Програмний комплекс ІІТ Користувача ЦСК

Версія 1.3.1

MASTERKEY®
Акредитований центр сертифікації ключів

Акредитований центр сертифікації ключів «Masterkey»
вул. Сурикова, 3 (літ. А), Київ, 03035, Україна
тел.: +380 44 206-13-78, факс: +380 44 206-13-79
Безкоштовна технічна підтримка за телефоном: 0 800 502-44-40
info@masterkey.ua www.masterkey.ua

АНОТАЦІЯ

Даний документ містить настанову оператора для роботи з програмним комплексом користувача центра сертифікації ключів (далі – програма). Настанова містить відомості щодо послідовності та особливостям інсталяції, встановлення параметрів роботи та використання програми.

ЗМІСТ

1 ПРИЗНАЧЕННЯ ПРОГРАМИ

Програма призначена для застосування на засобах ЕОТ користувача центра сертифікації ключів і виконує наступні функції:

- управління ключами користувача:
  - генерацію ключів користувача ЦСК, запис особистого ключа на НКІ та формування запита на формування сертифіката;
  - перевірку сформованого сертифіката користувача на відповідність запиту;
  - 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 з файлового сховища;
  - 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;
  - перевірку файлів;
  - зашифрування файлів;
  - розшифрування файлів.

2 УМОВИ ВИКОНАННЯ ПРОГРАМИ

Програма може бути завантажена та виконана на ЕОМ під керуванням ОС Microsoft Windows XP/Vista/ Windows 7/8/8.1/ Windows 10/2003 Server/2008 Server/

3 ІНСТАЛЯЦІЯ ПРОГРАМИ

Щоб почати використовувати програмне забезпечення, спочатку потрібно її завантажити з web-сторінки АЦСК «Masterkey» та запустити програму інсталяції (майстер інсталяції) **EUArtMInstall.exe**.

Програмний комплекс користувача (комп'ютерна програма) «ІІТ Користувач ЦСК-1.3» https://masterkey.ua/download/EUArtMInstall.exe

Після запуску програми інсталяції на першій сторінці (рис. 3.1) виводиться інформація про початок інсталяції. Для продовження інсталяції необхідно натиснути кнопку "Далі", а для завершення – "Відміна".

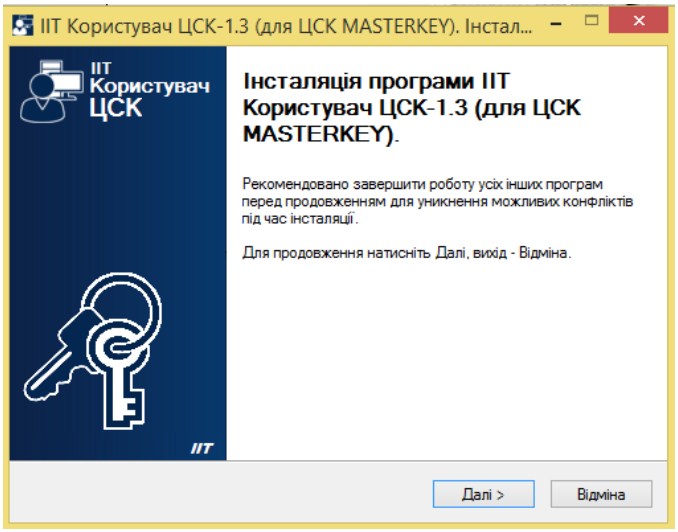


Рисунок 3.1

На наступній сторінці майстра (рис. 3.2) необхідно ознайомитись з ліцензійною угодою щодо використання програми та погодитись. Для продовження інсталяції необхідно встановити позначку "Я приймаю цю угоду" та натиснути кнопку "Далі".

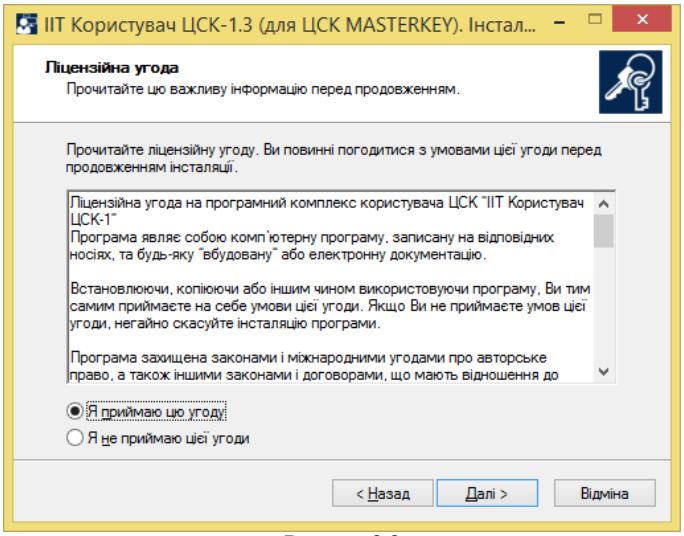


Рисунок 3.2

На наступній сторінці майстра (рис. 3.3) за необхідністю можна вказати каталог на диску до якого буде встановлено програму. Для продовження інсталяції необхідно натиснути кнопку "Далі".

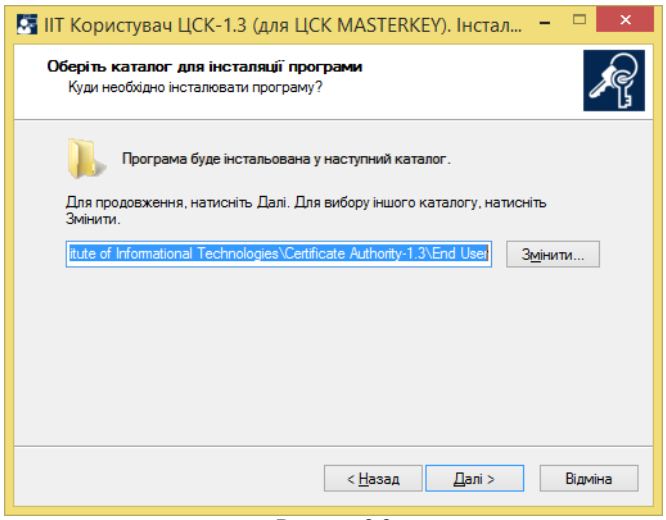


Рисунок 3.3

На наступній сторінці майстра (рис. 3.4) за необхідністю можна вказати розділ меню “Пуск” до якого буде встановлено значки запуску та деінсталяції програми. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

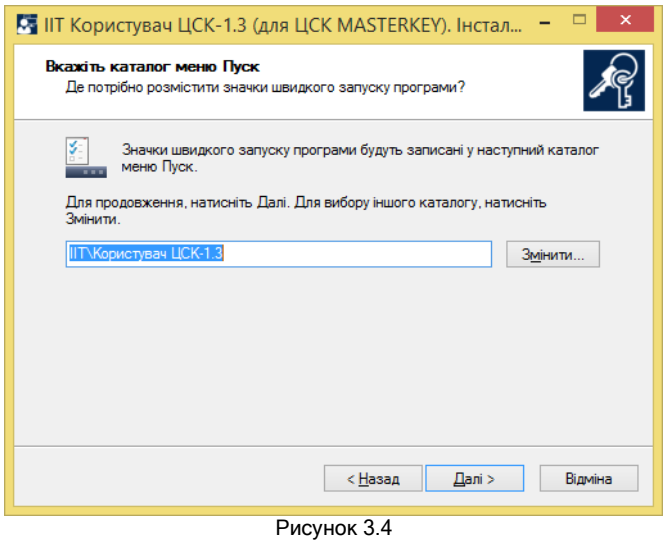


Рисунок 3.4

На наступній сторінці майстра (рис. 3.5) необхідно вказати каталог до якого будуть завантажуватись та зберігатися сертифікати і СВС. У параметрах роботи самої програми даний каталог визначається як “Каталог з сертифікатами та СВС” у параметрах файлового сховища (див. п. 4.2.2). Для зміни каталогу необхідно натиснути кнопку “Змінити” та обрати існуючий каталог чи створити новий. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

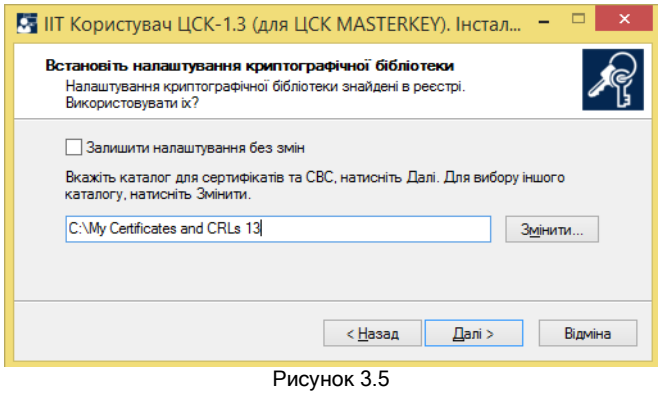


Рисунок 3.5

На наступній сторінці майстра (рис. 3.6) потрібно встановити признаки необхідності виконання майстром додаткових завдань - створення значку запуску програми на робочому столі та запуску програми після завершення інсталяції. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

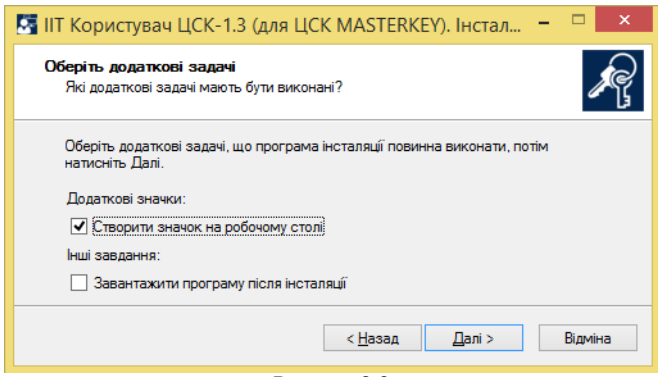


Рисунок 3.6

На наступній сторінці майстра (рис. 3.7) буде виведено інформацію про операції, що будуть виконані майстром. Для виконання інсталяції необхідно натиснути кнопку “Встановити”.

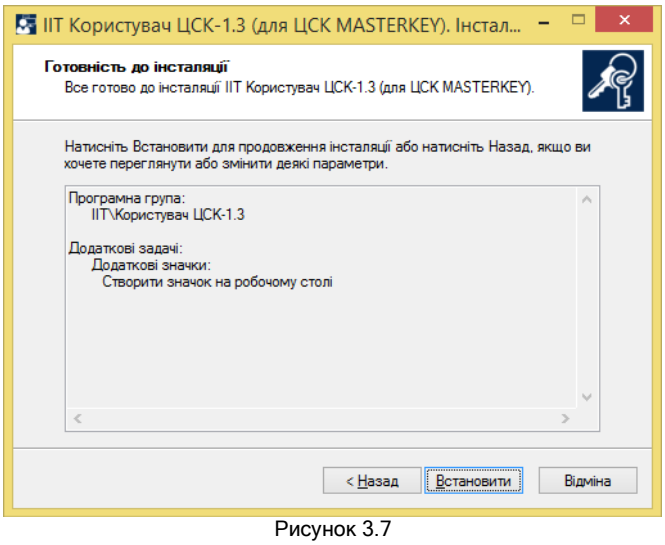


Рисунок 3.7

Після інсталяції програми, майстер завершує свою роботу.

Якщо було встановлено признак необхідності завантаження програми після інсталяції, то після завершення роботи майстра буде автоматично завантажено інстальовану програму.

Під час інсталяції також встановлюються драйвери електронного ключа “ІІТ. Кристал-1”. Під час інсталяції драйверів може бути видане наступне вікно (рис. 3.8) із попередженням про можливу несумісність драйверів електронного ключа із ОС. Необхідно натиснути ”Все равно продолжить”.

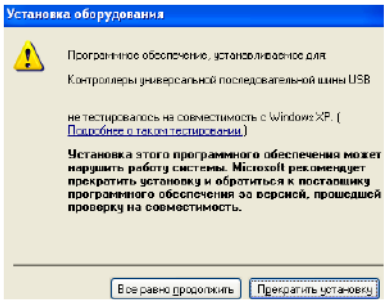


Рисунок 3.8

4 ПОЧАТОК РОБОТИ З ПРОГРАМОЮ

4.1 Завантаження програми

Для початку роботи програми у каталозі із сертифікатами та СВС обов'язково повинні бути записані:

- сертифікат ЦСК;
- сертифікати серверів ЦСК (за необхідністю);
- діючі СВС (за необхідністю).

