Інформаційно-довідковий департамент Міндоходів

Акредитований центр сертифікації ключів

НАСТАНОВА КОРИСТУВАЧА

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

Київ 2014 р.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ЕОМ	–	Електронно-обчислювальна машина;
ЕЦП	–	Електронний цифровий підпис;
НКІ	–	Носій ключової інформації;
ОС	–	Операційна система;
ПЕОМ	–	Персональна електронно-обчислювальна машина;
ПЗ	–	Програмне забезпечення;
СВС	–	Список відкликаних сертифікатів;
ЦСК	–	Центр сертифікації ключів Інформаційно-довідкового департаменту Міндоходів;
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);
веб-сайт	–	Офіційний інформаційний ресурс АЦСК ІДД Міндоходів (http://acskidd.gov.ua)
файлове сховище	–	Каталог (папка), призначений для зберігання посилених сертифікатів та СВС

Призначення програми

Програмне забезпечення «ІІТ Користувач ЦСК-1» (далі – програма) є надійним засобом ЕЦП та призначене для застосування на засобах ЕОМ, ПЕОМ користувача ЦСК і виконує наступні функції:

- **управління ключами користувача:**
  - генерацію ключів користувача ЦСК, запис особистого ключа на НКІ та формування запита на формування сертифіката;
  - резервне копіювання особистого ключа з одного НКІ на інший;
  - зміну паролю захисту особистого ключа;
  - знищення особистого ключа на НКІ;
  - формування та передачу у ЦСК запита на блокування сертифіката користувача;
  - формування та передачу запита на формування нового сертифіката;
- **доступ до сертифікатів ЦСК, серверів ЦСК, 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 ЕЦП;
  - шифрування файлів;
  - розшифрування файлів.

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

Завантажити архівний файл з інсталяційним пакетом програми з веб-сайту за наступним посиланням: http://acskidd.gov.ua/korustyvach_csk.

Далі потрібно розпакувати архівний файл, здійснити інсталяцію програмного забезпечення виконавши наступні дії:

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

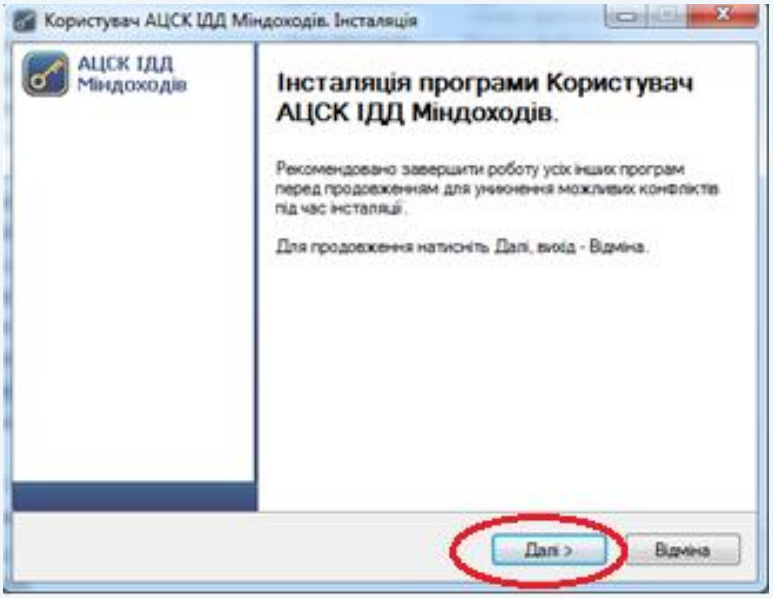

Рисунок 1.1

1.2 Ознайомлюємось з ліцензійною угодою та погоджуємось з її умовами, для продовження інсталяції натискаємо кнопку «Далі» (рис. 1.2).

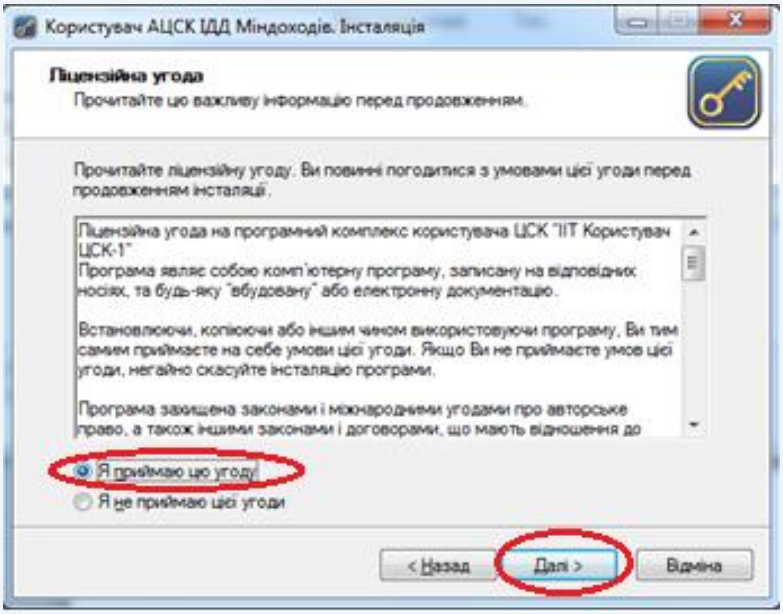

Рисунок 1.2

1.3. Каталог розміщення програми створюється автоматично (за замовченням C:\Program Files\Institute of Informational Technologies\Certificate Authority-1.3\End

User), змінювати його не рекомендується. Для продовження інсталяції натискаємо кнопку «Далі» (рис. 1.3).

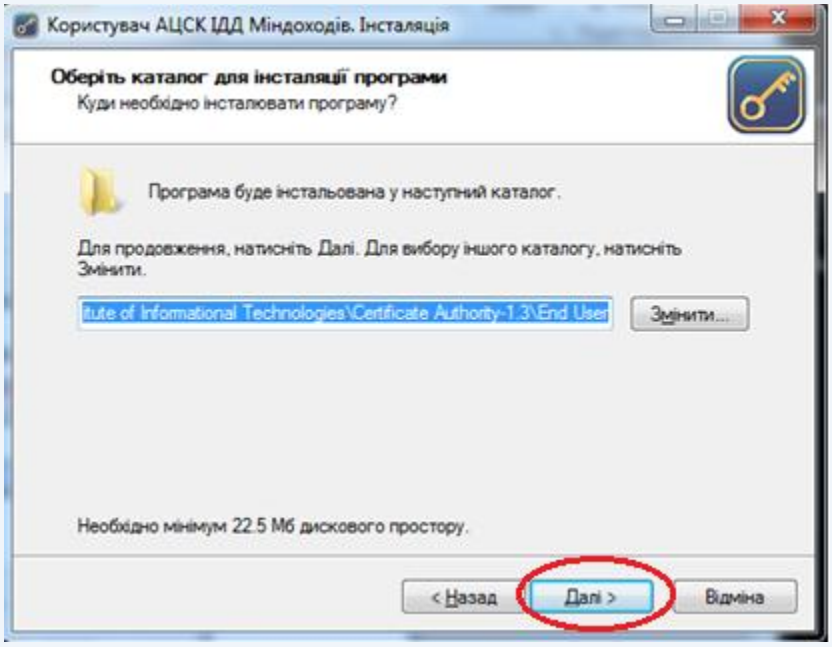

Рисунок 1.3

1.4 Каталог програми у меню «Пуск» створюється автоматично, змінювати його не рекомендується, натискаємо кнопку «Далі» (рис. 1.4).

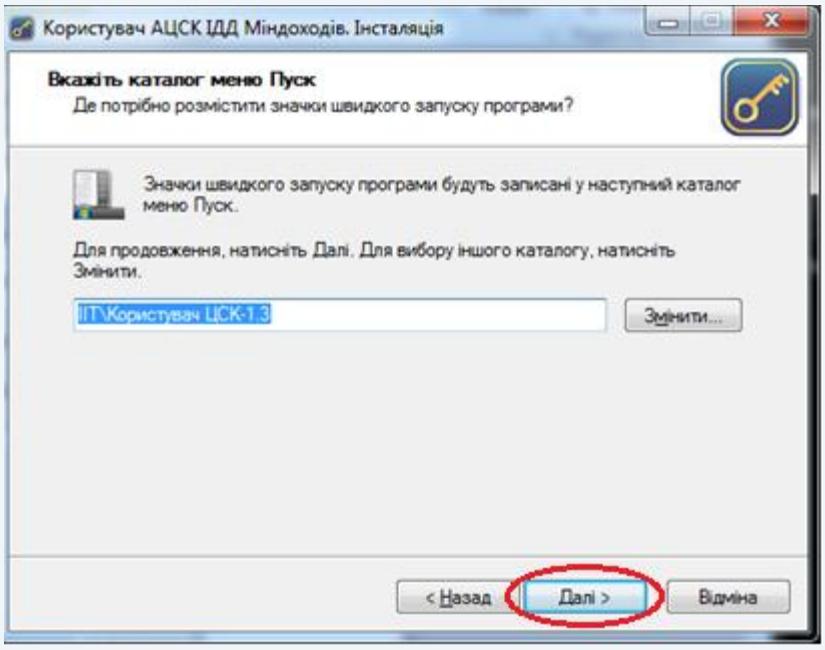

Рисунок 1.4

1.5 Під час встановлення програми файлове сховище для посилених сертифікатів та СВС створюється автоматично. Для зміни розташування файлового сховища потрібно натиснути кнопку «Змінити» та обрати відповідний каталог. Для продовження інсталяції натискаємо кнопку «Далі» (рис. 1.5).

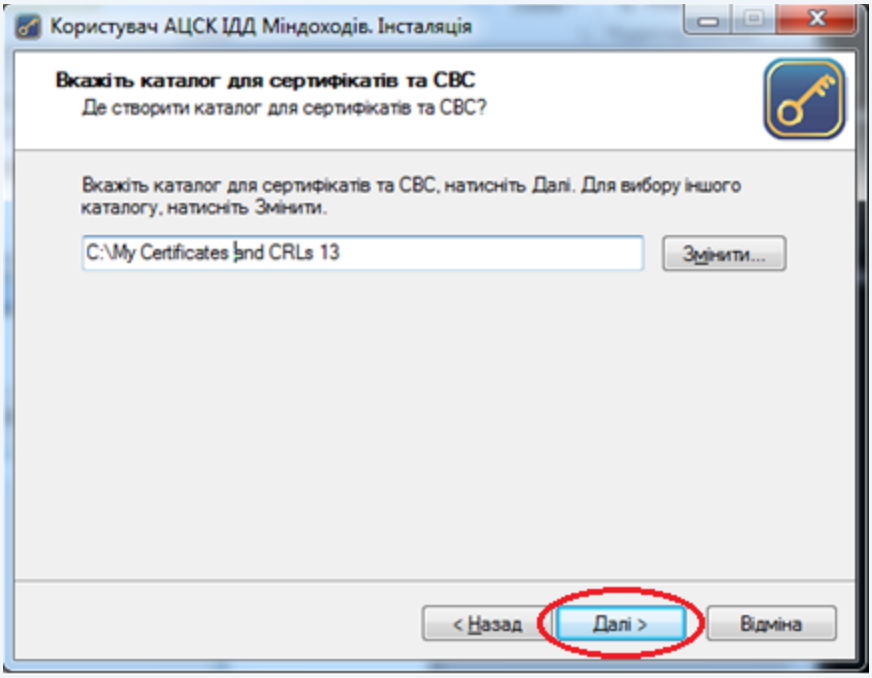

Рисунок 1.5

1.6 За необхідності можна створити ярлик на робочому столі та запустити програму після завершення її інсталяції, для цього проставити відповідні позначки (рис. 1.6). Для продовження інсталяції натискаємо кнопку «Далі».

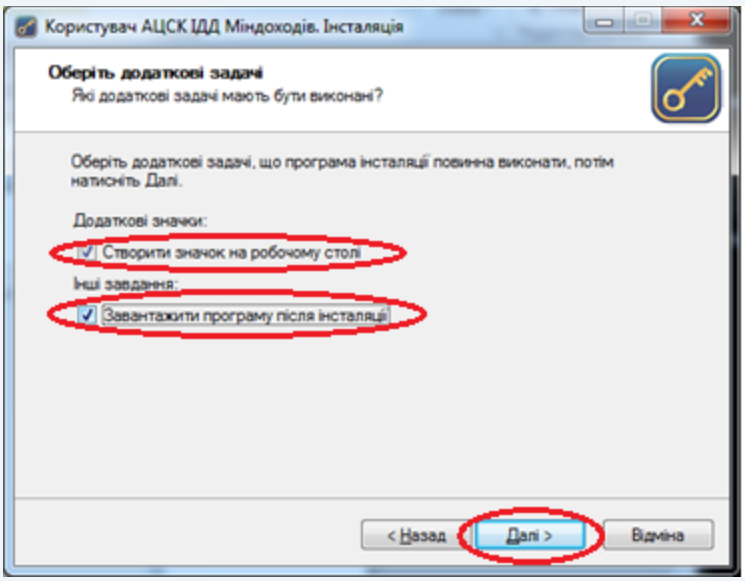

Рисунок 1.6

1.7 У вікні готовності до інсталяції натискаємо кнопку «Встановити». Якщо параметри інсталяції не задовольняють користувача, їх можна змінити натиснувши кнопку «Назад». Для виходу з програми потрібно натиснути «Відміна» (рис. 1.7).

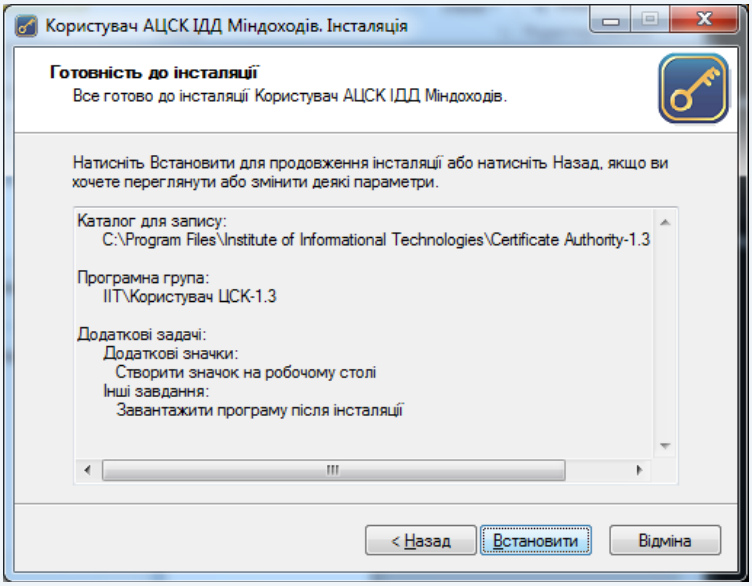

Рисунок 1.7

1.8 Після завершення інсталяції запущена програма має такий вигляд (рис. 1.8). Перед використанням програму необхідно налаштувати.

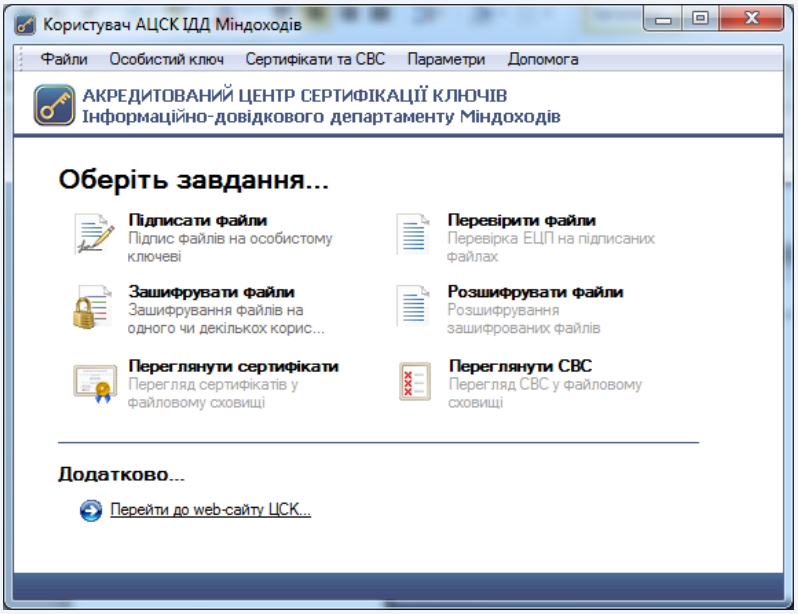

Рисунок 1.8

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

Після інсталяції програми до **файлового сховища** потрібно додати сертифікати користувача/підписувача.

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

У разі необхідності, розташування файлового сховища можна змінити (рис. 2.1).

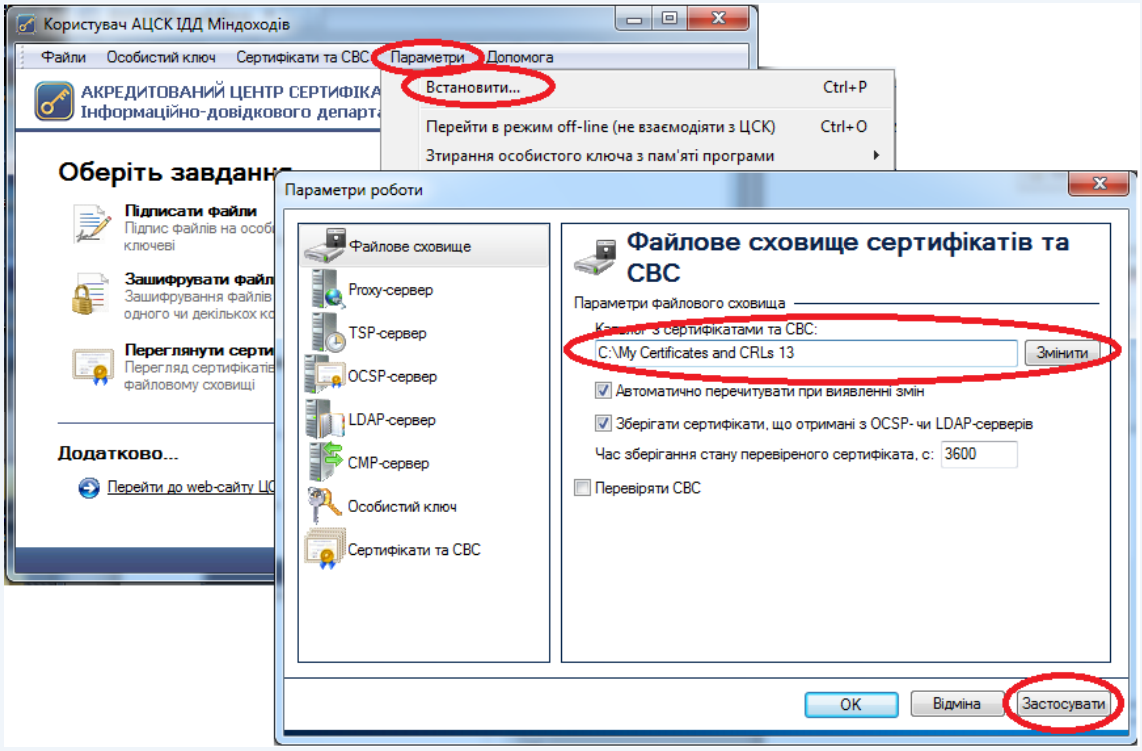

Рисунок 2.1

Виконати пошук сертифіката можна на веб-сайті в розділі «Пошук сертифікатів», використовуючи поле «Загальне ім’я» (ввівши ПІБ підписувача) або поле «Код платника податків» (ввівши реєстраційний номер облікової картки платника податків) (рис. 2.2) та натиснути кнопку «Пошук».

