Державне підприємство «Національні інформаційні системи»

Кваліфікований надавач електронних довірчих послуг
"АЦСК органів юстиції України"

Надійний засіб електронного цифрового підпису
«ІІТ Користувач ЦСК-1»

НАСТАНОВА ОПЕРАТОРА

Київ 2019

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

КЕП	-	Кваліфікований електронний підпис;
ЗКЕПП	-	Засіб кваліфікованого електронного підпису чи печатки;
ЗНОК	-	Захищений носій особистих ключів;
НОК	-	Носій особистих ключів;
ПК	-	Персональний комп’ютер;
ПЗ	-	Програмне забезпечення «ІІТ Користувач ЦСК-1»;
СВС	-	Список відкликаних сертифікатів;
АЦСК	-	Кваліфікований надавач електронних довірчих послуг "АЦСК органів юстиції України";
CMP	-	Certificate Management Protocol (протокол управління обслуговуванням сертифікатів);
LDAP	-	Lightweight Directory Access Protocol (протокол доступу до каталогу);
OCSP	-	On-line Certificate Status Protocol (протокол визначення статусу сертифіката);
TSP	-	Time Stamp Protocol (протокол фіксування часу);
вебсайт	-	Офіційний інформаційний ресурс АЦСК (https://ca.informjust.ua);
файлове сховище	-	Каталог (папка), призначений для зберігання посилених сертифікатів та СВС.

Призначення програми

ПЗ «ІІТ Користувач ЦСК-1» є надійним ЗКЕПП та призначене для застосування на ПК користувача/підписувача АЦСК і виконує наступні функції:

- **управління ключами користувача:**
  - генерацію ключів користувача АЦСК, запис особистого ключа на ЗНОК/ НОК та формування запита на формування сертифіката;
  - резервне копіювання особистого ключа з одного НОК на інший;
  - зміну паролю захисту особистого ключа;
  - знищення особистого ключа на ЗНОК/ НОК;
  - формування та передачу до АЦСК запита на блокування сертифіката користувача;
  - формування та передачу до АЦСК запита на скасування сертифіката користувача;
- **доступ до сертифікатів АЦСК, серверів АЦСК, сертифікатів інших користувачів та СВС:**
  - перегляд сертифікатів та СВС у файловому сховищі;
  - пошук сертифікатів у файловому сховищі, LDAP-каталозі та за допомогою протоколу OCSP;
  - визначення статусу сертифікатів за допомогою СВС та за протоколом OCSP;
  - перевірку чинності та цілісності сертифікатів та ін.;
- **захист файлів користувача:**
  - підпис файлів;
  - перевірка підпису;
  - шифрування файлів;
  - розшифрування файлів.

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

Завантажити інсталяційний пакет програми з вебсайту за наступним посиланням:

https://ca.informjust.ua/download/Soft/EUInstall_for_CA_Informjust.exe

Далі необхідно здійснити інсталяцію ПЗ, виконавши наступні дії:

1.1 Запускаємо інсталятор ПЗ – EUInstall_for_CA_Informjust.exe (рис. 1.1):

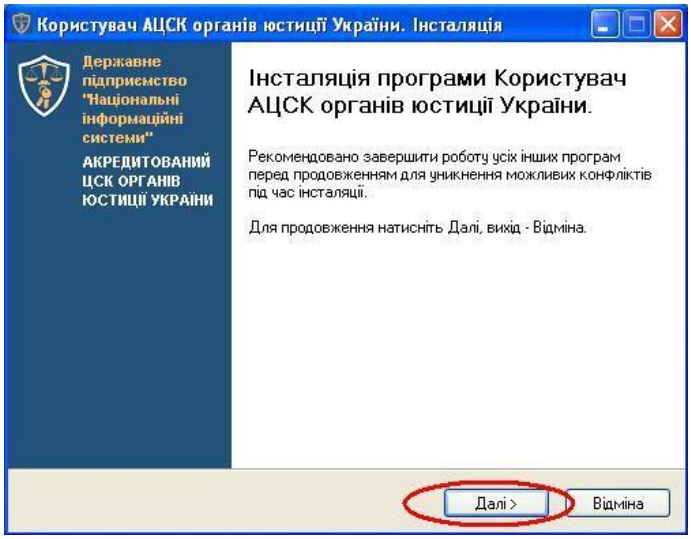


Рисунок 1.1

1.2 Каталог розміщення програми створюється автоматично (за замовчуванням «C:\Program Files\Institute of Informational Technologies\Certificate Authority-1.3\End User» - для 32-бітних ОС, та «C:\Program Files (x86)\Institute of Informational Technologies\Certificate Authority-1.3\End User» - для 64-бітних ОС), змінювати його не рекомендується. Для продовження інсталяції натискаємо кнопку «Далі» (рис. 1.2):

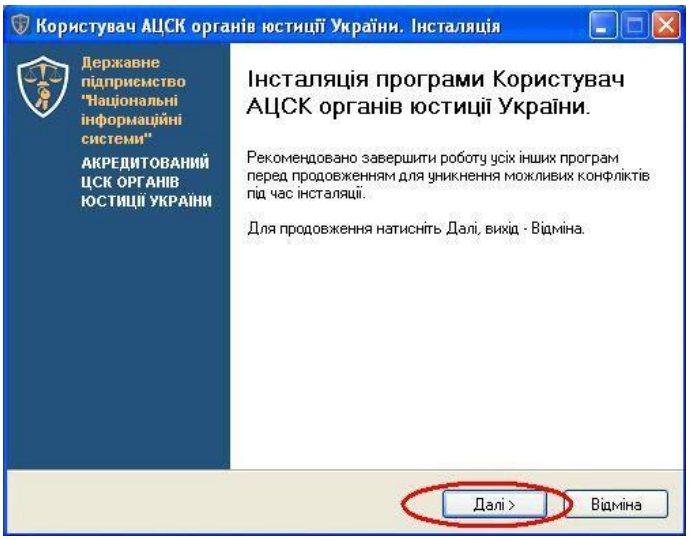


Рисунок 1.2

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

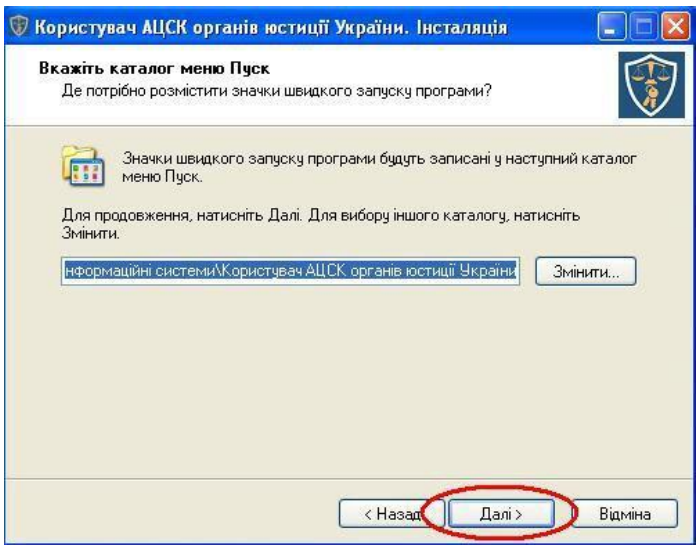


Рисунок 1.3

1.4 Під час встановлення ПЗ файлове сховище для посилених 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):

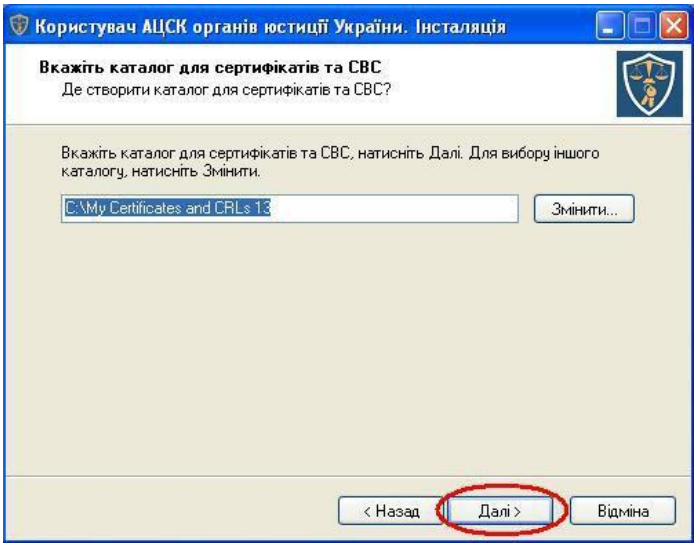


Рисунок 1.4

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» :

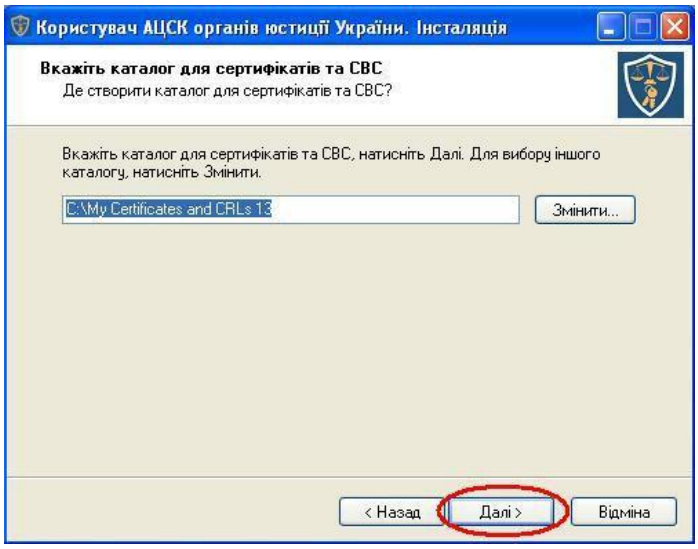


Рисунок 1.5

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 програми необхідно натиснути «Відміна» :

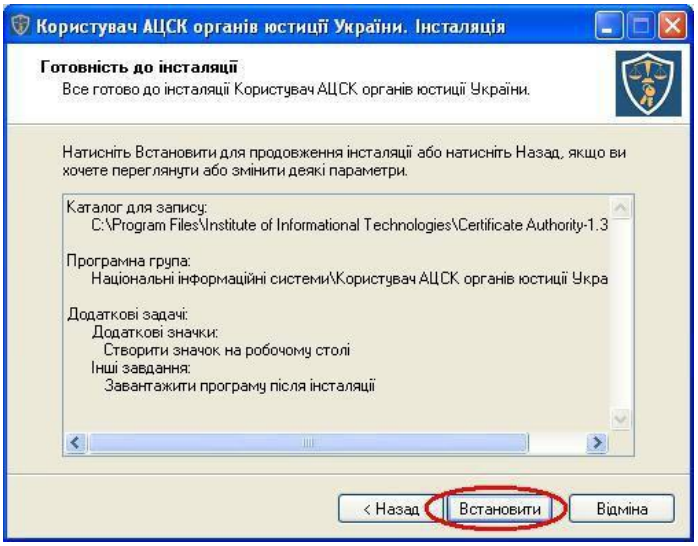


Рисунок 1.6

1.7 Після завершення інсталяції запущена програма має такий вигляд (рис. 1.7). Перед використанням програму необхідно налаштувати:

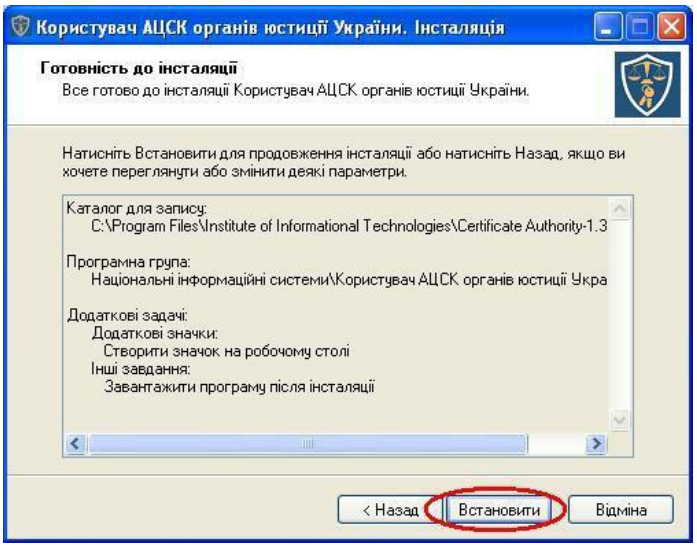


Рисунок 1.7

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

Після інсталяції ПЗ до файлового сховища необхідно додати сертифікати підписувача.

Здійснити перевірку розташування файлового сховища можна у меню ПЗ «Параметри/Встановити/Файлове сховище».

За необхідності, розташування файлового сховища можна змінити (рис. 2.1 та 2.2).

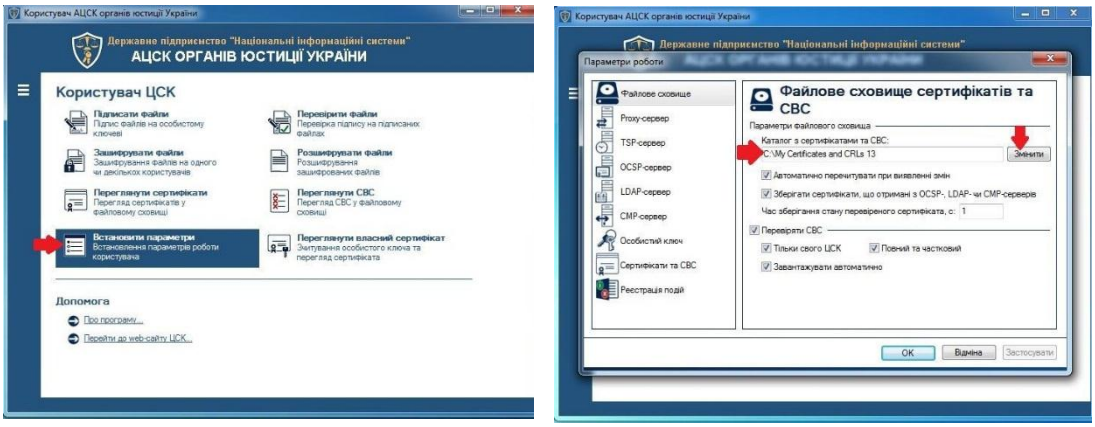


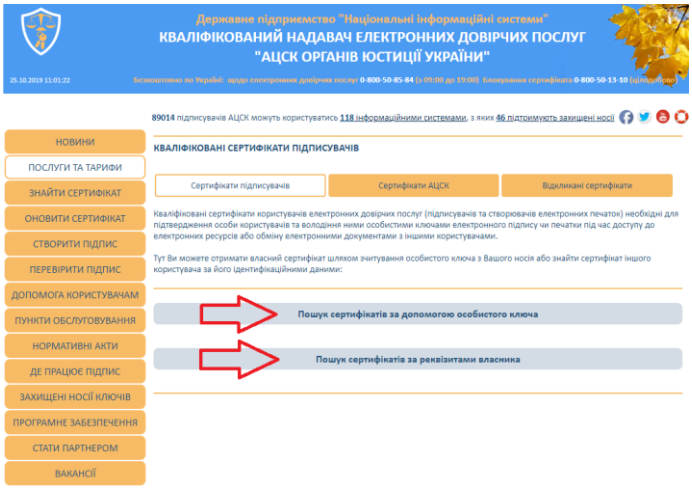
Рисунок 2.1 та 2.2

Виконати пошук сертифіката можна на вебсайті в розділі «Знайти сертифікат -> Сертифікати підписувачів» https://ca.informjust.ua/certificates-search.

Пошук власних кваліфікованих сертифікатів відкритих ключів користувачів можливий за такими критеріями:

- Пошук кваліфікованих сертифікатів відкритих ключів користувачів за допомогою особистого ключа;
- Пошук кваліфікованих сертифікатів відкритих ключів користувачів за реквізитами власника

(рис. 2.3)



Для пошуку власного сертифікату за допомогою особистого ключа перейдіть до розділу інформаційного ресурсу «ЗНАЙТИ СЕРТИФІКАТ» -> Сертифікати підписувачів(1) та натисніть на меню «Пошук сертифікатів за допомогою особистого ключа»(2). Після розгортання меню оберіть тип носія особистого ключа(3), КНЕДП(4) особистий ключ(5), введіть пароль захисту ключа(6) та натисніть "Зчитати"(7) (рис. 2.4 та 2.5):

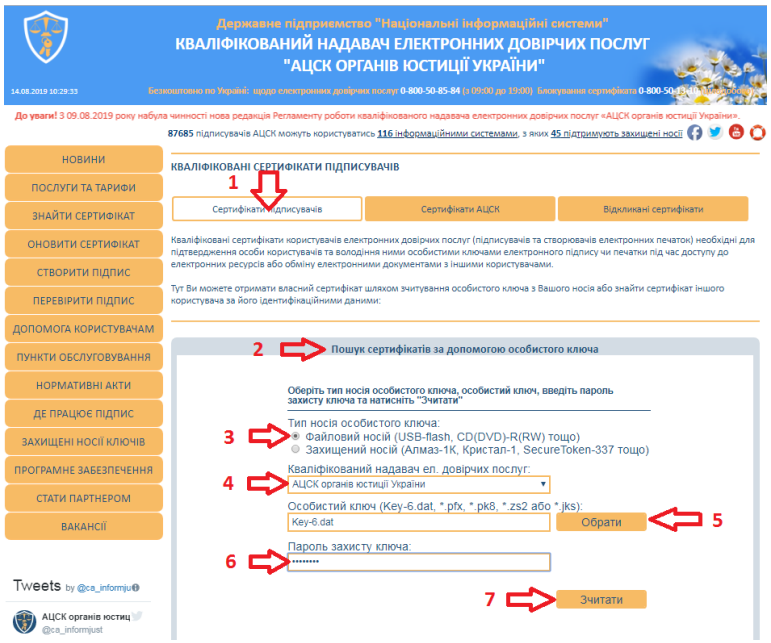


Рисунок 2.4

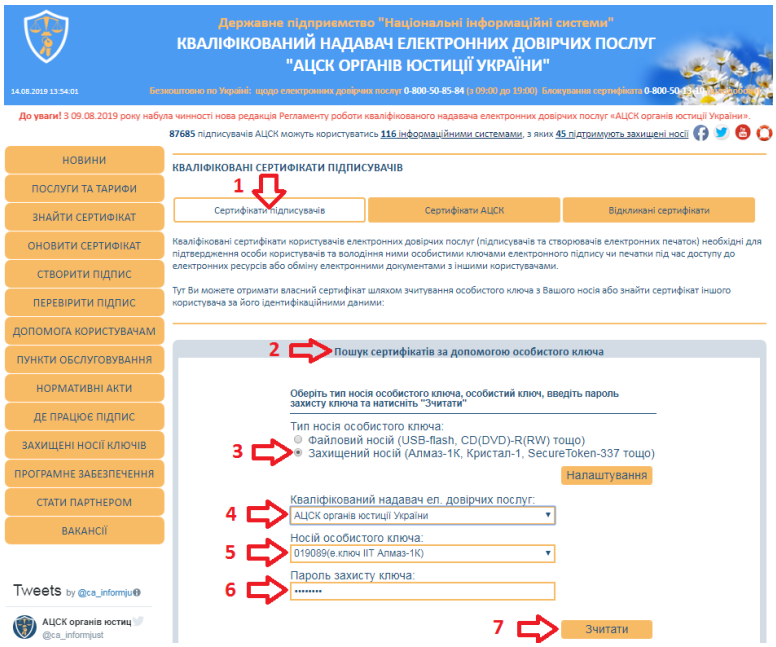


Рисунок 2.5

У разі обрання пункту «Захищений носій (Алмаз-1К, Кристал-1, SecureToken-337 тощо)» та відсутності встановленого спеціалізованого програмного забезпечення на комп'ютері користувача, система запропонує його встановити (буде надане актуальне посилання). Після встановлення необхідного ПЗ оновіть сторінку інтернет-переглядача.

