа (рис. 6.3).

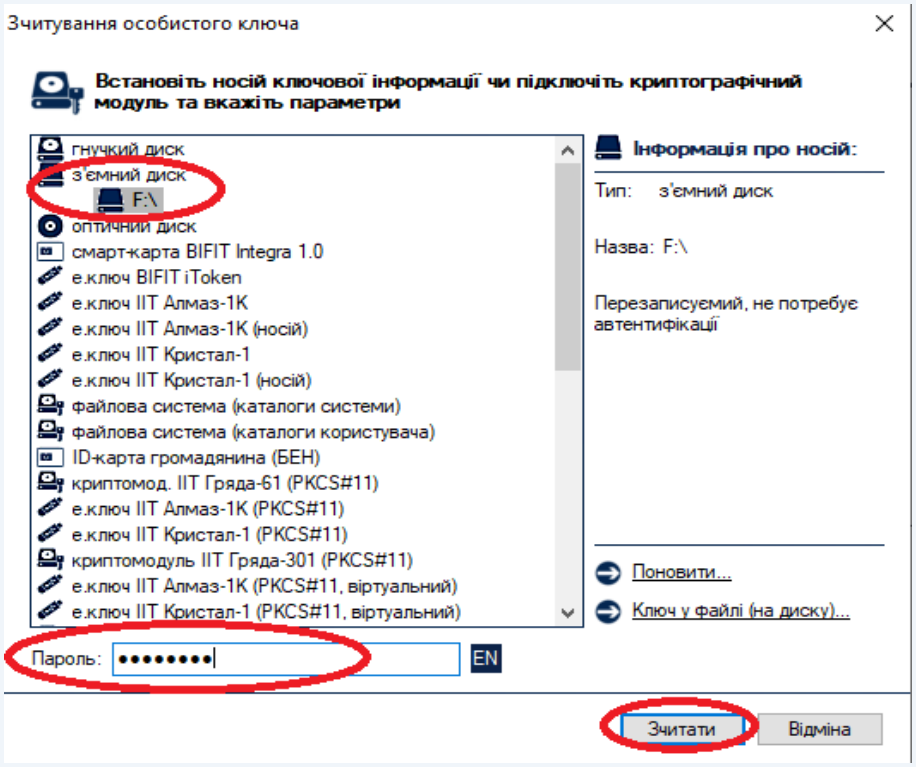


Рисунок 6.3

Після зчитування особистого ключа відкриється вікно «Формування нових сертифікатів», в якому необхідно ознайомитись з Договором приєднання до послуг Надавача. Для цього натискаємо посилання «Переглянути» (рис. 6.4).

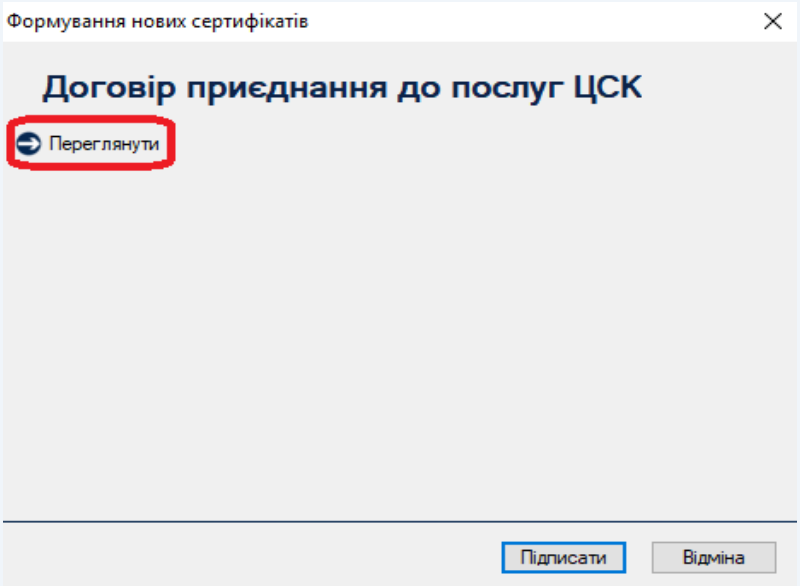


Рисунок 6.4

Для прийняття умов Договору приєднання до послуг Надавача необхідно натиснути «Підписати» (рис. 6.5).