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

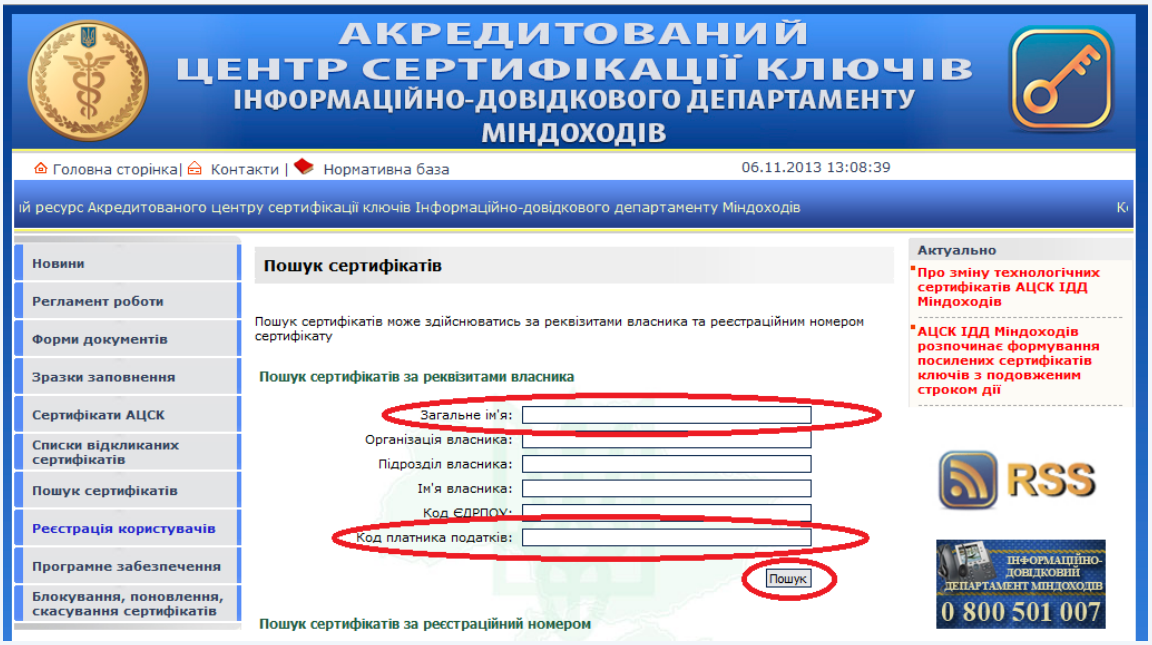

Рисунок 2.2

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

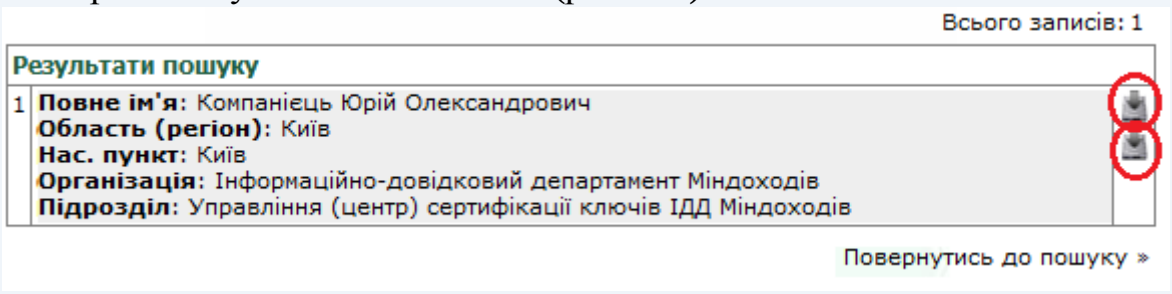

Рисунок 2.3

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

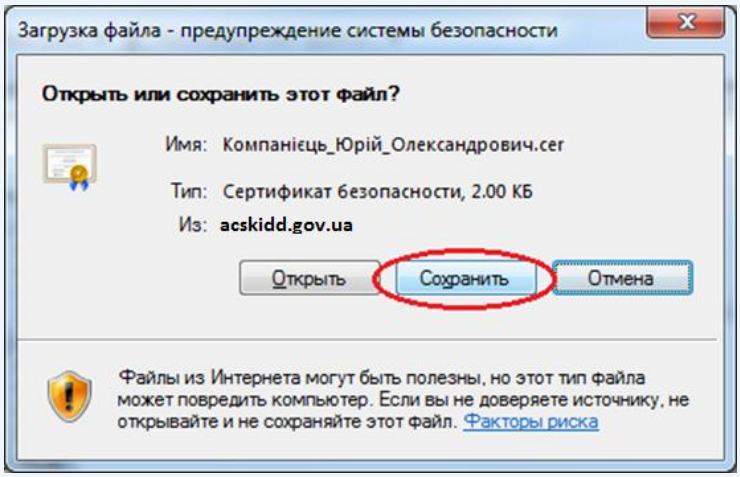

Рисунок 2.4

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

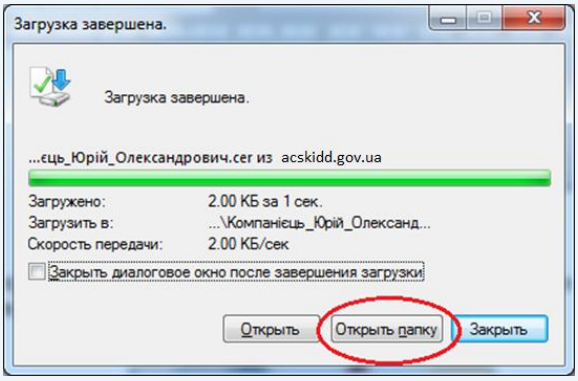

Рисунок 2.5

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

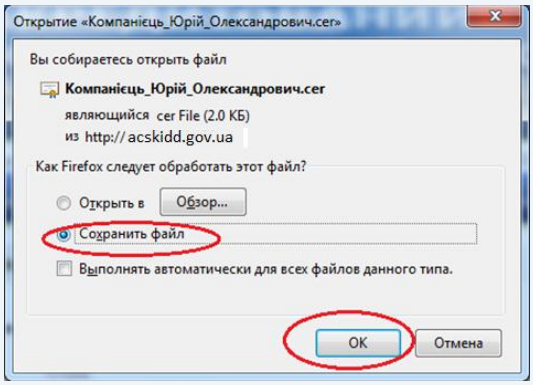

Рисунок 2.6

Далі у вікні «Загрузки», після закінчення процесу завантаження потрібно обрати свій сертифікат та натиснувши праву кнопку миші обрати пункт меню «Открыть папку с файлом» (рис. 2.7).

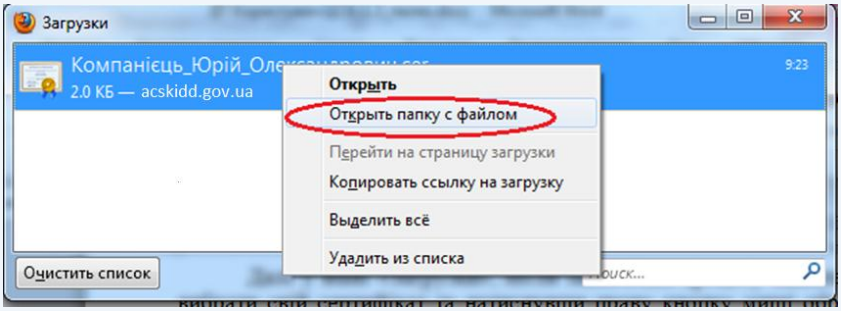

Рисунок 2.7

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

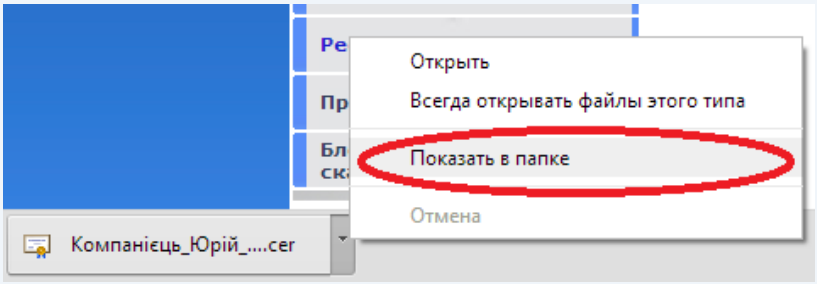

Рисунок 2.8

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

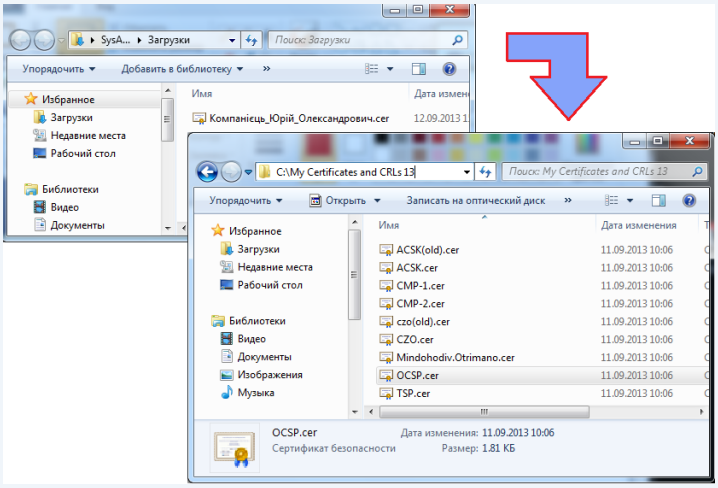

Рисунок 2.9

Окрім сертифікатів користувачів у файловому сховищі знаходяться **технологічні сертифікати**, що використовуються при шифруванні/розшифруванні файлів, накладанні/перевірці підпису та інше.

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

Якщо технологічні сертифікати відсутні у файловому сховищі їх необхідно завантажити з веб-сайту (розділ Сертифікати АЦСК) (рис. 2.10).

Рисунок 2.10

Також можна 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. 2.11).

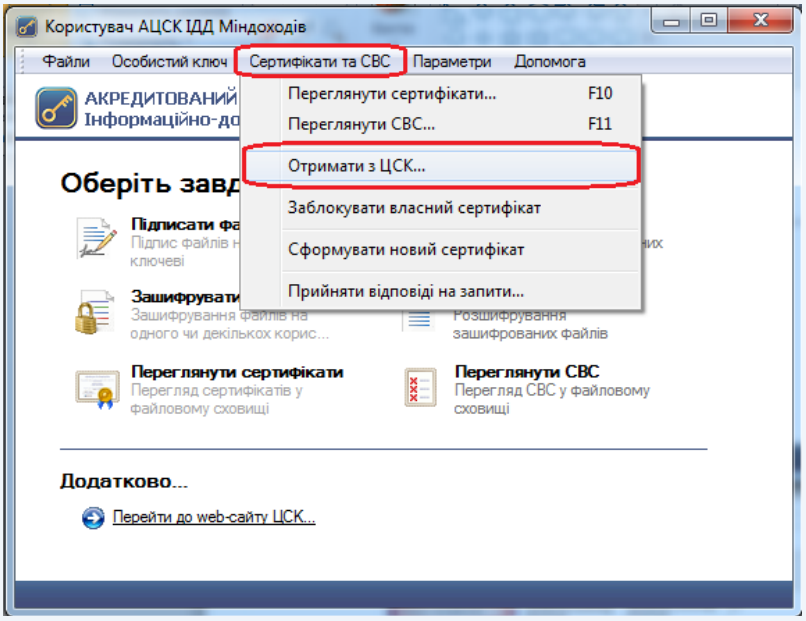

Рисунок 2.11

Після чого буде виведене вікно, що наведене на рис. 2.12. Для продовження формування запиту на автоматичне завантаження сертифікатів натиснути «Далі».

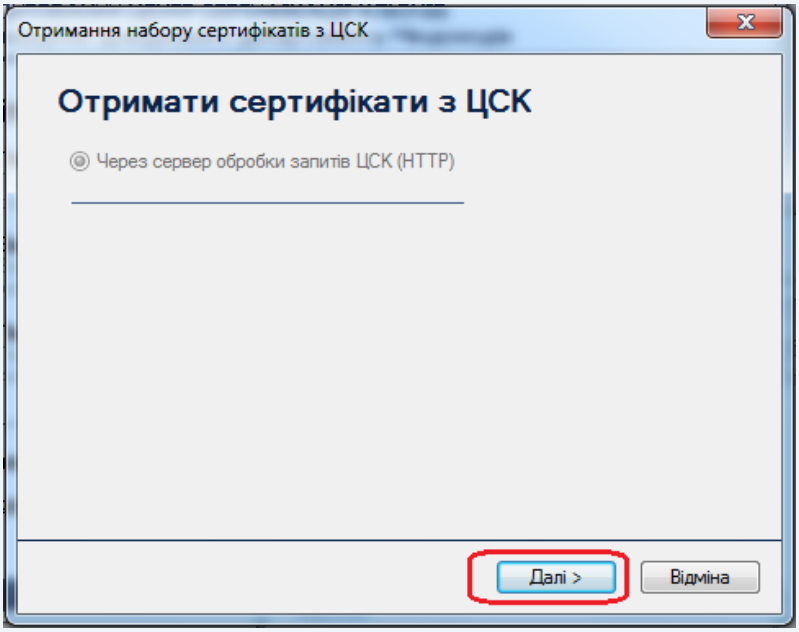

Рисунок 2.12

Після чого з'являється захищений робочий стіл, у якому необхідно обрати носій ключової інформації та ввести пароль захисту особистого ключа (рис. 2.13).

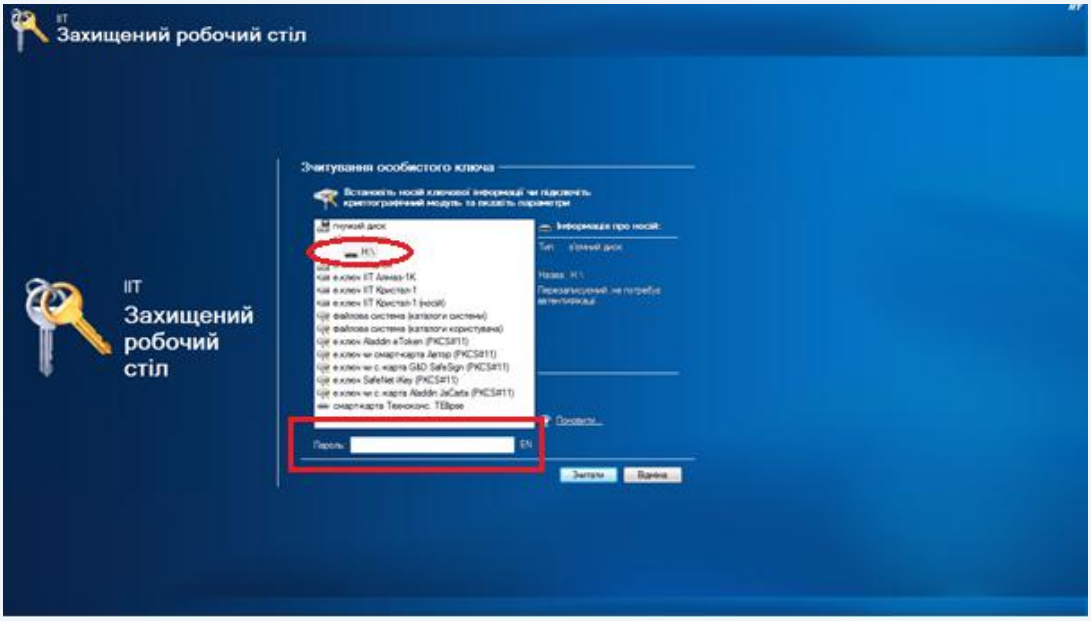

Рисунок 2.13

Після зчитування особистого ключа буде виведене вікно (рис. 2.14) у якому необхідно вказати параметри доступу до сервера обробки АЦСК ІДД Міндоходів (у полі DNS-ім'я вказати – **acskidd.gov.ua**, та в полі TCP-порт – **80**).

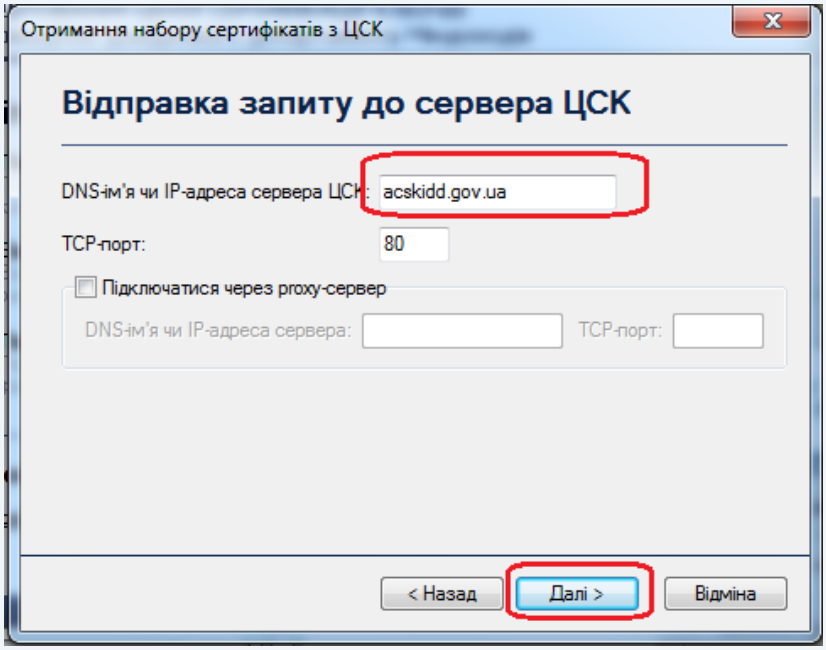

Рисунок 2.14

При відкритті вікна «Завантажені сертифікати» (рис. 2.15), необхідно зберегти їх до файлового сховища натиснувши кнопку «Да».