У разі позитивного результату пошуку інформація про користувача, а також посилання для завантаження кваліфікованих сертифікатів відкритих ключів (жовті стрілки донизу) буде надана, як на рис. 2.6:

Рисунок 2.6

Для пошуку власного сертифікату за реквізитами власника перейдіть до розділу інформаційного ресурсу «ЗНАЙТИ СЕРТИФІКАТ» -> Сертифікати підписувачів(1) та натисніть на меню «Пошук сертифікатів за реквізитами власника»(2). Після розгортання меню у формі пошуку кваліфікованих сертифікатів необхідно ввести **один** із можливих критеріїв пошуку(3), а саме

«Код ЄДРПОУ» **або** «Код платника податків (у разі відсутності серія та номер паспорта)» **або** «Реєстраційний номер сертифіката», пройти перевірку CAPTCHA від сервісу Google "Я не робот"(4) і натиснути кнопку "Пошук"(5) (рис 2.7)

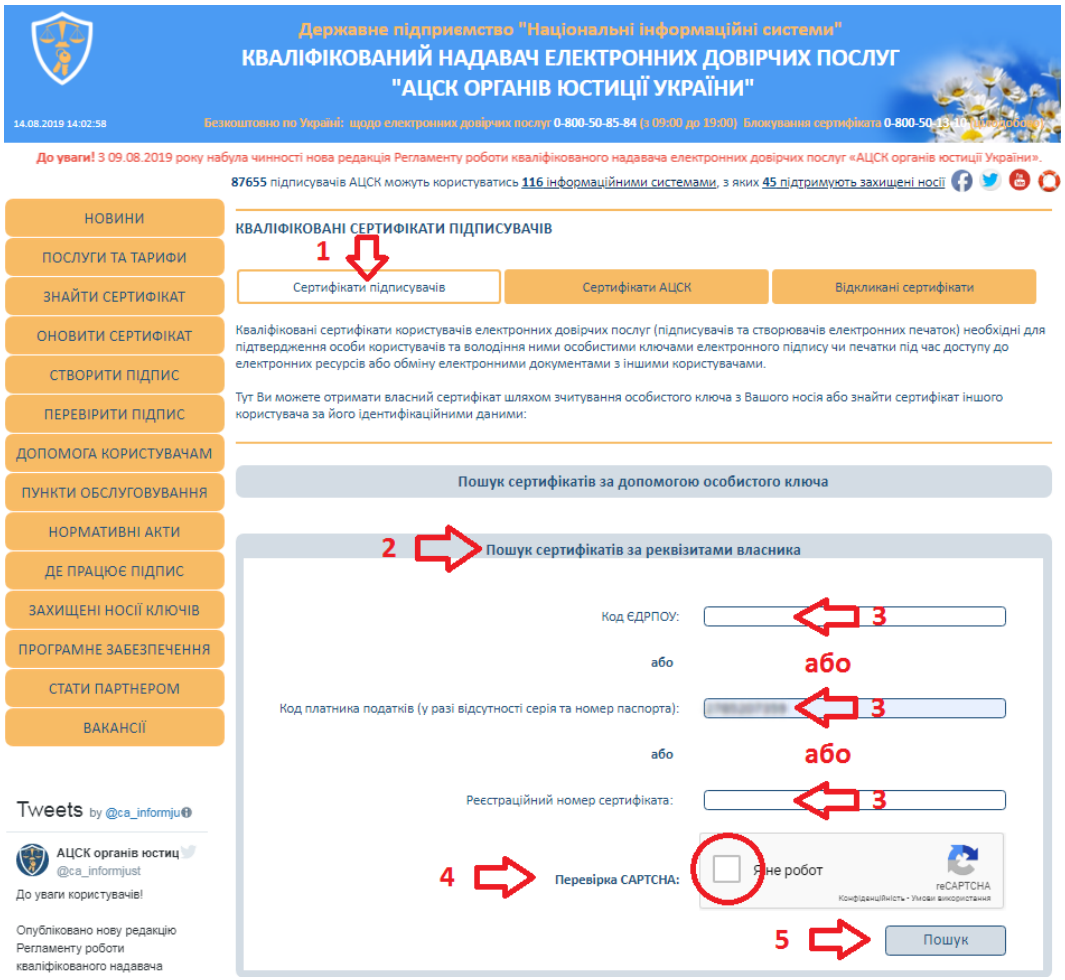


Рисунок 2.7

У разі позитивного результату пошуку інформація про користувача, а також посилання для завантаження кваліфікованих сертифікатів відкритих ключів (жовті стрілки донизу) буде надана, як на рис. 2.8.

Зазначимо, що у одного користувача може бути більше одного ключа і, відповідно, більше однієї пари сертифікатів, як і є у прикладі на вказаному малюнку.

Необхідно завантажити у файлову систему комп’ютера потрібні кваліфіковані сертифікати.

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

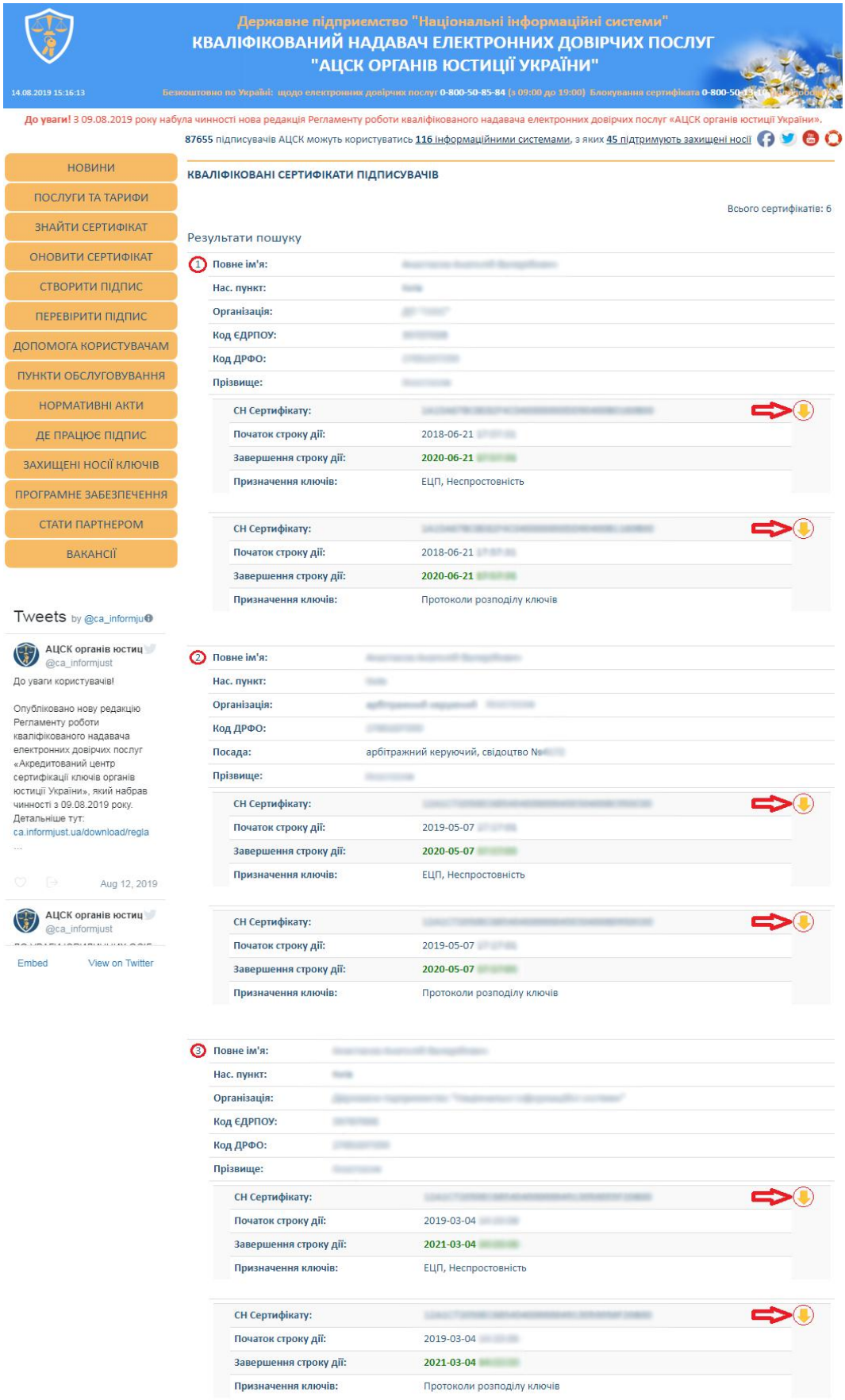

Державне підприємство "Національні інформаційні системи"
КВАЛІФІКОВАНИЙ НАДАВАЧ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ
"АЦСК ОРГАНІВ ЮСТИЦІЇ УКРАЇНИ"
14.08.2019 15:16:13
До уваги! З 09.08.2019 року набула чинності нова редакція Регламенту роботи кваліфікованого надавача електронних довірчих послуг «АЦСК органів юстиції України».
87655 підписувачів АЦСК можуть користуватись 116 інформаційними системами, з яких 45 підтримують захищені носії
НОВИНИ
ПОСЛУГИ ТА ТАРИФИ
ЗНАЙТИ СЕРТИФІКАТ
ОНОВИТИ СЕРТИФІКАТ
СТВОРИТИ ПІДПИС
ПЕРЕВІРИТИ ПІДПИС
ДОПОМОГА КОРИСТУВАЧАМ
ПУНКТИ ОБСЛУГОВУВАННЯ
НОРМАТИВНІ АКТИ
ДЕ ПРАЦЮЄ ПІДПИС
ЗАХИЩЕНІ НОСІЇ КЛЮЧІВ
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
СТАТИ ПАРТНЕРОМ
ВАКАНСІЇ
КВАЛІФІКОВАНІ СЕРТИФІКАТИ ПІДПИСУВАЧІВ
Всього сертифікатів: 6
Результати пошуку
1
Повне ім'я:
Нас. пункт:
Організація:
Код ЄДРПОУ:
Код ДРФО:
Прізвище:
СН Сертифікату:
Початок строку дії: 2018-06-21
Завершення строку дії: 2020-06-21
Призначення ключів: ЕЦП, Неспростовність
СН Сертифікату:
Початок строку дії: 2018-06-21
Завершення строку дії: 2020-06-21
Призначення ключів: Протоколи розподілу ключів
2
Повне ім'я:
Нас. пункт:
Організація:
Код ДРФО:
Посада: арбітражний керуючий, свідоцтво №
Прізвище:
СН Сертифікату:
Початок строку дії: 2019-05-07
Завершення строку дії: 2020-05-07
Призначення ключів: ЕЦП, Неспростовність
СН Сертифікату:
Початок строку дії: 2019-05-07
Завершення строку дії: 2020-05-07
Призначення ключів: Протоколи розподілу ключів
3
Повне ім'я:
Нас. пункт:
Організація:
Код ЄДРПОУ:
Код ДРФО:
Прізвище:
СН Сертифікату:
Початок строку дії: 2019-03-04
Завершення строку дії: 2021-03-04
Призначення ключів: ЕЦП, Неспростовність
СН Сертифікату:
Початок строку дії: 2019-03-04
Завершення строку дії: 2021-03-04
Призначення ключів: Протоколи розподілу ключів
Tweets by @ca_informju
АЦСК органів юстиц
@ca_informjust
До уваги користувачів!
Опубліковано нову редакцію Регламенту роботи кваліфікованого надавача електронних довірчих послуг «Акредитований центр сертифікації ключів органів юстиції України», який набрав чинності з 09.08.2019 року. Детальніше тут: ca.informjust.ua/download/regla ...
Aug 12, 2019
АЦСК органів юстиц
@ca_informjust
Embed
View on Twitter

Рисунок 2.8

При використанні браузера «Internet Explorer» збереження сертифіката необхідно підтвердити, натиснувши в діалоговому вікні кнопку «Сохранить» (рис. 2.9).

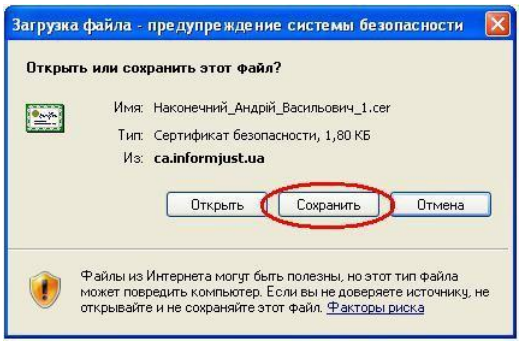


Рисунок 2.9

По завершенню процесу завантаження необхідно натиснути кнопку«Открыть папку» (рис. 2.10).

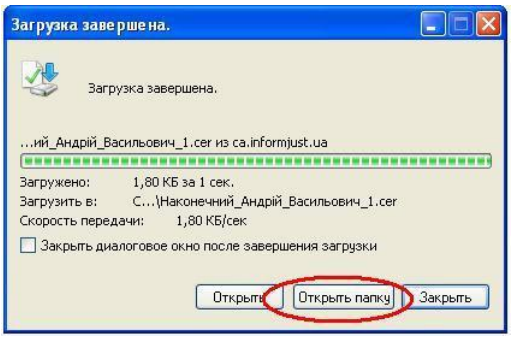


Рисунок 2.10

При використанні браузера «Mozilla Firefox», з’явиться діалогове вікно, в якому необхідно обрати «Сохранить файл» та натиснути «ОК» (рис. 2.11).

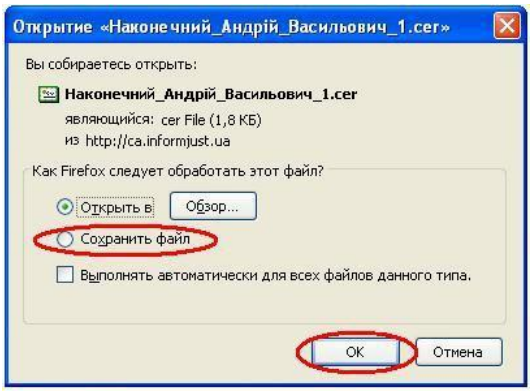


Рисунок 2.11

Далі у вікні «Загрузки», після закінчення процесу завантаження необхідно обрати свій сертифікат та натиснувши праву кнопку миші обрати пункт меню «Открыть папку с файлом» (рис. 2.12).

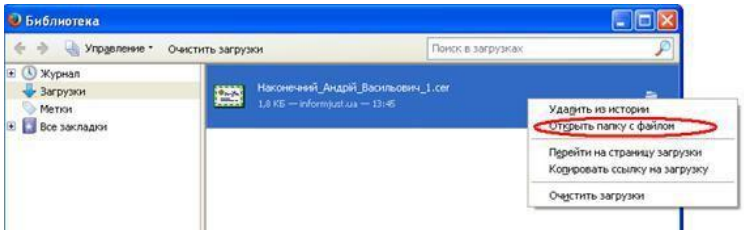


Рисунок 2.12

При використанні браузера «Google Chrome», після завантаження необхідно натиснути правою кнопкою миші на іконку та обрати в меню «Показать в папке» (рис. 2.13).

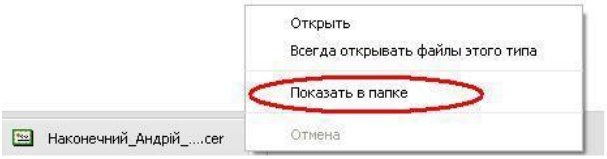


Рисунок 2.13

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

Окрім 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 програми.

У випадку, коли технологічні сертифікати відсутні у файловому сховищі, їх необхідно завантажити з вебсайту «ЗНАЙТИ СЕРТИФІКАТ»(1) -> Сертифікати АЦСК(2) -> Завантажити ланцюжок кваліфікованих сертифікатів АЦСК одним архівом(3) (рис. 2.14).

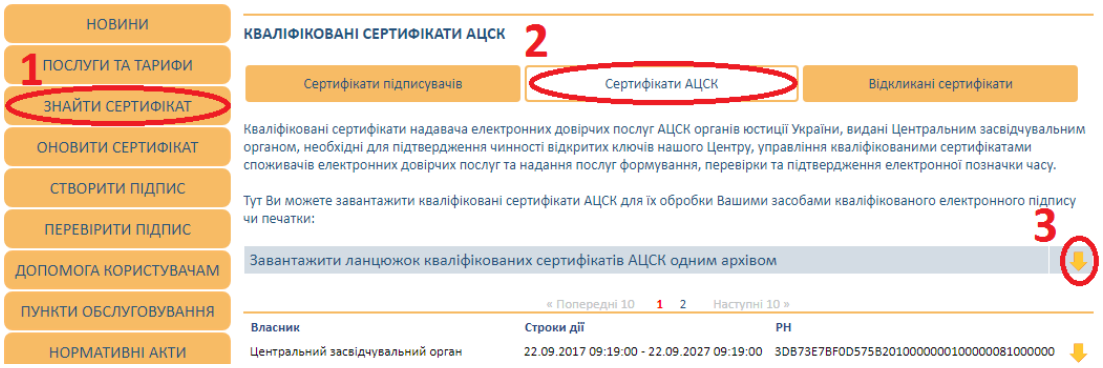


Рисунок 2.14

Також можливо виконати автоматичне завантаження усіх сертифікатів за допомогою запиту до серверу обробки запитів. Запит формується за допомогою особистого ключа підписувача. Для отримання пакету сертифікатів необхідно обрати підпункт «Отримати з ЦСК...» в пункті меню «Сертифікати та СВС» (рис. 2.15).