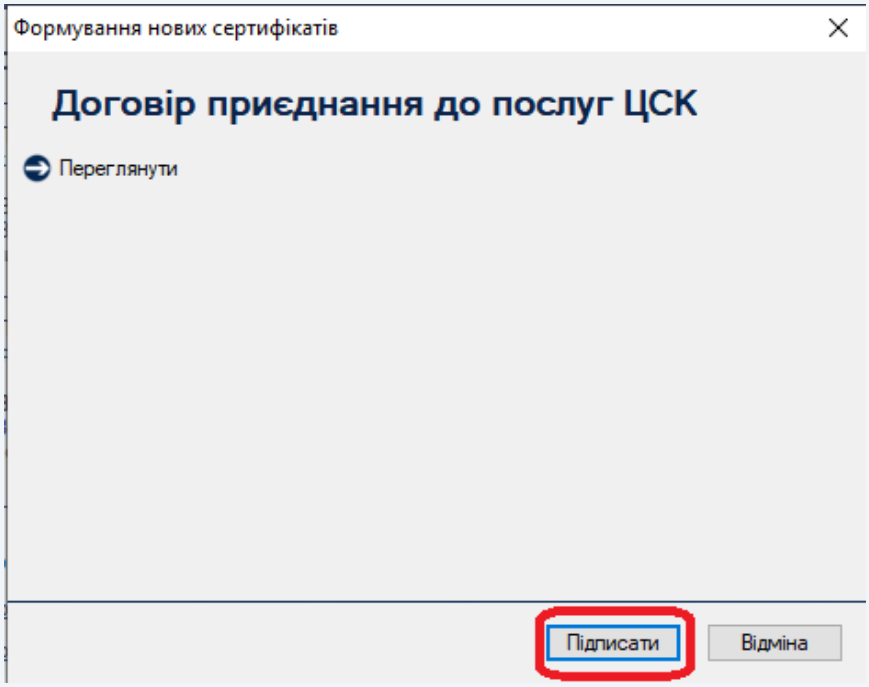


Рисунок 6.5

Після підписання Договору у вікні «Реєстраційні дані» необхідно ознайомитись з даними, які будуть внесені до нового сертифікату. Для цього натискаємо посилання «Переглянути» (рис. 6.6 – 6.7).