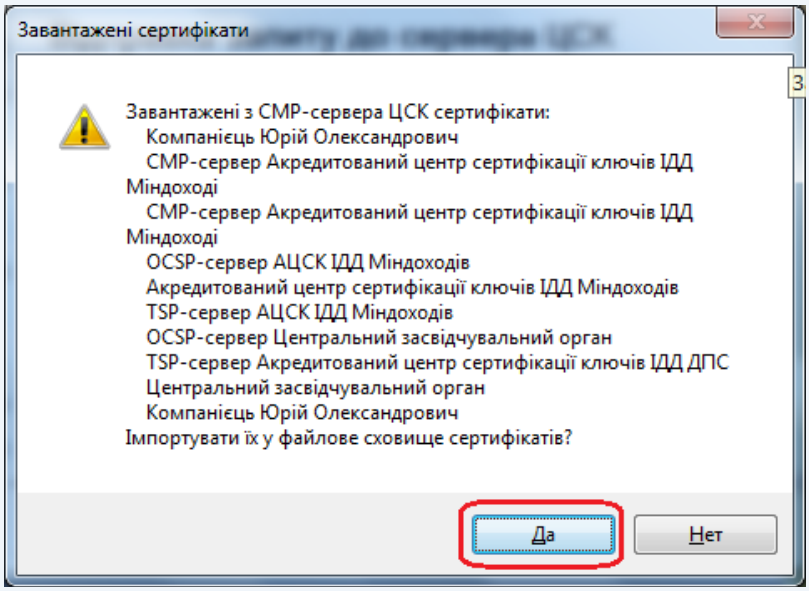

Рисунок 2.15

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

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

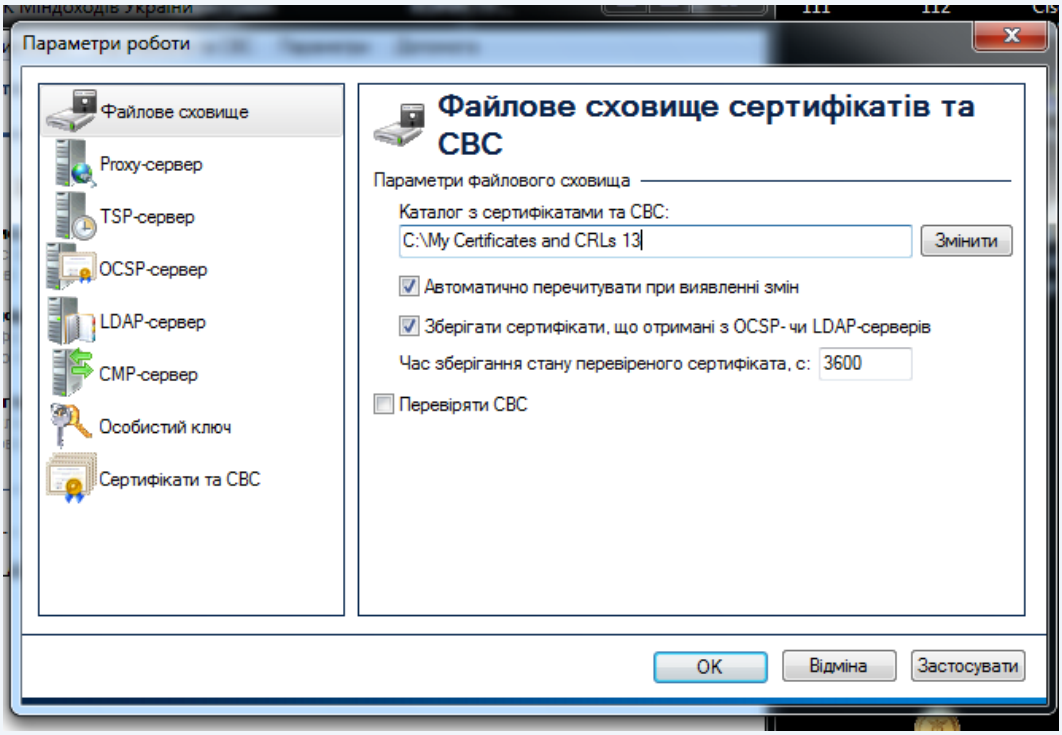

Рисунок 3.1

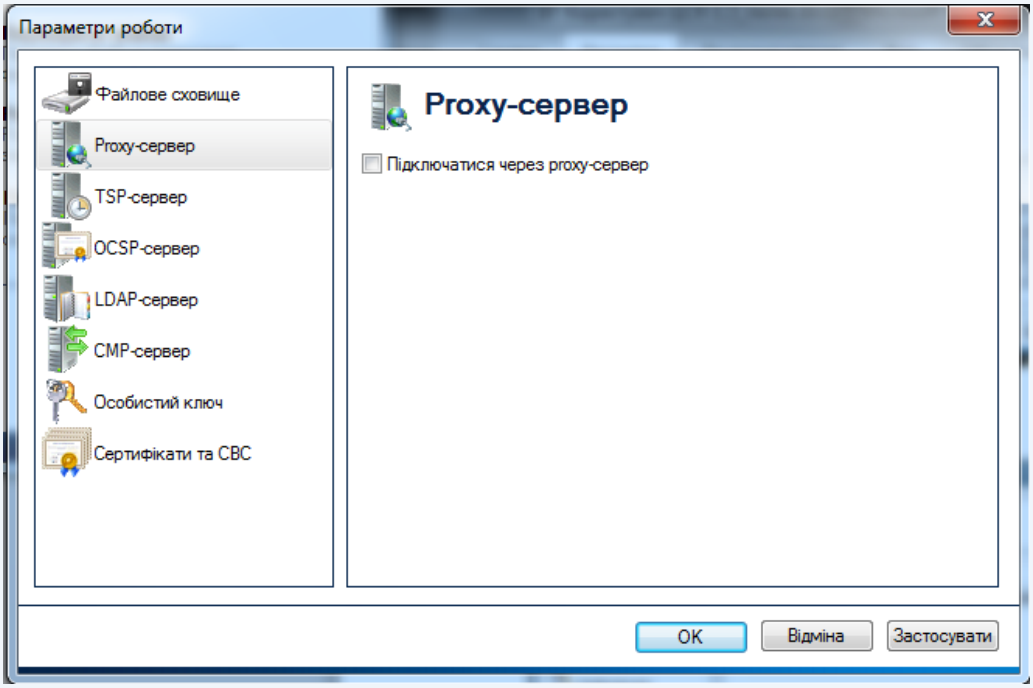

Рисунок 3.2

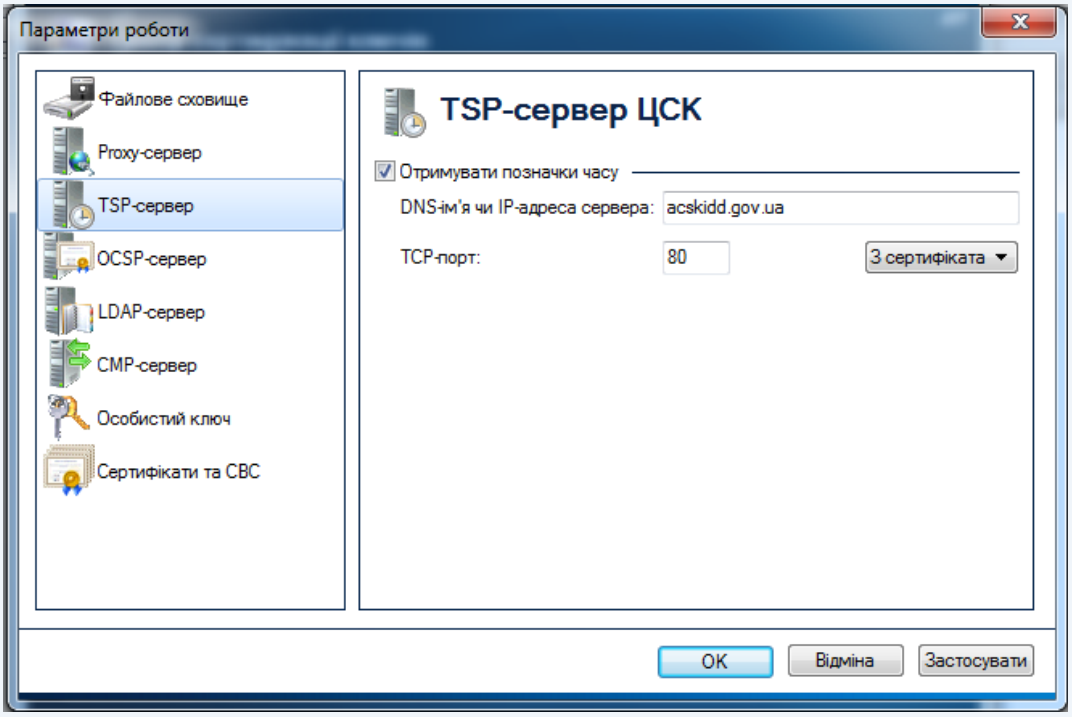

Рисунок 3.3

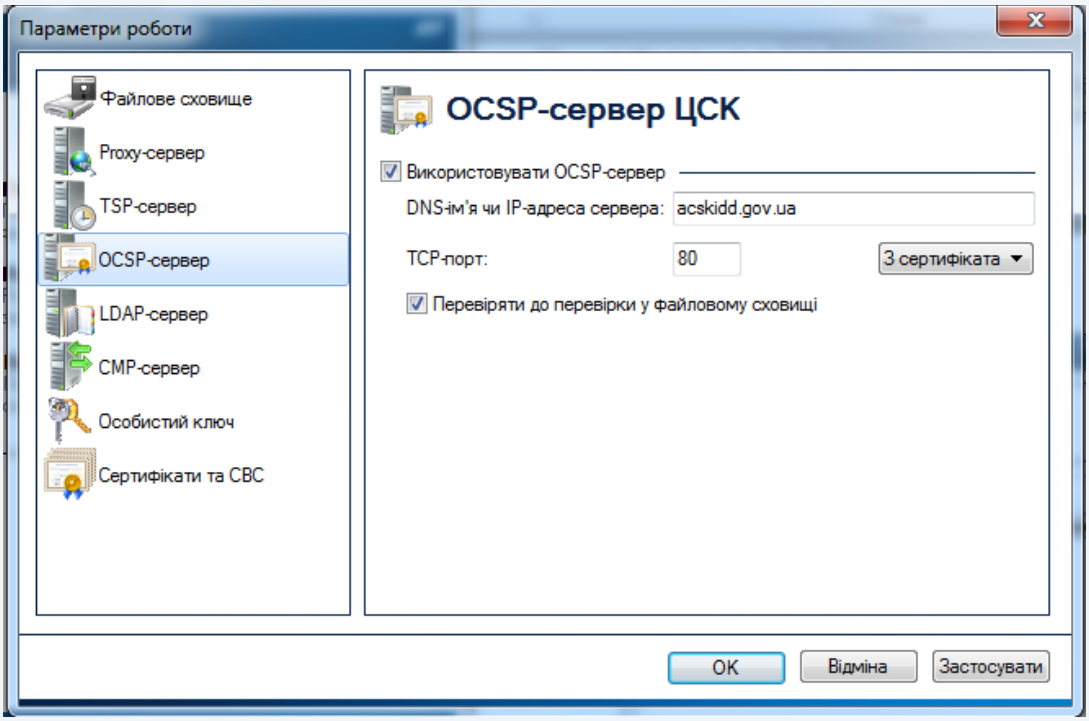

Рисунок 3.4

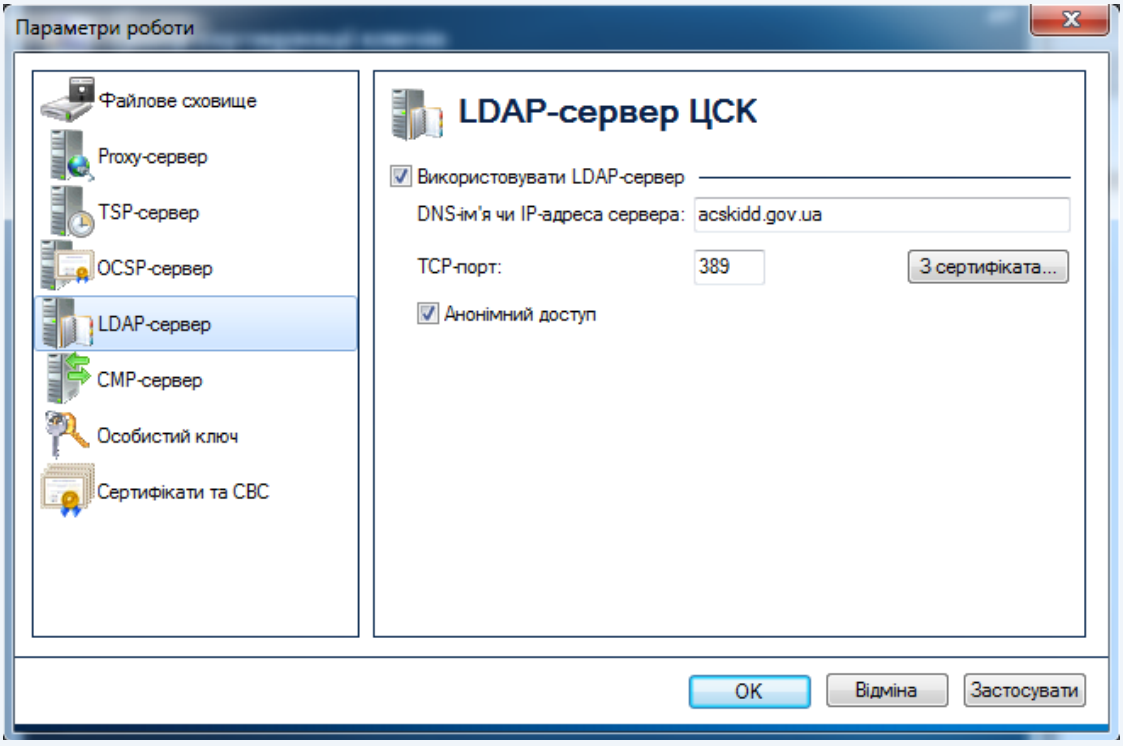

Рисунок 3.5

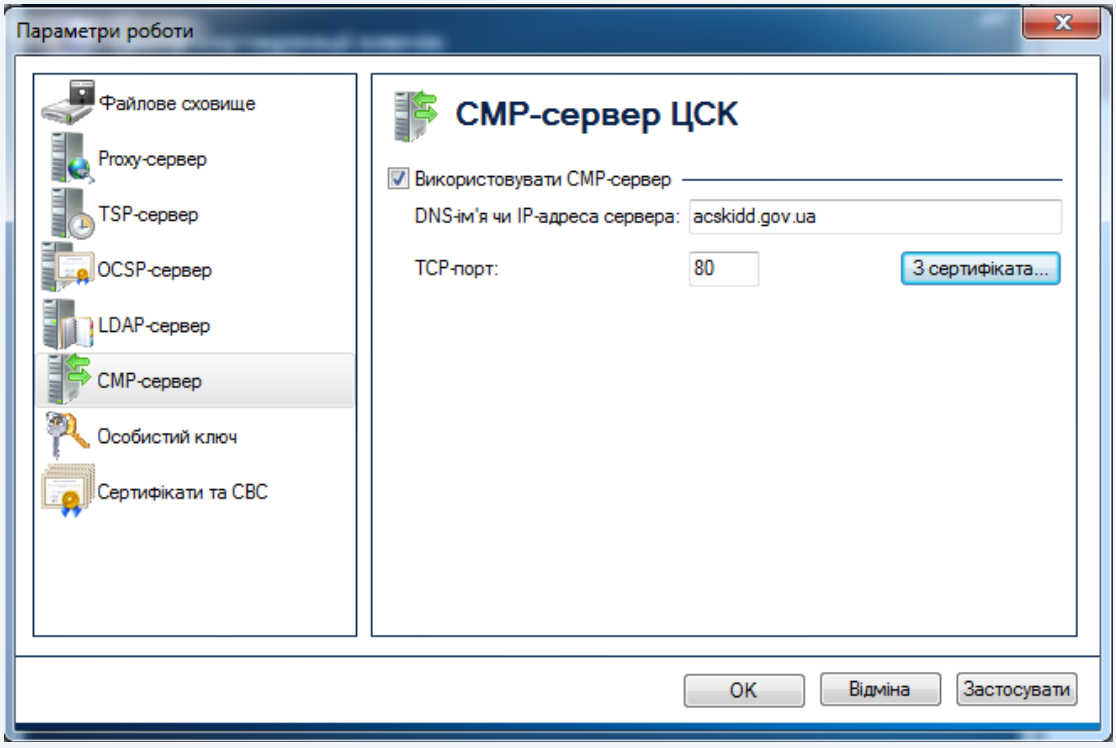

Рисунок 3.6

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

4.1 Підписання файлів

Для накладання ЕЦП на електронний документ необхідно у головному вікні програми обрати пункт «Підписати файли» (рис. 4.1).

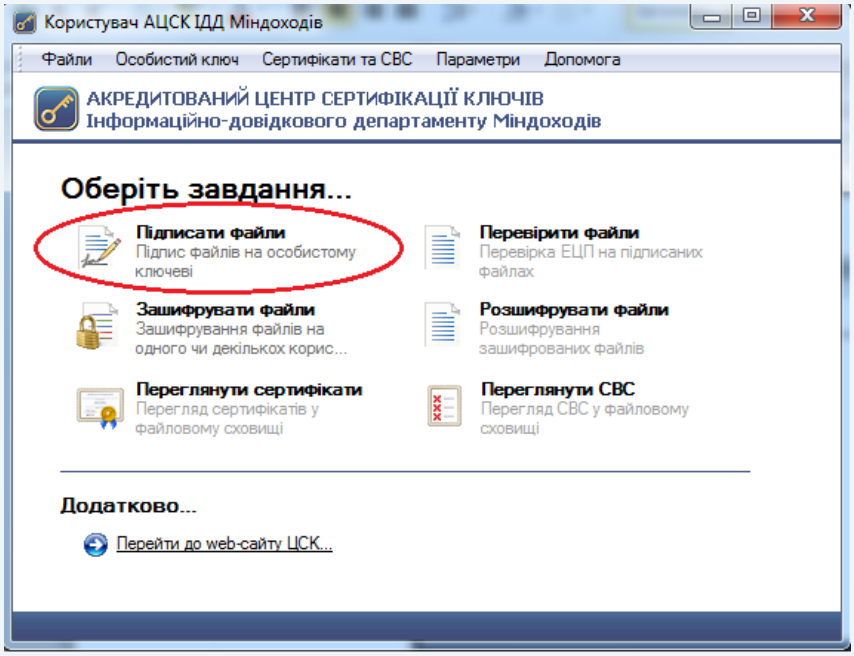

Рисунок 4.1

Після чого з’являється захищений робочий стіл, у якому необхідно обрати носій ключової інформації та ввести пароль захисту особистого ключа (рис. 4.2).