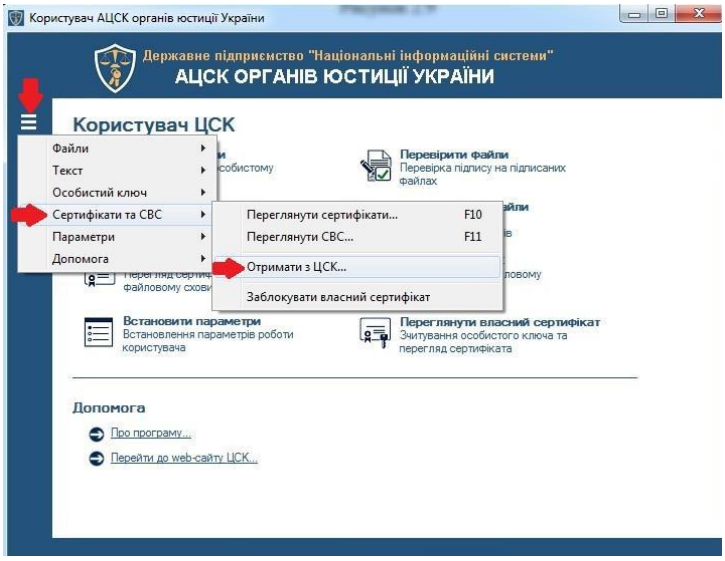


Рисунок 2.15

Після чого буде виведене діалогове вікно (рис. 2.16). Для продовження формування запиту на автоматичне завантаження сертифікатів натиснути «Да».

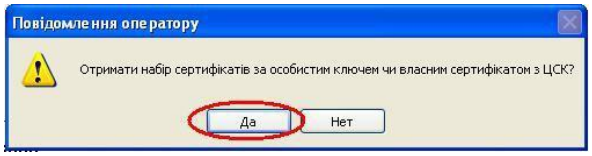


Рисунок 2.16

Після чого з’являється вікно зчитування особистого ключа, в якому необхідно обрати НКІ та ввести пароль захисту особистого ключа (рис. 2.17).

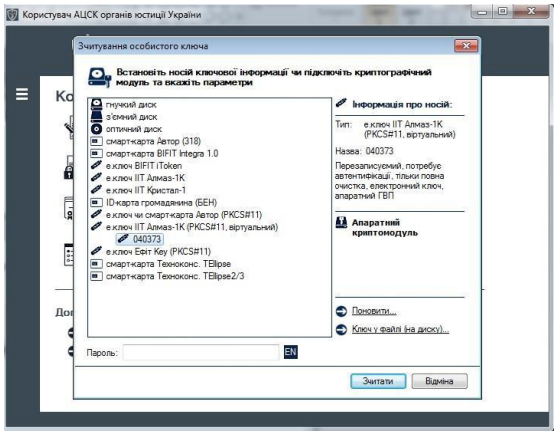


Рисунок 2.17

Після зчитування особистого ключа буде виведене вікно «Завантажені сертифікати» (рис. 2.18), в якому буде запропоновано імпортувати їх у файлове сховище сертифікатів. Необхідно зберегти їх до файлового сховища, натиснувши кнопку «Да».

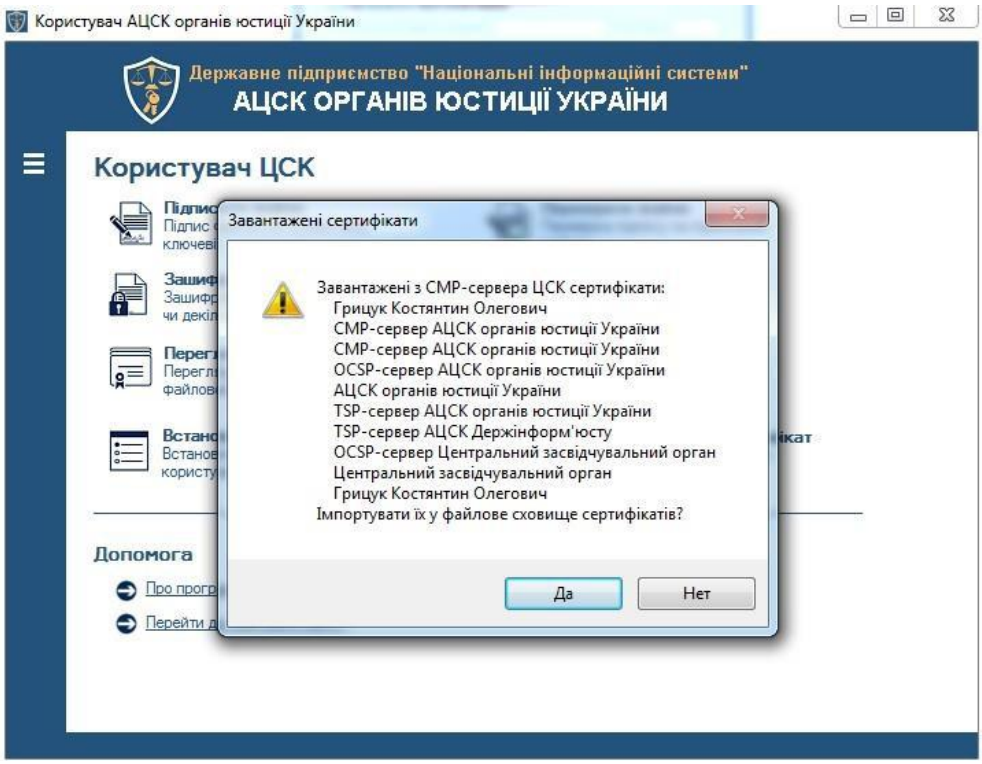


Рисунок 2.18

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

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

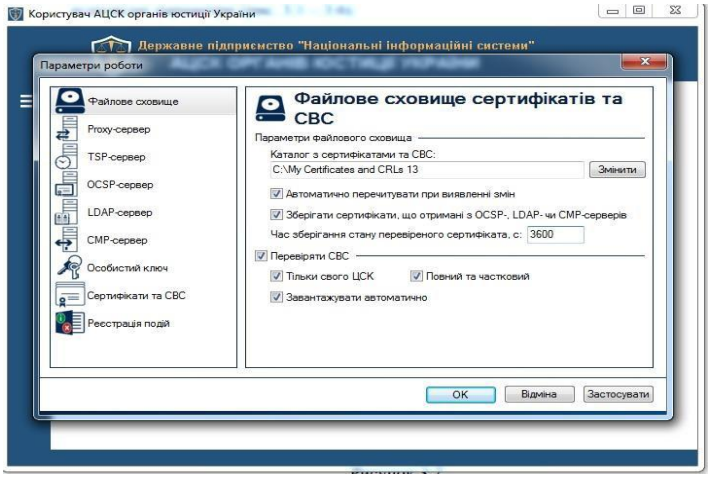


Рисунок 3.1

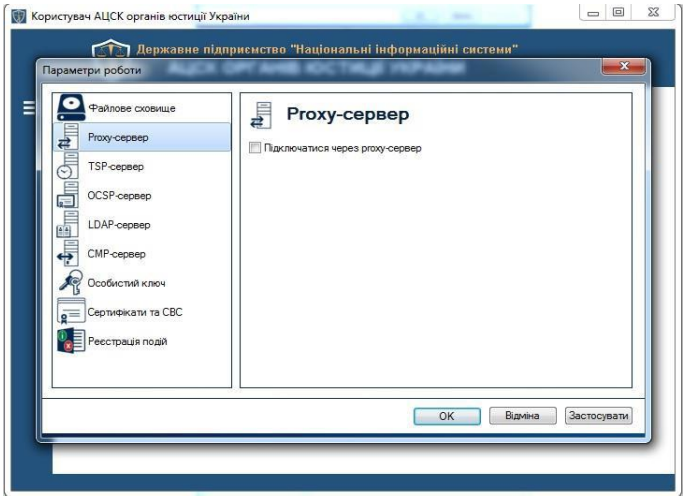


Рисунок 3.2

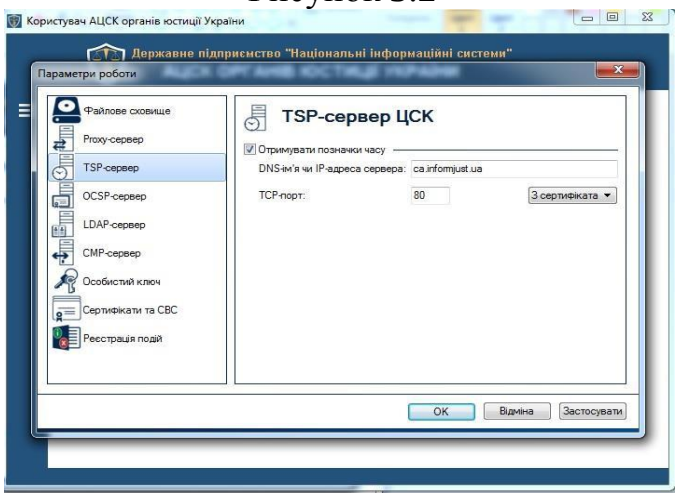


Рисунок 3.3

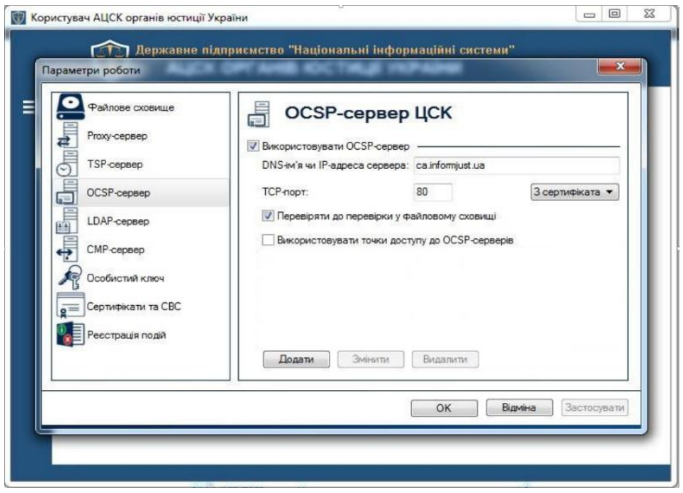


Рисунок 3.4

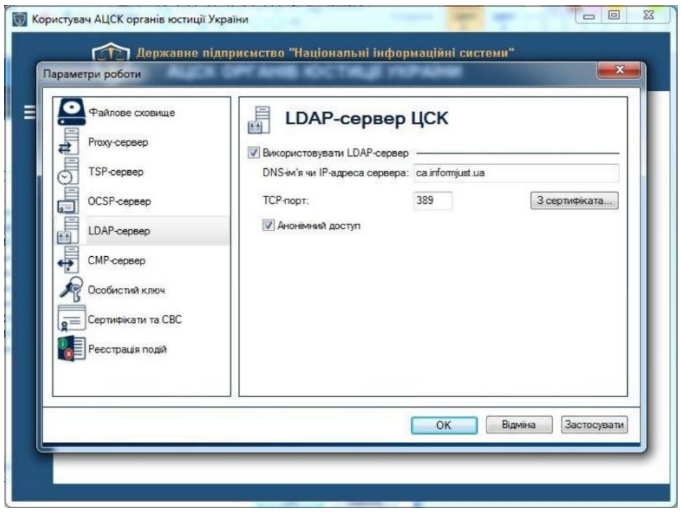


Рисунок 3.5

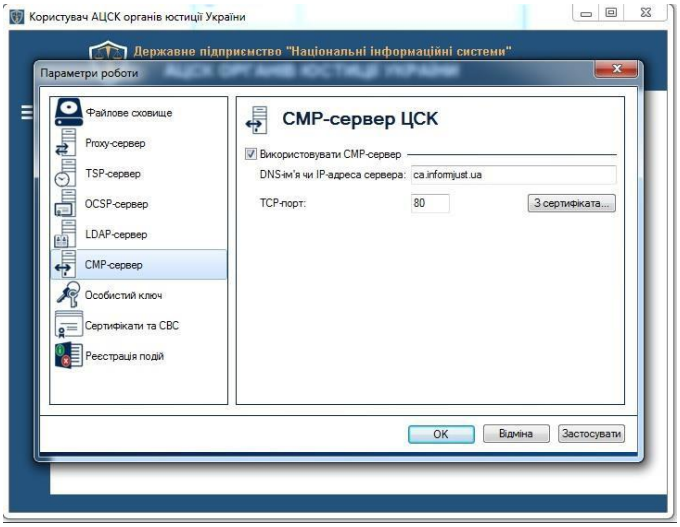


Рисунок 3.6

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

4.1 Підписання файлів

Для створення підпису на електронний документ необхідно у головному вікні ПЗ обрати пункт «Підписати файли» (рис. 4.1).

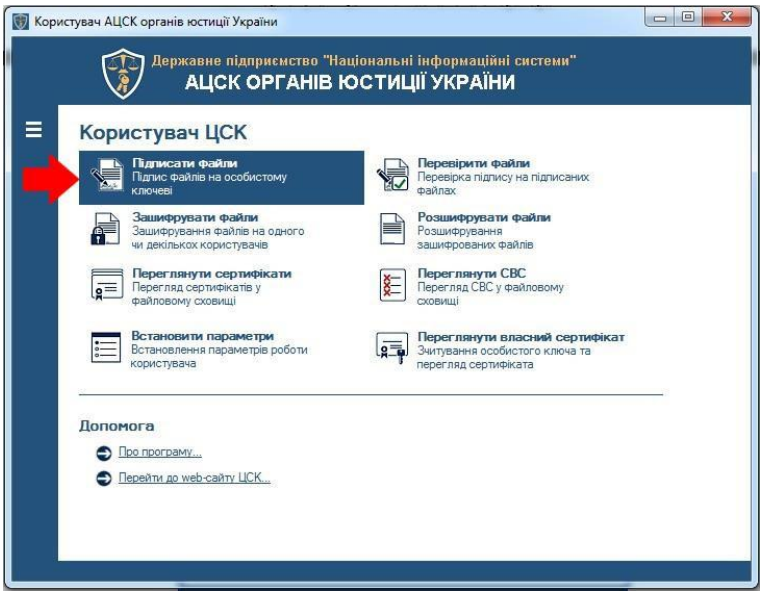


Рисунок 4.1

Після чого з’являється вікно зчитування особистого ключа, в якому необхідно обрати ЗНОК та ввести пароль захисту особистого ключа (рис. 4.2).

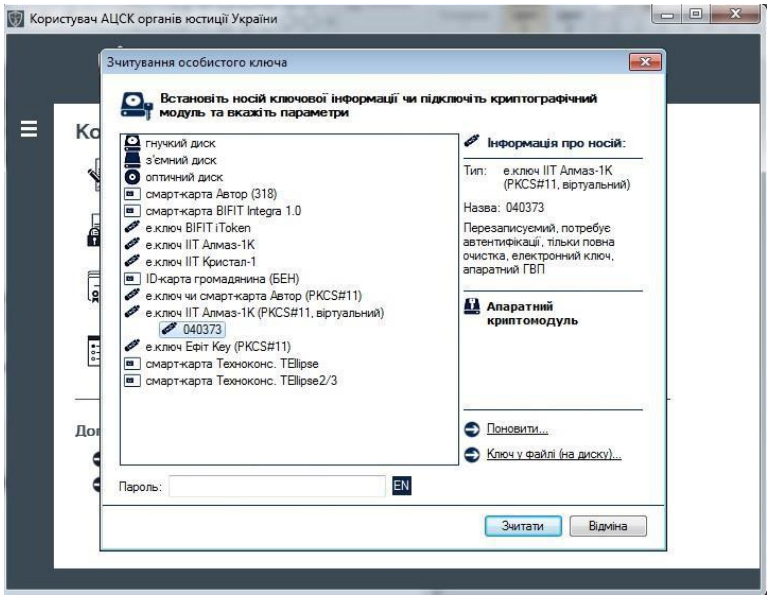


Рисунок 4.2

Після успішного зчитування паролю захисту особистого ключа з'являється вікно «Підпис файлів». Для додавання файлів, які потребують підписання, натискаємо кнопку «Додати» та обираємо розташування файлу (рис. 4.3).

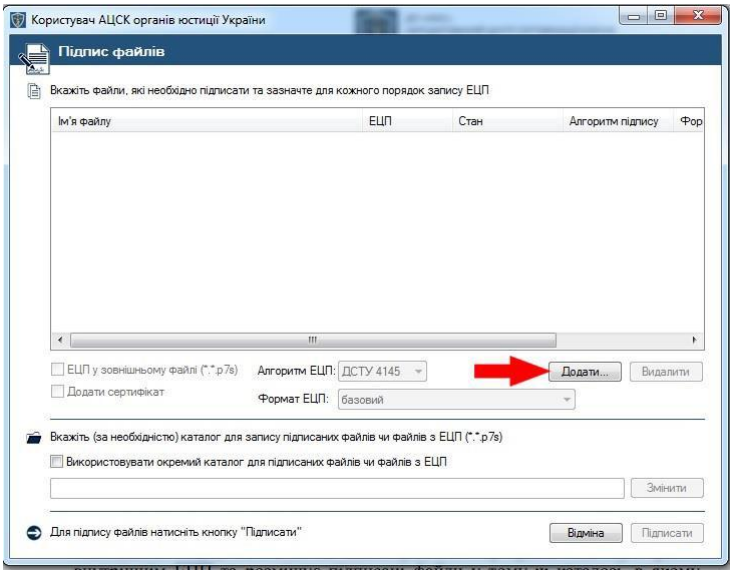


Рисунок 4.3

Додавши необхідний файл, варто звернути увагу на параметри створення підпису, оскільки за замовчуванням програма створює копію файлу, приєднує до нього підпис та розміщує підписаний файл у тому ж каталозі, в якому розміщується вхідний файл (рис. 4.4). Наприклад, якщо файл розташований на робочому столі, підписаний файл буде збережений також на робочому столі. Якщо необхідно інше – встановіть потрібну конфігурацію. Всі підписані файли мають розширення «.p7s».