Якщо сертифікати ЦСК, серверів ЦСК та СВС відсутні у інсталяційному пакеті, то необхідно завантажити їх з web-сторінки АЦСК «Masterkey» чи записати їх у відповідний каталог, отримавши іншими засобами з ЦСК.

Для завантаження діючих сертифікатів АЦСК переходимо на web-сторінки АЦСК «Masterkey» за наступним посиланням та загружаємо усі діючи сертифікати у відповідну директорію програмного забезпечення «**ІІТ Користувач ЦСК-1.3**» https://masterkey.ua/ca/ca-certificates?lang=ru

Для завантаження програми необхідно запустити модуль, що виконується **EUArtMInstall.exe** через файловий менеджер ОС або через меню "Пуск", обравши у розділі "ІІТ\Користувач ЦСК-1" підпункт "Користувач ЦСК" чи за допомогою значку на робочому столі. Після запуску на екрані буде відображене головне вікно програми, що наведене на рис. 4.1.

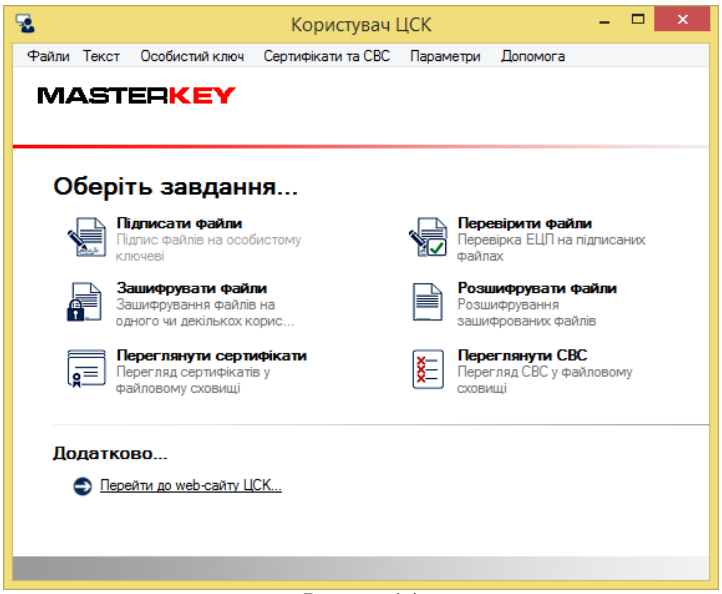


Рисунок 4.1

4.2 Встановлення параметрів роботи програми

Програма інсталяції під час свого виконання встановлює параметри роботи програми за замовчанням. При цьому встановлюються лише параметри файлового сховища з сертифікатами та СВС.

Для встановлення чи зміни параметрів роботи програми необхідно обрати підпункт "Встановити" в пункті меню "Параметри" (рис. 4.1). Вікно встановлення параметрів наведене на рис. 4.2.

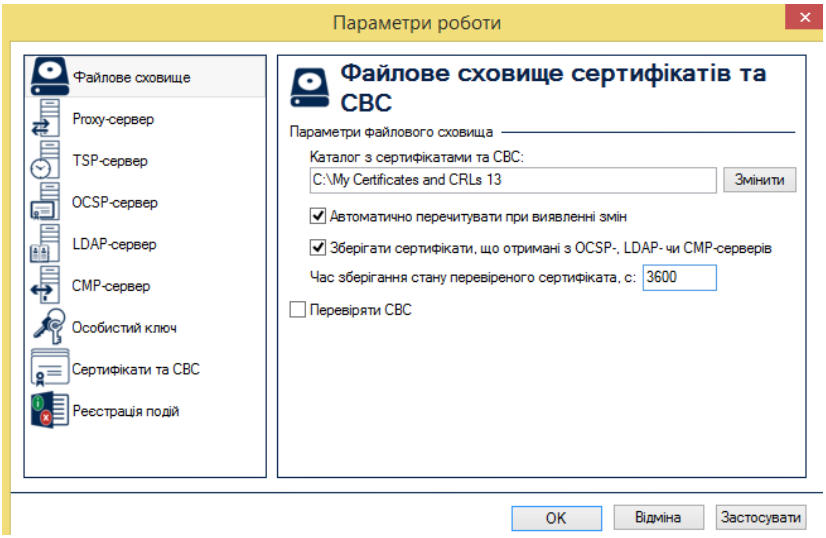


Рисунок 4.2

4.2.1 Файлове сховище

Для настроювання параметрів файлового сховища сертифікатів та СВС необхідно перейти до закладки “Файлове сховище”. Вікно “Параметри роботи” із сторінкою “Файлове сховище” наведене на рис. 4.2. На цій сторінці встановлюються наступні параметри роботи програми:

- “Каталог з сертифікатами та СВС”. Даний параметр встановлює каталог файлового сховища для зберігання сертифікатів та СВС.
  Всі сертифікати та СВС, що завантажуються не засобами програми повинні записуватися у даний каталог.
- “Автоматично перечитувати при виявлені змін”. Даний параметр визначає необхідність автоматичного перечитування каталогу файлового сховища програмою при внесенні будь-яких змін до цього каталогу (запису нового сертифіката чи СВС у каталог чи видалення файлу з сертифікатом або СВС).
  Якщо параметр не встановлено необхідно виконувати повторне зчитування файлового сховища після внесення змін. Для цього необхідно обрати підпункт “Зчитати сертифікати та СВС” в пункті меню “Сертифікати та СВС” або натиснути клавішу “F9” у головному вікні програми.
- “Зберігати сертифікати, що отримані з OCSP- чи LDAP-серверів”. Даний параметр визначає необхідність автоматичного збереження сертифікатів, що не знайдені у файловому сховищі, а отримані з OCSP- чи LDAP-серверів у файлове сховище.
- “Час зберігання стану перевіреного сертифікату”. Даний параметр визначає час протягом якого сертифікати що вже перевірені не будуть повторно перевірятися.
  Застосування такого механізму збереження стану сертифіката протягом певного часу забезпечує зменшення ресурсів системи на перевірку сертифіката при частих звертаннях (механізм кешування статусу сертифіката).
- “Перевіряти СВС”. Параметр вказує на необхідність використання СВС в якості засобу перевірки статусу сертифікатів відкритих ключів що використовуються.
- “Тільки свого ЦСК”. Даний параметр визначає необхідність використовувати при перевірці сертифікатів СВС лише свого ЦСК у ланцюжку.
  Для цього повинен бути зчитаний особистий ключ користувача, оскільки ЦСК користувача визначається за допомогою параметрів особистого ключа.
- “Повний та частковий”. Даний параметр визначає необхідність перевірки наявності двох діючих СВС (повного та часткового) при здійсненні перевірки сертифікатів.
  Якщо параметр не встановлено достатньо лише одного повного діючого СВС. Даний параметр дозволяє не виконувати постійне завантаження останнього діючого часткового СВС.
- “Завантажувати автоматично”. Даний параметр визначає можливість автоматичного завантаження СВС під час перевірки статусу сертифікатів, якщо у файловому сховищі не знайдено діючих СВС.
  Параметр має сенс якщо у сертифікатах ЦСК, або серверів ЦСК встановлено шлях отримання СВС.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

4.2.2 Proxy-сервер

«Proxy- сервер» прописуємо якщо він у Вас використовується. Для настроювання параметрів proxy-сервера необхідно перейти до закладки “Proxy-сервер” у вікні що наведене на рисунку 4.2. Вікно “Параметри роботи” із сторінкою “Proxy-сервер” наведене на рис. 4.3. На сторінці “Proxy-сервер” встановлюються наступні параметри роботи програми:

- “Підключатися через proxy-сервер”. Встановлює необхідність використання proxy-сервера під час підключення до серверів обробки запитів.
- “Ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я proxy-сервера.
- “TCP-порт”. Даний параметр встановлює TCP-порт proxy-сервера.
- “Автентифікуватися на proxy-сервері”. Встановлює необхідність автентифікації (вводу логіну та паролю) під час підключення до proxy-сервера.
- “Ім’я користувача”. Даний параметр встановлює ім’я користувача proxy-сервера.
  Якщо proxy-сервер працює в режимі без автентифікації даний параметр може не вводитися.
- “Пароль”. Даний параметр встановлює пароль доступу користувача до proxy-сервера.
  Якщо proxy-сервер працює в режимі без автентифікації даний параметр може не вводитися.
- “Зберегти пароль”. Даний параметр встановлює необхідність зберігати пароль доступу до proxy-сервера у реєстрі ОС.
  У випадку якщо даний параметр не встановлено, введення паролю буде запрошуватися при першому підключенні до proxy-сервера у програмі.

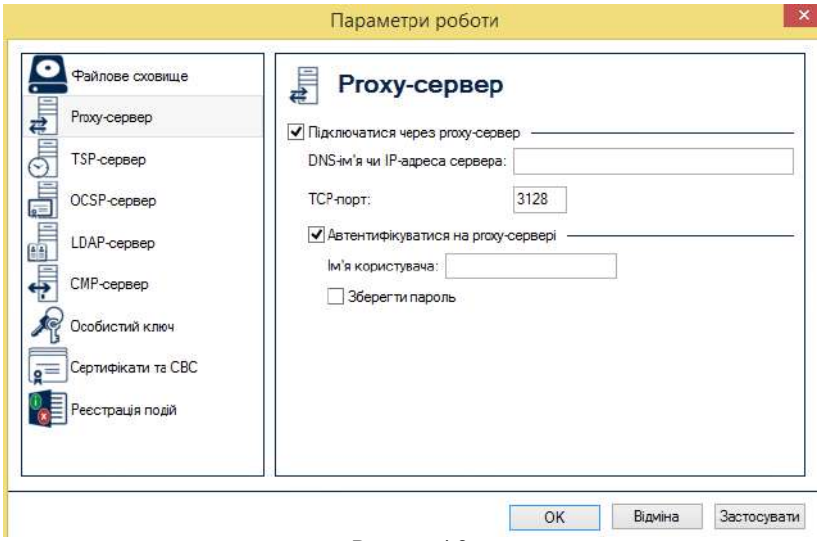


Рисунок 4.3

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

4.2.3 TSP-сервер

Для настроювання параметрів TSP-сервера необхідно перейти до закладки “TSP-сервер” у вікні що наведене на рисунку 4.2. Вікно “Параметри роботи” із сторінкою “TSP-сервер” наведене на рис. 4.4. На сторінці “TSP-сервер” встановлюються наступні параметри роботи програми:

- “Ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я TSP-сервера.
  Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
- “TCP-порт”. Даний параметр встановлює TCP-порт TSP-сервера.
  Як правило це порт протоколу HTTP (80).

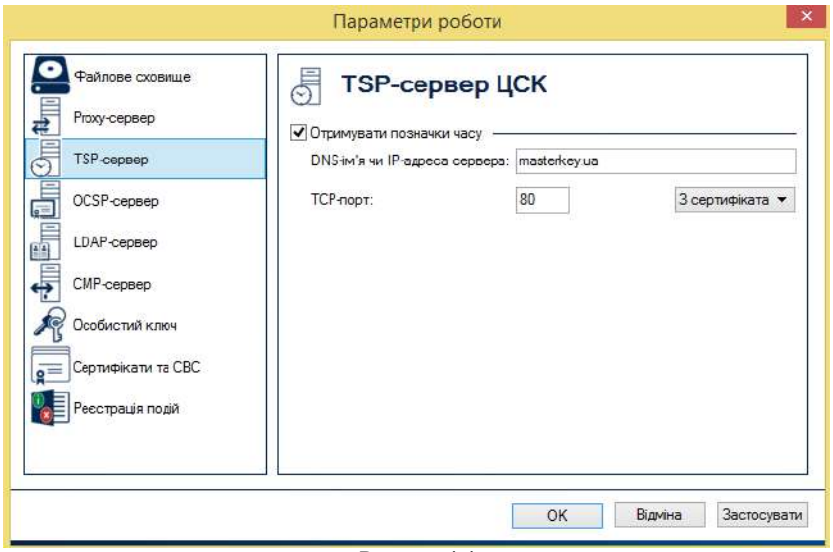


Рисунок 4.4

Для встановлення параметрів доступу до TSP-серверу з сертифіката сервера необхідно натиснути кнопку “З сертифіката сервера…”.