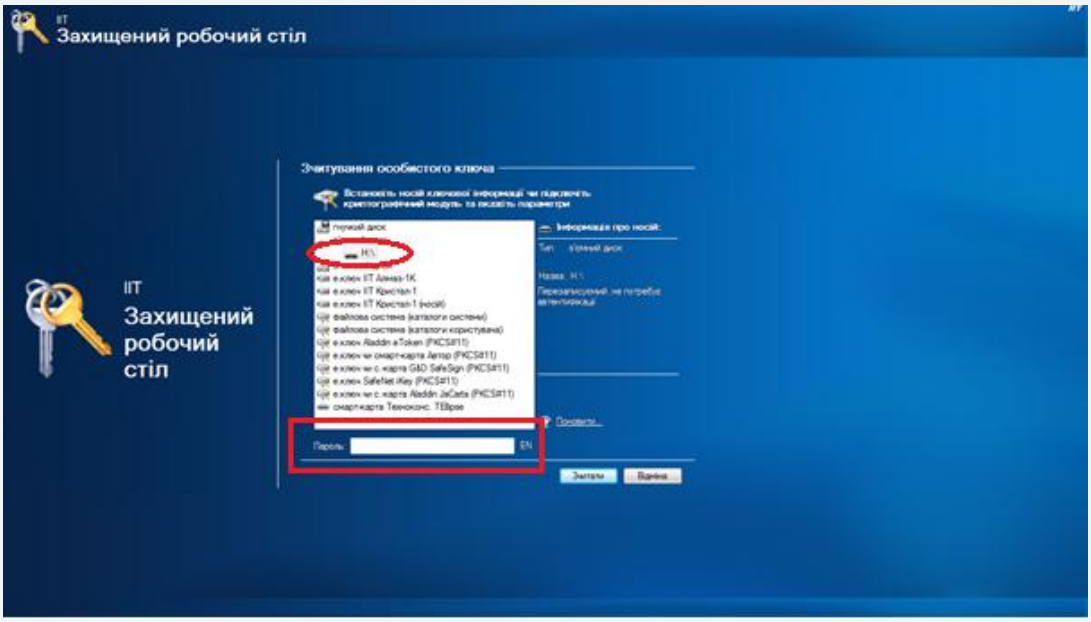

Рисунок 4.2

Після успішного зчитування паролю захисту особистого ключа з’являється вікно «Підпис файлів». Для додавання файлів на підпис натискаємо кнопку «Додати» та обираємо розташування файлу (рис. 4.3).

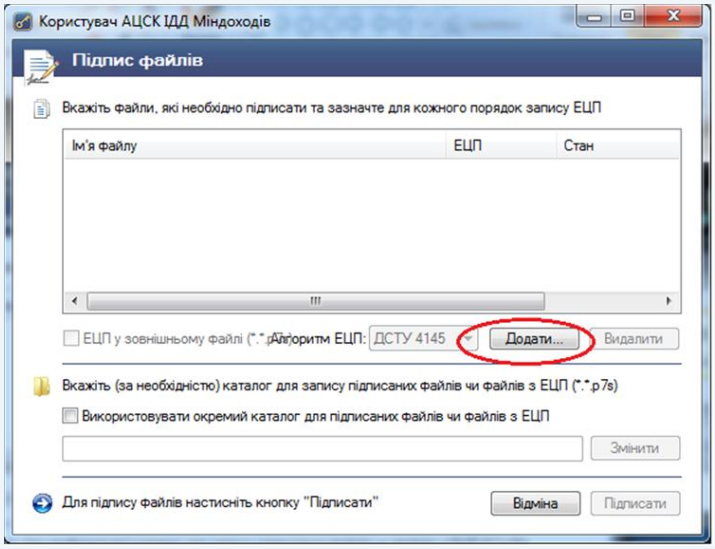

Рисунок 4.3

Додавши необхідний електронний документ, необхідно звернути увагу на параметри накладання ЕЦП, оскільки за замовчуванням програма підписує файли внутрішнім ЕЦП та розміщує підписані файли у тому ж каталозі. Наприклад, якщо файл розташований на робочому столі, то підписаний файл буде збережений також на робочому столі (рис. 4.4).

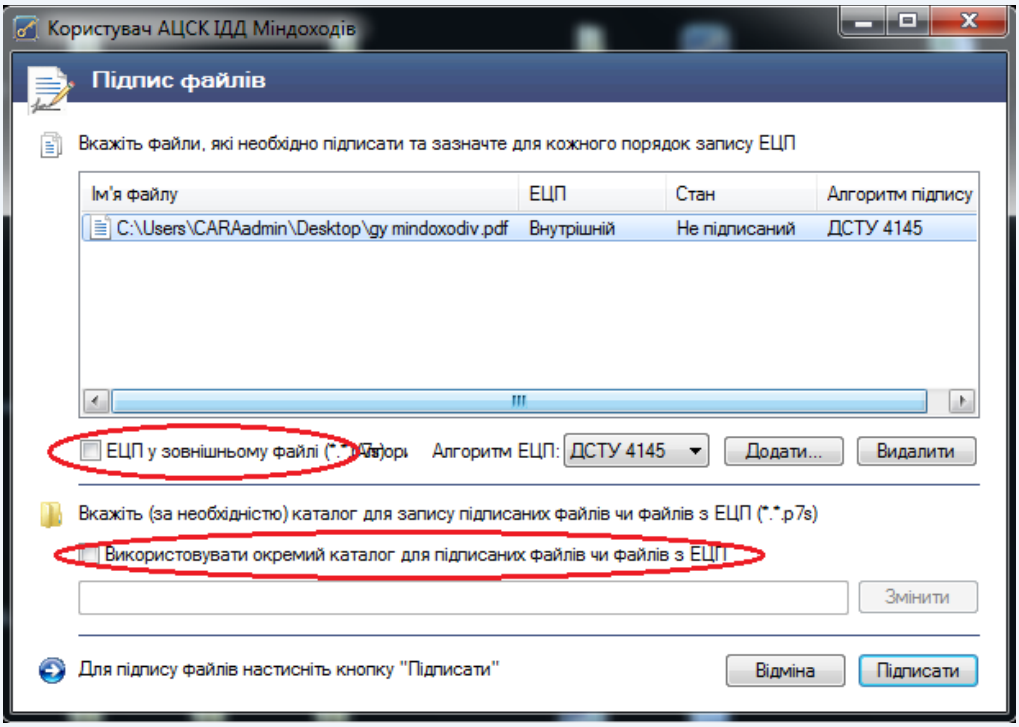

Рисунок 4.4

Програма дає можливість одночасно підписати декілька електронних документів та обрати спосіб накладання ЕЦП для кожного файлу окремо.

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

4.2 Перевірка ЕЦП

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

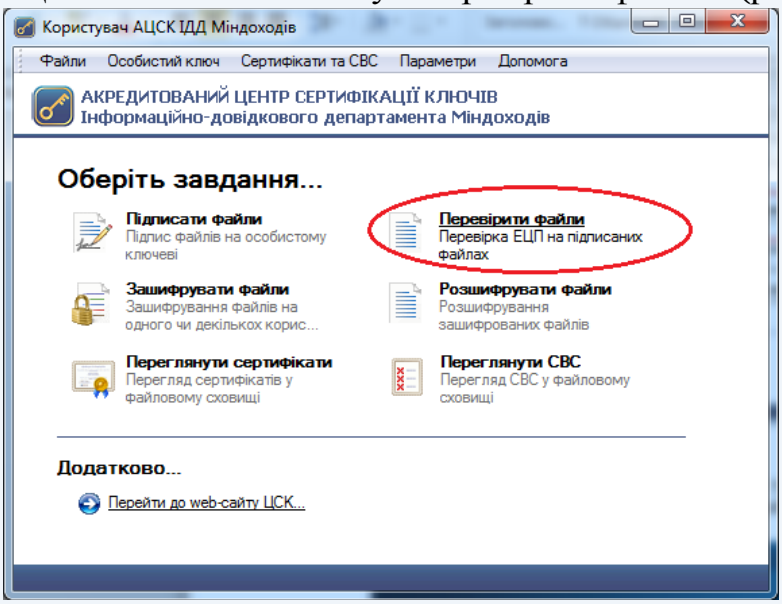

Рисунок 4.5

Після чого з’являється захищений робочий стіл, у якому необхідно обрати носій ключової інформації та ввести пароль захисту особистого ключа (рис. 4.6).

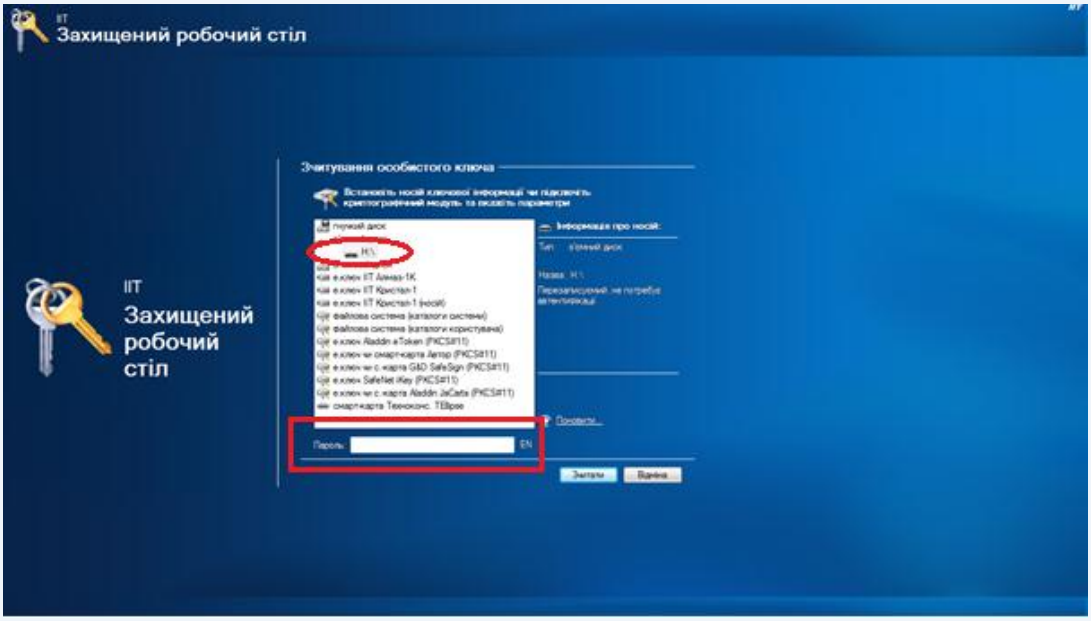

Рисунок 4.6

У вікні «Перевірка підписаних файлів» додати підписані файли (файли, що мають розширення **«.p7s»**) та натиснути кнопку «Перевірити» (рис. 4.7).

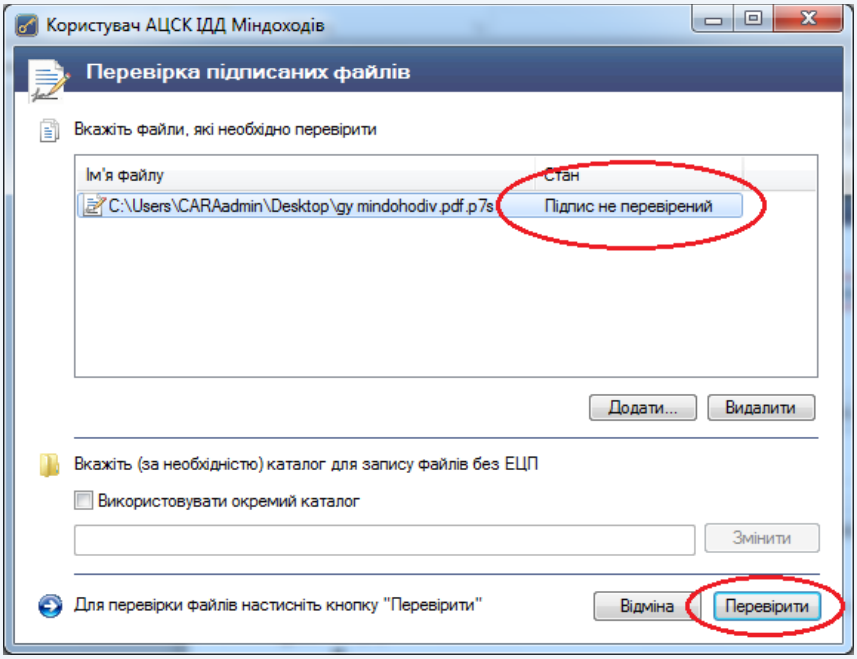

Рисунок 4.7

Підтвердженням успішної перевірки підпису буде поява наступного вікна (рис. 4.8).

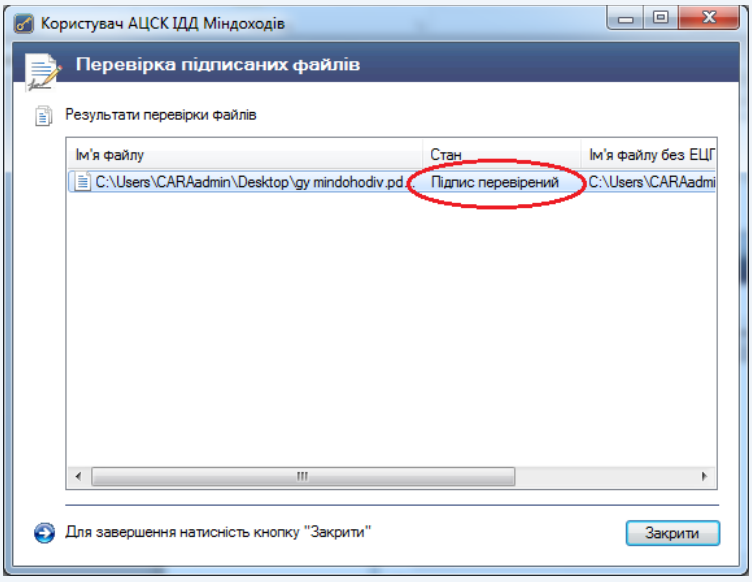

Рисунок 4.8

Для ідентифікації автора, користувачу необхідно відкрити посилання на підписаний файл (рис. 4.9).

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

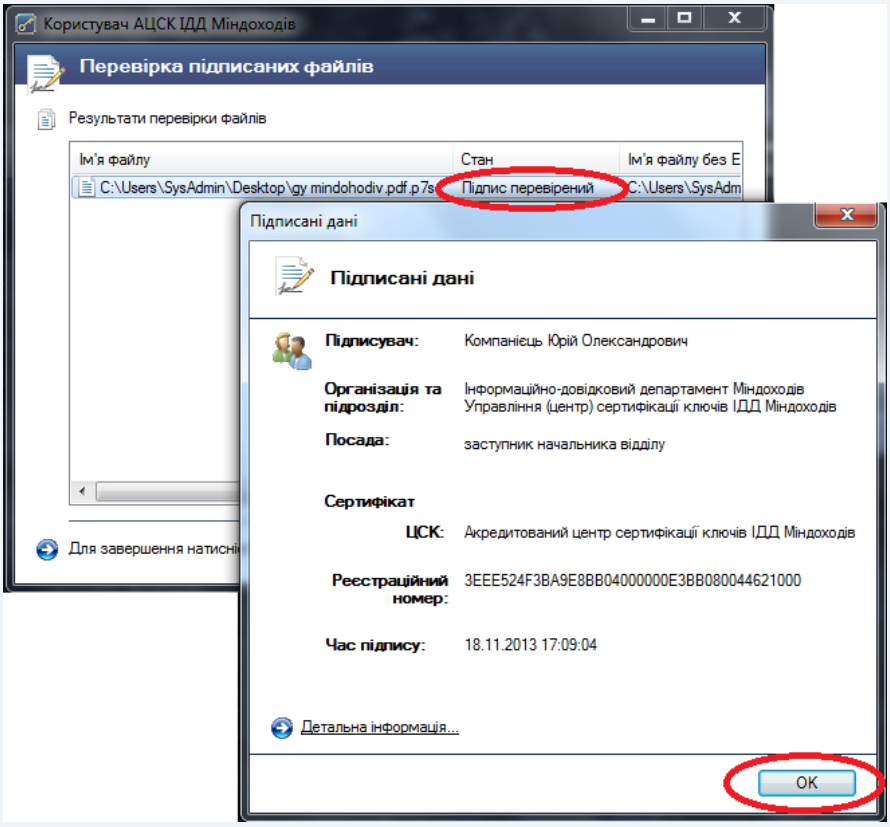

Рисунок 4.9

4.3 Шифрування файлів

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

Для початку шифрування файлів необхідно обрати у головному вікні програми пункт «Зашифрувати файли» (рис. 4.10).

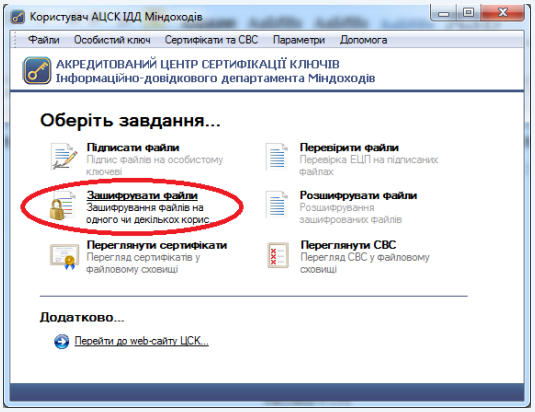

Рисунок 4.10

Наступним кроком є поява захищеного робочого столу, у якому необхідно обрати з'ємний носій ключової інформації та ввести пароль захисту особистого ключа (рис. 4.11).

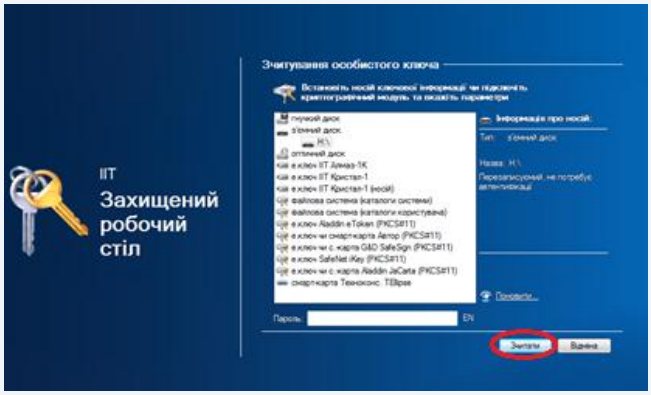

Рисунок 4.11

У новому вікні «Зашифрування файлів» підписувачу надається можливість одночасно з шифруванням файлів додатково їх підписати (рис. 4.12).