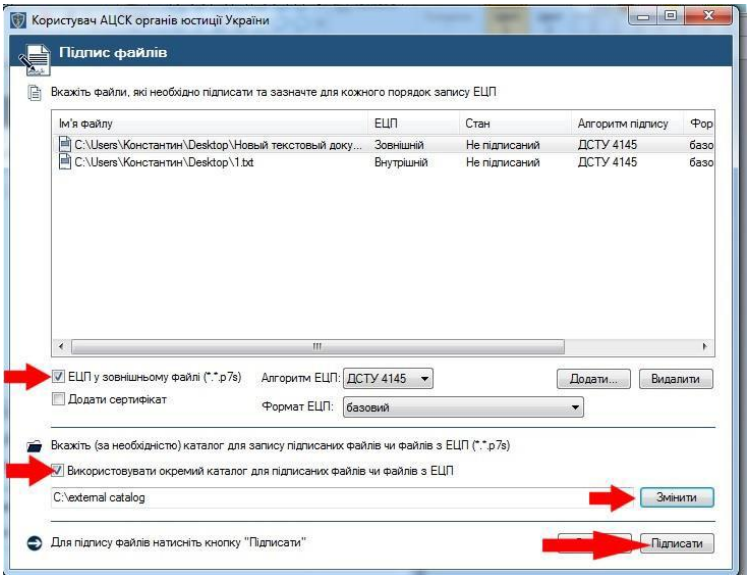


Рисунок 4.4

Програма дає можливість одночасно підписати декілька файлів та обрати спосіб створення підпису для кожного файлу окремо.

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

4.2 Перевірка підпису

Для перевірки підпису натискаємо кнопку «Перевірити файли» (рис. 4.5).

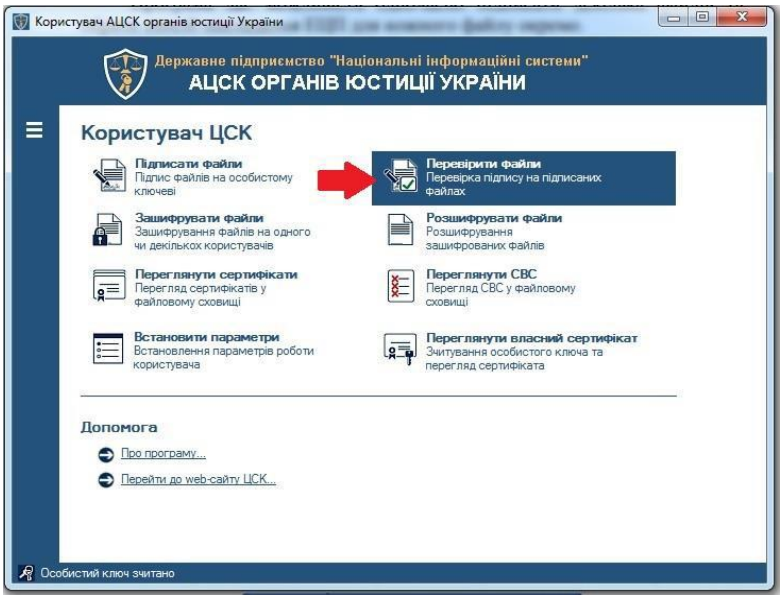


Рисунок 4.5

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

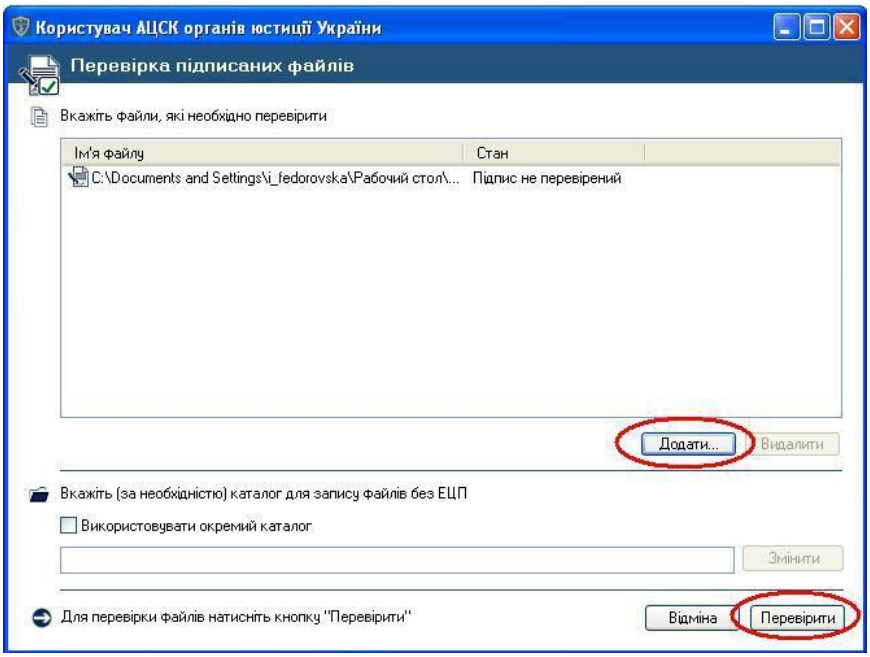


Рисунок 4.6

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

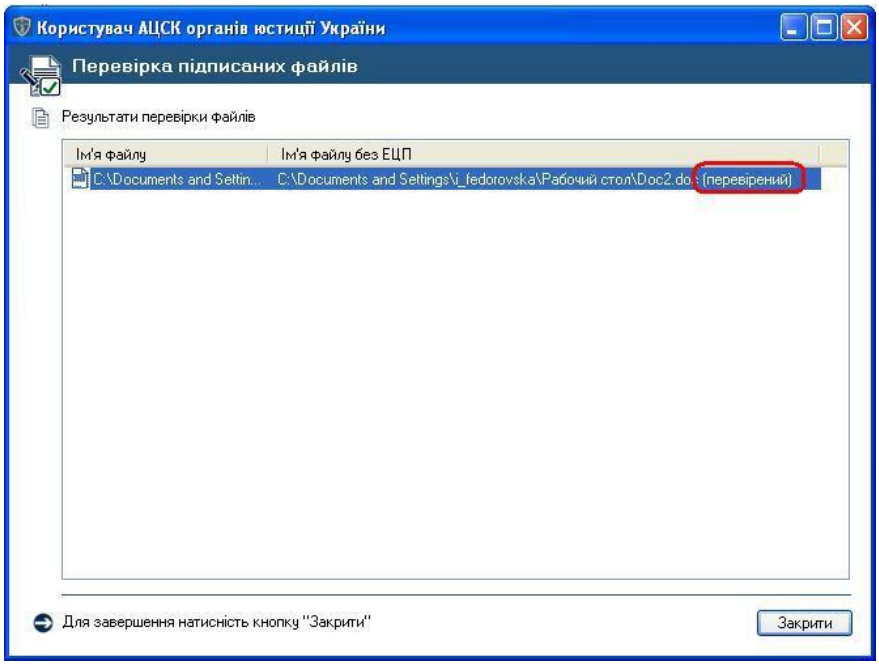


Рисунок 4.7

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, натиснувши «Детальна інформація».

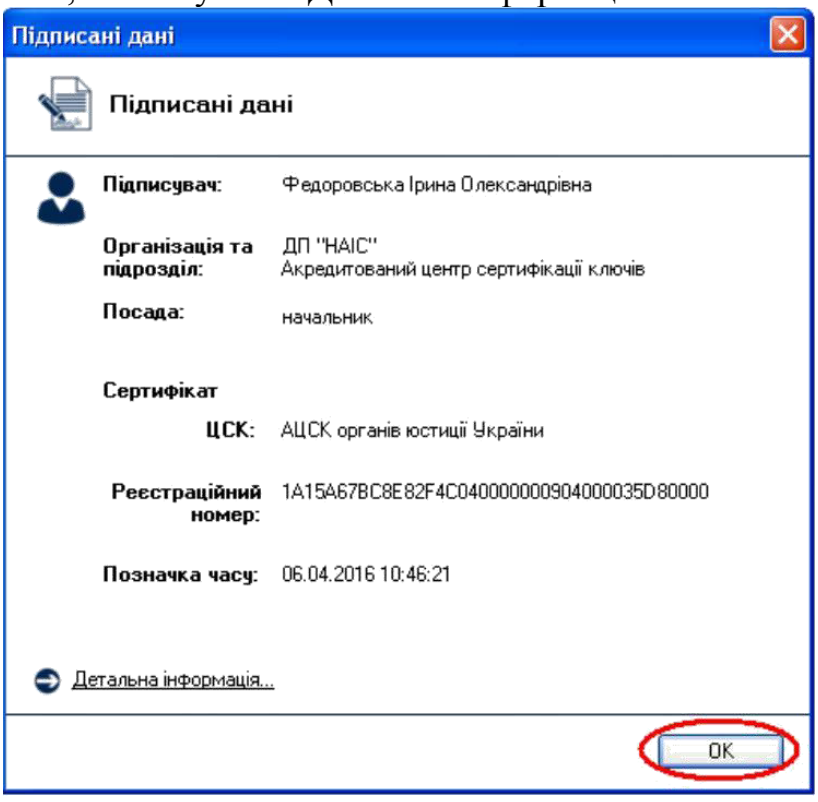


Рисунок 4.8

4.3 Шифрування файлів

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

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

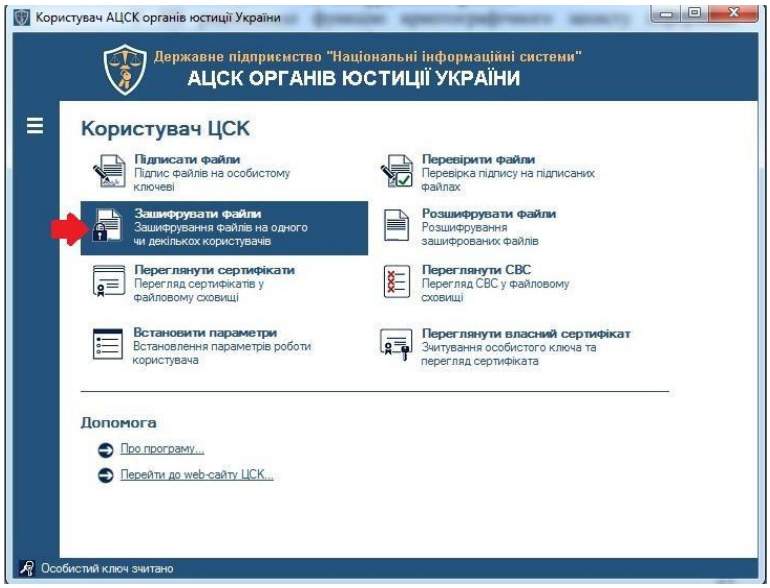


Рисунок 4.9

Наступним кроком є поява вікна зчитування особистого ключа, в якому необхідно обрати ЗНОК та ввести пароль захисту особистого ключа (рис. 4.10).

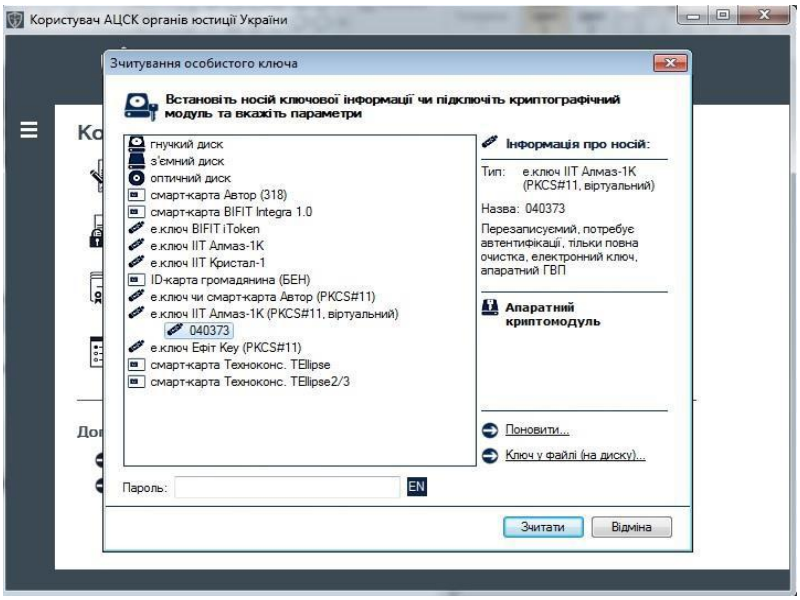


Рисунок 4.10

У новому вікні «Зашифрування файлів» підписувачу надається можливість одночасно з шифруванням файлів додатково їх підписати (рис. 4.11).

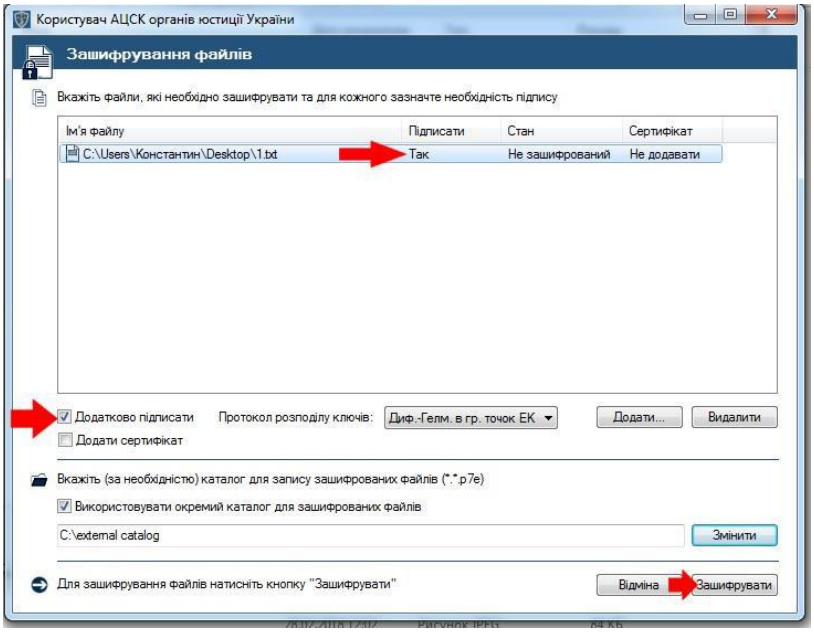


Рисунок 4.11

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

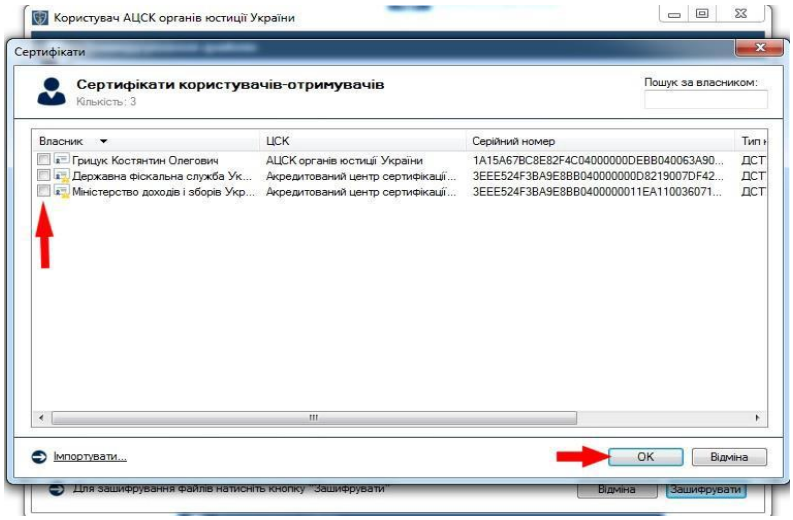


Рисунок 4.12

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

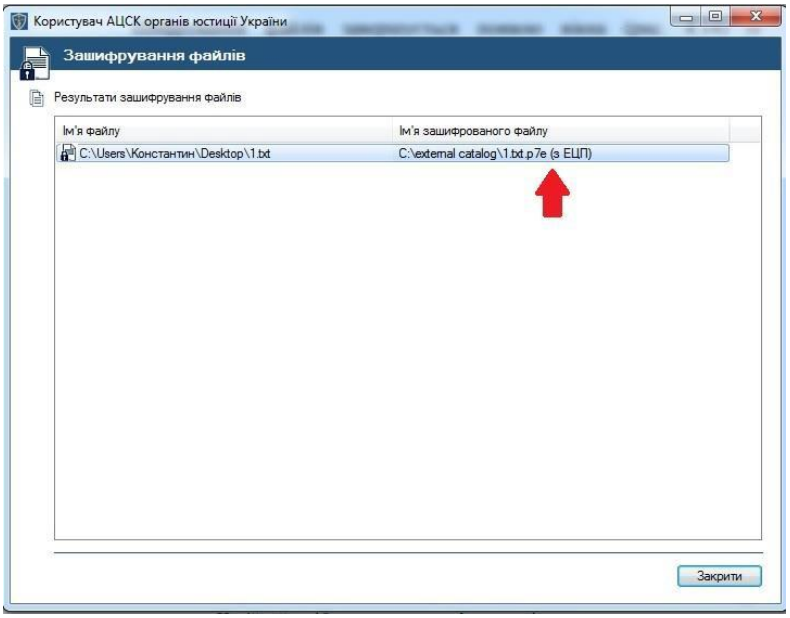


Рисунок 4.13

4.4 Розшифрування файлів

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

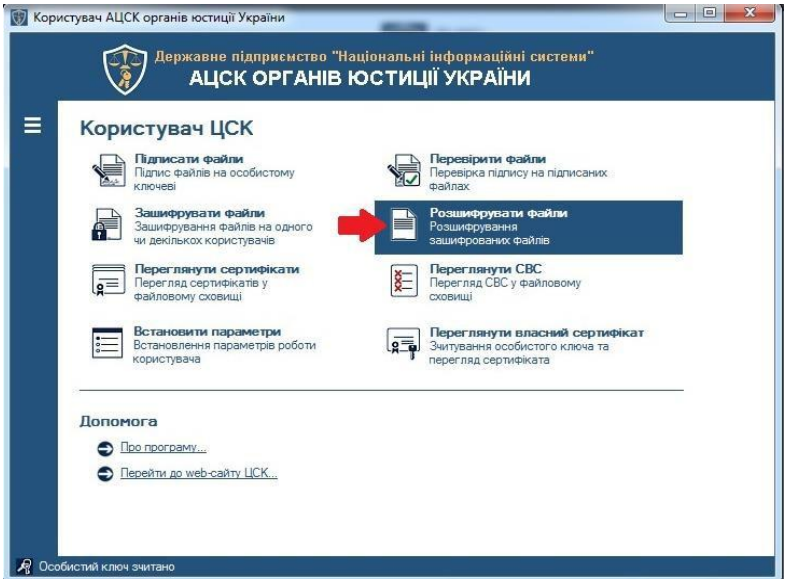


Рисунок 4.14

Після появи вікна зчитування особистого ключа, необхідно обрати з'ємний НКІ та ввести пароль захисту особистого ключа (рис. 4.15).