Для встановлення параметрів доступу до TSP-серверу з сертифіката користувача необхідно натиснути кнопку “З сертифіката користувача…”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

4.2.4 OCSP-сервер

Для настроювання параметрів OCSP-сервера необхідно перейти до закладки “OCSP-сервер” у вікні що наведене на рисунку 4.2. Вікно “Параметри роботи” із сторінкою “OCSP-сервер” наведене на рис. 4.5. На сторінці “OCSP-сервер” встановлюються наступні параметри роботи програми:

– “Ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я OCSP-сервера.
Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
– “TCP-порт”. Даний параметр встановлює TCP-порт OCSP-сервера.
Як правило це порт протоколу HTTP (80).
– “Перевіряти статус сертифікатів через OCSP до перевірки у файловому сховищі”. Даний параметр встановлює черговість перевірки статусу сертифіката.
Якщо параметр встановлено, статус сертифіката перевіряється спочатку за допомогою OCSP-протоколу, потім за допомогою файлового сховища.
Якщо параметр не встановлено, перевірка здійснюється спочатку за допомогою файлового сховища, а потім (за необхідністю) за допомогою OCSP-протоколу.

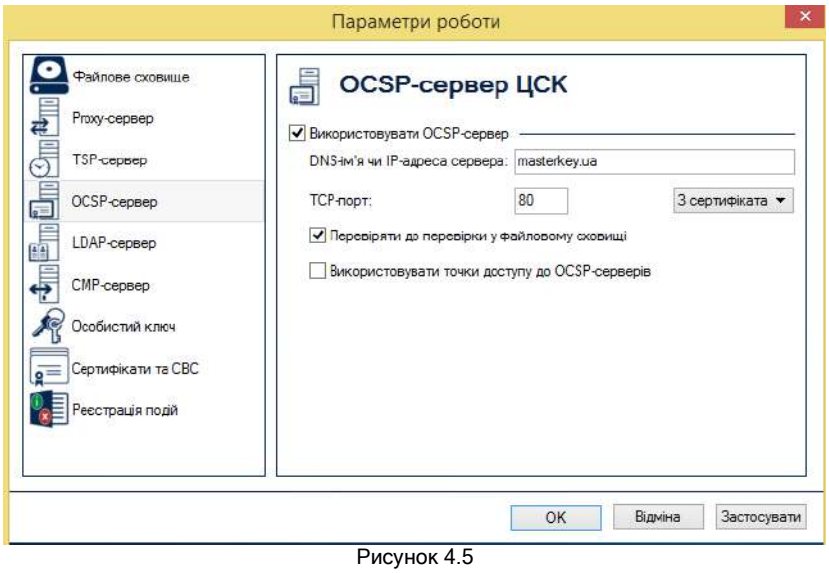


Рисунок 4.5

Для встановлення параметрів доступу до OCSP-серверу з сертифіката сервера необхідно натиснути кнопку “З сертифіката сервера…”.

Для встановлення параметрів доступу до OCSP-серверу з сертифіката користувача необхідно натиснути кнопку “З сертифіката користувача…”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

4.2.5 LDAP-сервер

Для настроювання параметрів LDAP-сервера перейти до закладки “LDAP-сервер” у вікні що наведене на рисунку 4.2. Вікно “Параметри роботи” із сторінкою “LDAP-сервер” наведене на рис. 4.6. На сторінці “LDAP-сервер” встановлюються наступні параметри роботи програми:

- “Ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я LDAP-сервера.
  Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
- “TCP-порт”. Даний параметр встановлює TCP-порт LDAP-сервера.
  Як правило це порт протоколу LDAP (389).
- “Анонімний доступ”. Даний параметр встановлює застосування анонімного доступу до LDAP-сервера (без використання імені користувача та паролю).
- “Ім’я користувача”. Даний параметр використовується якщо не встановлено параметр “Анонімний доступ” та встановлює ім’я користувача LDAP-сервера.
- “Пароль доступу”. Даний параметр використовується якщо не встановлено параметр “Анонімний доступ” та встановлює пароль доступу користувача до LDAP-сервера.
- “Шукати сертифікати у LDAP-каталозі”. Даний параметр встановлює необхідність пошуку сертифікатів у LDAP-каталозі, у випадку якщо сертифікат не знайдено у файловому сховищі та за допомогою OCSP-протоколу.

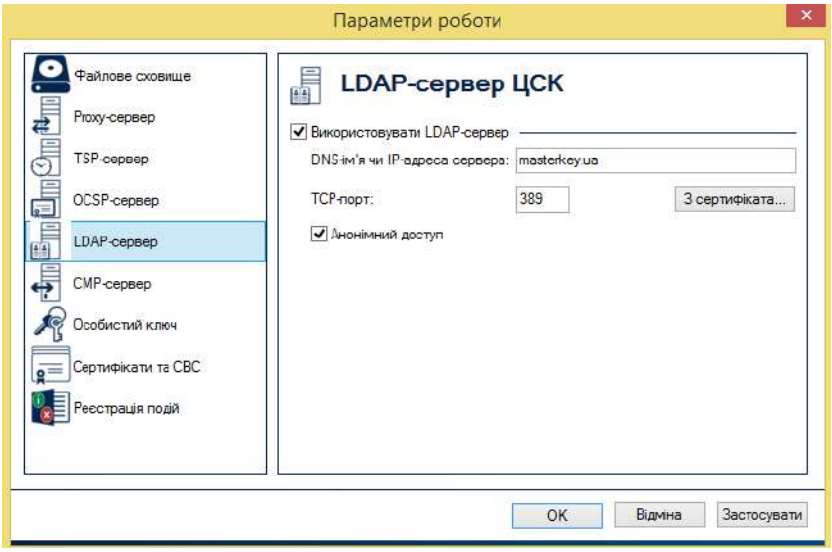


Рисунок 4.6

За замовчанням встановлюються параметри LDAP-сервера що вказані у відповідному сертифікаті сервера або ЦСК. Параметри LDAP-сервера можна також встановити з сертифіката за допомогою кнопки “З сертифіката…”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

4.2.6 CMP-сервер

Для настроювання параметрів CMP-сервера необхідно перейти до закладки “CMP-сервер” у вікні що наведене на рисунку 4.2. Вікно “Параметри роботи” із сторінкою “CMP-сервер” наведене на рис. 4.7. На сторінці “CMP-сервер” встановлюються наступні параметри роботи програми:

- “Ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я CMP-сервера.
  Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
- “TCP-порт”. Даний параметр встановлює TCP-порт CMP-сервера.
  Як правило це порт протоколу HTTP (80).

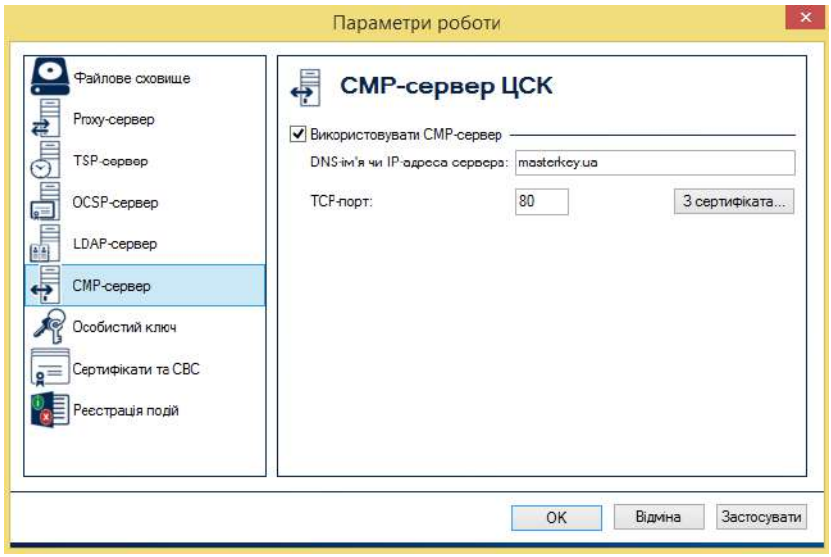


Рисунок 4.7

Параметри CMP-сервера можна також встановити з сертифіката за допомогою кнопки “З сертифіката…”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

4.3 Режими роботи програми

Програма може працювати у двох режимах:

- режим on-line (із взаємодією з ЦСК);
- режим off-line (без взаємодії з ЦСК).

В першому режимі програма може взаємодіяти з ЦСК (отримувати позначки часу, використовувати OCSP-протокол, завантажувати СВС з web-сервера тощо).

У другому режимі програма не взаємодіє з ЦСК, навіть якщо встановлені параметри серверів ЦСК. Даний режим використовується для роботи без підключення до мережі Internet без зміни встановлених параметрів.

Для встановлення режиму роботи з ЦСК необхідно обрати підпункт меню “Перейти в режим off-line (не взаємодіяти з ЦСК)/Перейти в режим on-line (взаємодіяти з ЦСК)” в пункті меню “Параметри”.

Якщо програма працює у режимі off-line інформацію про це буде виведено до нижньої частини головного вікна програми (рис.4.8).

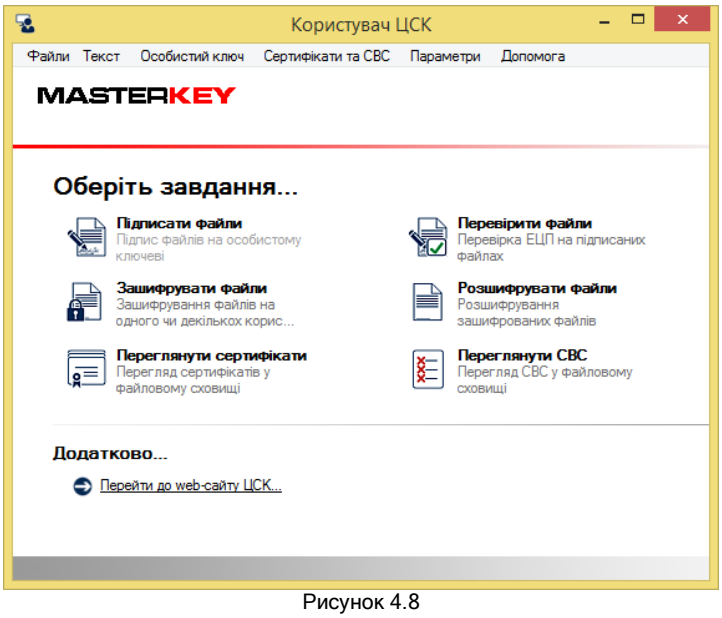


Рисунок 4.8

5 УПРАВЛІННЯ СЕРТИФІКАТАМИ ТА СВС

5.1 Отримання сертифікатів з ЦСК

Програма має засоби для отримання набору сертифікатів з ЦСК за допомогою запиту до сервера обробки запитів. До пакету сертифікатів входять сертифікат ЦЗО (якщо ЦСК акредитований), сертифікат ЦСК, сертифікати центральних серверів ЦСК (CMP, TSP, OCSP), та сертифікат користувача що робить запит. Запит формується за допомогою особистого ключа користувача.

Для отримання пакету сертифікатів необхідно обрати підпункт “Отримати з ЦСК...” в пункті меню “Сертифікати та СВС”. Після чого буде виведене вікно що наведене на рис. 5.1. У вікні необхідно натиснути “Далі”, після чого буде проведене зчитування особистого ключа користувача (більш детально у п.п. 6.2). Після отримання пакету сертифікатів користувачу буде виведене діалогове вікно (рис. 5.3) із переліком сертифікатів та пропозицією щодо збереження їх до файлового сховища. Для роботи із сертифікатами їх необхідно зберегти до файлового сховища.

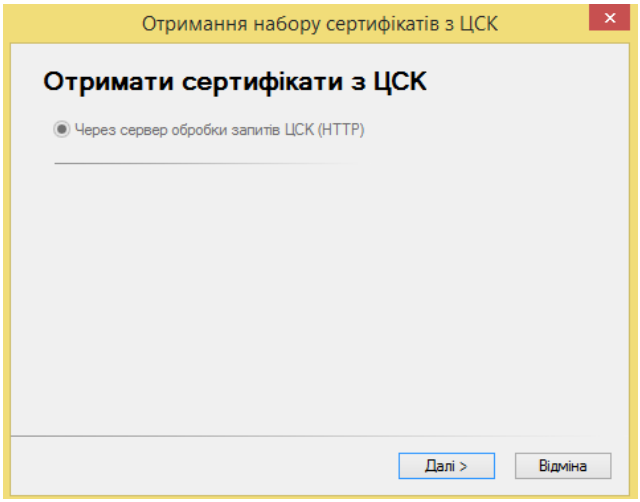


Рисунок 5.1

Після зчитування особистого ключа буде виведене вікно (рис. 5.2) у якому необхідно вказати параметри доступу до сервера взаємодії ЦСК. **Proxy- сервер** прописуємо якщо він у Вас використовується.