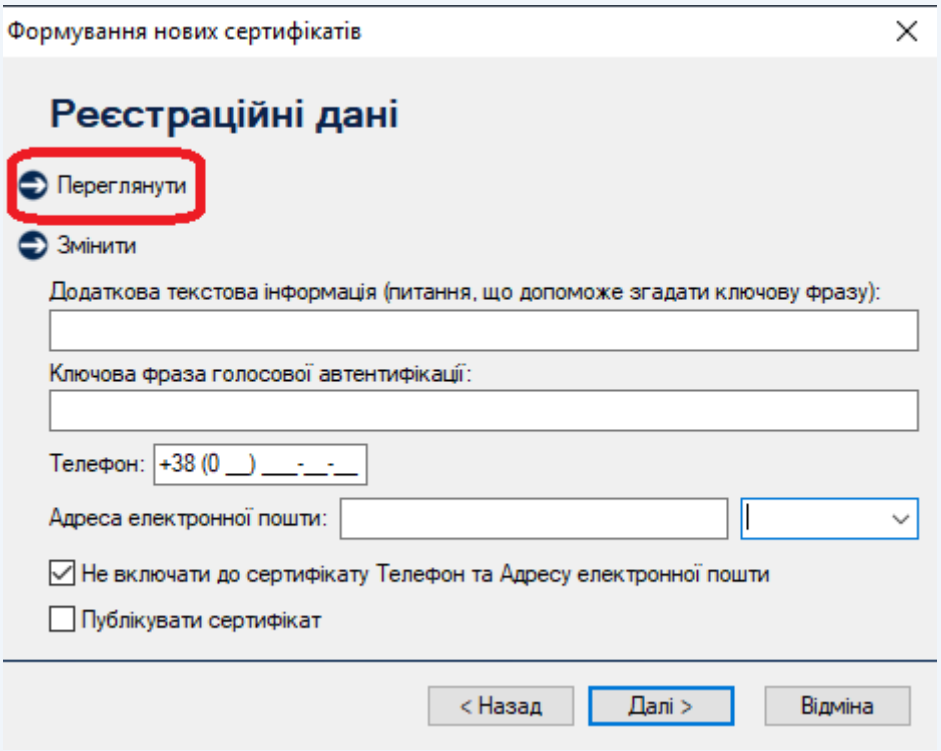


Рисунок 6.6

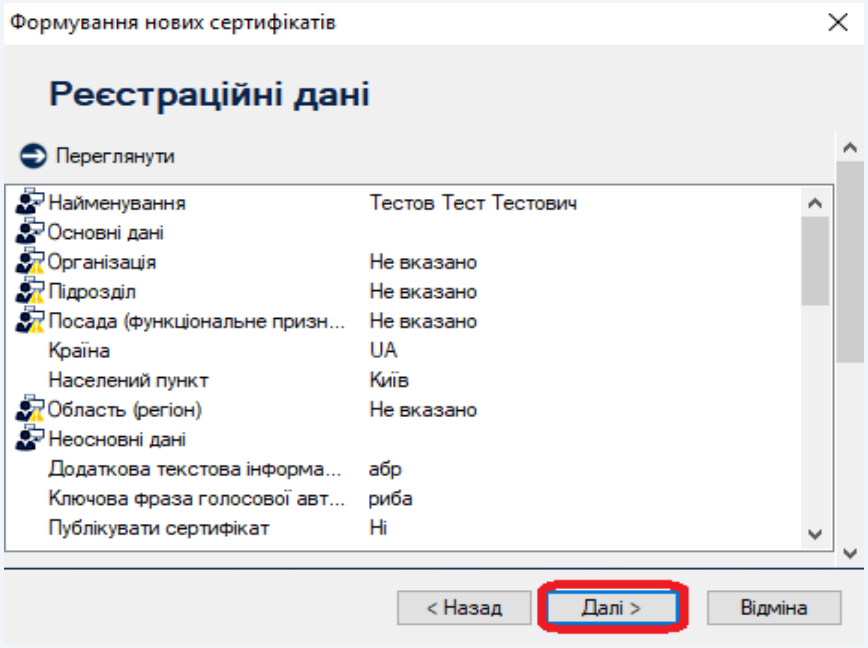


Рисунок 6.7

Увага! У разі невідповідності реєстраційних даних або наявності змін, необхідно скасувати власний сертифікат та звернутися до відокремленого пункту реєстрації користувачів Надавача для формування нових сертифікатів.

Додатково у вікні «Реєстраційні дані» є можливість змінити ключову фразу голосової автентифікації, питання, що допоможе згадати ключову фразу голосової автентифікації, телефон та адресу електронної пошти. Також надано можливість не включати або включати до сертифікату номер телефону, адресу електронної пошти та погодитись або відмовитись від публікації сертифіката на вебсайті Надавача (рис. 6.8).

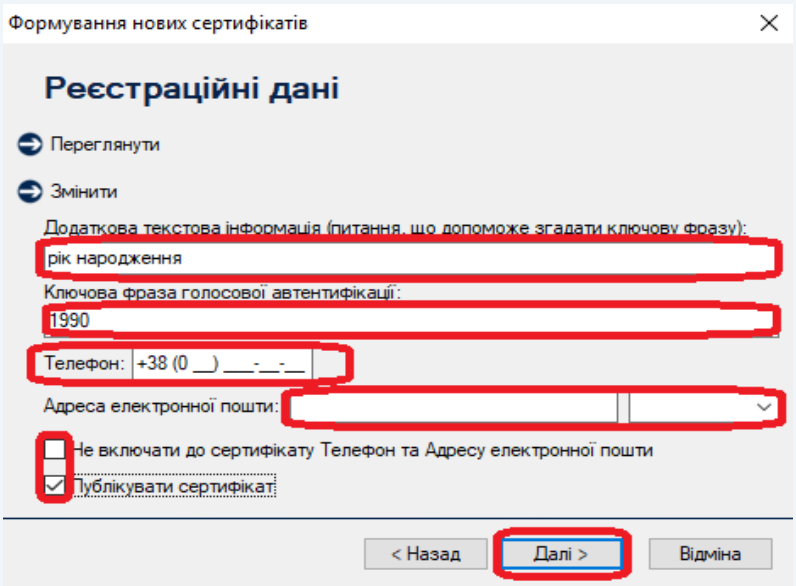


Рисунок 6.8

Після перевірки та, за необхідності, зміни даних необхідно натиснути «Далі» та обрати носій для генерації нових ключів (рис. 6.9).