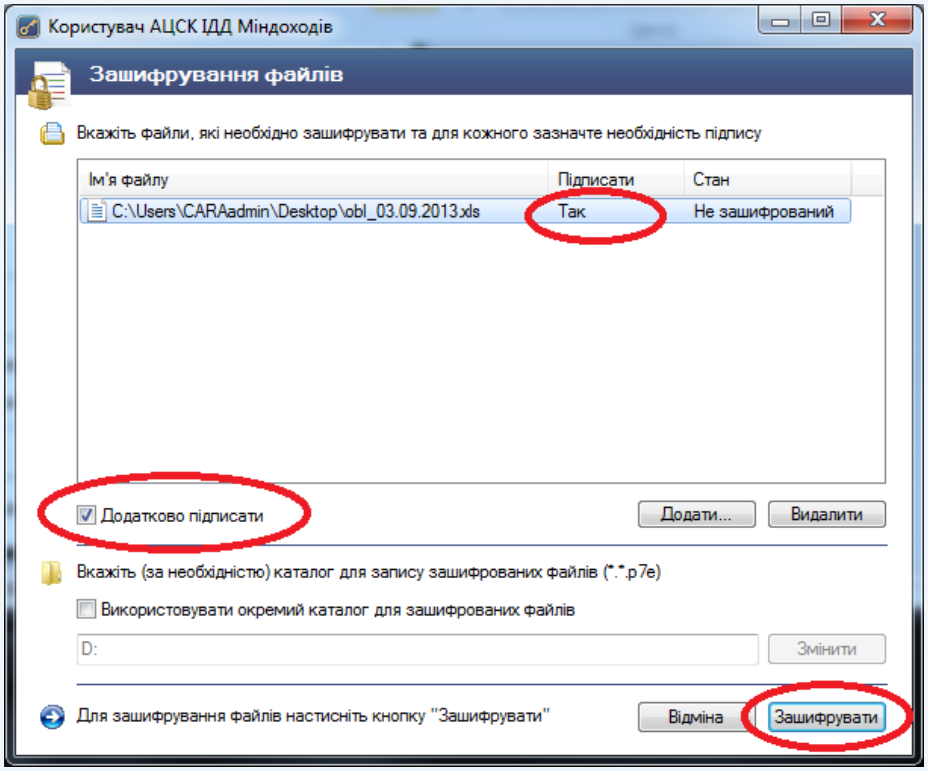

Рисунок 4.12

Після налаштування способу шифрування натискаємо кнопку «Зашифрувати» та у вікні «Сертифікати користувачів-отримувачів» обираємо сертифікат отримувача або сертифікати декількох отримувачів. Розшифрувати файл зможуть лише обрані вами власники сертифікатів (рис. 4.13).

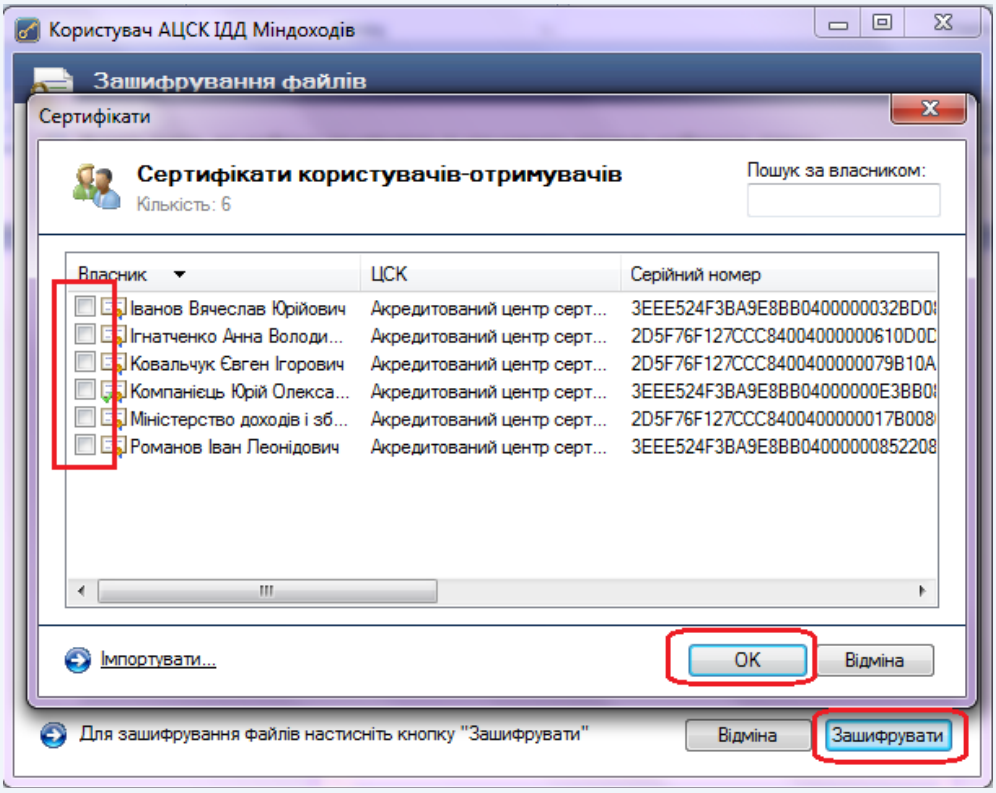

Рисунок 4.13

Підтвердженням закінчення процесу шифрування файлів є поява вікна, зображеного на рис. 4.14.

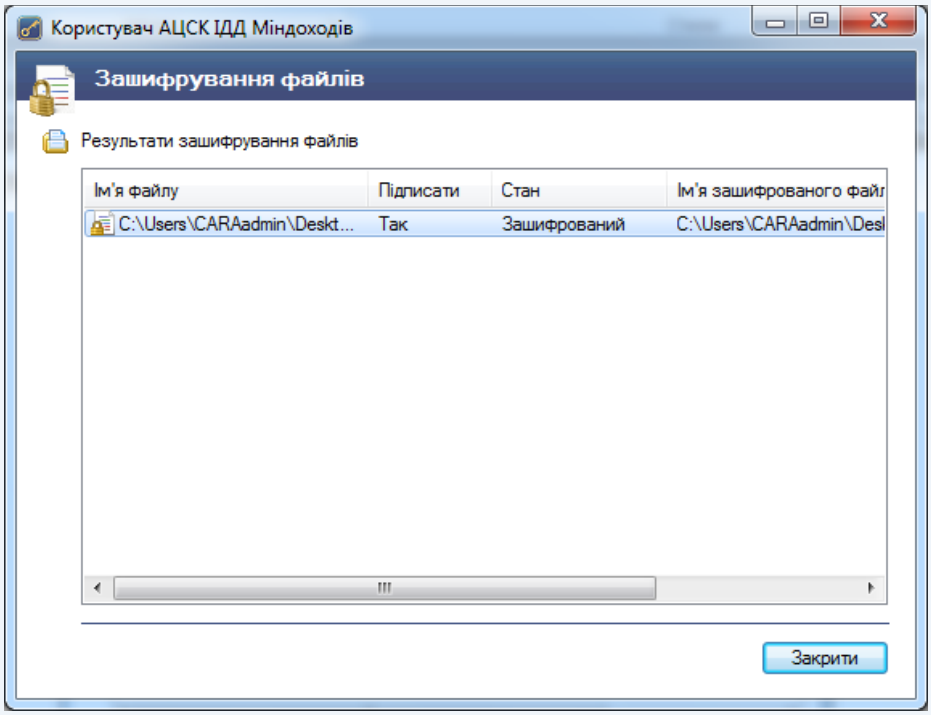

Рисунок 4.14

4.4 Розшифрування файлів

Для розшифрування файлів необхідно обрати у головному вікні програми пункт «Розшифрувати файли» (рис. 4.15).

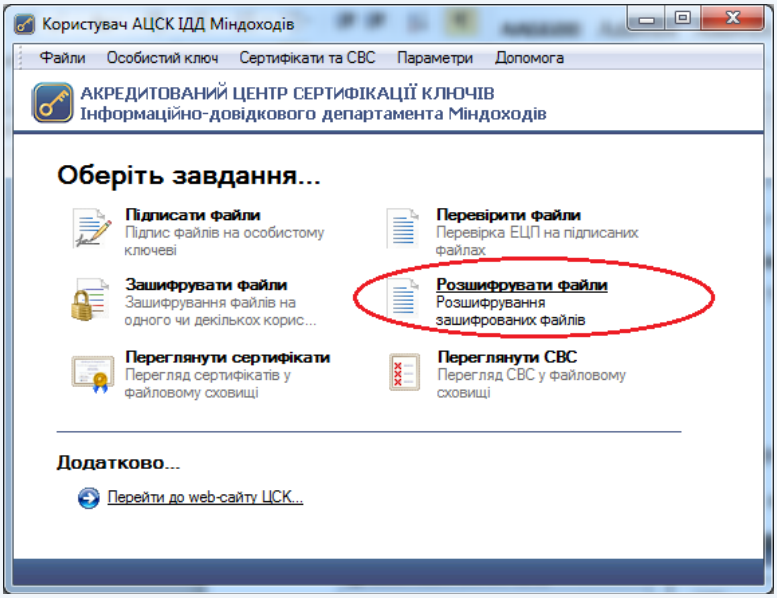

Рисунок 4.15

Наступним кроком є поява захищеного робочого столу, у якому необхідно обрати з'ємний носій ключової інформації та ввести пароль захисту особистого ключа (рис. 4.16).

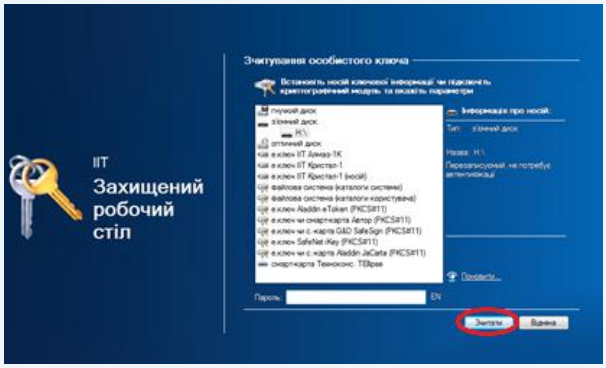

Рисунок 4.16

У вікні «Розшифрування зашифрованих файлів» потрібно додати необхідні документи та натиснути кнопку «Розшифрувати» (рис. 4.17).

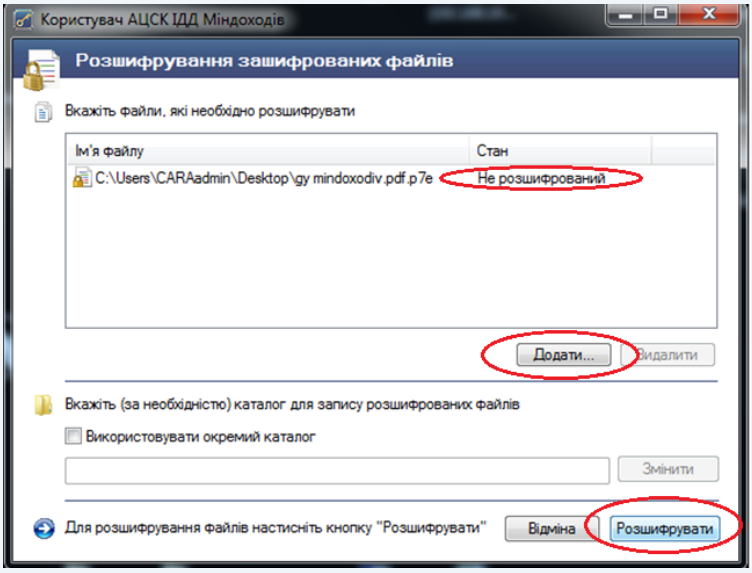

Рисунок 4.17

Електронний документ можна переглянути після його розшифрування.

У випадку відсутності у користувача прав доступу до зашифрованого файлу з’явиться вікно «Повідомлення оператору» (рис. 4.18).

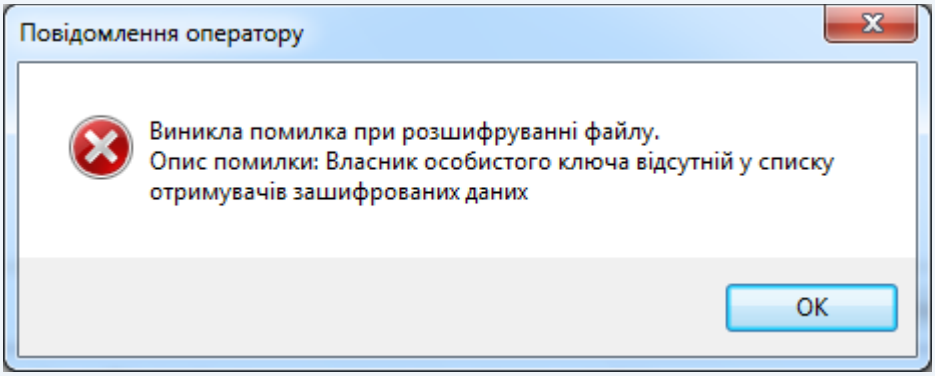

Рисунок 4.18

4.5 Перегляд сертифікатів

Для перегляду сертифікатів що містяться у файловому сховищі необхідно обрати підпункт «Переглянути сертифікати» у головному меню або натиснути клавішу F10 (рис. 4.19).

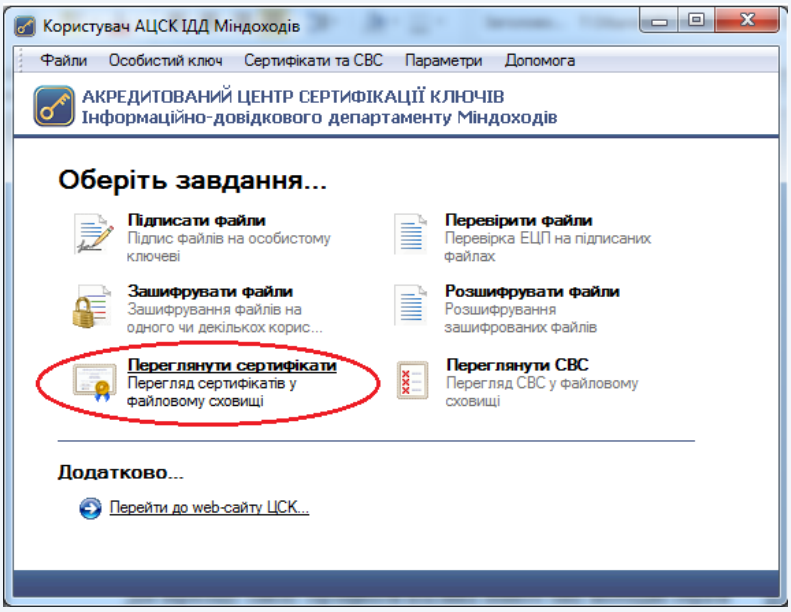

Рисунок 4.19

У вікні перегляду сертифікатів (рис. 4.20) можна переглянути, перевірити та видалити обраний сертифікат.

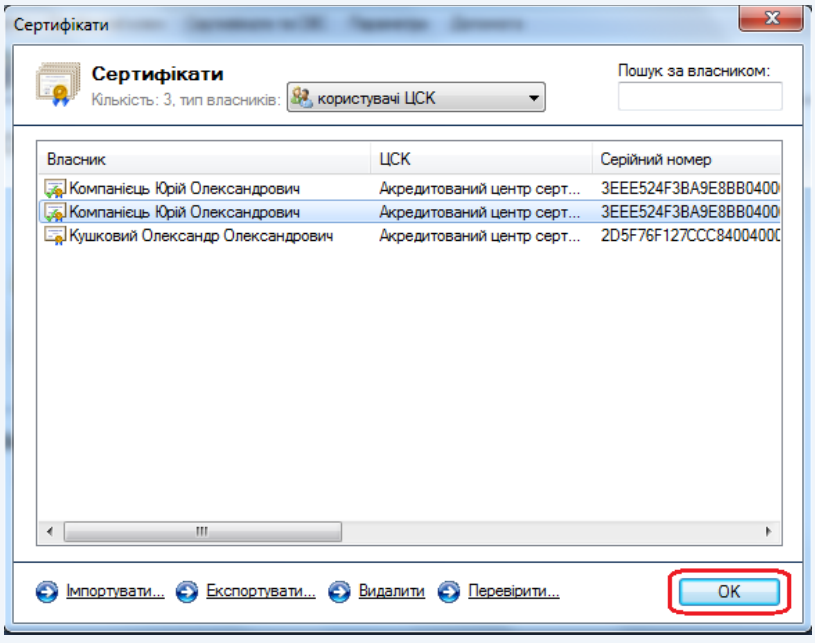

Рисунок 4.20

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. Дані сертифіката будуть відображені, як наведено на рис. 4.21 та 4.22.

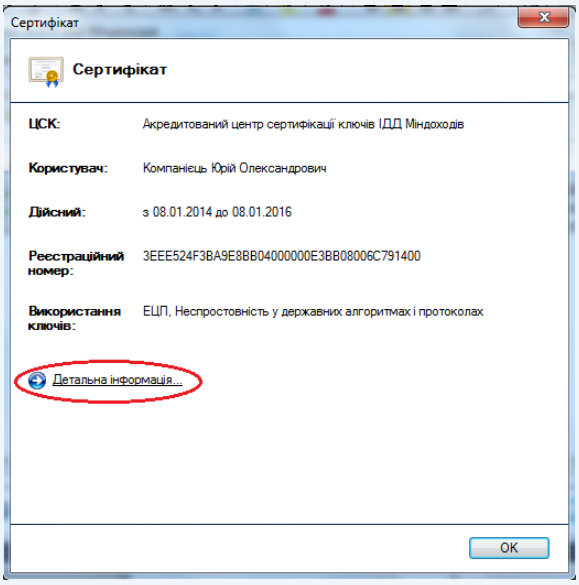

Рисунок 4.21

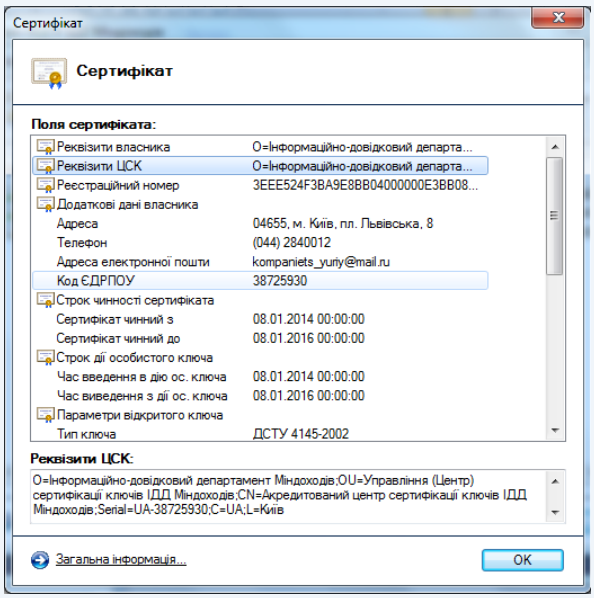

Рисунок 4.22

Для видалення сертифікатів з файлового сховища необхідно виділити у списку (рис. 4.20) відповідні записи та натиснути кнопку «Видалити».

Для перевірки сертифіката необхідно виділити 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. Результатом перевірки буде поява вікна (рис. 4.23). Якщо у цьому вікні натиснути «Сертифікат», то відповідний сертифікат буде відображено у вікні детального перегляду.