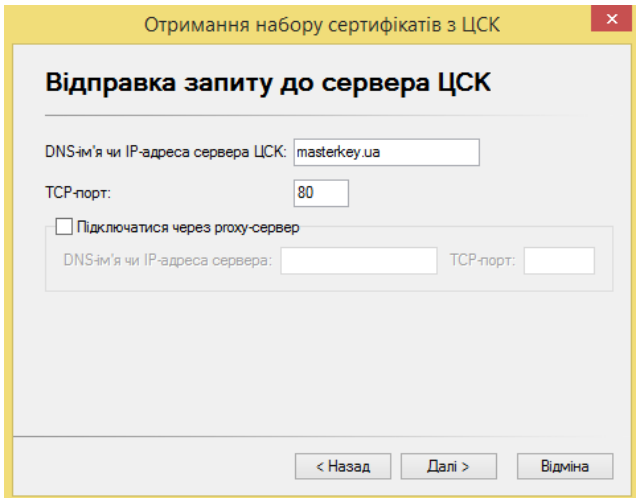


Рисунок 5.2

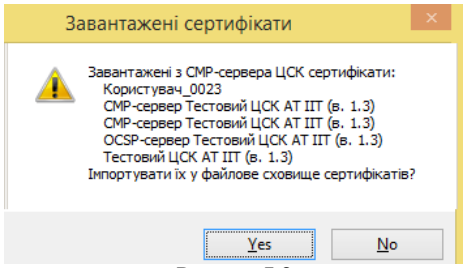


Рисунок 5.3

5.2 Зчитування сертифікатів та СВС

Програма автоматично виконує зчитування сертифікатів та СВС з файлового сховища при першій необхідності після свого запуску. При внесенні змін (запису чи видалення сертифікатів чи СВС) до файлового сховища під час роботи програми, якщо не встановлено параметр “Автоматично перечитувати файлове сховище при виявленні змін” (див п. 4.2.1), необхідно перечитати файлове сховище. Для цього необхідно обрати підпункт “Зчитати сертифікати та СВС” в пункті меню “Сертифікати та СВС” або натиснути клавішу F9.

5.3 Перегляд сертифікатів

Для перегляду сертифікатів що містяться у файловому сховищі необхідно обрати підпункт “Переглянути сертифікати...” в пункті меню “Сертифікати та СВС” або натиснути клавішу F10. Вікно із сертифікатами наведене на рис. 5.4.

За допомогою даного вікна можна видаляти сертифікати з файлового сховища, перевіряти та переглядати сертифікати.

Сертифікати у вікні відсортовані за типами власників (тип власника обирається у верхній частині вікна у випадаючому списку):

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

Для перегляду списку сертифікатів власника певного типу необхідно обрати відповідний тип власника у верхній частині вікна у списку що випадає.

Для перегляду сертифіката необхідно натиснути на відповідному записі про сертифікат у списку. Сертифікат буде відображено у вікні що наведене на рисунках 5.5 та 5.6.

Для видалення сертифікатів з файлового сховища необхідно виділити у списку відповідні записи про сертифікати 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 (див п. 4.2) - за допомогою СВС, OCSP-протоколу тощо. Результатом перевірки буде вікно що наведене на рис. 5.7. Якщо у цьому вікні натиснути “Сертифікат”, сертифікат буде відображений у вікні детального перегляду (рис. 5.6).

Для імпорту сертифіката до файлового сховища необхідно натиснути “Імпортувати”, та обрати потрібний сертифікат на будь-якому носії інформації.

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

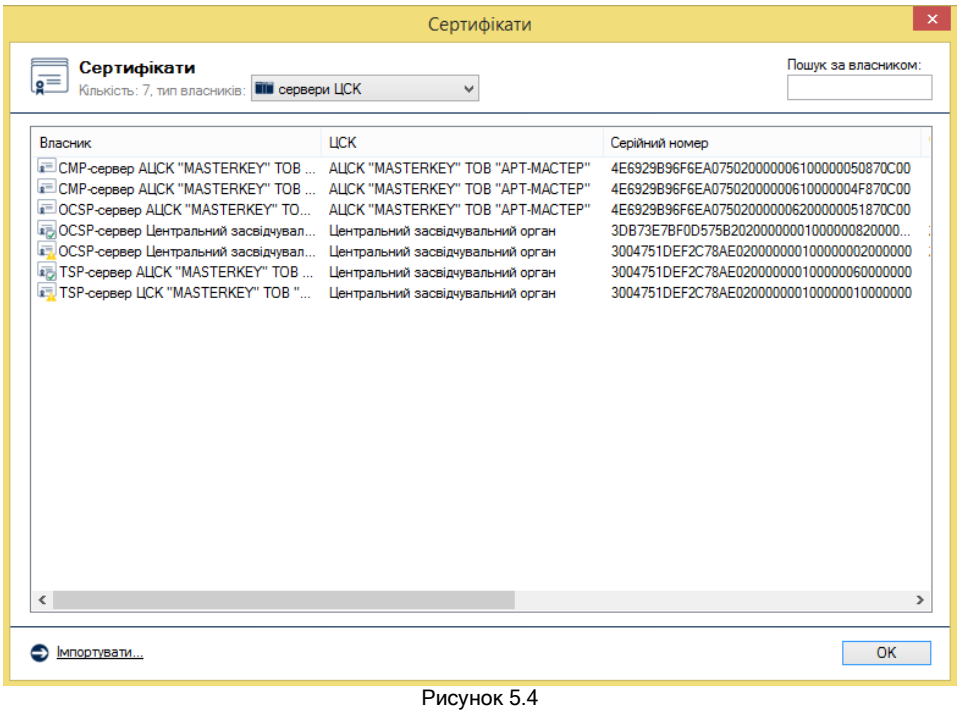


Рисунок 5.4

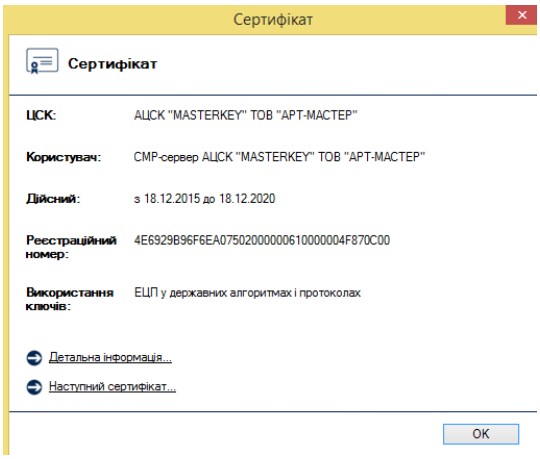


Рисунок 5.5

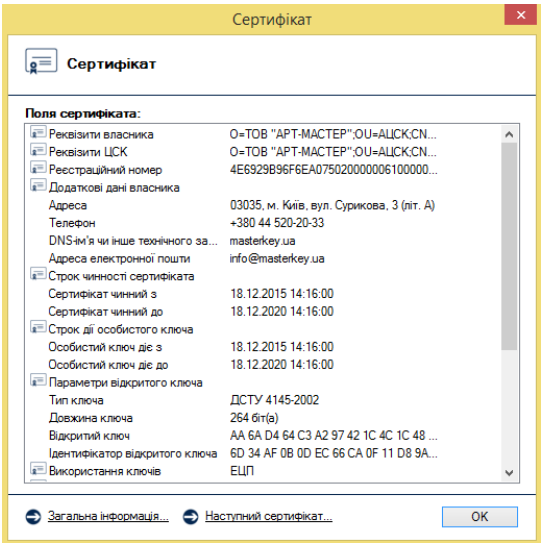


Рисунок 5.6

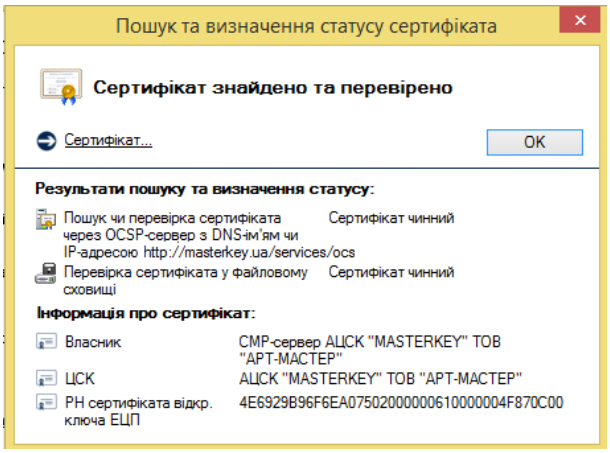


Рисунок 5.7

5.4 Перегляд СВС

Для перегляду списків відкликаних сертифікатів (СВС) необхідно натиснути підпункт “Переглянути СВС...” в пункті меню “Сертифікати та СВС” або натиснути клавішу F11. Вікно із списками відкликаних сертифікатів наведене на рис. 5.8.

Вікно перегляду СВС дозволяє видаляти СВС з файлового сховища, переглядати СВС та завантажувати СВС з web-сервера ЦСК.

Для перегляду СВС необхідно натиснути на відповідному записі про СВС у списку. СВС буде відображено у вікні що наведене на рисунках 5.9 та 5.10.

Для видалення файлу СВС з файлового сховища необхідно виділити відповідний запис про СВС у списку та натиснути кнопку “Видалити”.

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

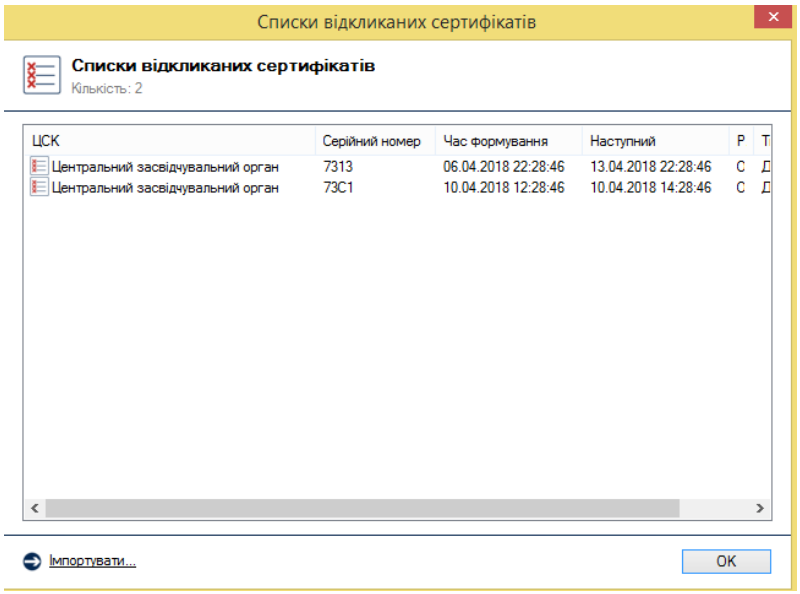


Рисунок 5.8

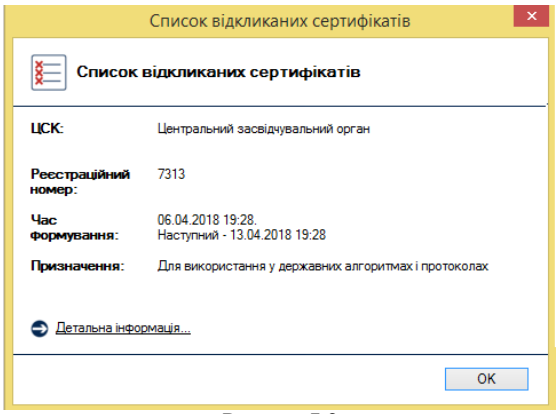


Рисунок 5.9

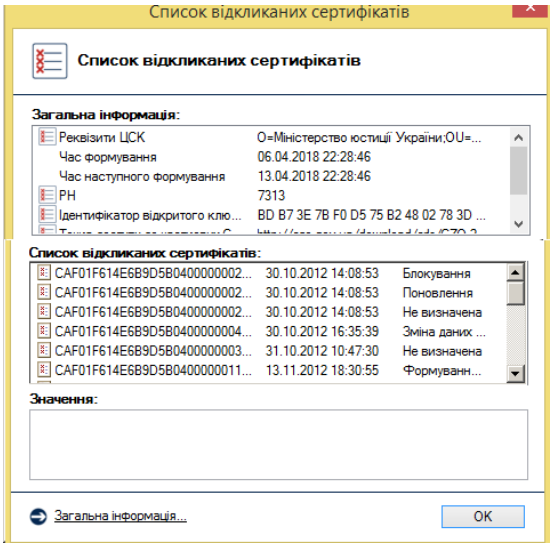


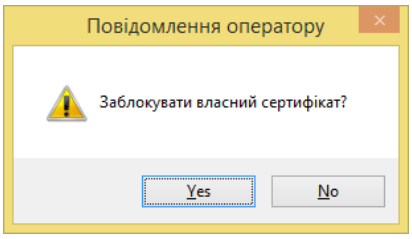
Рисунок 5.10

5.5 Завантаження СВС

Для автоматичного завантаження списку відкликаних сертифікатів з web-сервера ЦСК необхідно відповідну позначку (“Завантажувати автоматично”) у вікні параметрів що наведене на рис. 4.2.