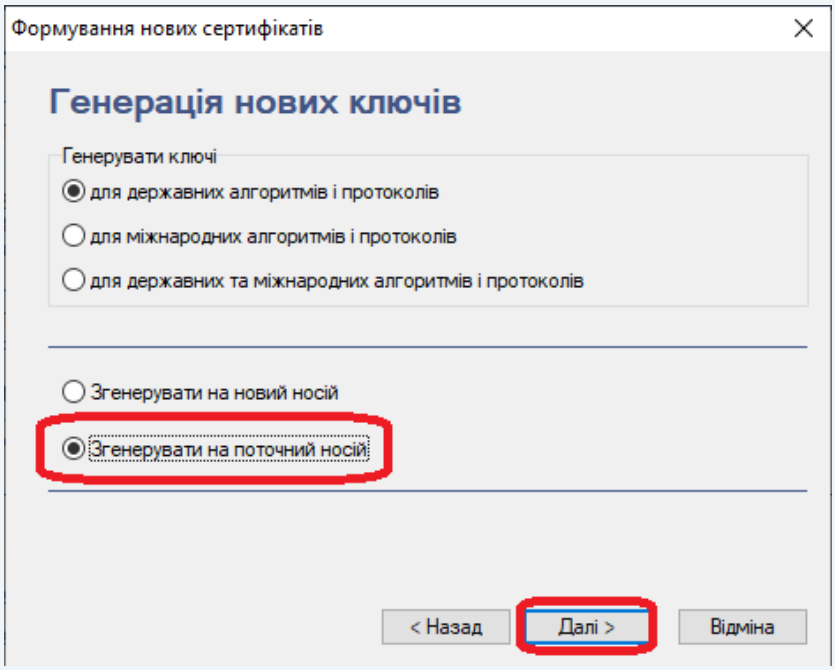


Рисунок 6.9

У наступному вікні необхідно залишити позначку навпроти «Використовувати окремий ключ для протоколу розподілу» та натиснути «Далі» (рис.6.10).

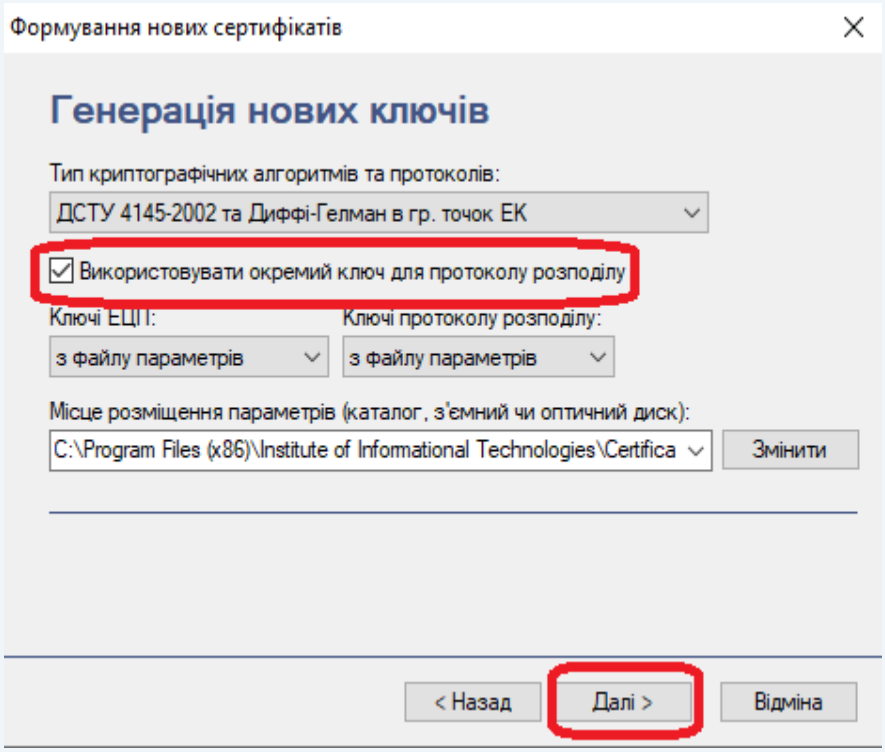


Рисунок 6.10

Після появи «Захищеного меню генерації особистого ключа» необхідно ввести пароль доступу до нового особистого ключа, підтвердити його та натиснути «ОК» (рис. 6.11).