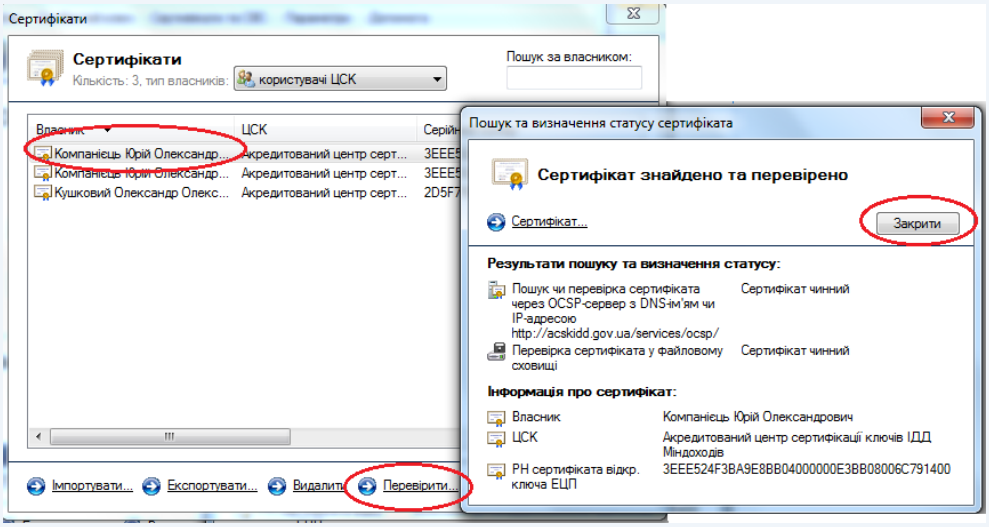

Рисунок 4.23

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. 4.24). Вікно із списками відкликаних сертифікатів наведене на рис. 4.25.

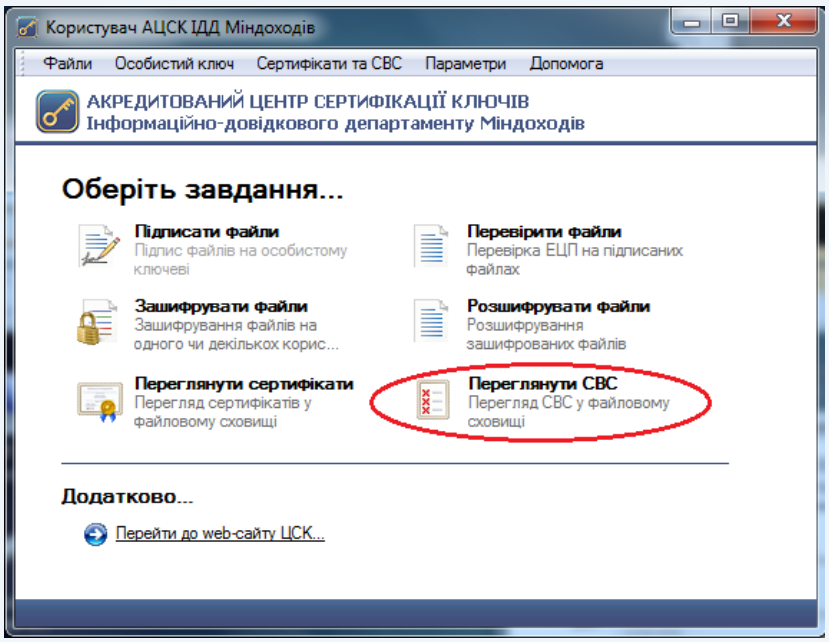

Рисунок 4.24

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

Завантажити СВС можна на веб-сайті в розділі «Списки відкликаних сертифікатів» (рис. 4.25) та імпортувати до програми.

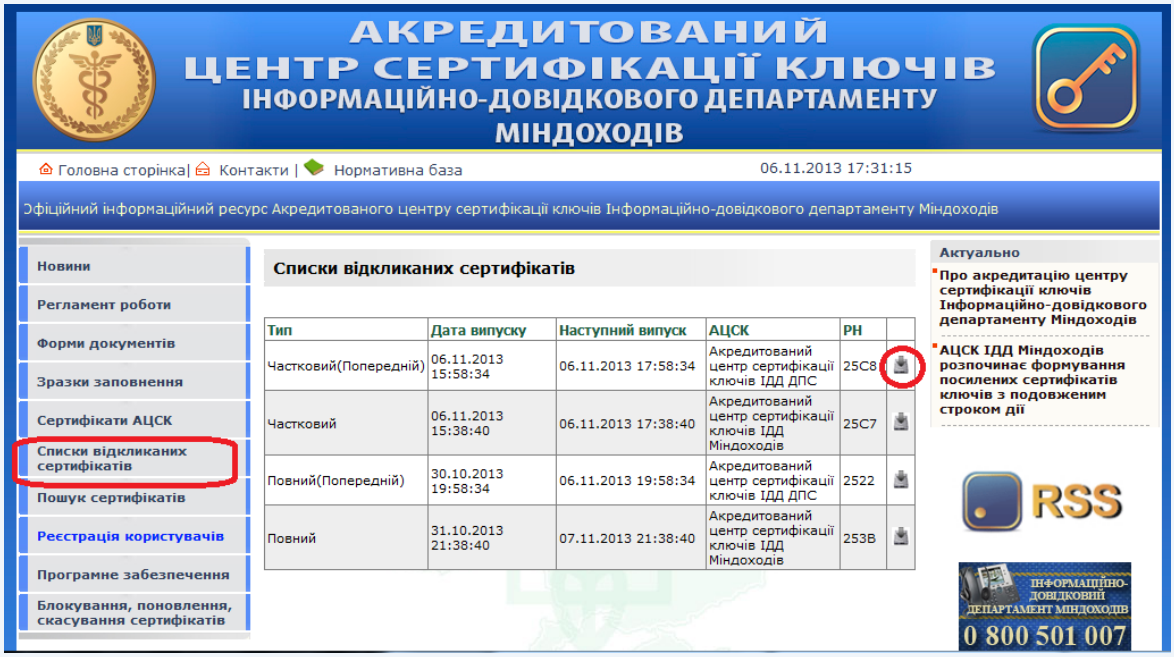

Рисунок 4.25

Для імпорту СВС до файлового сховища необхідно натиснути «Імпортувати», та обрати потрібний СВС на будь-якому носії інформації.

Для перегляду СВС необхідно натиснути на відповідному записі про СВС у списку. СВС буде відображено у вікні, що наведене на рис. 4.26, 4.27 та 4.28.

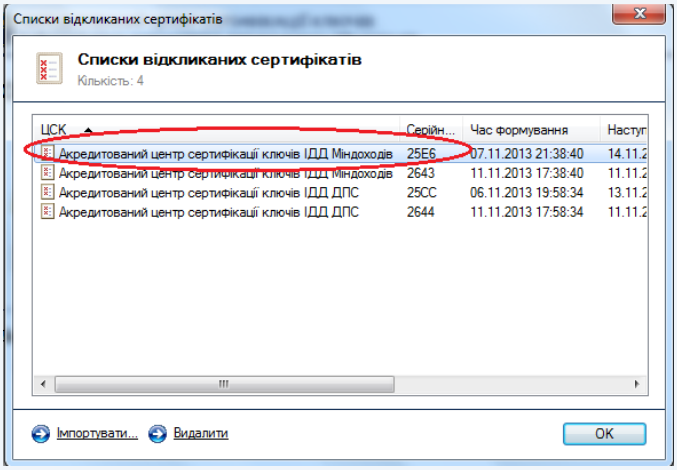

Рисунок 4.26

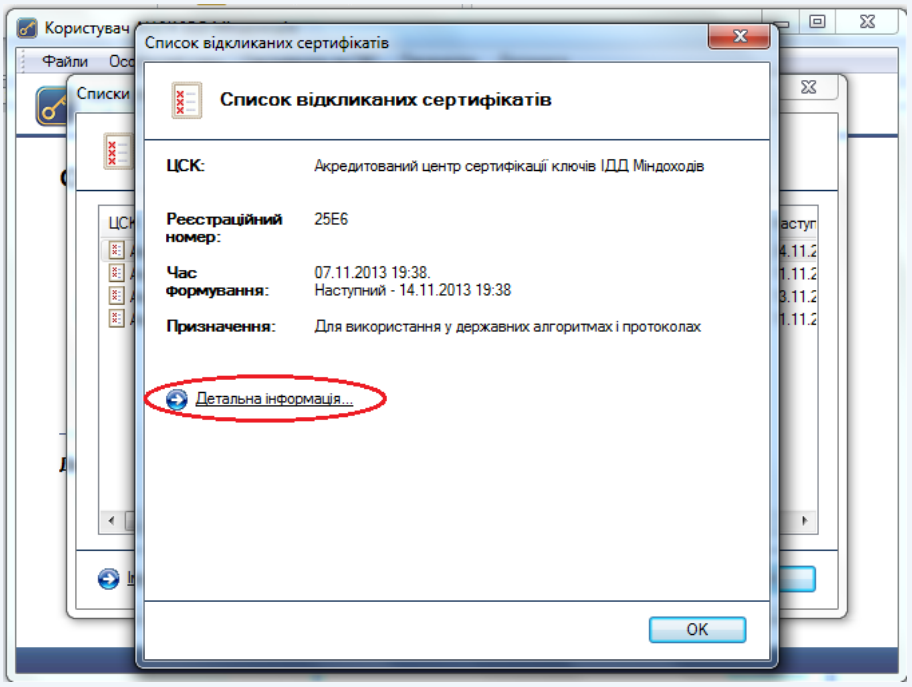

Рисунок 4.27

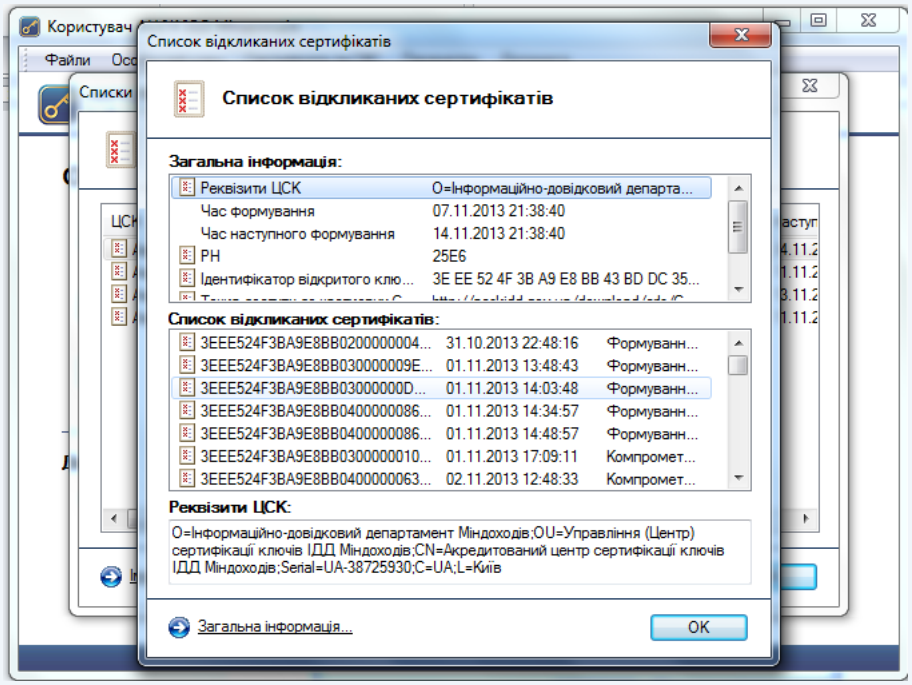

Рисунок 4.28

Для видалення файлу СВС з файлового сховища необхідно виділити 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).

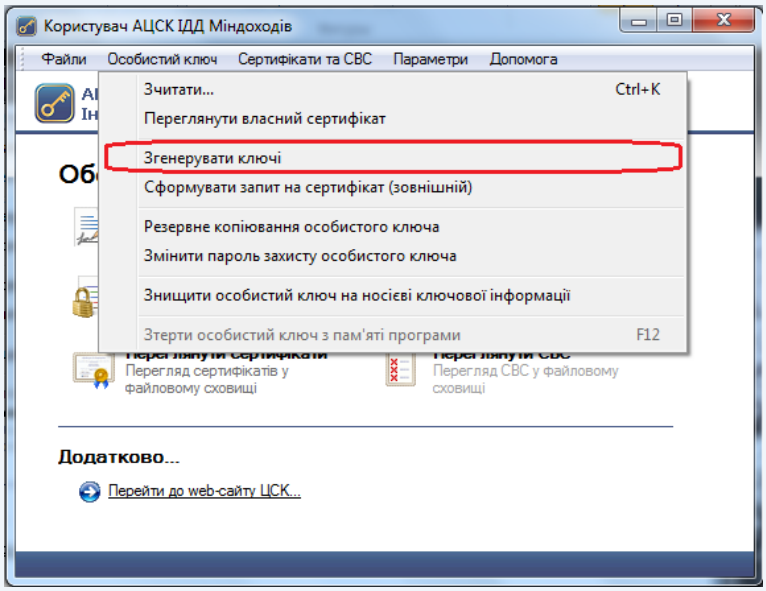

Рисунок 5.1

У вікні генерації ключів потрібно 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 потрібно натиснути кнопку «Далі» (рис 5.2).

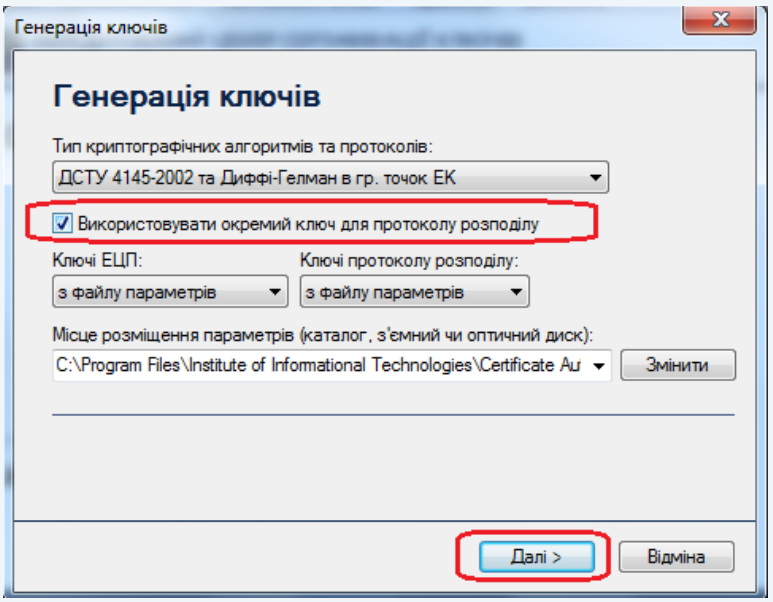

Рисунок 5.2

Наступним кроком є поява захищеного робочого столу, у якому необхідно обрати носій ключової інформації на який буде записано особистий ключ та ввести пароль захисту особистого ключа і натиснути кнопку «Записати» (рис.5.3).

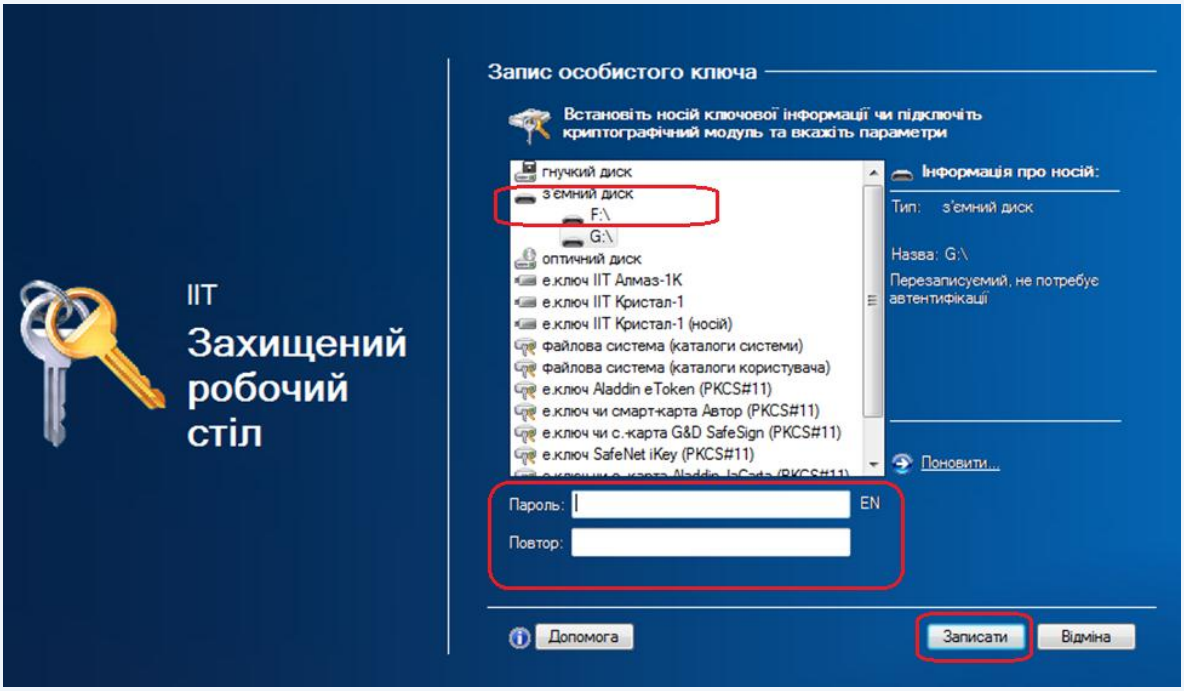

Рисунок 5.3

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

Після запису особистого ключа на зʼємний носій буде виведено вміст запиту на формування сертифіката з відкритим ключем ЕЦП та запиту на формування сертифіката з відкритим ключем протоколу розподілу. Для продовження генерації натискаємо кнопку «ОК» (рис 5.4, 5.5).