5.6 Блокування власного сертифіката

Для блокування власного сертифіката необхідно обрати підпункт “Заблокувати власний сертифікат” в пункті меню “Сертифікати та СВС”. Підтвердити повідомлення блокування сертифіката.



Наступним кроком є зчитування особистого ключа та сертифіката користувача (див. п. 6.2).

Після зчитування особистого ключа почне роботу майстер блокування сертифіката. Запит буде переданий через сервер взаємодії ЦСК за протоколом HTTP де у наступному вікні (рис. 5.11) необхідно ввести параметри підключення до сервера взаємодії ЦСК:

- DNS-ім’я чи IP-адресу сервера (як правило це DNS-ім’я чи IP-адреса сервера взаємодії ЦСК);
- TCP-порт (як правило порт протоколу HTTP (80));
- параметри доступу до proxy-сервера (за необхідністю та якщо вони не встановлювались в параметрах роботи).

Після встановлення параметрів необхідно натиснути кнопку “Далі”.;

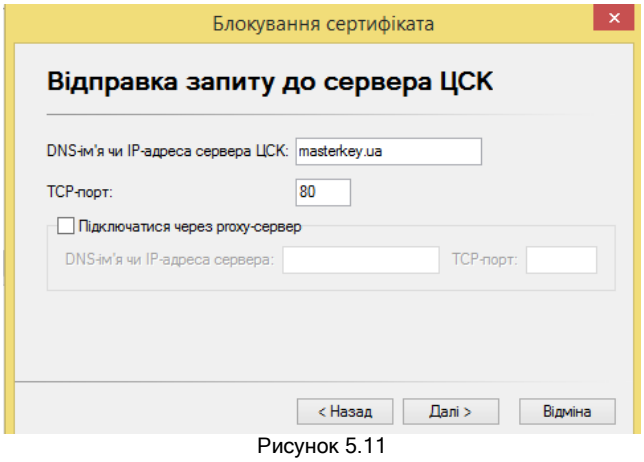


Рисунок 5.11

Якщо під час відправки запита не виникало помилок буде виведено вікно що наведене на рис. 5.12.

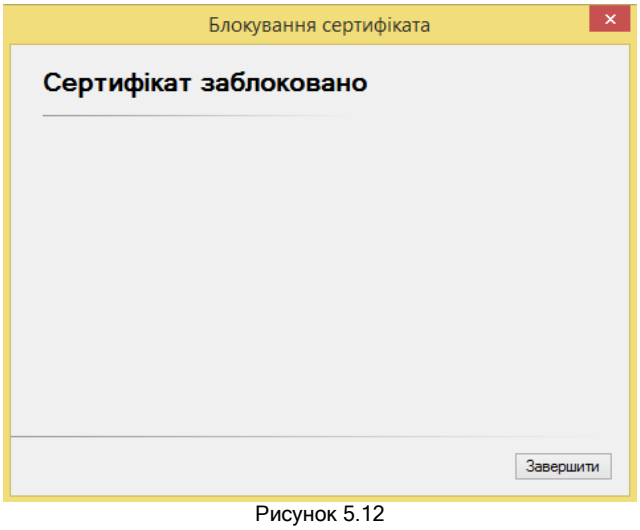


Рисунок 5.12

5.7 Формування нового сертифіката

Користувач може самостійно формувати нові сертифікати якщо має діючий ключ та такі операції дозволяються регламентом роботи ЦСК.

Примітка. Після формування нового сертифіката сервер обробки запитів здійснює автоматичне скасування попереднього сертифіката.

Для формування нового сертифіката необхідно обрати підпункт “Сформувати новий сертифікат” в пункті меню “Сертифікати та СВС”. Перше вікно майстра формування нового сертифіката наведене на рис. 5.13. За допомогою цього вікна здійснюється генерація нових ключів користувача. Якщо обирається генерація на новий носій, спочатку виконується генерація ключа (рис. 5.14), а потім зчитування діючого особистого ключа (рис. 5.15). Якщо генерація здійснюється на текучий носій, спочатку виконується зчитування діючого ключа, а потім генерація нового.

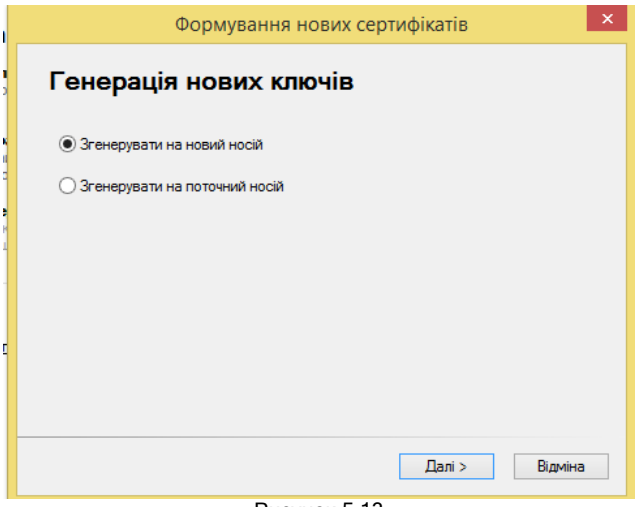


Рисунок 5.13

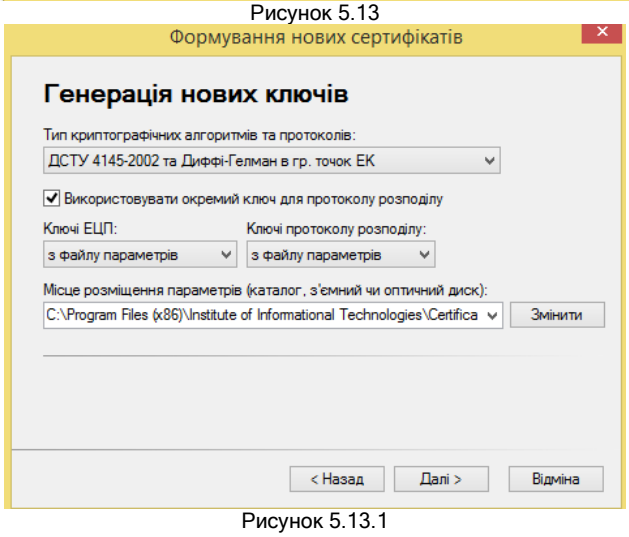


Рисунок 5.13.1

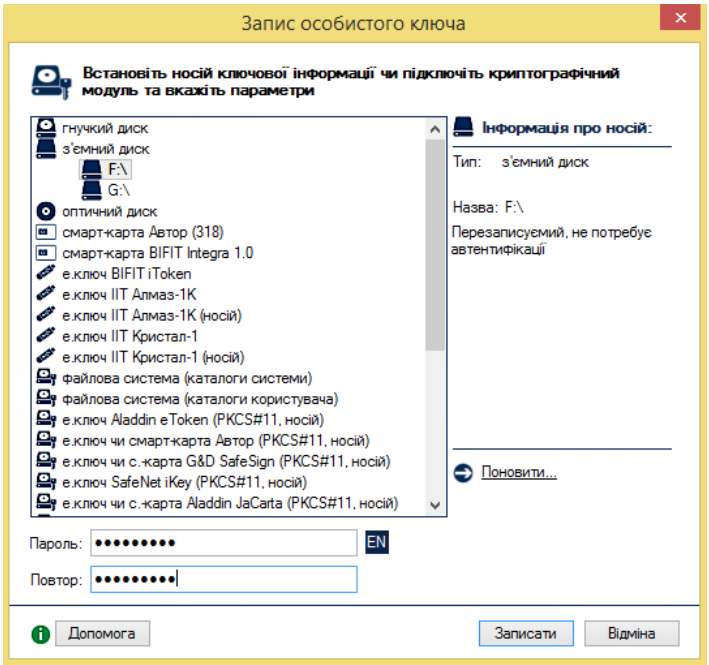


Рисунок 5.14

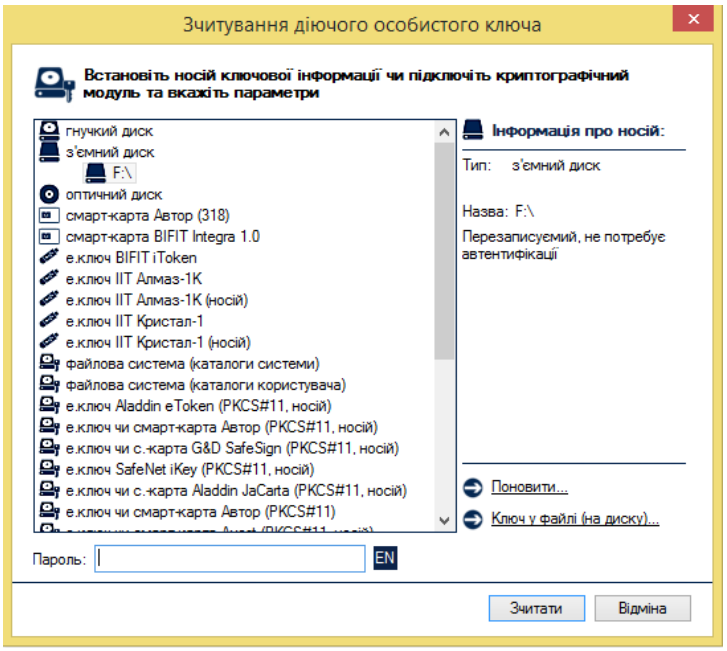


Рисунок 5.15

Після зчитування діючого особистого ключа, та генерації нового ключа, у наступному вікні майстра формування нового сертифіката (рис. 5.16) необхідно вказати спосіб за який буде передано запит до сервера обробки запитів ЦСК.

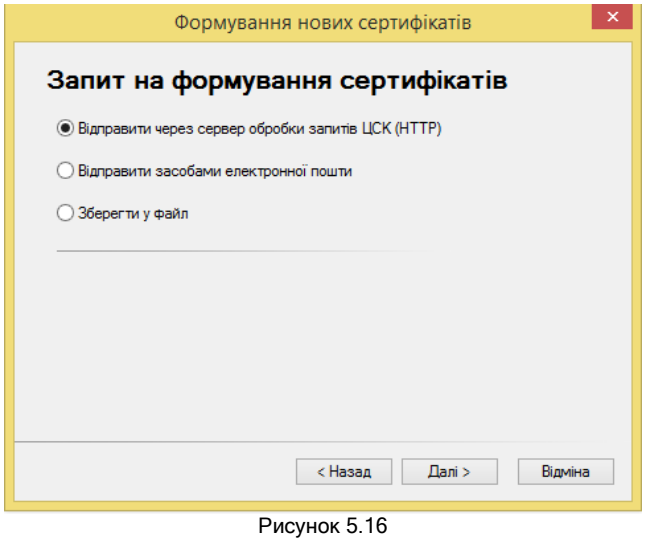


Рисунок 5.16

5.7.1 Передача запита за допомогою сервера обробки запитів ЦСК

У разі якщо запит повинен бути переданий через сервер взаємодії ЦСК за протоколом HTTP у наступному вікні (рис. 5.17) необхідно ввести параметри підключення до сервера взаємодії ЦСК:

- DNS-ім'я чи IP-адресу сервера (як правило це DNS-ім'я чи IP-адреса сервера взаємодії ЦСК);
- TCP-порт (як правило порт протоколу HTTP (80));
- параметри доступу до proxy-сервера (за необхідністю та якщо вони не встановлювались в параметрах роботи).

Після встановлення параметрів необхідно натиснути кнопку "Далі".