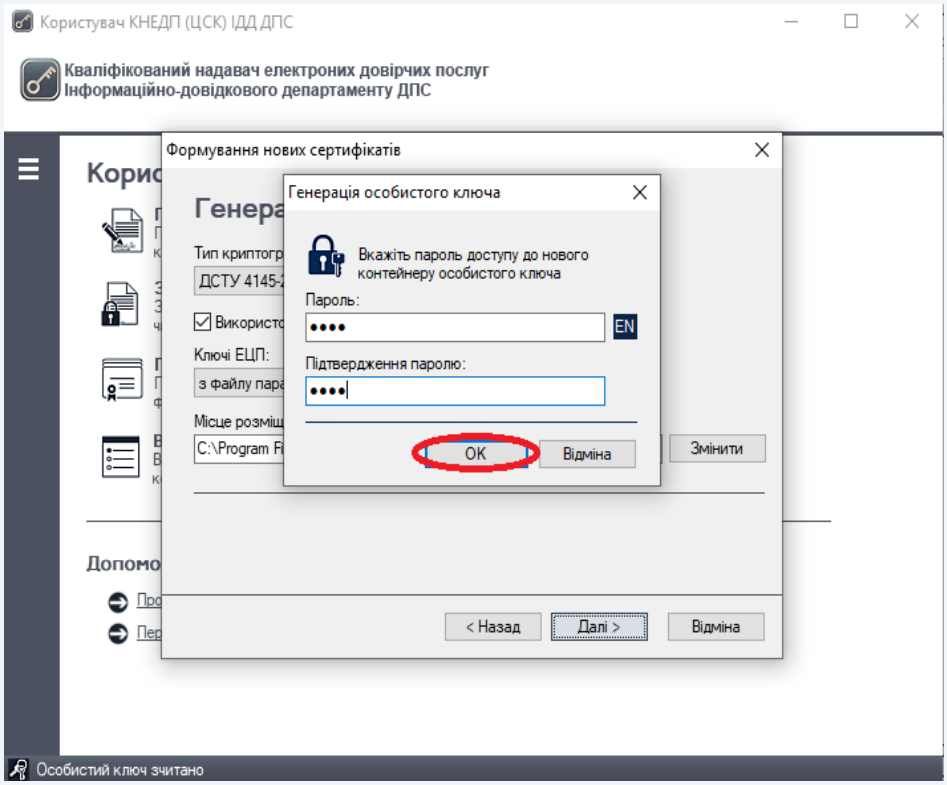


Рисунок 6.11

У вікні «Отримані нові сертифікати», після ознайомлення з інформацією необхідно натиснути «ОК» (рис. 6.12).