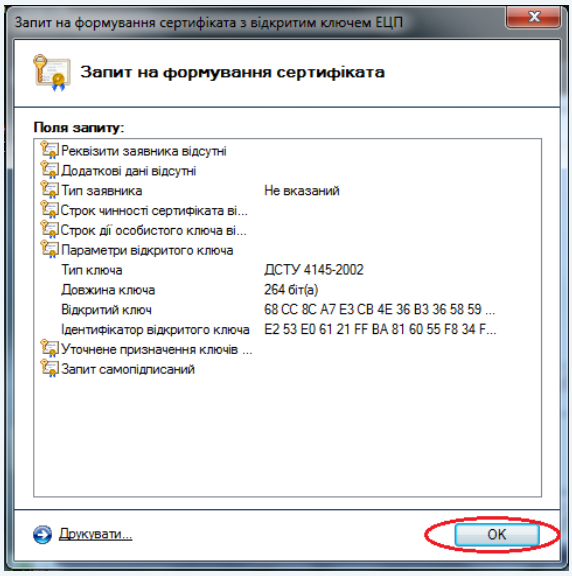

Рисунок 5.4

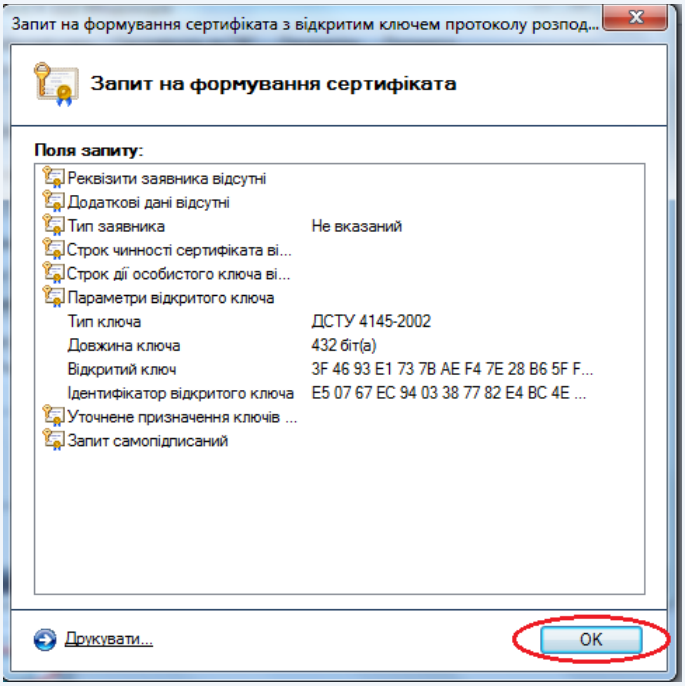

Рисунок 5.5

Для передачі запитів на формування посилених сертифікатів до центру сертифікації ключів потрібно зберегти їх у файл (рис. 5.6). Для цього встановити параметр «Зберегти у файл» та натиснути кнопку «Далі».

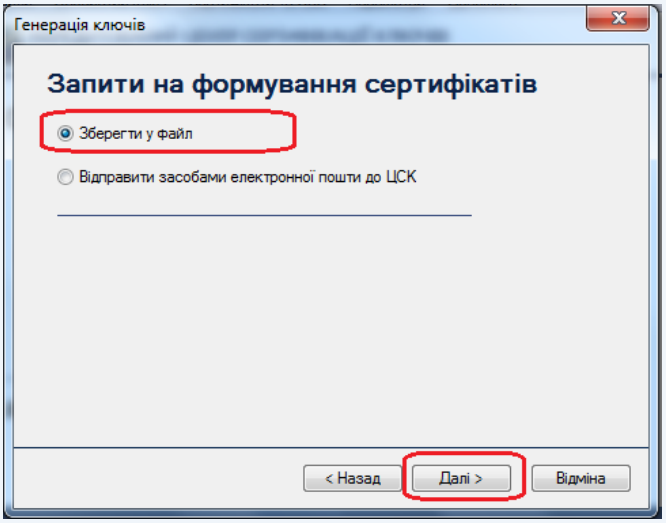

Рисунок 5.6

Запити повинні бути записані на носій інформації чи на жорсткий диск. Для цього потрібно натиснути кнопку «Змінити» (рис. 5.7) та вказати необхідний носій інформації та ім’я запитів на формування сертифікатів у файл.

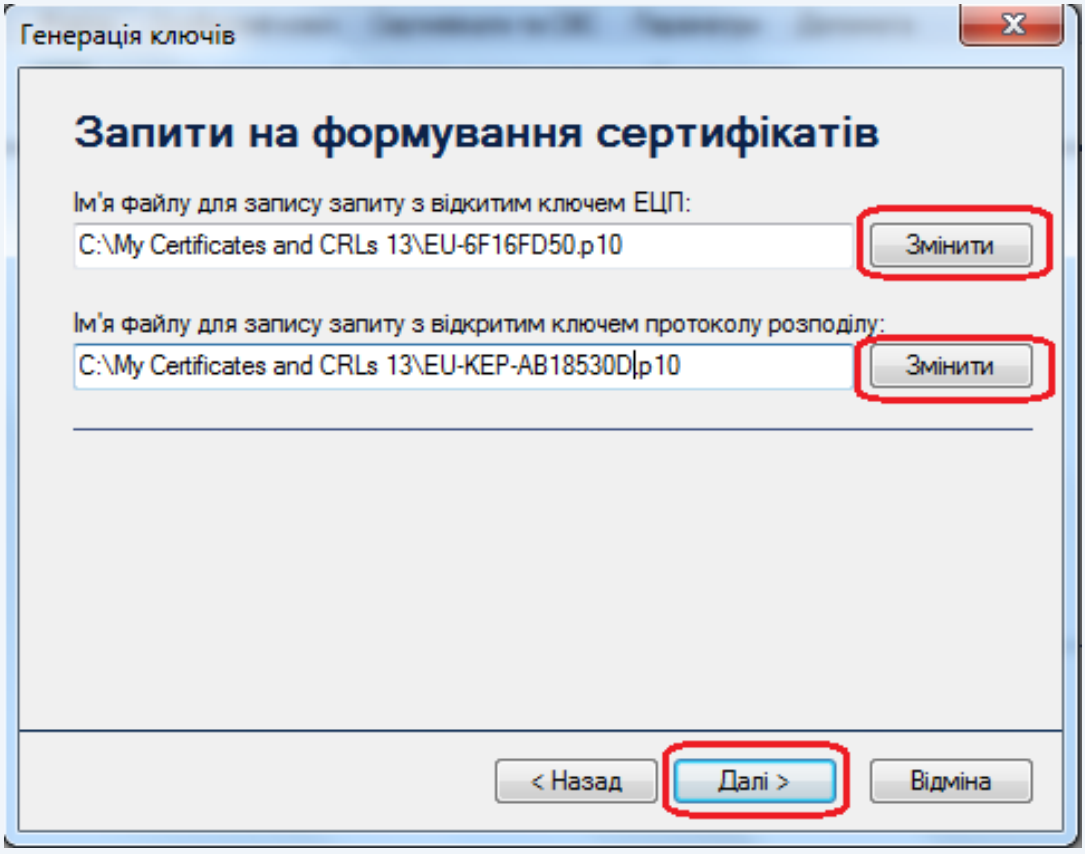

Рисунок 5.7

Увага! Для коректної ідентифікації запитів з відкритим ключем ЕЦП та протоколом розподілу користувача файл запиту на формування 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 або EU-KEP-XXXXXXXX.p10 – унікальне ім'я файлу запиту, що формується програмним забезпеченням за замовчуванням.

Наприклад: **Компанієць Юрій Олександрович EU-69PH0S9W.p10;**
Компанієць Юрій Олександрович EU-KEP-KB50S67Z.p10.

Для завершення генерації потрібно натиснути кнопку «Завершити» (рис. 5.8).

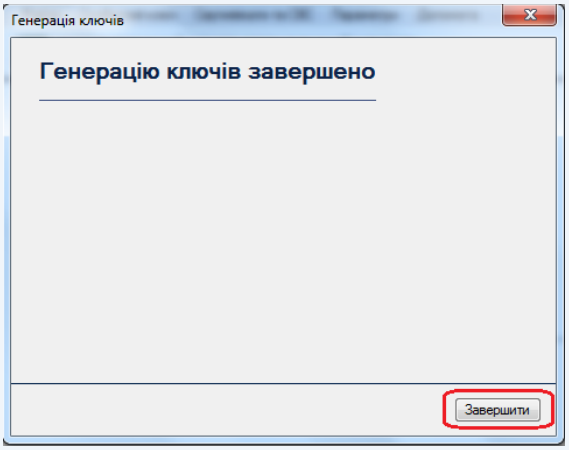

Рисунок 5.8

Після цього, запити можуть бути передані до пункту реєстрації користувачів АЦСК ІДД Міндоходів для формування посилених сертифікатів.

5.2 Зчитування особистого ключа

Для роботи з більшістю функцій програми (захист файлів та ін.) необхідне попереднє зчитування особистого ключа підписувача.

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

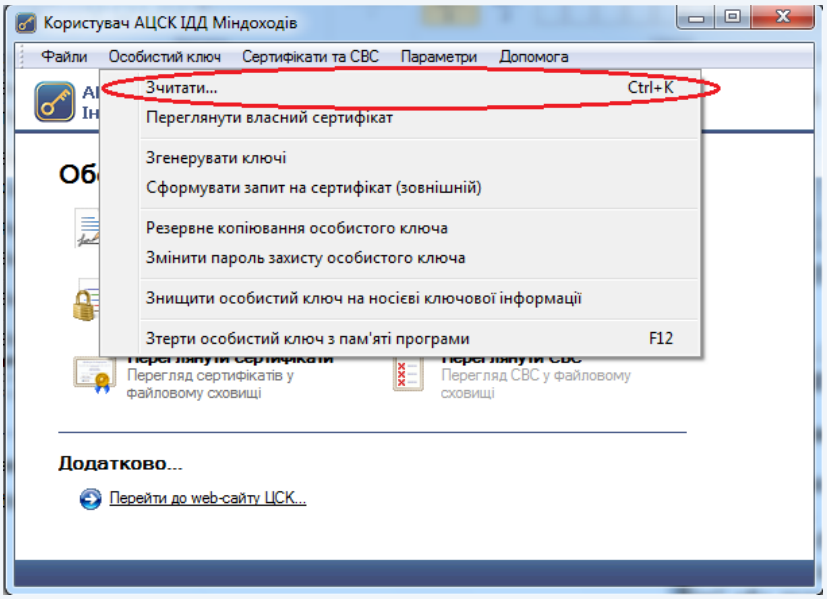

Рисунок 5.9

У вікні, що з’явиться (рис. 5.10) необхідно вказати:

– тип НКІ з особистим ключем;

– назву носія;
– пароль захисту особистого ключа.

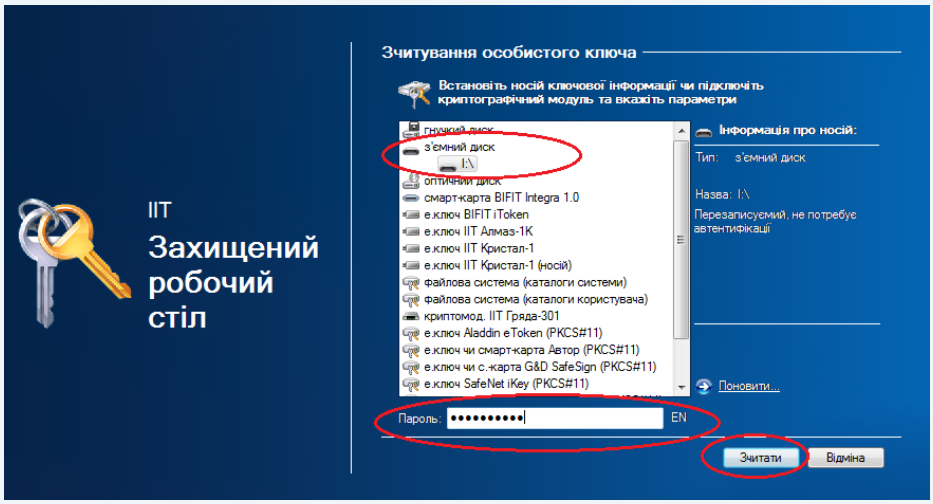

Рисунок 5.10

Після введення параметрів необхідно натиснути кнопку «Зчитати».

Інформація про те, що особистий ключ зчитаний та знаходиться в пам'яті ПЕОМ відображається у панелі стану вікна, як наведено на рис. 5.11.

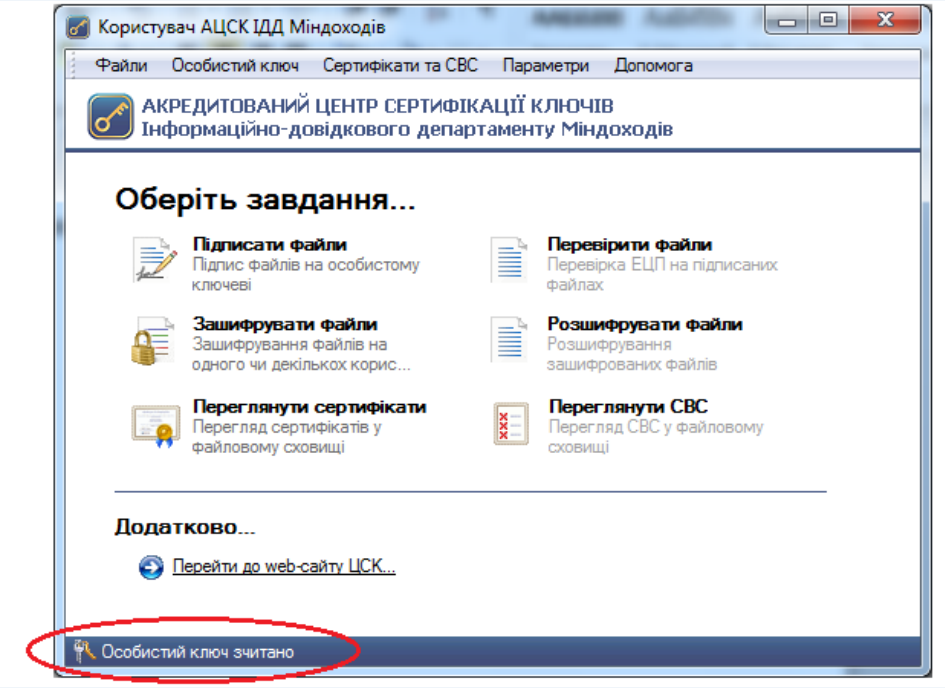

Рисунок 5.11

5.3 Зміна паролю захисту особистого ключа

Для зміни паролю захисту особистого ключа необхідно обрати підпункт «Змінити пароль захисту особистого ключа» в пункті меню «Особистий ключ». Вікно зміни паролю захисту особистого ключа наведене на рис. 5.12.

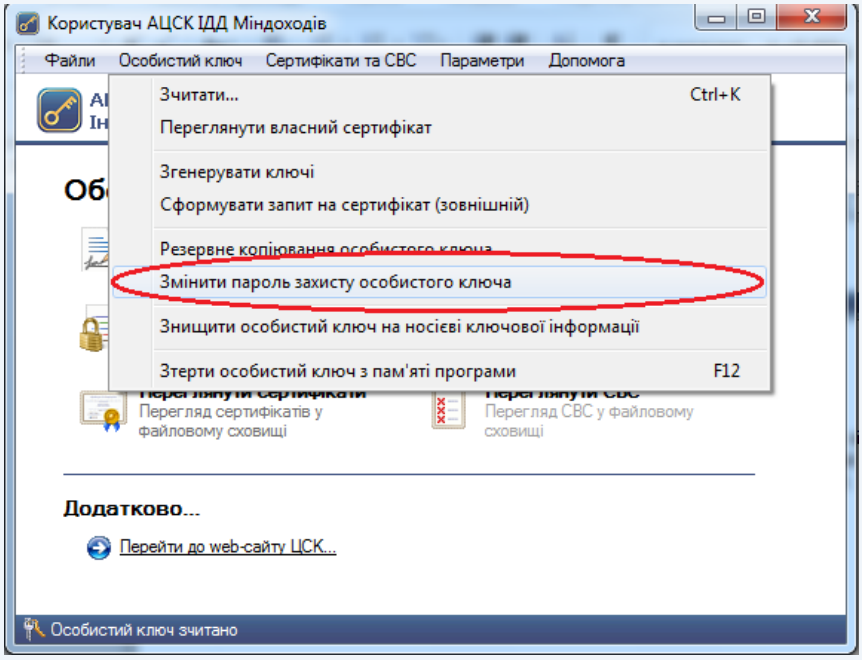

Рисунок 5.12

У вікні, що з’явиться (рис. 5.13) необхідно вказати:

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

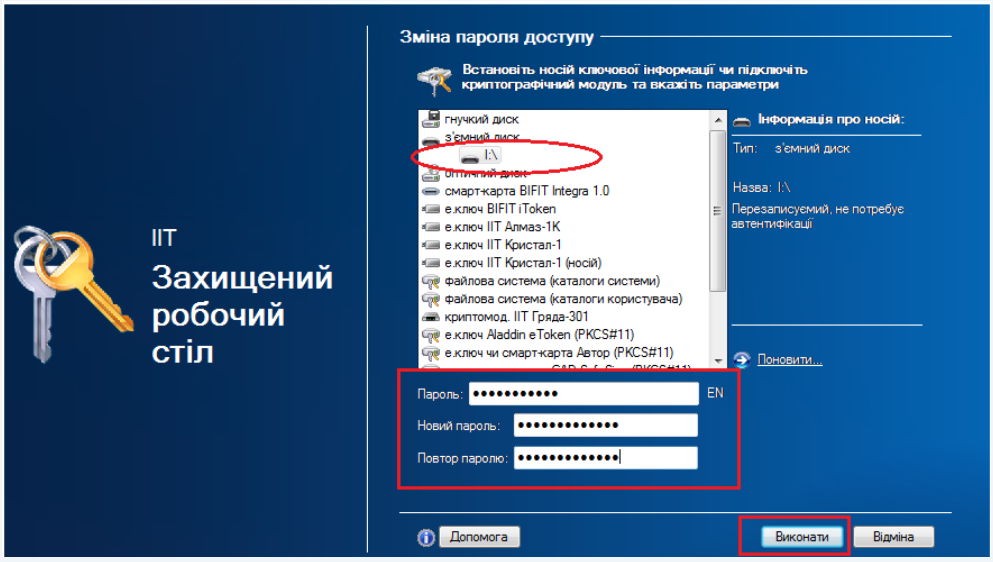

Рисунок 5.13

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. 5.14).

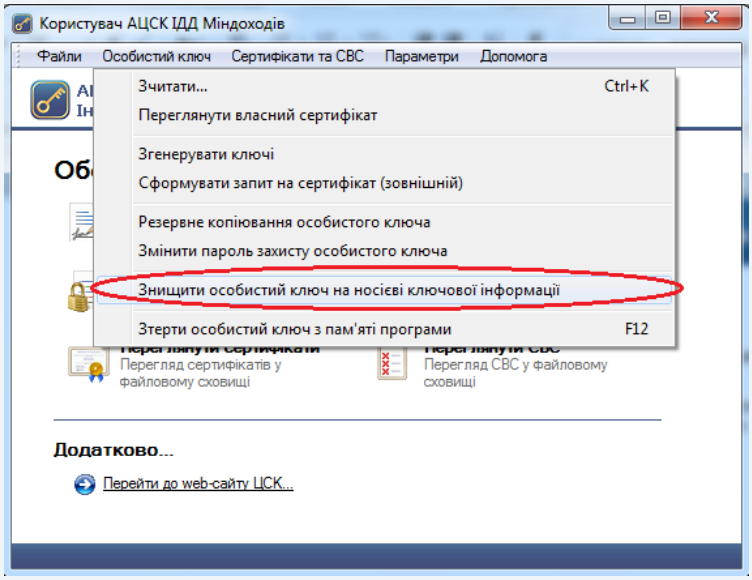

Рисунок 5.14

У вікні необхідно вказати тип та назву НКІ, ввести пароль захисту особистого ключа та натиснути кнопку «Знищити» (рис. 5.15).