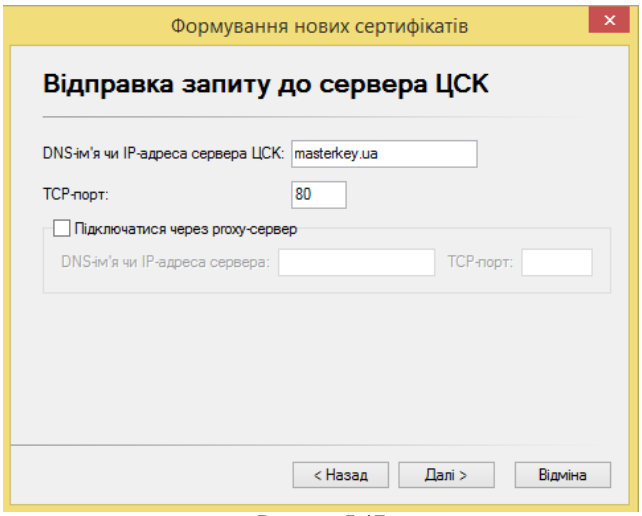


Рисунок 5.17

Якщо під час відправки запита не виникало помилок, буде виведено новий сертифікат користувача у вікні що наведене на рис. 5.18, та вікно що наведене на рис. 5.19.

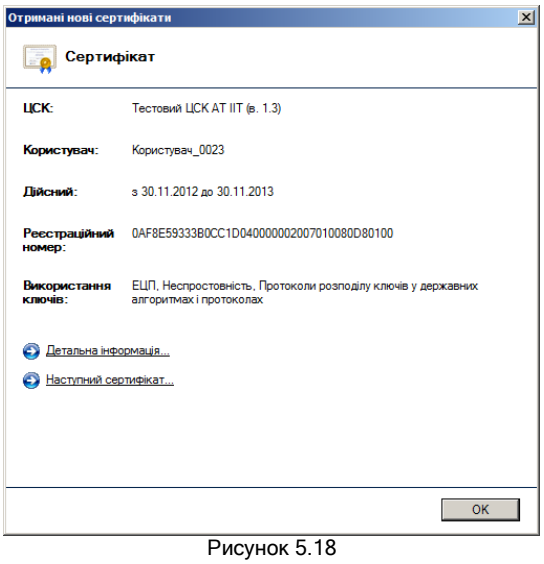


Рисунок 5.18

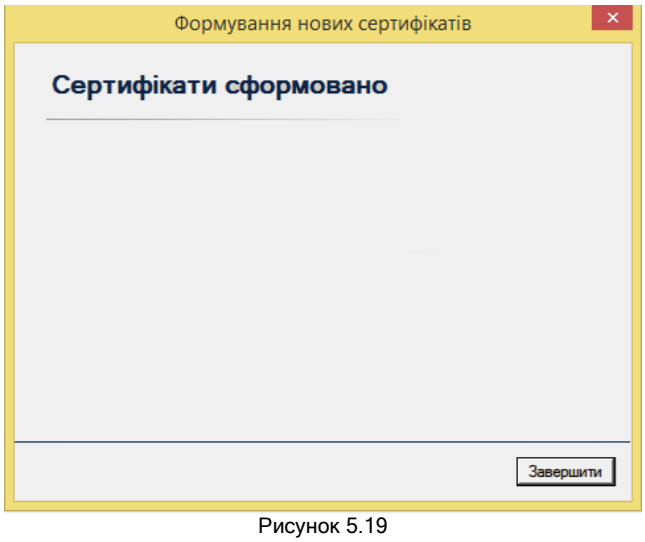


Рисунок 5.19

5.7.2 Передача запита засобами електронної пошти

У разі якщо запит повинен бути переданий засобами електронної пошти у наступному вікні (рис. 5.20) необхідно ввести параметри підключення до поштового сервера:

- DNS-ім'я чи IP-адресу поштового сервера;
- TCP-порт (як правило це порт протоколу SMTP (25));
- ім'я користувача поштового сервера;
- поштову адресу сервера взаємодії ЦСК;
- поштову адресу відправника.

Після встановлення параметрів необхідно натиснути кнопку "Далі".

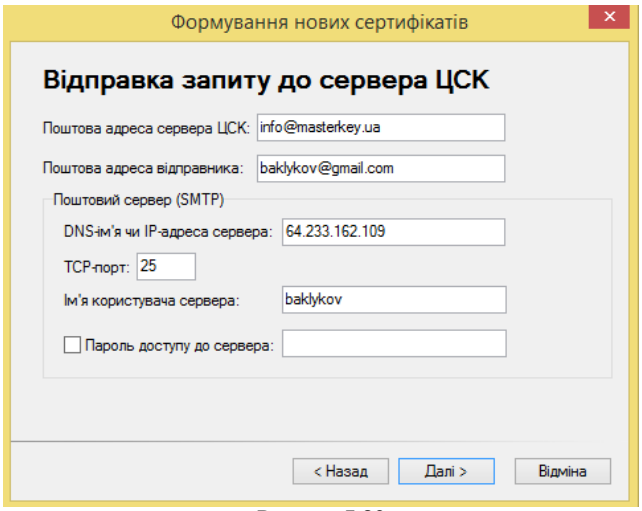


Рисунок 5.20

Після відправлення поштового повідомлення майстер завершує свою роботу (рис.5.21).

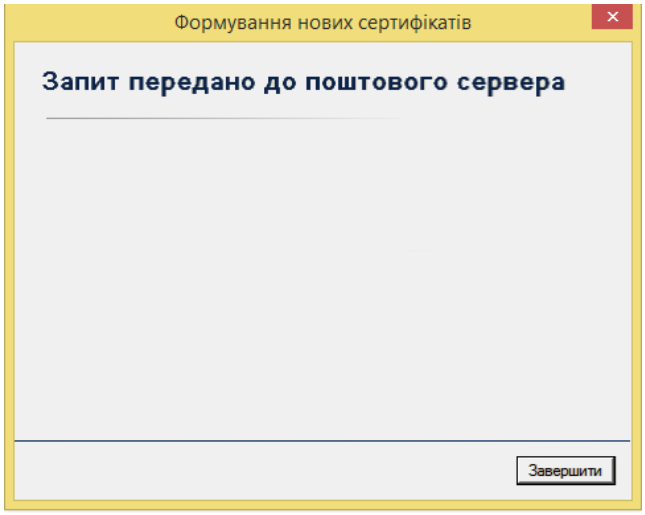


Рисунок 5.21

5.7.3 Передача запита за допомогою файлу запита

Для відправки запита іншими засобами (нештатними засобами електронної пошти програми чи ін.) запит може бути збережений у файл (рис. 5.22).

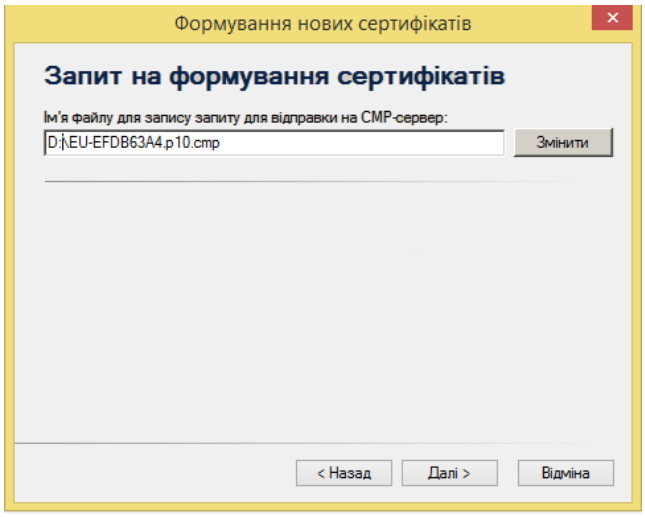


Рисунок 5.22

Після збереження запиту до файлу майстер завершує свою роботу (рис. 5.23).

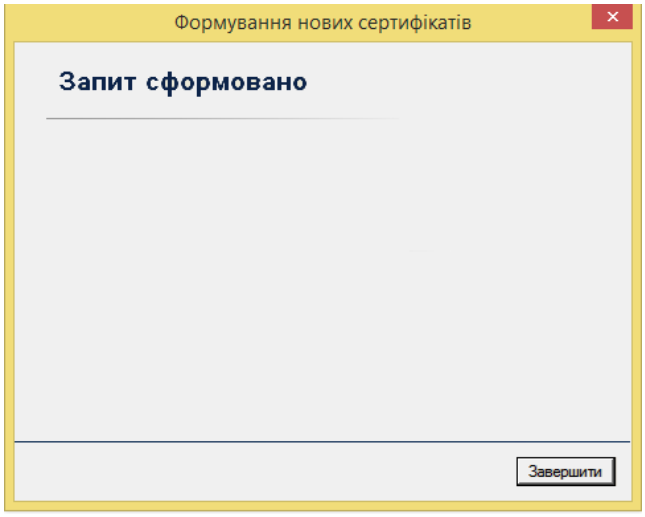


Рисунок 5.23

5.8 Помилки, що можуть виникати під час роботи програми

5.7.1 Помилка під час завантаження СВС

Вікно з повідомленням про помилку наведене на рисунку 5.24.

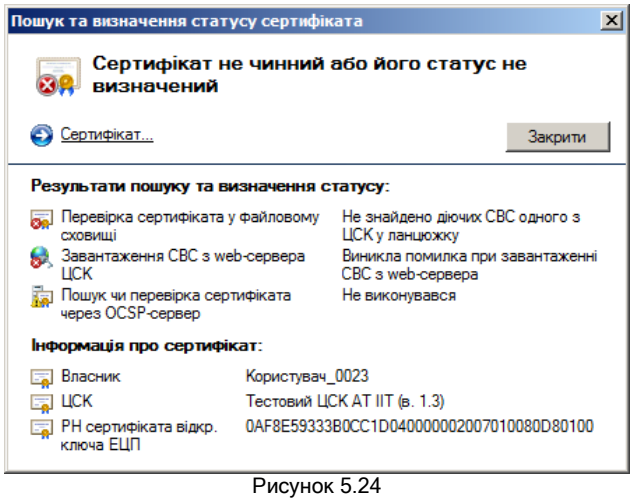


Рисунок 5.24

Така помилка може виникати:

- не вказано адресу proxy-сервера (або не встановлено признак необхідності його використання) у параметрах роботи програми;
- якщо не вірно вказані параметри аутентифікації proxy-сервера;
- у сертифікаті, що вказувався як джерело шляху отримання СВС не вказано, або вказано невірний шлях отримання СВС;
- не має доступу до web-сторінки завантаження СВС.

5.7.2 Помилки під час перевірки сертифікатів

Під час перевірки сертифікатів можуть виникати помилки аналогічні до помилок що описані у п.п. 5.7.1 та пов’язані із доступом серверів обробки запитів ЦСК по каналам зв’язку. При виникненні помилок насамперед необхідно перевірити параметри роботи програми у відповідності до розділу 4.

6 УПРАВЛІННЯ КЛЮЧАМИ

6.1 Генерація ключів

Для генерації ключів необхідно обрати підпункт “Згенерувати ключі” в пункті меню “Особистий ключ”. На першій сторінці майстра (рис. 6.1) за необхідністю можна вказати параметри криптографічних алгоритмів та протоколів (для більшості випадків ці параметри можна залишити за замовчанням).

Якщо параметр "Використовувати окремий ключ для протоколу розподілу" встановлено, то буде згенеровано 2 ключа: один для ЕЦП, другий для протоколу розподілу. Якщо параметр не встановлено, то буде згенеровано один ключ, що буде використовуватись як для ЕЦП, так і для зашифрування.

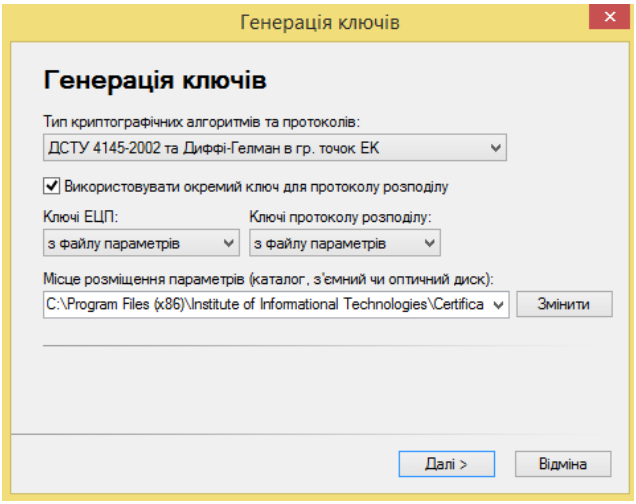


Рисунок 6.1

Далі необхідно встановити HKI для запису особистого ключа у пристрій запису та на наступній сторінці майстра (рис. 6.2) вказати:

- тип носія ключової інформації (HKI);
- назву носія;
- пароль доступу до ключового носія (якщо в якості носія використовується криптомодуль) або пароль захисту особистого ключа (з підтвердженням).