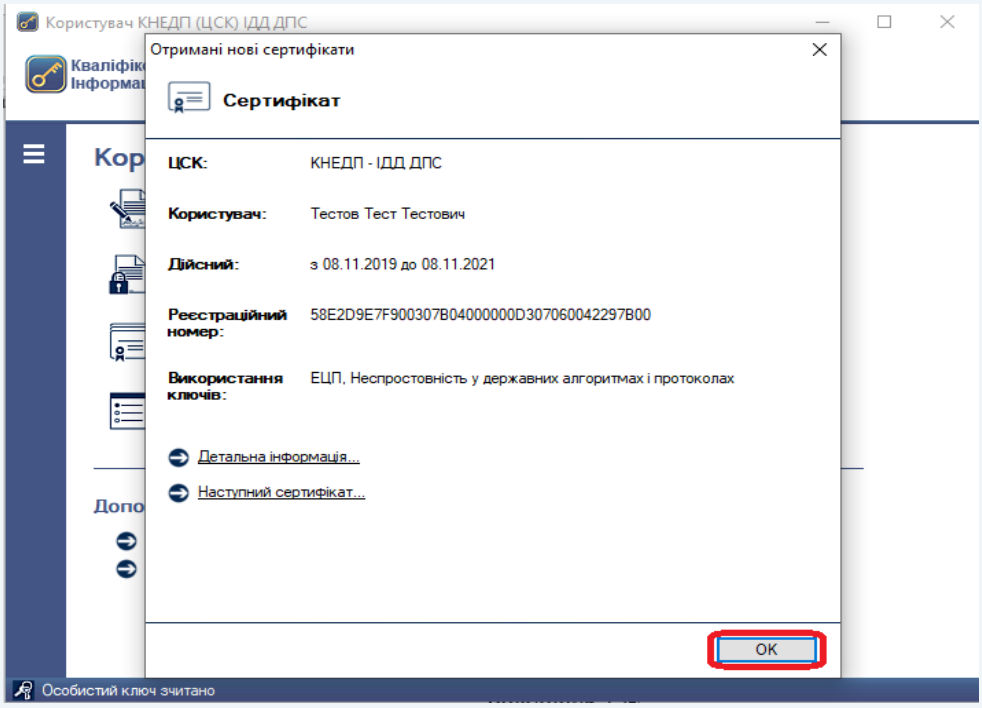


Рисунок 6.12

Натисканням відповідної кнопки (рис. 6.13) завершуємо формування нових сертифікатів за допомогою електронного запиту.