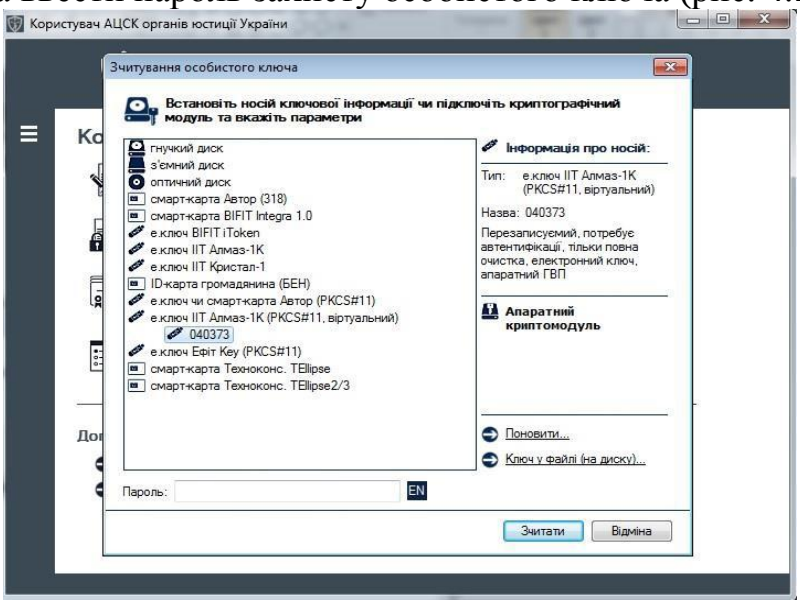


Рисунок 4.15

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

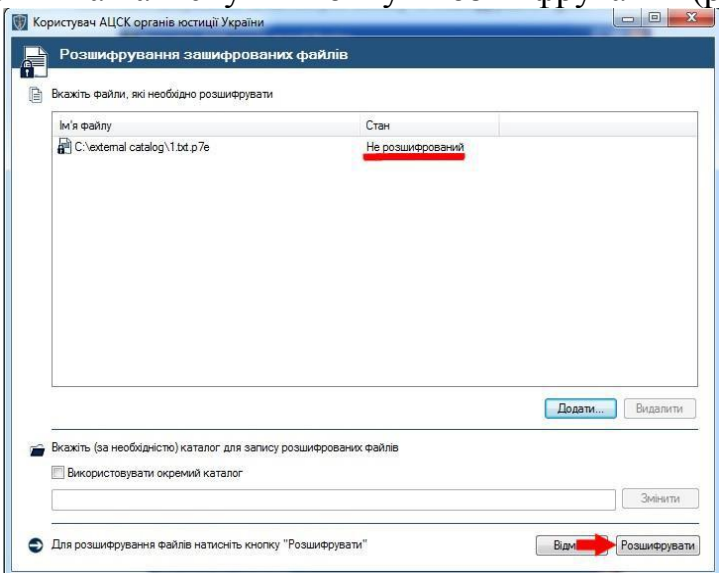


Рисунок 4.16

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).

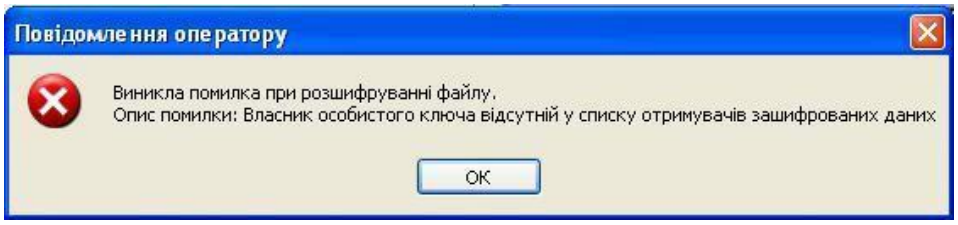


Рисунок 4.17

4.5 Перегляд сертифікатів

Для перегляду сертифікатів, що містяться у файловому сховищі необхідно обрати підпункт «Переглянути сертифікати» або натиснути клавішу F10 (рис. 4.18).

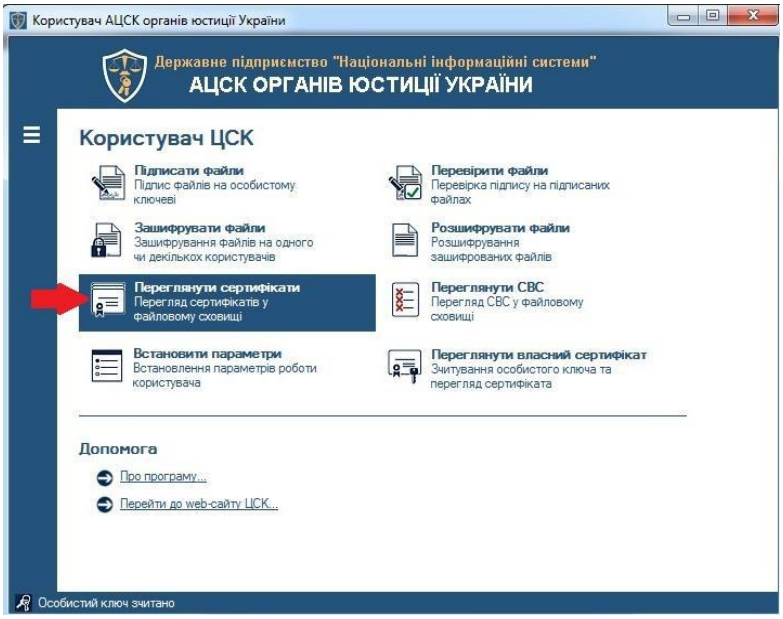


Рисунок 4.18

У вікні перегляду сертифікатів (рис. 4.19) можна переглянути, перевірити та видалити обраний сертифікат.

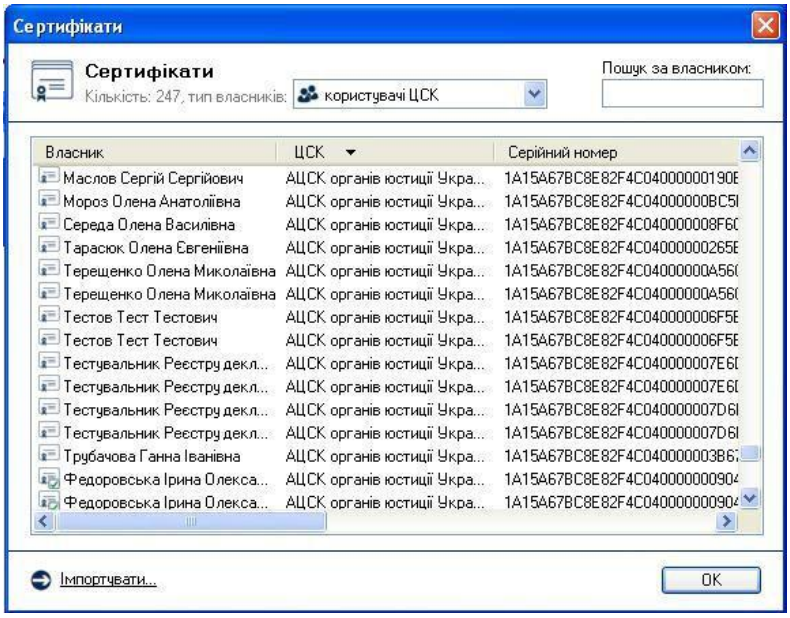


Рисунок 4.19

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

– всі сертифікати;

– сертифікати центрів сертифікації ключів;
– сертифікати серверів ЦСК;
– сертифікати CMP-серверів; – сертифікати TSP-серверів;
– сертифікати OCSP-серверів;
– сертифікати користувачів ЦСК.

Для перегляду даних про власника сертифіката необхідно натиснути на відповідному записі про сертифікат у списку, після чого будуть відображені дані сертифіката (рис. 4.20 та 4.21).

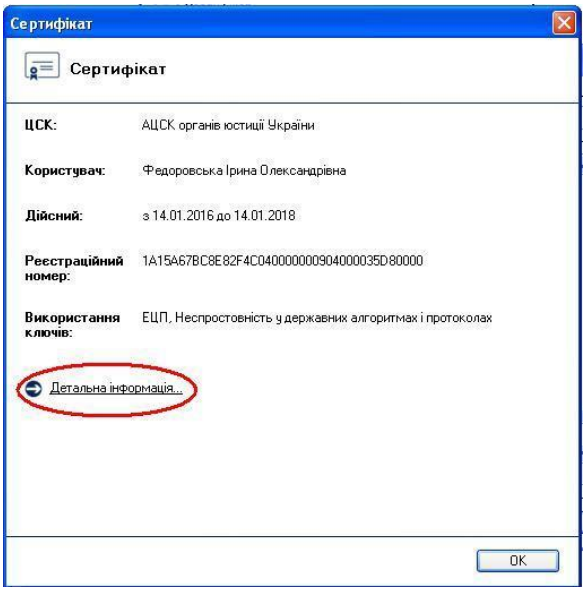


Рисунок 4.20

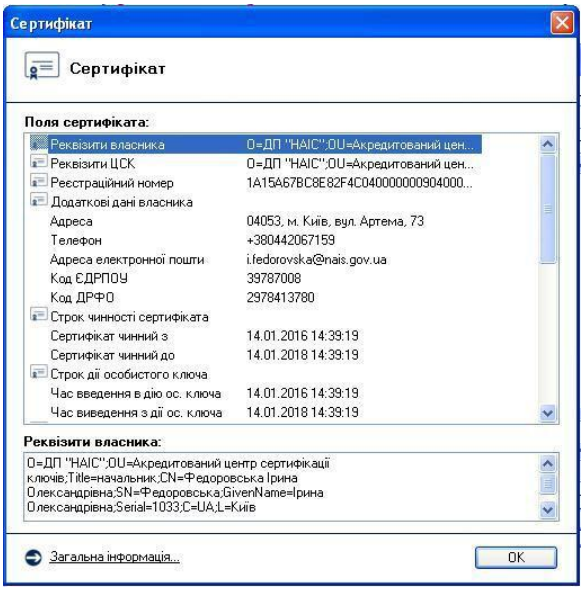


Рисунок 4.21

Для видалення сертифікатів з файлового сховища необхідно відмітити у списку (рис. 4.19) відповідні записи та натиснути кнопку «Видалити».

Для перевірки сертифіката необхідно відмітити відповідний запис про сертифікат у списку та натиснути кнопку «Перевірити». Перевірка сертифіката здійснюється відповідно до встановлених параметрів роботи програми, за допомогою СВС чи OCSP-протоколу.

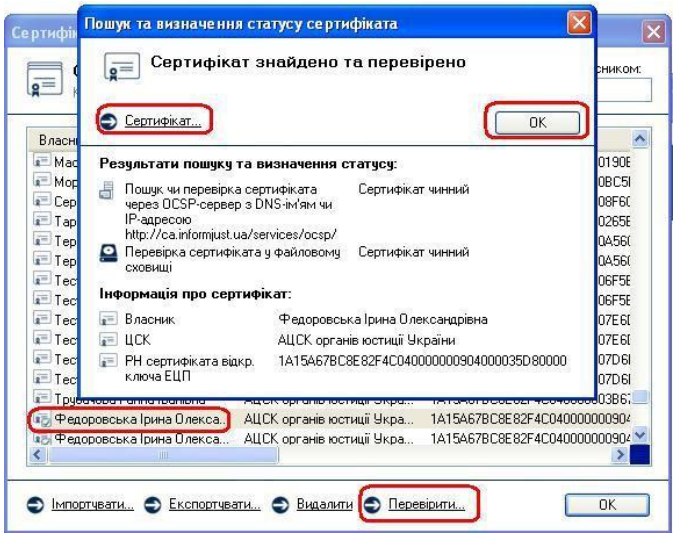


Рисунок 4.22

Появою вікна «Пошук та визначення статусу сертифіката» (рис. 4.22) закінчується перевірка сертифіката. Детальну інформацію про сертифікат можна переглянути обравши пункт «Сертифікат».

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

4.6 Перегляд СВС

Для перегляду СВС необхідно натиснути підпункт «Переглянути СВС» у головному меню або натиснути клавішу F11 (рис. 4.23). Вікно перегляду СВС наведене на рис. 4.25.

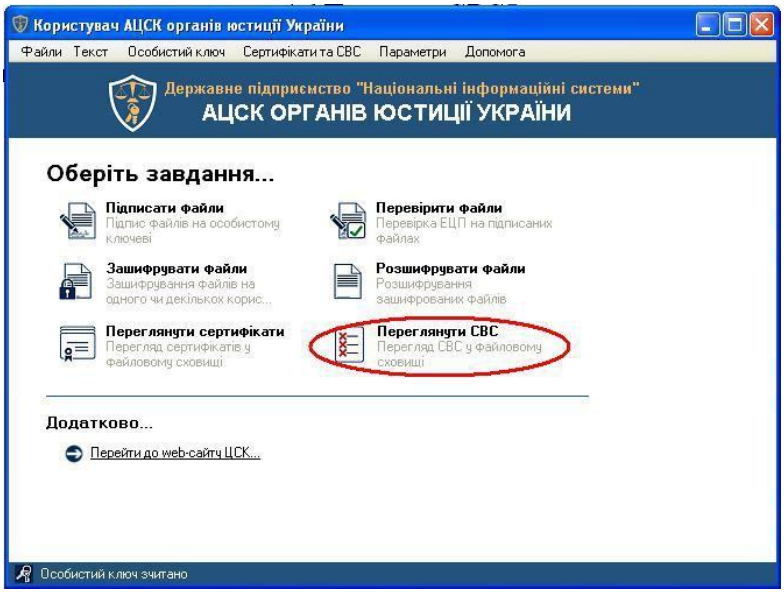


Рисунок 4.23

Вікно перегляду СВС дозволяє імпортувати, видаляти чи переглядати СВС, що завантажені з веб-сайту.

Самостійно завантажити СВС можна у розділі «Відкликані сертифікати» веб-сайту (рис. 4.24) та імпортувати до програми.

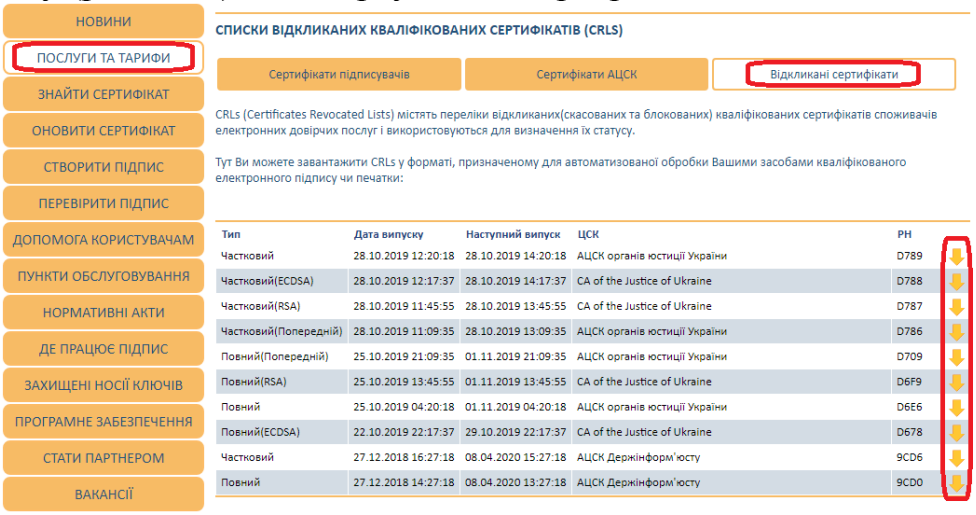


Рисунок 4.24

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. 4.25-4.27).

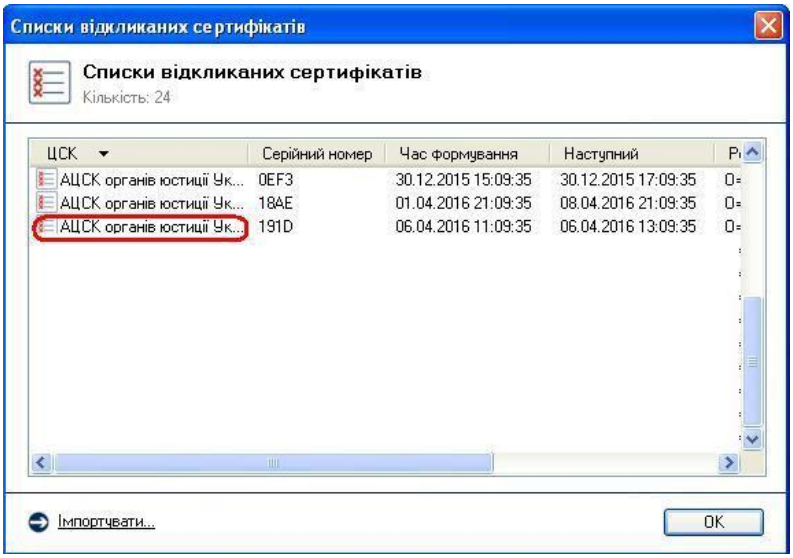


Рисунок 4.25

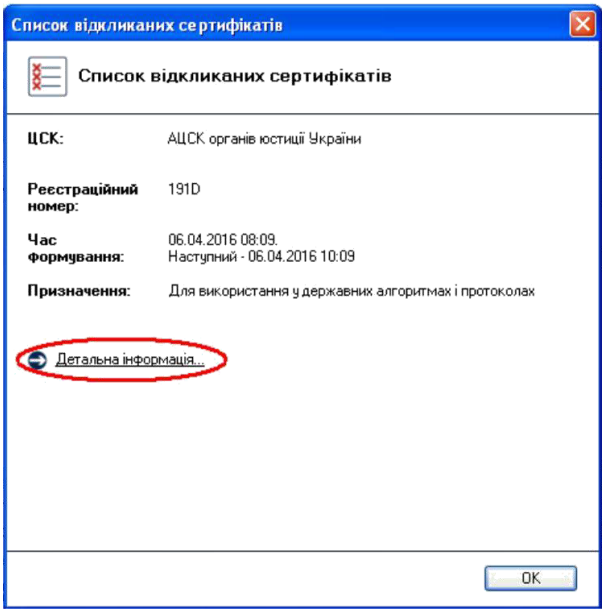


Рисунок 4.26

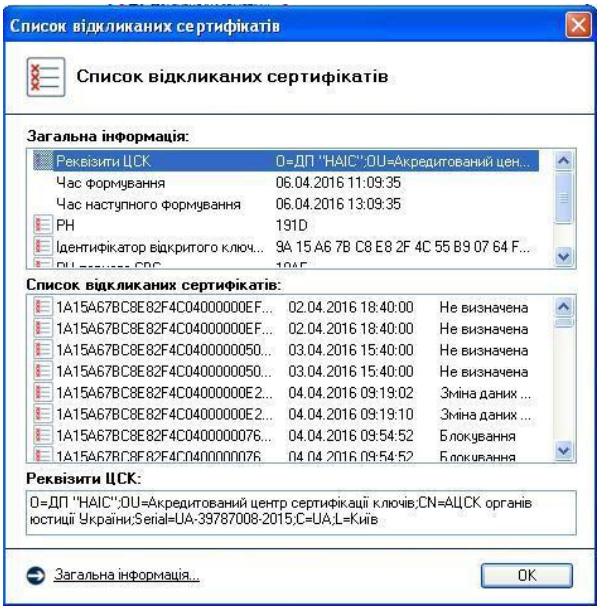


Рисунок 4.27

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 необхідно обрати підпункт «Згенерувати ключі» в пункті меню «Особистий ключ» (рис 5.1)