Ключові носії можуть бути наступних типів:

- гнучкі диски 3,5” (дискети);
- з’ємні диски (flash-диски);
- оптичні диски (CD-R, CD-RW, DVD-R або DVD-RW);
- електронні ключі (“IIT.Кристал-1”, , Aladdin eToken R2, PRO, Технотрейд uaToken та інші).

Пароль захисту особистого ключа повинен відповідати наступним вимогам:

- довжина - не менше 8 символів;
- не повинен містити однакові символи;
- не повинен містити підряд більше ніж 2 символи з розкладинки клавіатури;
- дозволені символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка. Такі вимоги носять рекомендаційний характер.

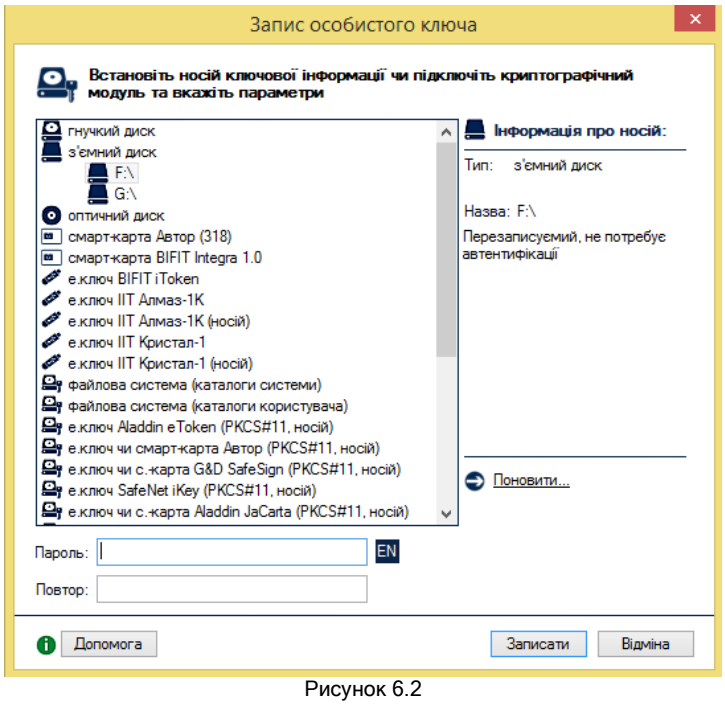


Рисунок 6.2

Після запису особистого ключа на НКІ, буде виведено вміст простого запиту на формування сертифікату з відкритим ключем ЕЦП для державних алгоритмів та протоколів (рис. 6.3), після перевірки вмісту простого запиту необхідно натиснути ”ОК”.

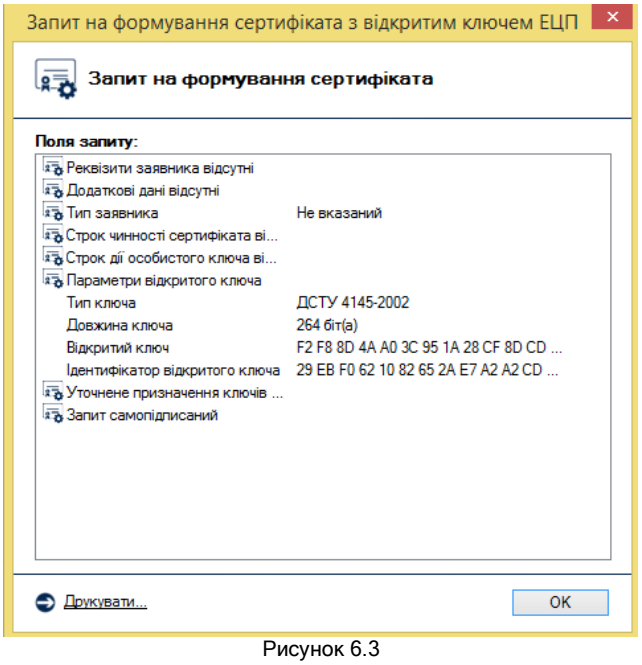


Рисунок 6.3

На наступній сторінці майстра (рис. 6.4) необхідно вказати спосіб передачі запиту до центру сертифікації ключів: за допомогою файлу, або відправити електронною поштою.

У першому випадку у наступному вікні (рис. 6.5) необхідно буде вказати ім’я файлу для запису простого запиту на формування сертифіката у файл. Запит повинен бути записаний на носій інформації чи на жорсткий диск. Після цього запит повинен бути переданий у пункт реєстрації ЦСК для формування сертифіката.

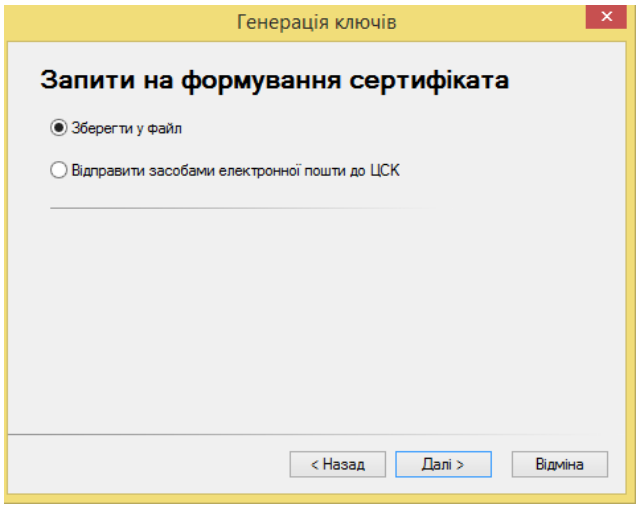


Рисунок 6.4

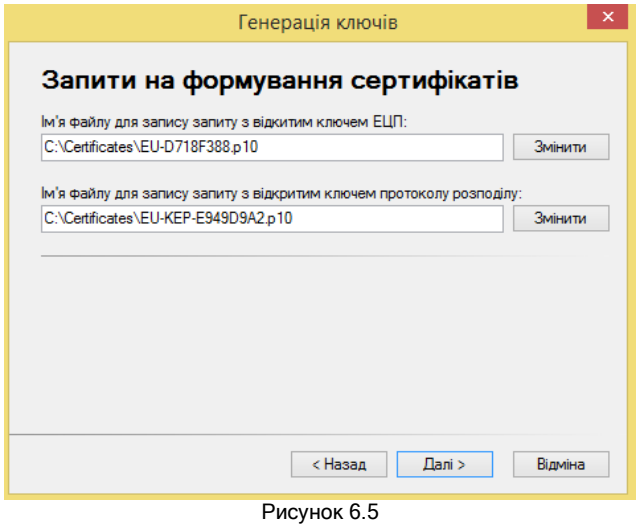


Рисунок 6.5

У випадку якщо запит передається за допомогою електронної пошти, у вікні (рис. 6.6) необхідно буде вказати параметри доступу до поштового сервера, та електронну поштову адресу центра сертифікації ключів.

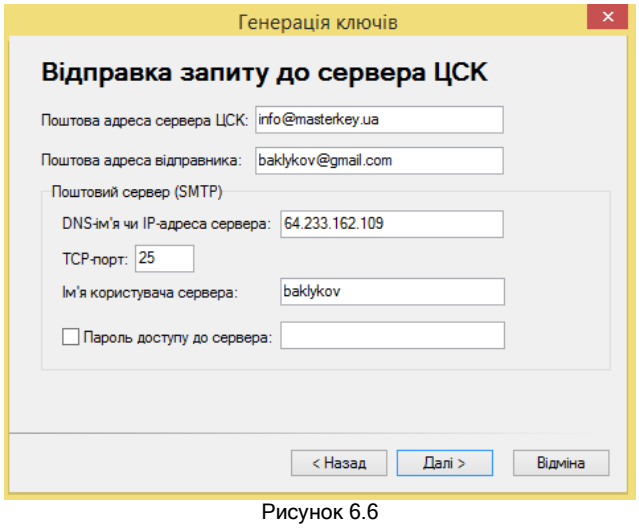


Рисунок 6.6

Після виконання всіх дій майстер завершує свою роботу (рис. 6.7).

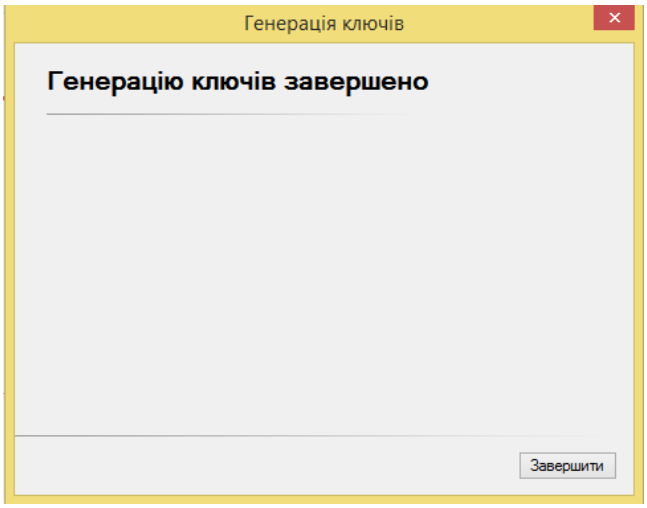


Рисунок 6.7

6.2 Зчитування особистого ключа

Для роботи з більшістю функцій програми (захисту файлів та ін.) необхідне попереднє зчитування особистого ключа користувача. Ініціювання зчитування особистого ключа може бути виконане автоматично при виборі певної функції програми чи виконане шляхом вибору підпункту “Зчитати ...” в пункті меню “Особистий ключ” або шляхом натискання комбінації клавіш Ctrl+K.

У вікні, що з’явиться (рис. 6.8) необхідно вказати:

- тип НКІ з особистим ключем;
- назву носія;
- пароль доступу до носія та захисту особистого ключа.

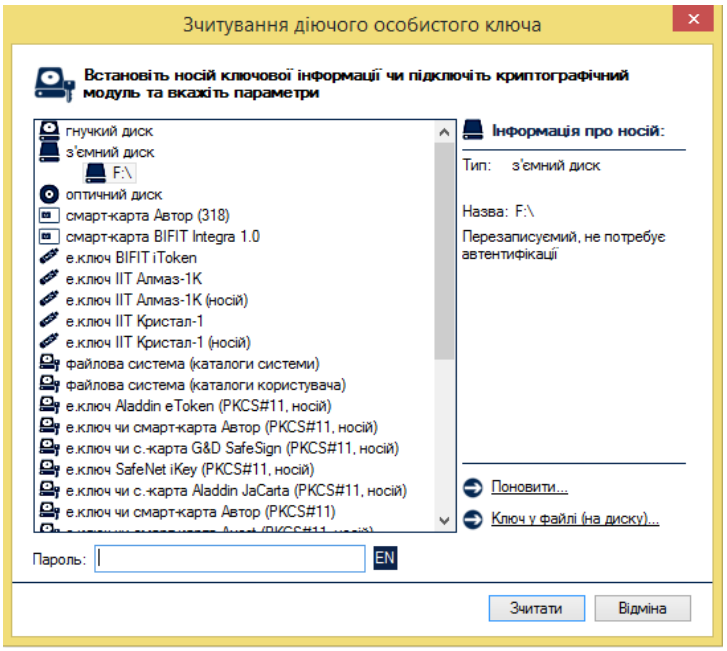


Рисунок 6.8

Після введення параметрів необхідно натиснути кнопку “Зчитати”.

Інформація про те, що особистий ключ зчитаний та знаходиться в пам’яті ПЕОМ відображається до панелі стану вікна, як наведено на рисунку 6.9.

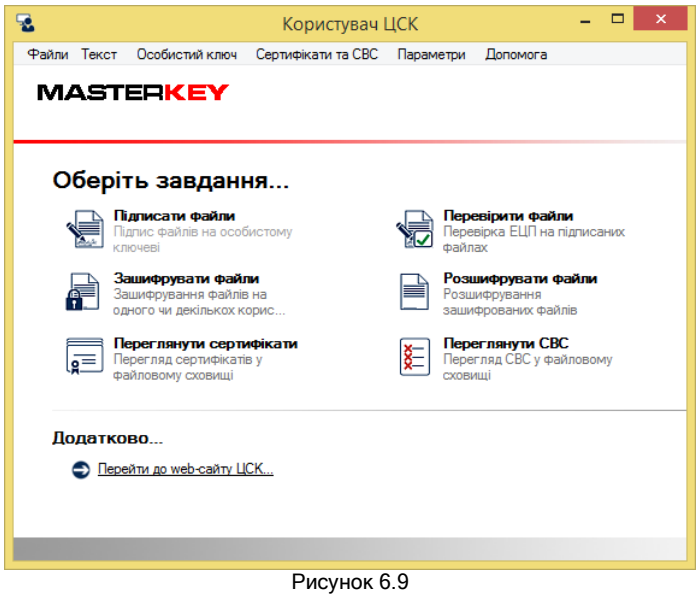


Рисунок 6.9

6.3 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”.