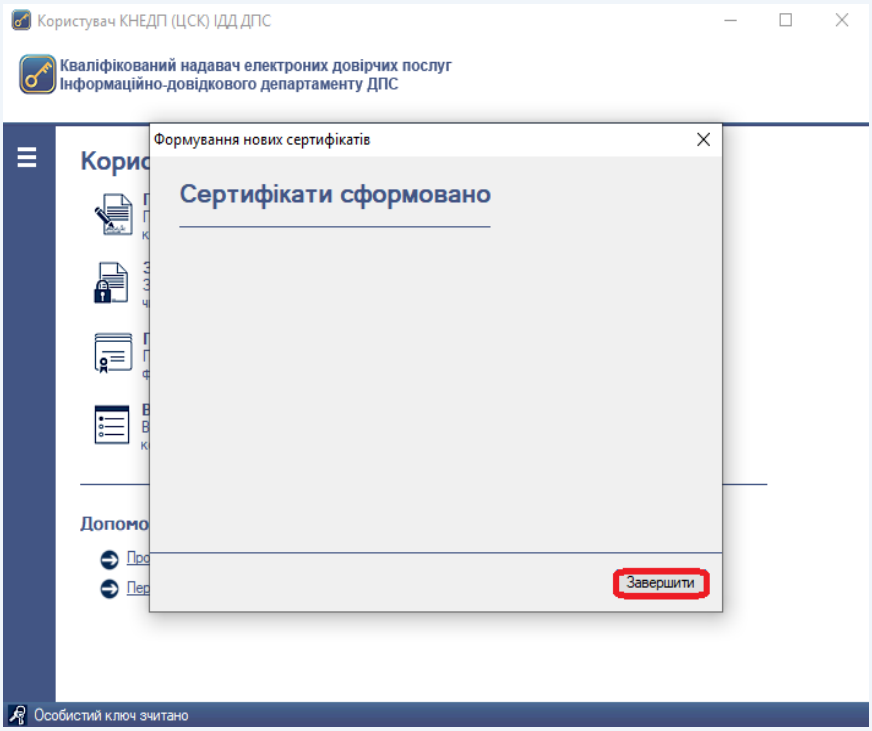


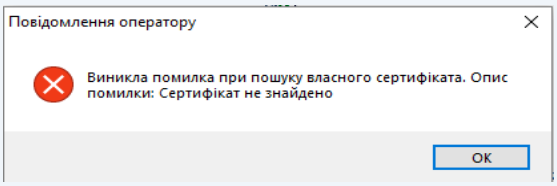
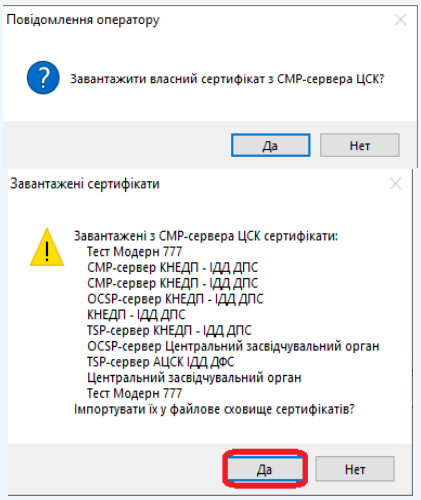
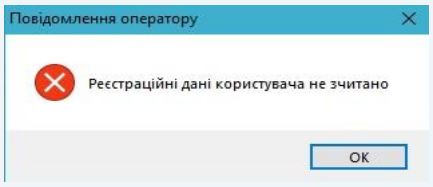
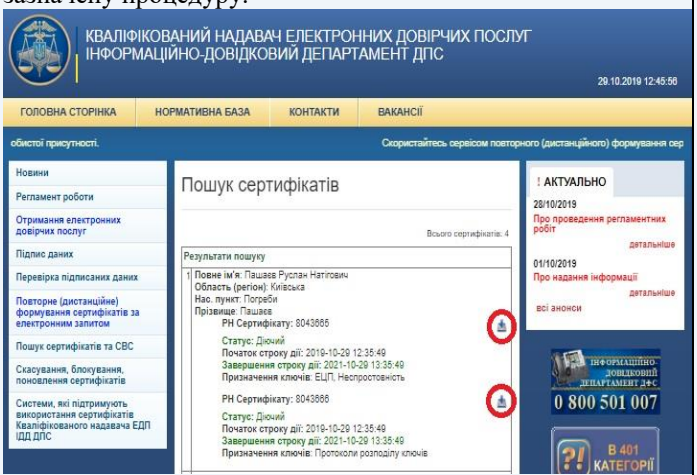
Рисунок 6.13

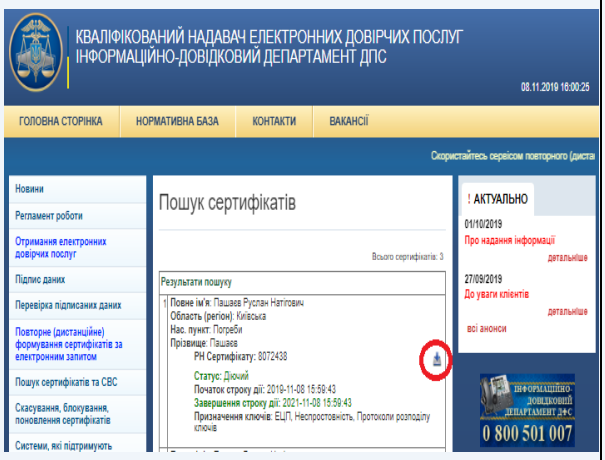
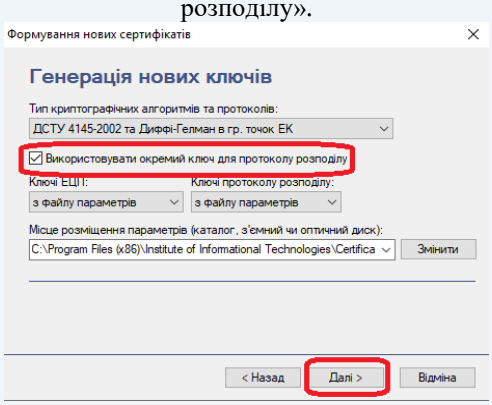
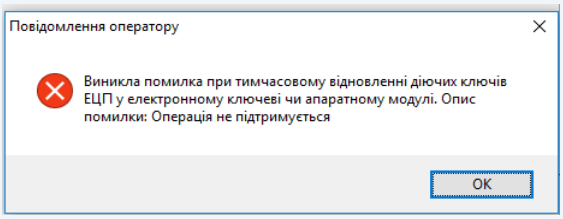
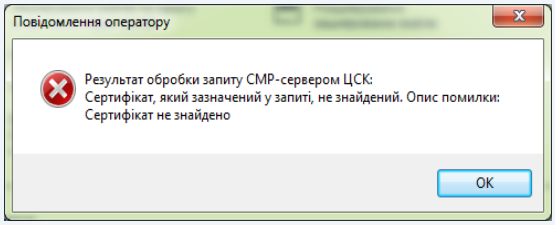
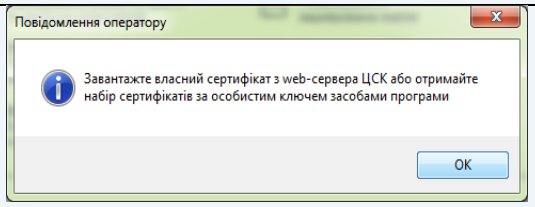
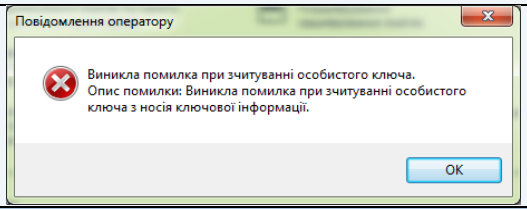
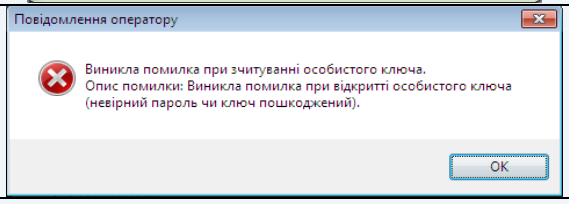
7. Заходи щодо забезпечення режиму безпеки