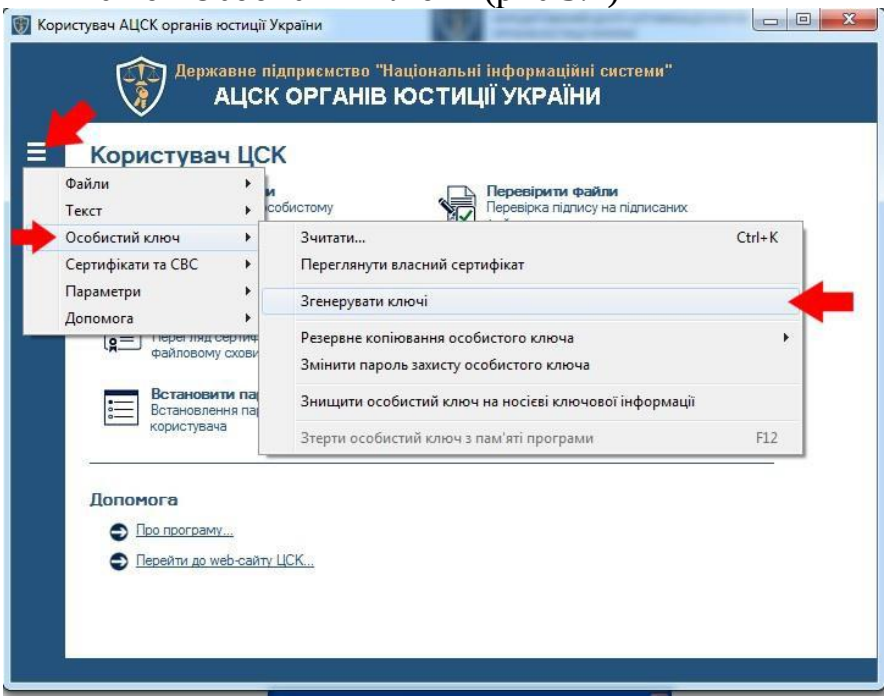


Рисунок 5.1

В наступному кроці оберіть тип алгоритму, за яким буде проводитись генерація ключів. Зазвичай, у більшості випадків необхідно обрати пункт «для державних алгоритмів та протоколів». Інші варіанти генерації необхідно обирати у тому випадку, коли користувач впевнений, що йому потрібний саме такий варіант генерації. На рис.5.2 зображений варіант за замовчуванням

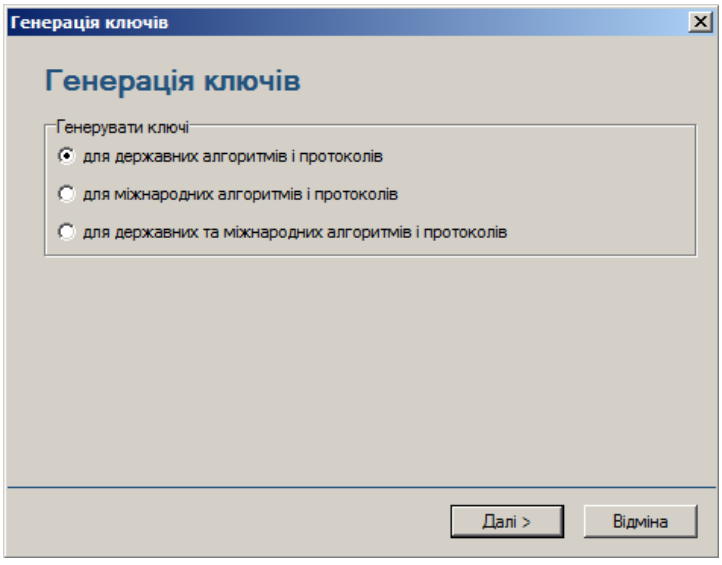


Рисунок 5.2

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 5.3):

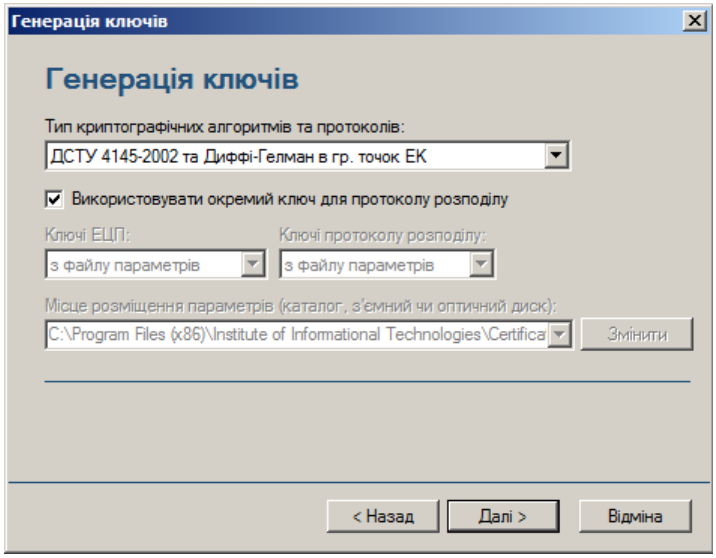


Рисунок 5.3

Після появи вікна запису особистого ключа, необхідно обрати носій, на якому буде згенеровано (або на який буде записано) особистий ключ, ввести пароль захисту до нього (з підтвердженням) та натиснути кнопку «Записати» (рис.5.4).

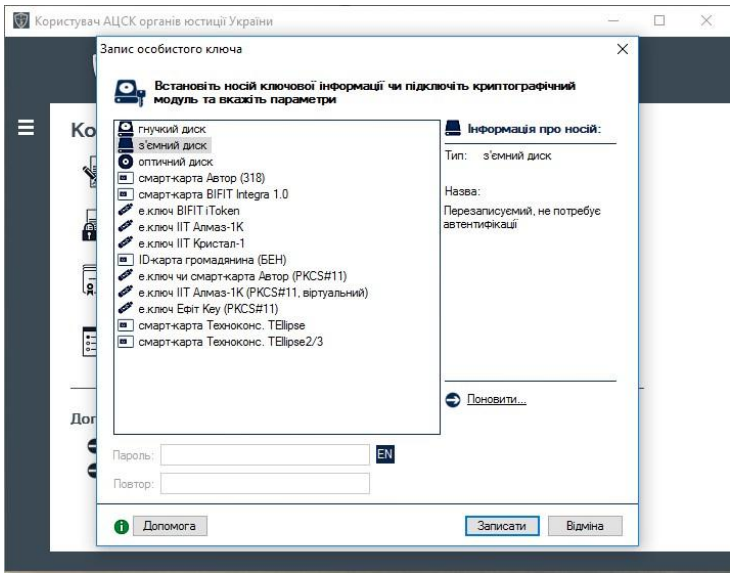


Рисунок 5.4

Обидва особистих ключа (для підпису та шифрування) будуть об'єднані в один файловий контейнер і записані у вигляді одного файлу особистого ключа – Key-6.dat.

Після генерування особистого ключа на ЗНОК (або запису його на з'ємний носій) буде виведено вміст запиту на формування сертифіката з відкритим ключем та запиту на формування сертифіката з відкритим ключем протоколу розподілу. Для продовження генерації натискаємо кнопку «ОК» (рис. 5.5, 5.6).

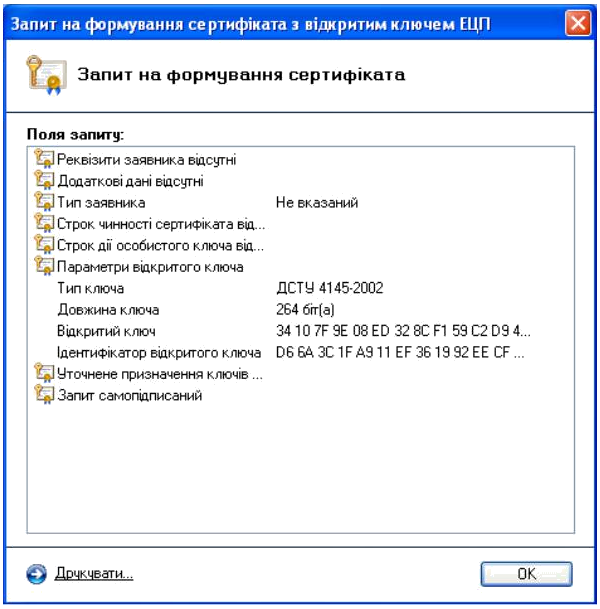


Рисунок 5.5

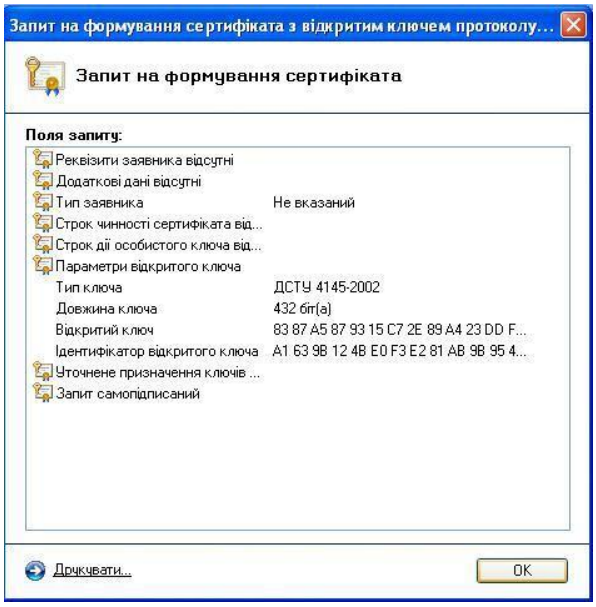


Рисунок 5.6

Для передачі запитів на формування кваліфікованих сертифікатів до АЦСК необхідно зберегти їх у файл (рис. 5.7). Для цього встановіть параметр «Зберегти у файл» та натисніть кнопку «Далі»

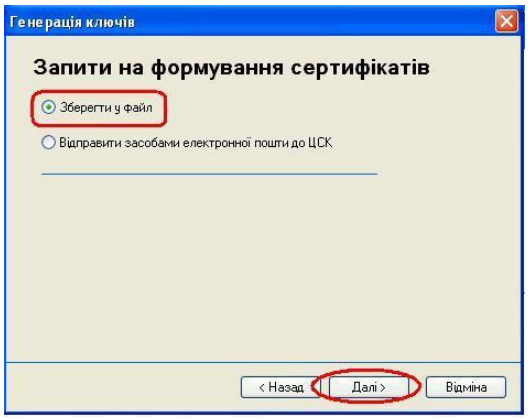


Рисунок 5.7

Запити повинні бути записані на носій інформації чи на жорсткий диск. Для цього необхідно обрати шлях до каталогу, де планується зберегти запити, натиснувши кнопку «Змінити» (рис. 5.8), та вказати необхідний носій інформації, ім’я запитів на формування сертифікатів, після чого натиснути «Далі»:

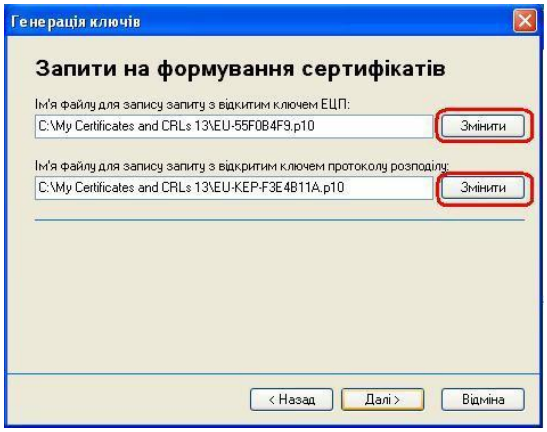


Рисунок 5.8

Увага! Для коректної ідентифікації запитів з відкритим ключем та протоколом розподілу користувача файл запиту на формування сертифіката повинен обов’язково зберігатись з ім’ям у наступному форматі:
«EU-XXXXXXXX-Прізвище.p10» та
«EU-KEP-XXXXXXXX-Прізвище.p10»,
де: Прізвище – прізвище 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:

EU-69PH0S9W-Іванов.p10; EU-KEP-KB50S67Z-Іванов.p10.

Для завершення генерації необхідно натиснути кнопку «Завершити» (рис. 5.9).

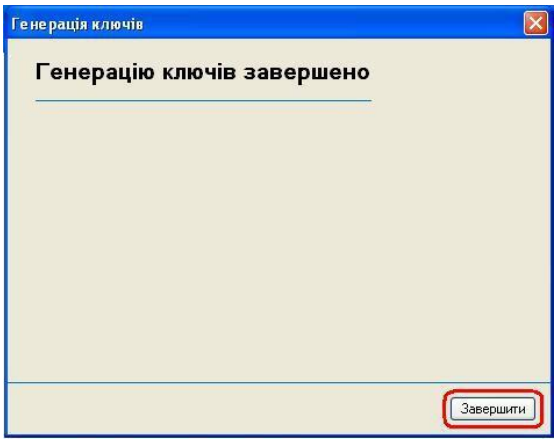


Рисунок 5.9

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

5.2 Зчитування особистого ключа

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 програми або шляхом вибору підпункту «Зчитати ...» в пункті меню «Особистий ключ» або шляхом натискання комбінації клавіш **Ctrl+K** (рис. 5.10)

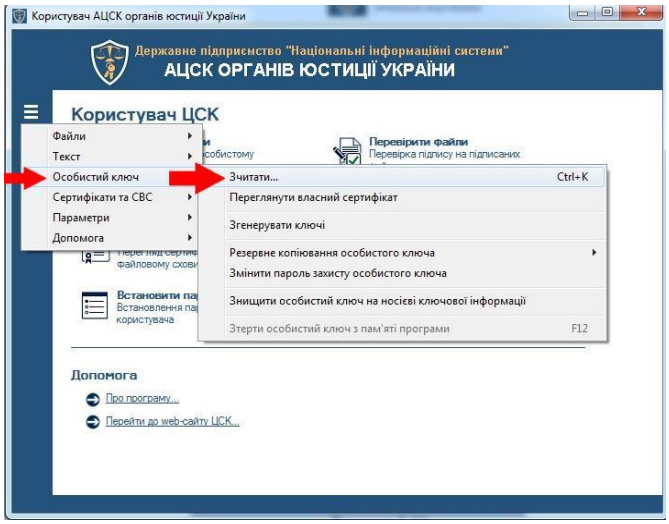


Рисунок 5.10

Після появи вікна зчитування особистого ключа (рис. 5.11), необхідно обрати НКІ, ввести пароль захисту особистого ключа та натиснути кнопку «Зчитати»

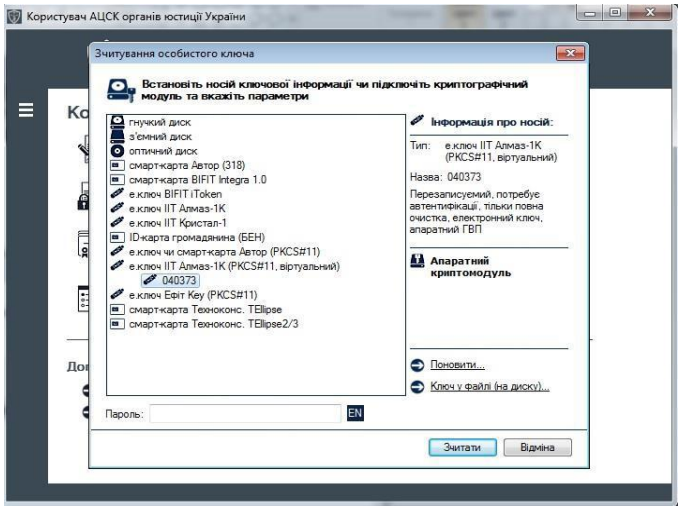


Рисунок 5.11

У випадку, коли сертифікат відкритого ключа ще відсутній у файловому сховищі, програма про це сповіщає користувача (рис. 5.12). Натисніть «ОК»:

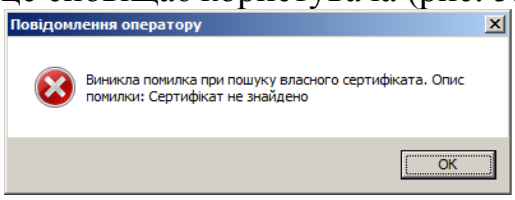


Рисунок 5.12

В наступному кроці діалогу буде запропоновано завантажити власний сертифікат з серверу АЦСК (рис. 5.13). Натисніть «Да»:

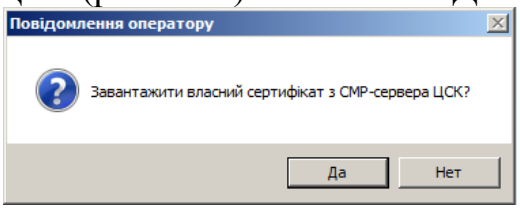


Рисунок 5.13

Програма після звернення із запитом до АЦСК виводить перелік сертифікатів, які будуть завантажені у разі позитивної відповіді користувача (рис. 5.14). Натисніть «Да»:

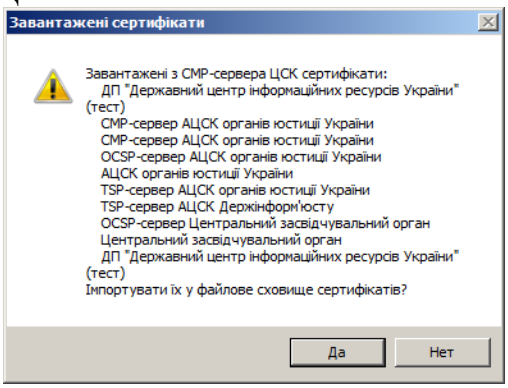


Рисунок 5.14

Інформація про те, що особистий ключ зчитаний та знаходиться в пам’яті ПК відображається у панелі стану вікна (рис. 5.15):

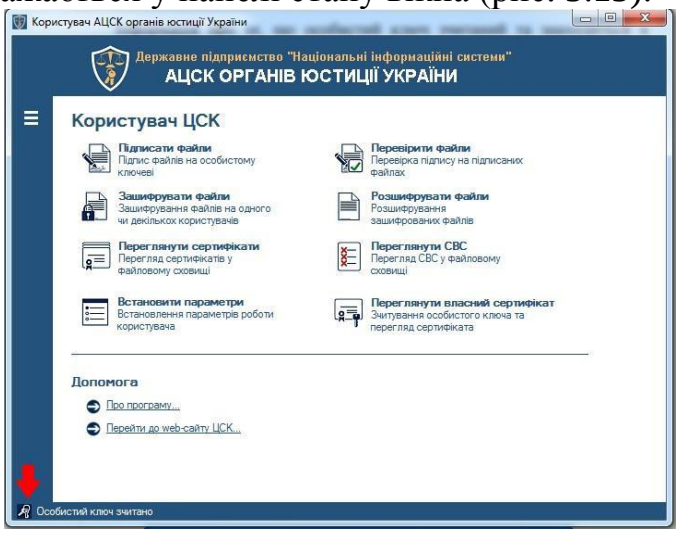


Рисунок 5.15

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. 5.16):

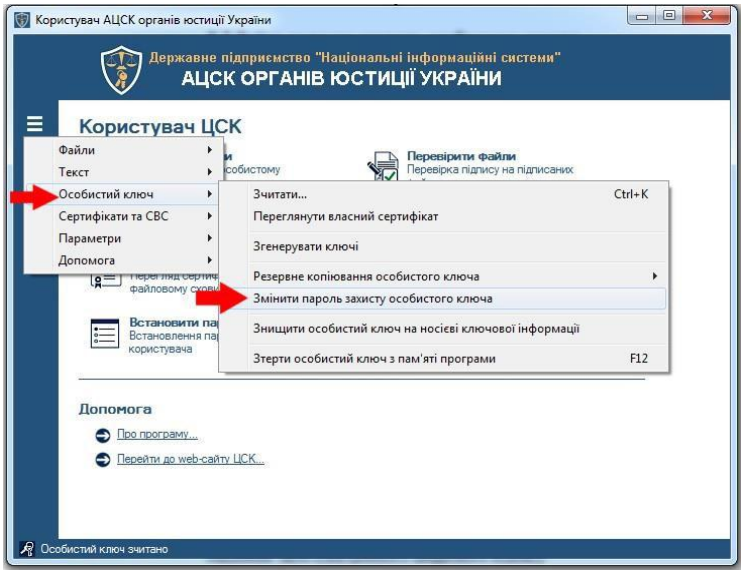


Рисунок 5.16

Після появи вікна зміни пароля доступу (рис. 5.17), необхідно вказати:
– тип НКІ;
– назву носія;
– пароль захисту особистого ключа;
– новий пароль захисту особистого ключа (з підтвердженням).