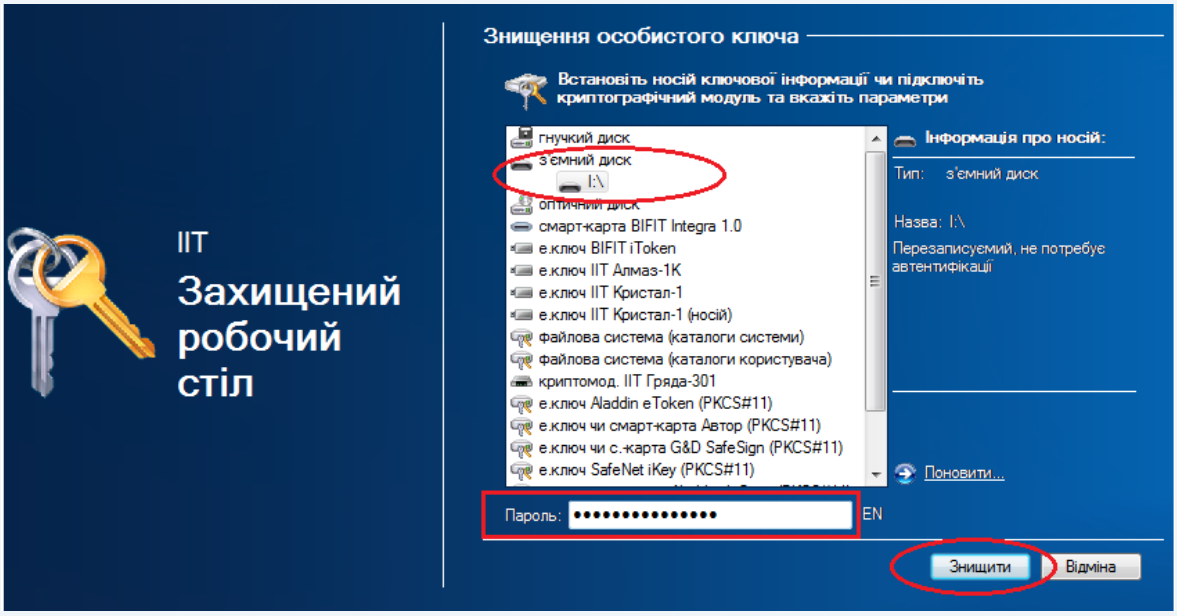

Рисунок 5.15

5.5 Знищення особистого ключа з пам’яті ПЕОМ

Програма передбачає можливість знищення особистого ключа з пам’яті ПЕОМ після кожної операції. Для встановлення зазначеного параметру необхідно в меню програми «Параметри-Зтирання особистого ключа з пам’яті програми» обрати пункт «Зтирати після кожної операції» (рис. 5.16), в іншому випадку особистий ключ залишається у пам’яті до завершення роботи програми.

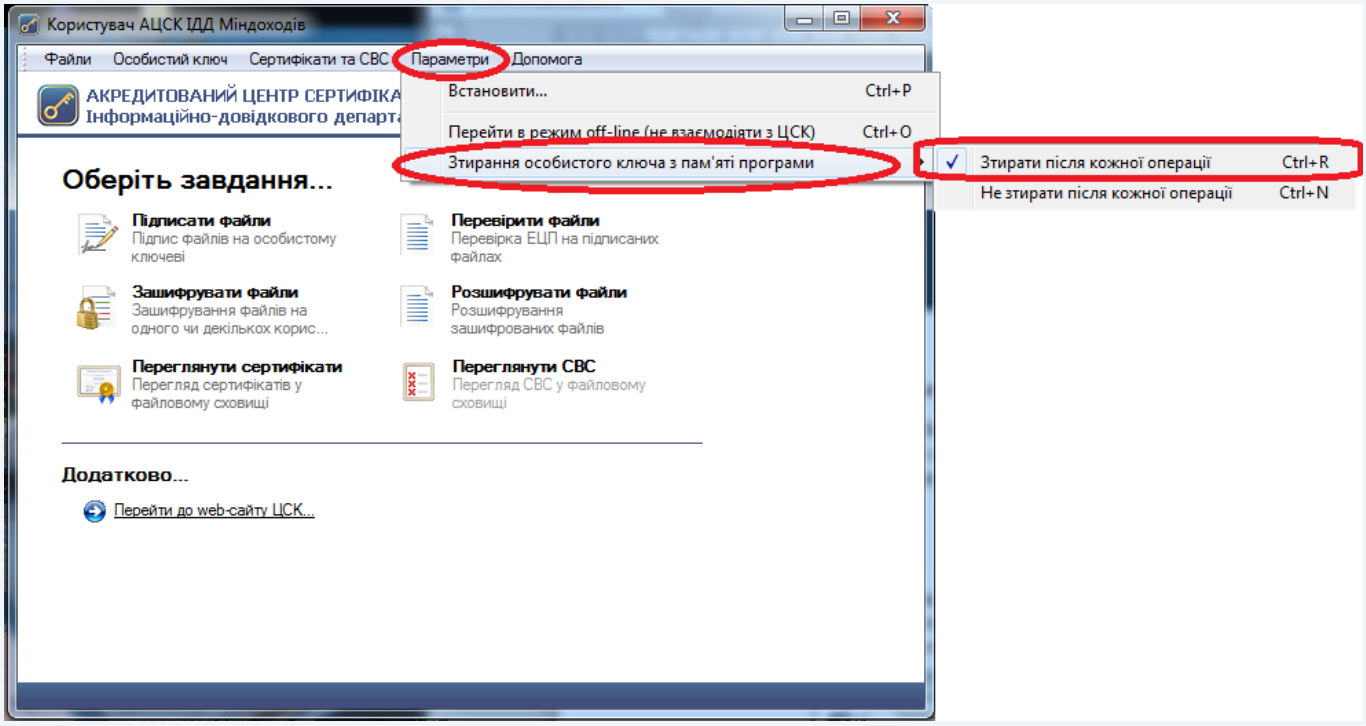

Рисунок 5.16

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. 5.17).

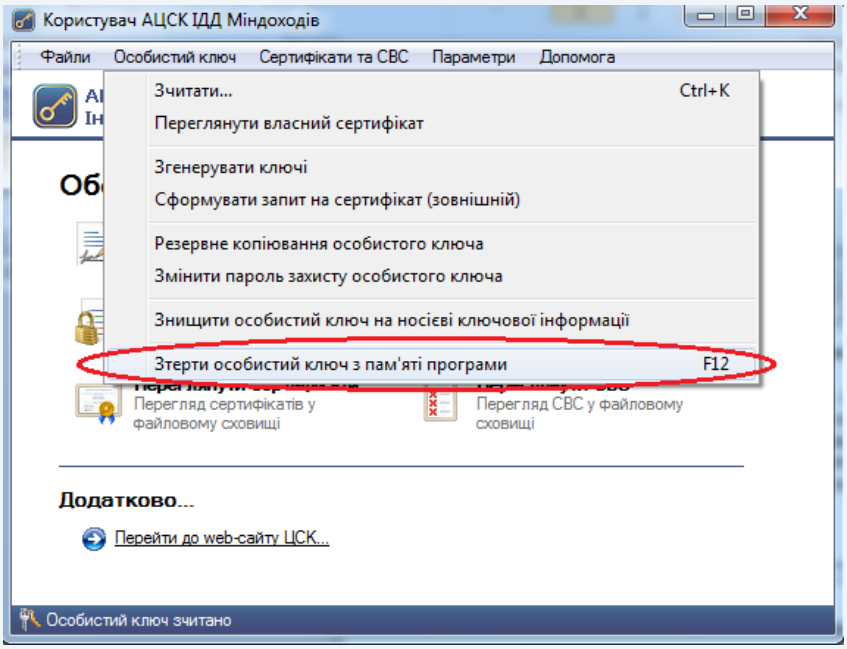

Рисунок 5.17

5.6 Резервне копіювання особистого ключа

Для резервного копіювання особистого ключа з одного НКІ на інший необхідно обрати підпункт «Резервне копіювання особистого ключа» в пункті меню «Особистий ключ» (рис. 5.18).

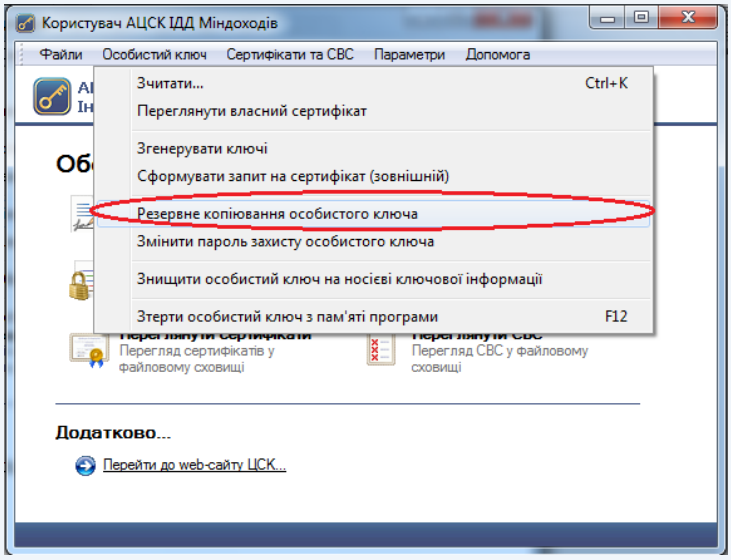

Рисунок 5.18

Далі з'являється захищений робочий стіл, у якому необхідно обрати з'ємний носій ключової інформації, з якого буде знята копія, та ввести пароль захисту особистого ключа як наведене на рис. 5.19.

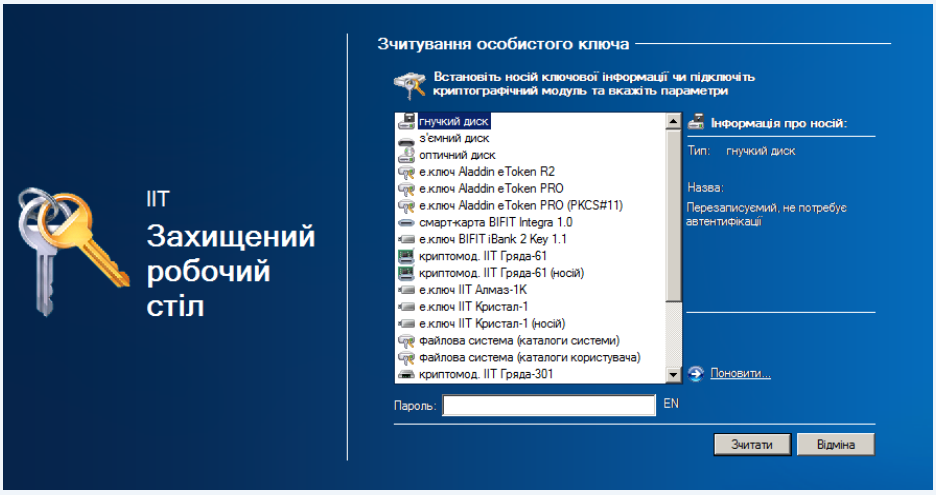

Рисунок 5.19

В наступному вікні необхідно обрати з'ємний носій ключової інформації на який буде записана копія та ввести пароль захисту особистого ключа, як наведено на рис. 5.20.

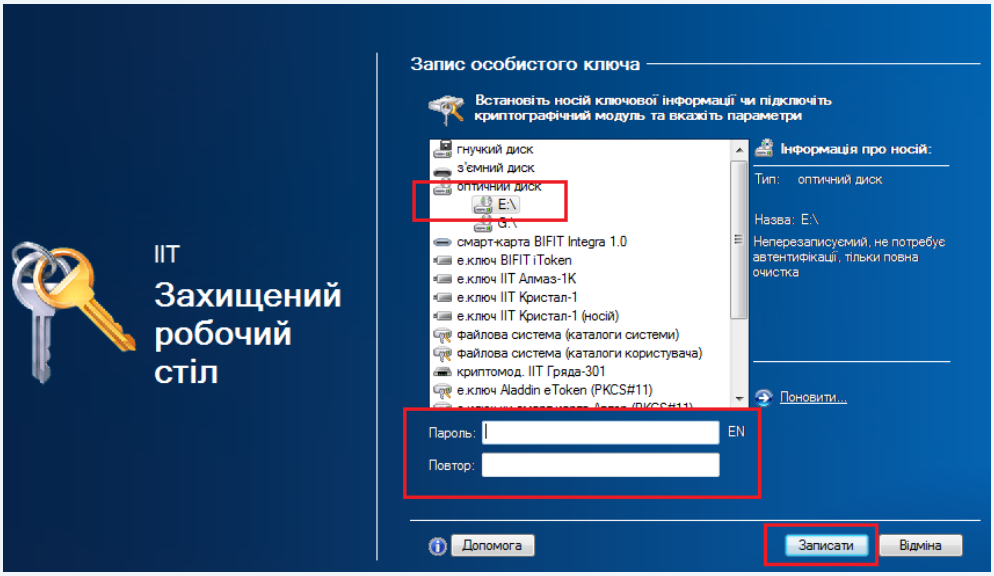

Рисунок 5.20

5.7 Off-line режим роботи програми

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

В off-line режимі програма не взаємодіє з 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 потрібно виконати завантаження СВС (більш детально див. п. 4.6) та у налаштуваннях програми увімкнути параметр «Перевіряти СВС» (рис. 5.21).

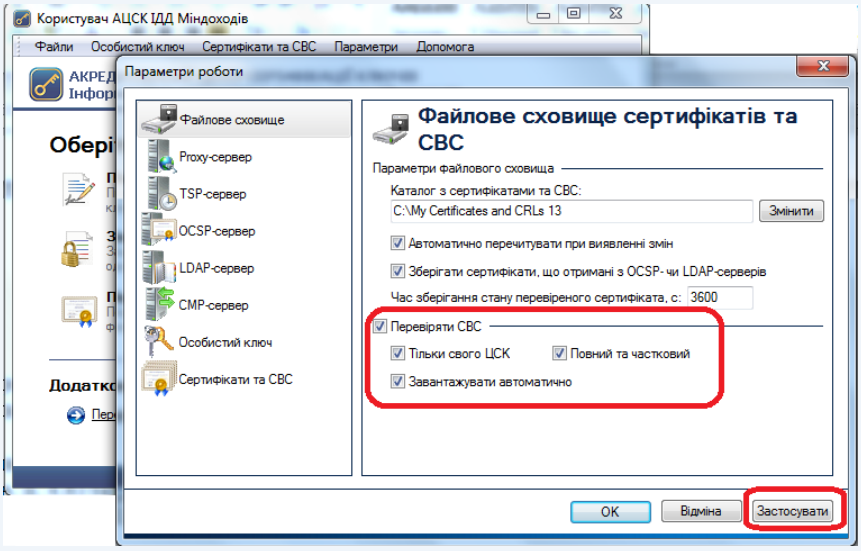

Рисунок 5.21

Для переходу в режим off-line потрібно обрати підпункт «Перейти в режим off-line (не взаємодіяти з ЦСК)» в пункті меню «Параметри» або шляхом натискання комбінації клавіш **Ctrl+O** (рис. 5.22-5.24).

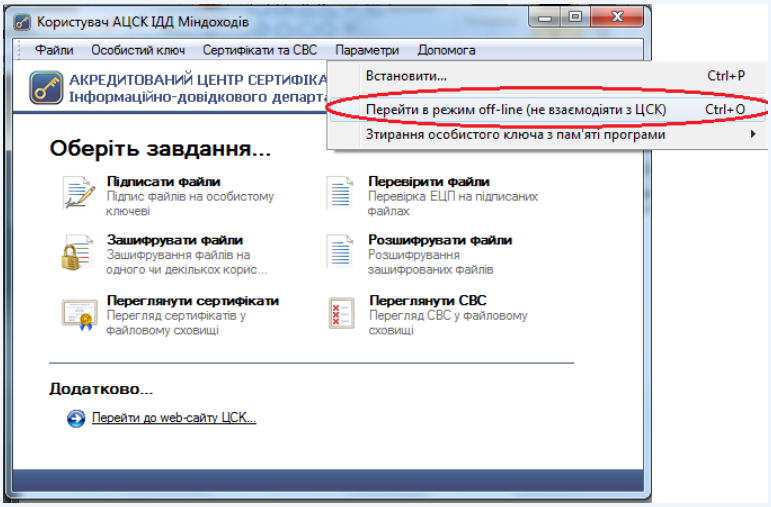

Рисунок 5.22

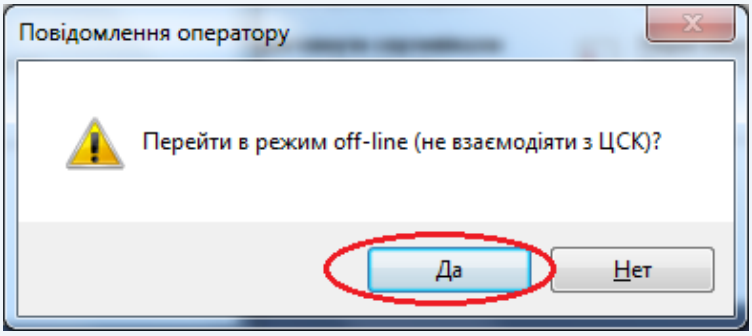

Рисунок 5.23

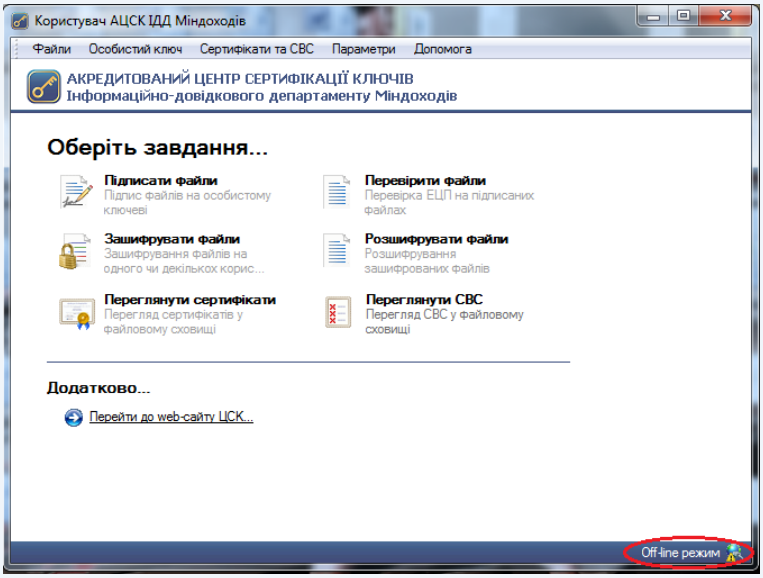

Рисунок 5.24