Для безпечного використання особистого ключа підписувач повинен:

- зберігати особистий ключ у таємниці та у спосіб, що не унеможливлює ознайомлення з ним інших осіб. Наприклад, використовувати захищений НКІ або інший з'ємний носій, який не містить іншої інформації, окрім особистого ключа, та зберігати його у сейфі (не передавати особистий ключ іншим особам);
- не розголошувати (не повідомляти) іншим особам пароль захисту особистого ключа та/або ключову фразу голосової автентифікації;
- негайно інформувати Надавача про факт компрометації особистого ключа та не використовувати особистий ключ у разі його компрометації;
- використовувати та своєчасно оновлювати програмне забезпечення антивірусного захисту інформації.

8. Можливі помилки та шляхи їх вирішення

№ з/п	Помилка	Метод усунення
1		Якщо під час процедури повторного формування сертифікатів, виникає зазначена помилка необхідно натиснути кнопку «ОК». Після чого буде запропоновано здійснити автоматичне завантаження необхідних сертифікатів до файлового сховища. 
2		Зазначена помилка виникає у двох випадках: 1. У файловому сховищу ПК відсутні сертифікати. Для вирішення помилки необхідно завантажити на комп'ютер у файлове сховище **два сертифіката** з офіційного інформаційного ресурсу Надавача у розділі «Пошук сертифікатів та СВС» (https://acskidd.gov.ua/certificates-search) та повторити зазначену процедуру. 

№ з/п	Помилка	Метод усунення
3		Якщо після процедури повторного формування сертифікатів, сформувався лише один сертифікат, необхідно переформувати сертифікати. Під час формування нових сертифікатів, обов'язково поставити галочку «Використовувати окремий ключ для протоколу розподілу». 
4		1. Для вирішення зазначеної помилки необхідно файл «Key-6.dat» з папки перемістити в кореневий каталог та повторити зазначену процедуру. 2. Помилка виникає, при генерації нового особистого ключа на носій «CD-R диск», на якому вже записаний особистий ключ. Необхідно провести генерацію на новий носій.
5		 Для вирішення зазначеної помилки необхідно завантажити на комп'ютер у файлове сховище два сертифіката з офіційного інформаційного ресурсу Надавача у розділі «Пошук сертифікатів та СВС» (https://acskidd.gov.ua/certificates-search). Якщо після цього помилка повторюється, потрібно підготувати новий пакет документів для повторної реєстрації.
6		Перевірити, чи знаходиться особистий ключ «Key-6.dat» в корневому каталозі, як що ні, то скопіювати його в корневий каталог.
7		Необхідно переконатись в тому, що під час введення паролю до особистого ключа на комп'ютері увімкнена англійська розкладка клавіатури. Також має значення регістр (великі або маленькі літери), вкл./відкл. NumLock.