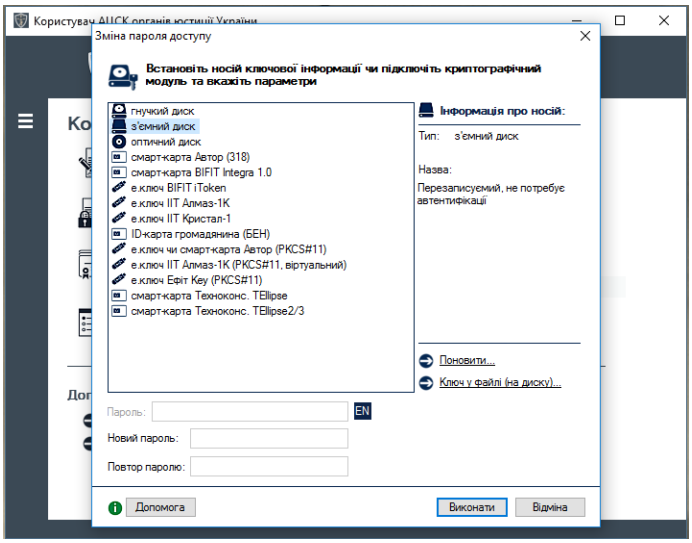


Рисунок 5.17

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. 5.18):

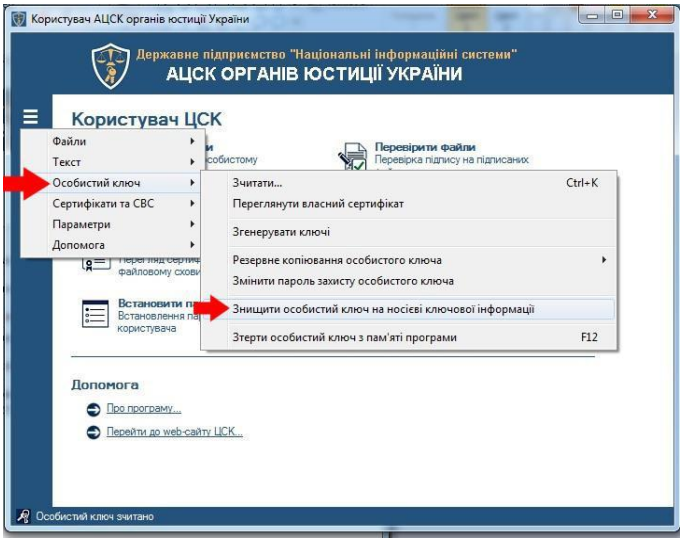


Рисунок 5.18

Після появи вікна знищення особистого ключа необхідно вказати тип та назву НКІ, ввести пароль захисту особистого ключа та натиснути кнопку «Знищити» (рис. 5.19):

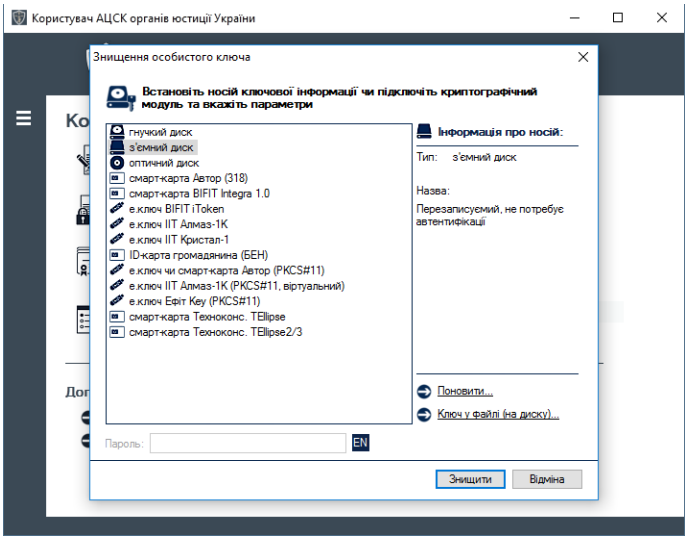


Рисунок 5.19

5.5 Знищення особистого ключа з пам’яті ПК

Програма 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» (рис. 5.20):

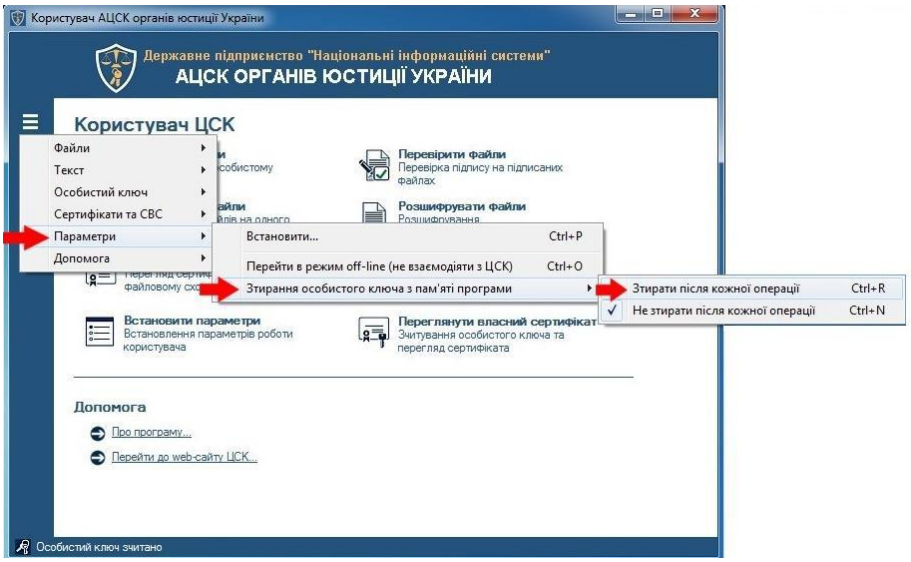


Рисунок 5.20

Якщо необхідно знищити ключ з пам’яті, не виходячи з програми, необхідно обрати пункт «Знищити особистий ключ з пам’яті програми» в меню програми «Особистий ключ» або натиснути клавішу F12 (рис. 5.21):

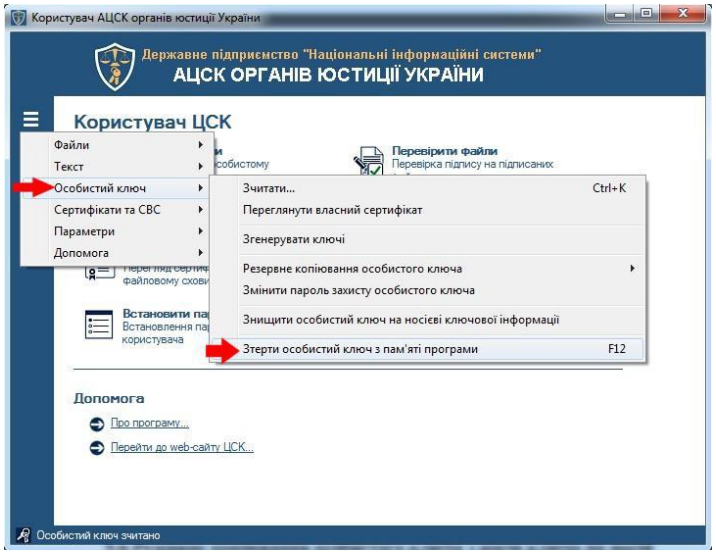


Рисунок 5.21

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. 5.22):

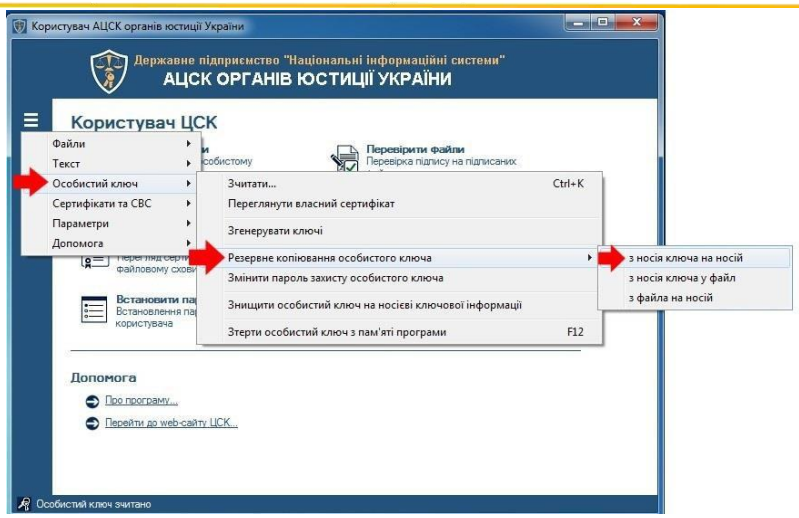


Рисунок 5.22

Після появи вікна зчитування особистого ключа необхідно обрати з'ємний НКІ, з якого буде знята копія, та ввести пароль захисту особистого ключа (рис. 5.23).

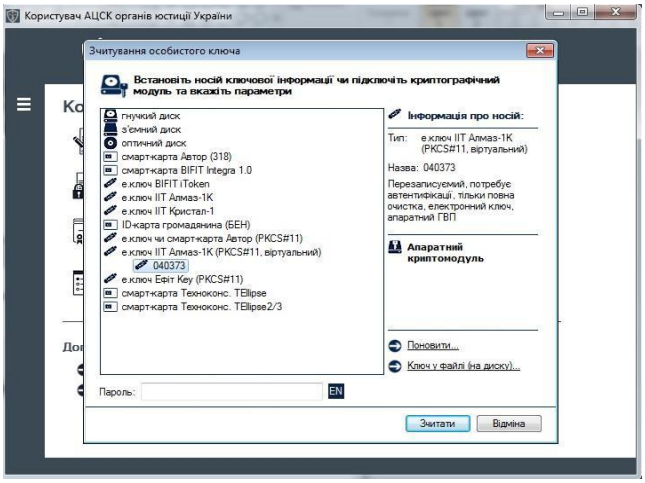


Рисунок 5.23

Далі необхідно обрати з'ємний НКІ, на який буде записана копія особистого ключа та ввести пароль захисту до нього (рис. 5.24)

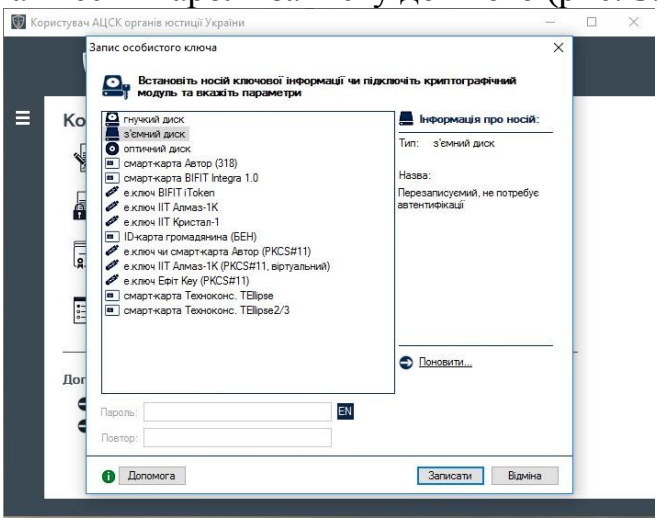


Рисунок 5.24

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 на носій» (рис. 5.25).

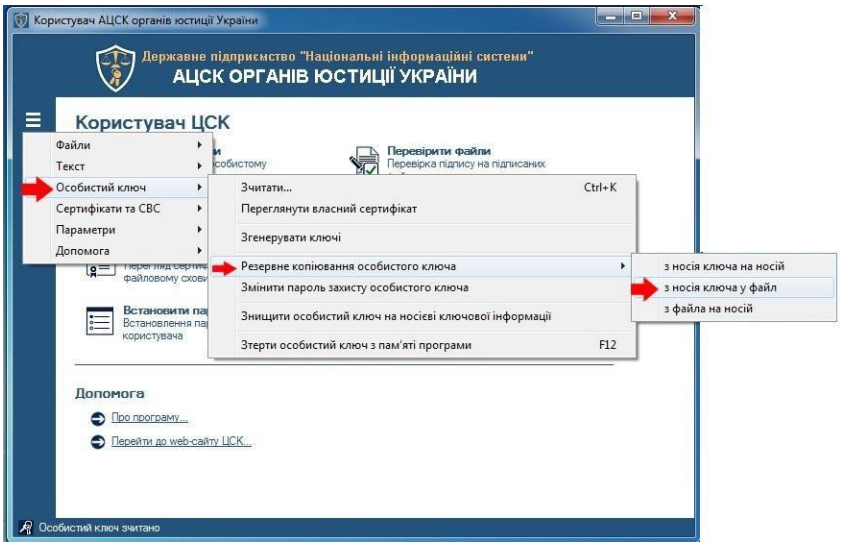


Рисунок 5.25

Після появи захищеного робочого столу необхідно обрати з’ємний НКІ, з якого буде знята копія, та ввести пароль захисту особистого ключа (рис. 5.26):

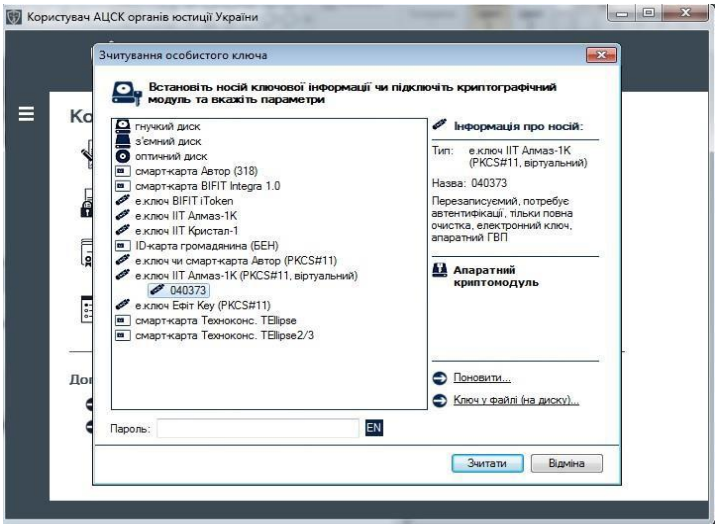


Рисунок 5.26

В наступному вікні необхідно обрати місце на жорсткому диску ПК, де буде записана копія особистого ключа (рис. 5.27).

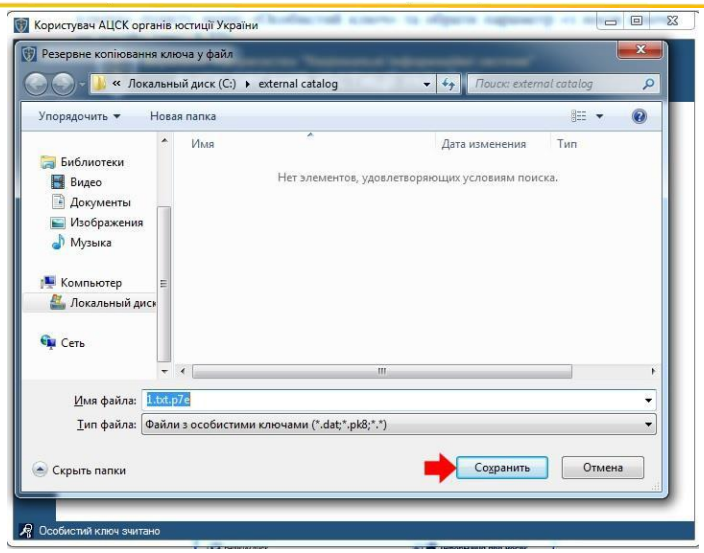


Рисунок 5.27

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

Після завершення резервного копіювання необхідно натиснути кнопку «ОК» (рис. 5.28):

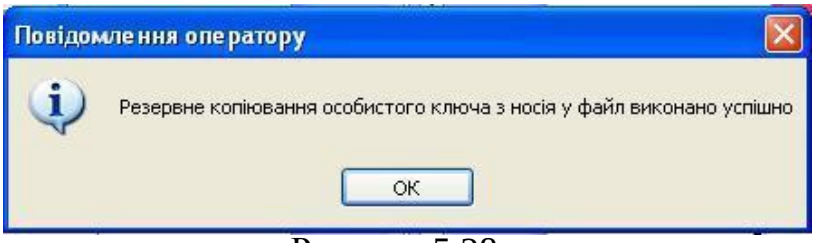


Рисунок 5.28

5.8 Резервне копіювання особистого ключа з файлу 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. 5.29):

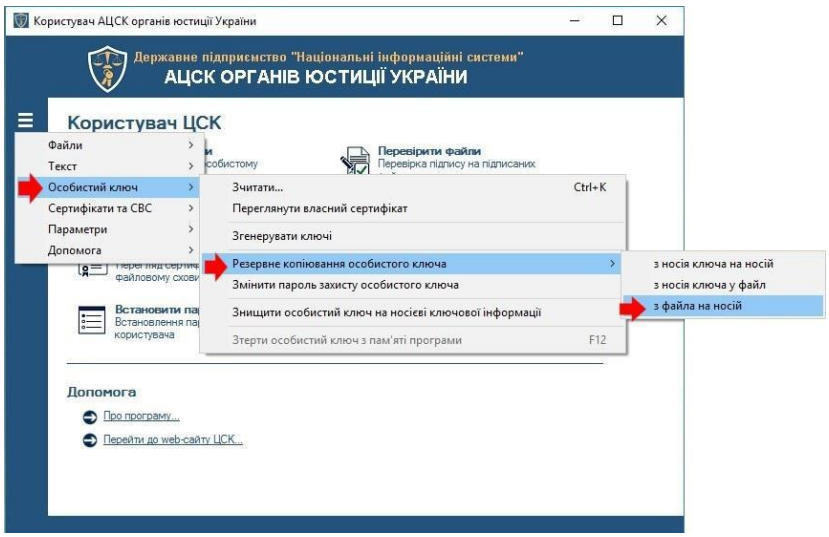


Рисунок 5.29

В наступному вікні необхідно обрати копію особистого ключа «Key-6.dat», розміщену на жорсткому диску ПК (рис. 5.30):

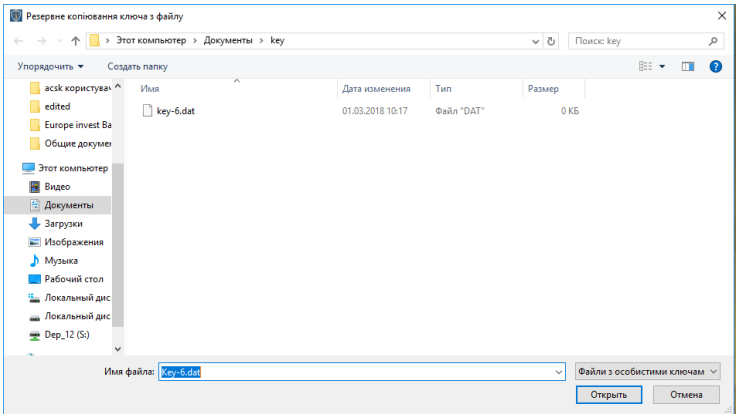


Рисунок 5.30

Після появи вікна запису особистого ключа захищеного робочого столу необхідно обрати НКІ, на який буде записана копія особистого ключа та ввести пароль захисту особистого ключа (рис. 5.31):

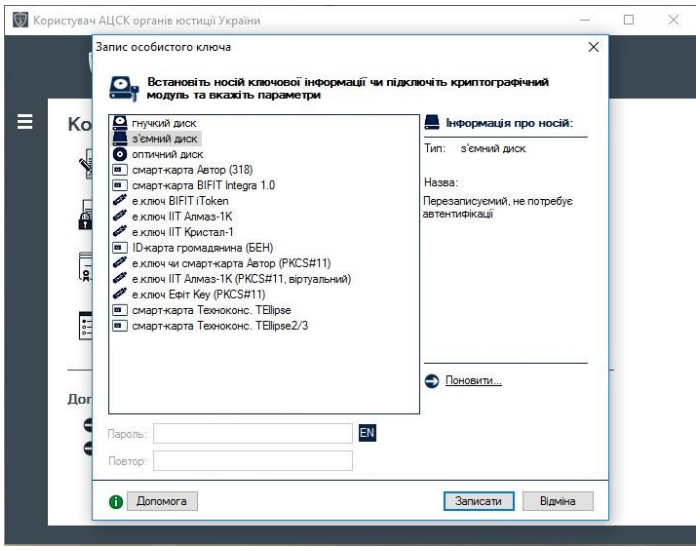


Рисунок 5.31

Після завершення резервного копіювання необхідно натиснути кнопку «ОК» (рис. 5.32):

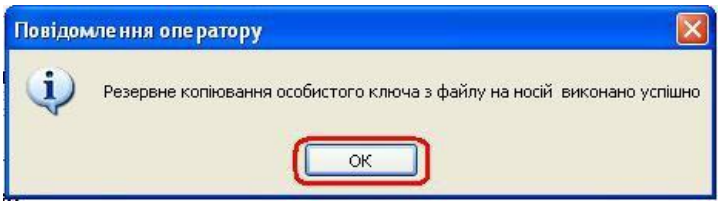


Рисунок 5.32

5.9 Блокування власного сертифіката

Для блокування власного сертифіката необхідно обрати підпункт «Заблокувати власний сертифікат» в пункті меню «Сертифікати та СВС» (рис. 5.33)

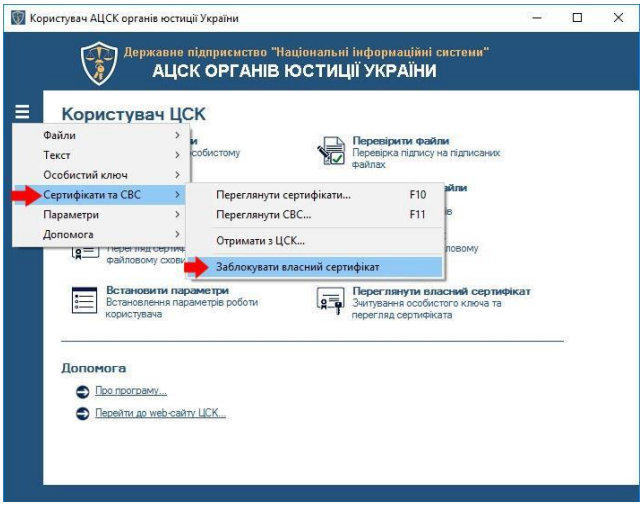


Рисунок 5.33

Далі з’являється повідомлення щодо блокування сертифіката, для підтвердження блокування натискаємо кнопку «Да» (рис. 5.34):

Рисунок 5.34

Після появи вікна зчитування особистого ключа захищеного робочого столу необхідно обрати НКІ та ввести пароль захисту особистого ключа (рис.5.35):

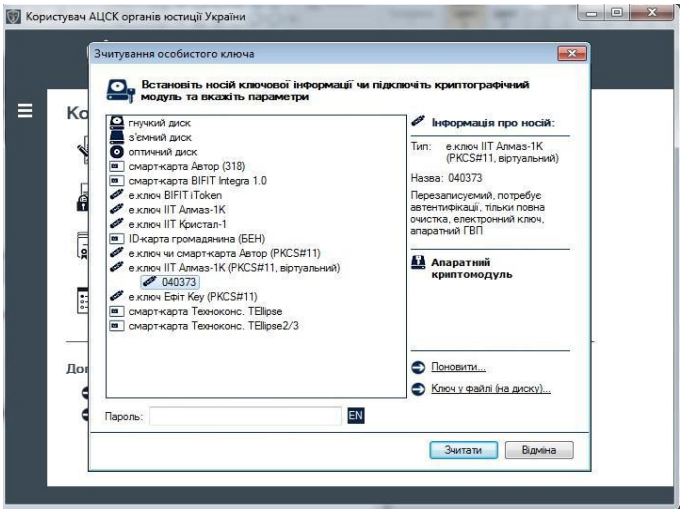


Рисунок 5.35

Після зчитування особистого ключа розпочне роботу майстер блокування сертифіката. На сторінці майстра необхідно ввести параметри підключення до сервера взаємодії ЦСК:

– DNS-ім’я чи IP-адресу сервера (ca.informjust.ua);

– TCP-порт (80);

– параметри доступу до proxy-сервера (за необхідністю та якщо не встановлено в параметрах роботи).

Після встановлення параметрів необхідно натиснути кнопку «Далі» (рис. 5.36):

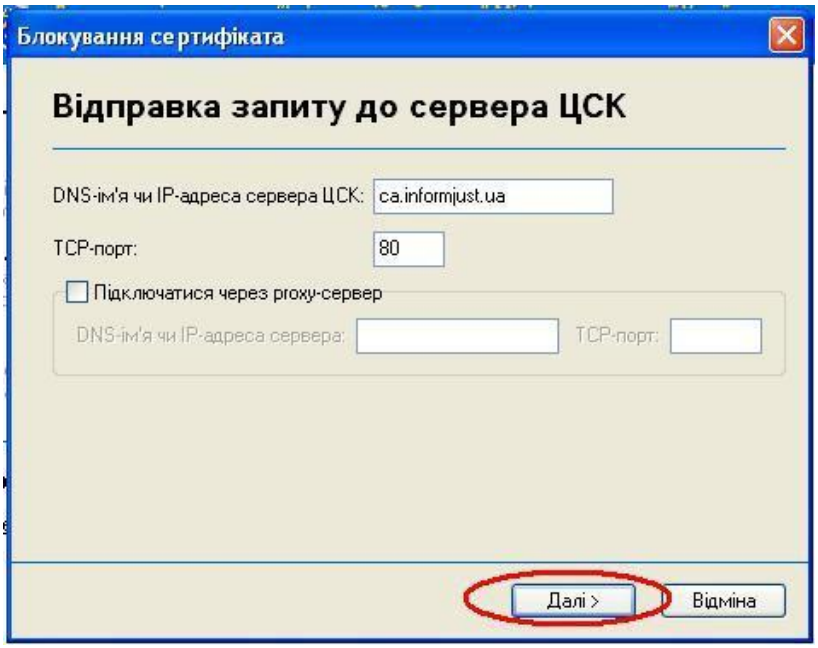


Рисунок 5.36

Після відправки запита на блокування сертифіката з’явиться вікно «Результат обробки запиту» (рис. 5.37):

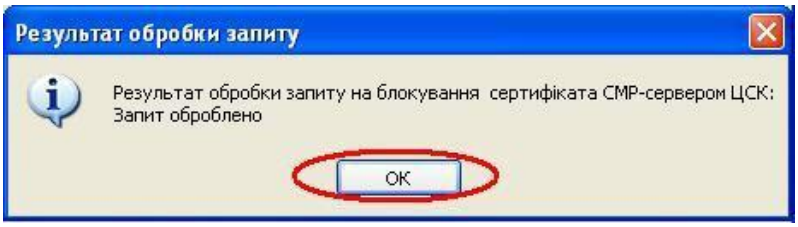


Рисунок 5.37

Для завершення роботи майстра натиснути кнопку «Завершити» (рис. 5.38):

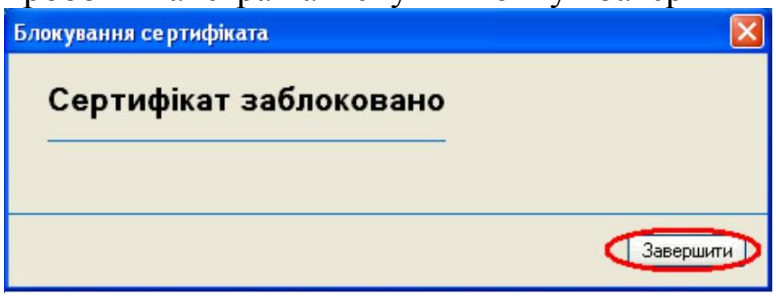


Рисунок 5.38

5.10 Off-line режим роботи програми

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

В off-line режимі програма не взаємодіє із ЦСК, тому on-line перевірка статусу сертифіката та позначка часу будуть недоступні.

Для перевірки статусу сертифікатів в off-line режимі необхідно використовувати СВС. Для цього необхідно виконати завантаження СВС (більш детально див. п. 4.6) та в налаштуваннях програми увімкнути параметр «Перевіряти СВС» (рис. 5.39 – 5.40):

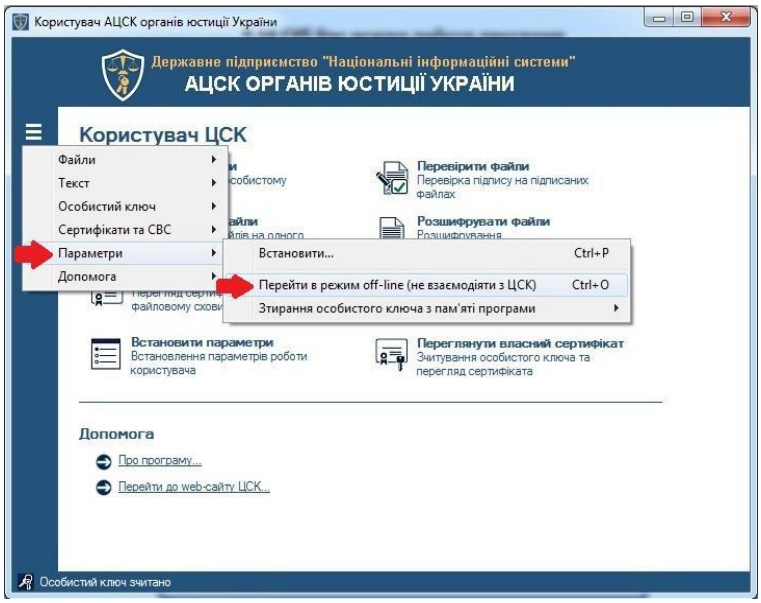


Рисунок 5.39

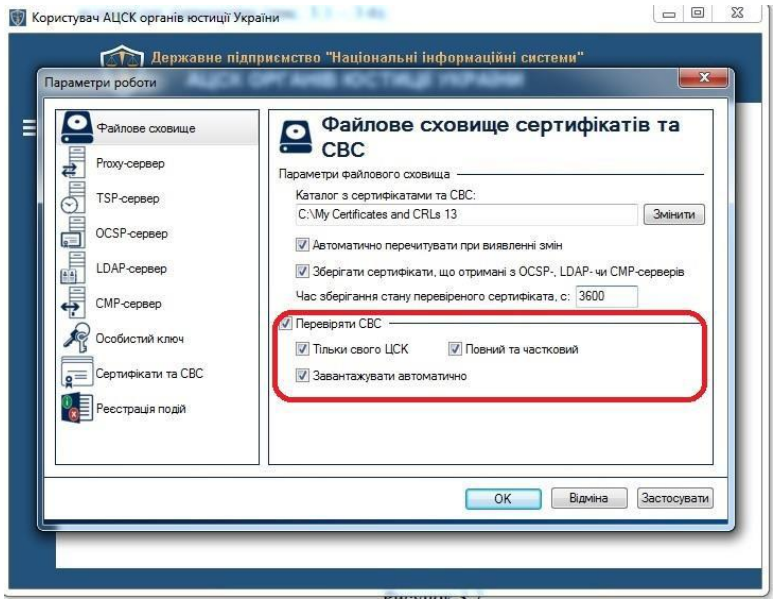


Рисунок 5.40

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. 5.41 - 5.43)

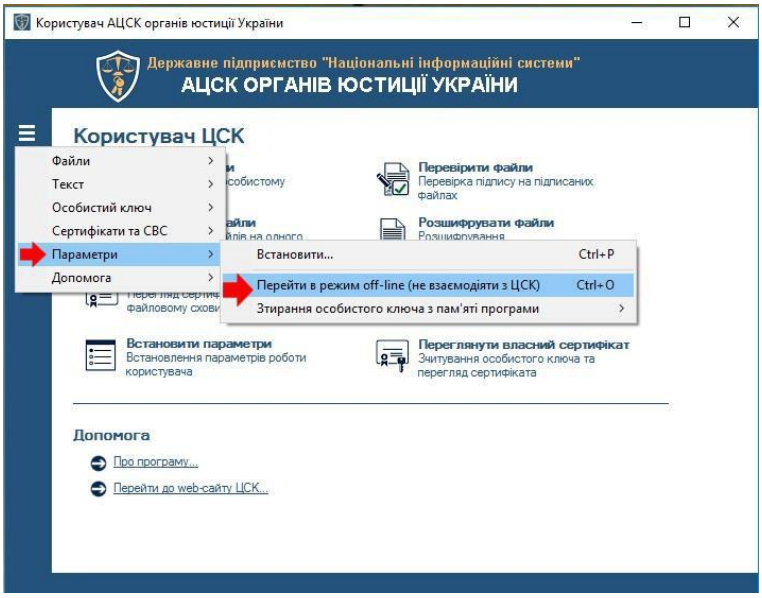


Рисунок 5.41

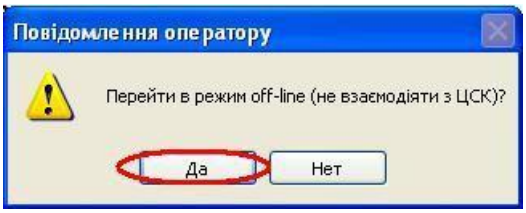


Рисунок 5.42

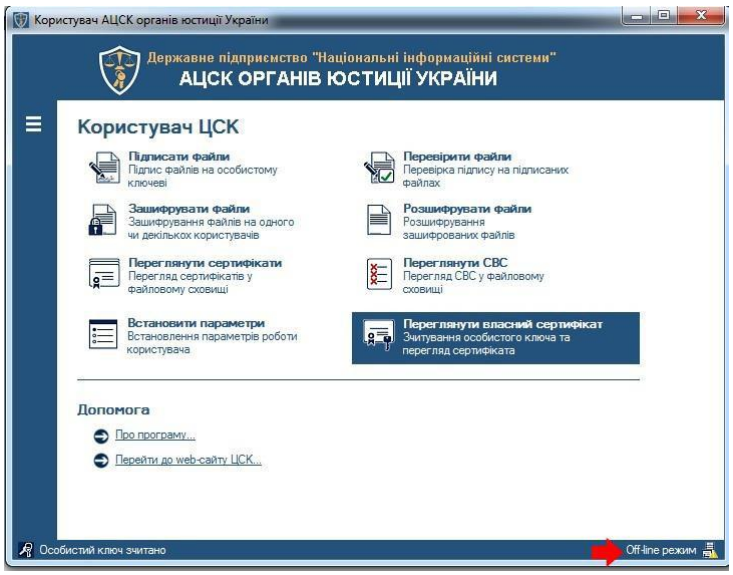


Рисунок 5.43