Під час резервного копіювання особистий ключ зчитується за допомогою вікна що наведене на рисунку 6.10. Під час резервного копіювання пароль захисту особистого ключа не вказується, та змінити його не можливо.

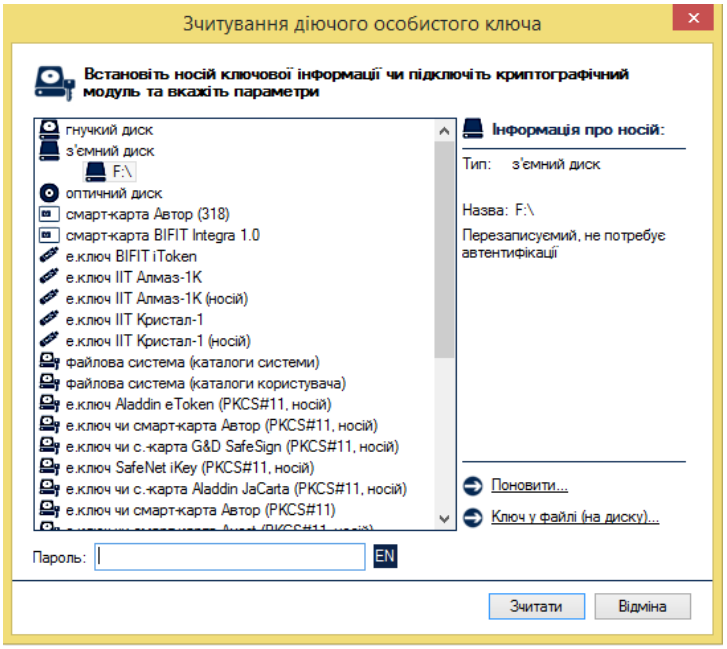


Рисунок 6.10

Після зчитування особистий ключ записується до резервного носія за допомогою вікна що наведене на рисунку 6.11.

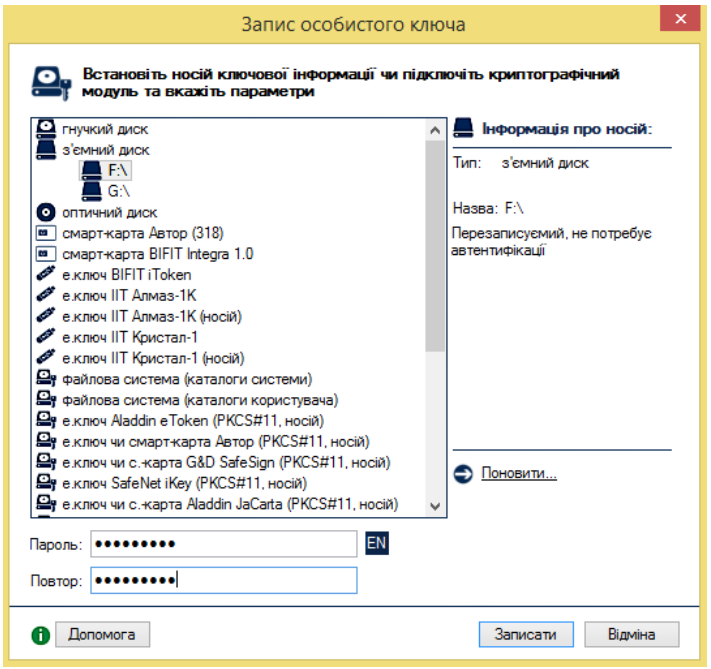


Рисунок 6.11

6.4 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. 6.12. У вікні необхідно вказати:

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

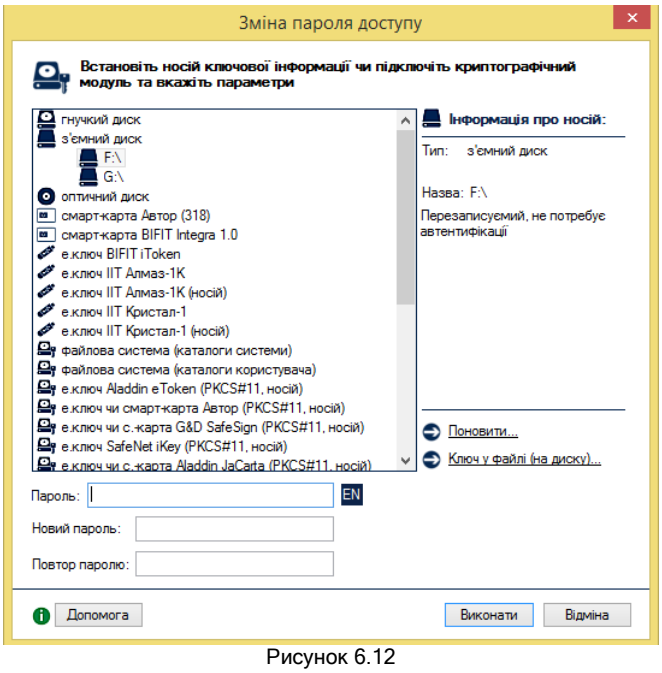


Рисунок 6.12

6.5 Знищення особистого ключа на носієві

Особистий ключ на НКІ повинен знищуватись спеціальними засобами, які вбудовані у програму, що забезпечують його гарантоване знищення.

Для знищення особистого ключа необхідно обрати підпункт “Знищити особистий ключ на носієві ключової інформації” в пункті меню “Особистий ключ”. Вікно знищення особистого ключа наведене на рис. 6.13. У вікні необхідно вказати тип та назву НКІ і натиснути кнопку “Виконати”.

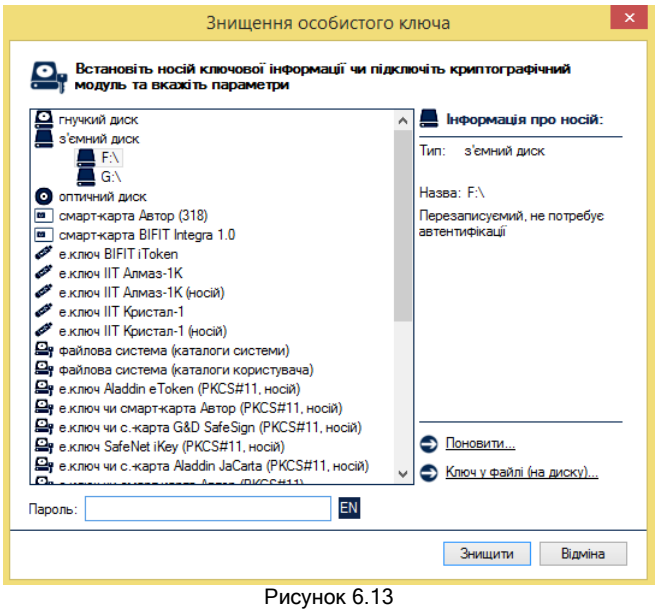


Рисунок 6.13

6.6 Знищення особистого ключа в пам’яті ПЕОМ

Якщо при зчитуванні особистого ключа не було встановлено параметр “Зчитувати повторно при кожній операції”, ключ залишається у пам’яті до завершення роботи програми (див. п. 6.2). Якщо необхідно знищити ключ з пам’яті не виходячи з програми необхідно обрати підпункт “Знищити особистий ключ у пам’яті” в пункті меню “Особистий ключ” або натиснути клавішу F12.

6.7 Перегляд власного сертифіката

Після зчитування особистого ключа користувач може переглянути власний сертифікат. Для перегляду власного сертифіката необхідно обрати підпункт “Переглянути власний сертифікат” в пункті меню “Особистий ключ”. Сертифікат буде відображено до вікон що наведені на рисунках 5.2, 5.3.

6.8 Помилки, що можуть виникати під час роботи програми

6.8.1 Помилка під час зчитування особистого ключа

Вікно з повідомленням про помилку наведене на рисунку 6.14.

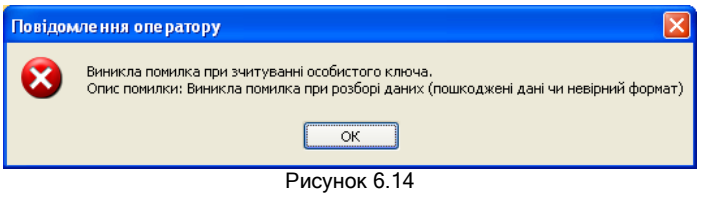


Рисунок 6.14

Така помилка може виникати:

- якщо не вірно вказаний пароль доступу до особистого ключа;
- пошкоджений носій ключової інформації;
- пошкоджені дані на носії ключової інформації.

Найчастіше така помилка трапляється у наслідок вказування невірного паролю захисту особистих ключів.

6.8.2 Помилка під час зчитування особистого ключа

Вікно з повідомленням про помилку наведене на рисунку 6.15.

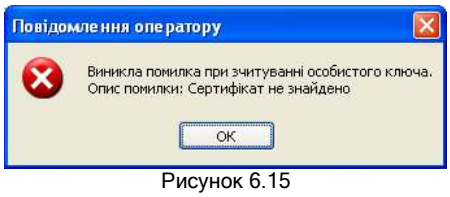


Рисунок 6.15

Така помилка може виникати:

- якщо не знайдено сертифікат ЦСК у файловому сховищі під час зчитування особистого ключа користувача;
- якщо не знайдено сертифікат відкритих ключів користувача у файловому сховищі.

6.8.3 Помилка під час блокування власного сертифіката

Вікно з повідомленням про помилку наведене на рисунку 6.17.

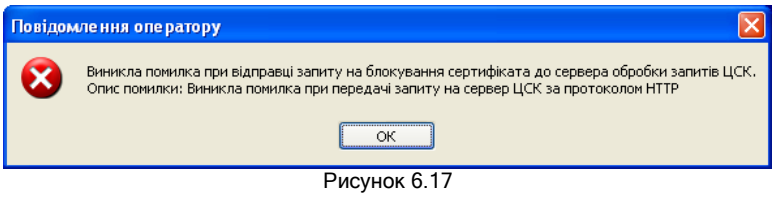


Рисунок 6.17

Така помилка може виникати:

- якщо не вказано параметри (адреса, порт) proxy-сервера, а підключення до сервера обробки запитів ЦСК здійснюється за допомогою нього;
- якщо не вірно вказано параметри аутентифікації proxy-сервера;
- якщо особистий ключ користувача не є дійсним;
- якщо відсутній доступ до сервера обробки запитів ЦСК.

7 ЗАХИСТ ФАЙЛІВ

7.1 Підпис файлів

Для підпису файлів (накладання ЕЦП) необхідно натиснути на панелі “Підписати файли” у головному вікні програми, або обрати підпункт “Підписати” у пункті меню “Файли”, або натиснути клавішу F5. Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 6.2.

Вікно підпису файлів наведене на рис. 7.1. Вікно містить наступні параметри:

- список файлів, які необхідно підписати;
- признак запису ЕЦП у зовнішній файл;
- признак запису підписаних файлів чи файлів з ЕЦП у окремий каталог;
- ім’я каталогу для запису підписаних даних чи файлів з ЕЦП.

Список файлів містить імена файлів що необхідно підписати. Файли додаються до списку за допомогою кнопки “Додати” та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку “Видалити”.

Признак запису ЕЦП у зовнішньому файлі встановлює необхідність запису ЕЦП у окремий файл з розширенням “.p7s” без включення вмісту файлу що підписується. За замовчанням підпис записується до вихідного файлу та до розширення файлу додається суфікс “.p7s”. Запис ЕЦП до зовнішнього файлу потрібен у випадку, коли файл підписується декількома користувачами, або при необхідності доступу до структури (вмісту) файлу без зняття з нього ЕЦП.

Признак запису підписаних файлів у окремий каталог встановлює необхідність запису підписаних файлів або файлів з ЕЦП до окремого каталогу що задається параметром “Каталог для запису підписаних даних чи файлів з ЕЦП ”. Якщо признак не встановлено підписані файли чи файли з ЕЦП будуть записуватися у каталог з вихідними файлами.

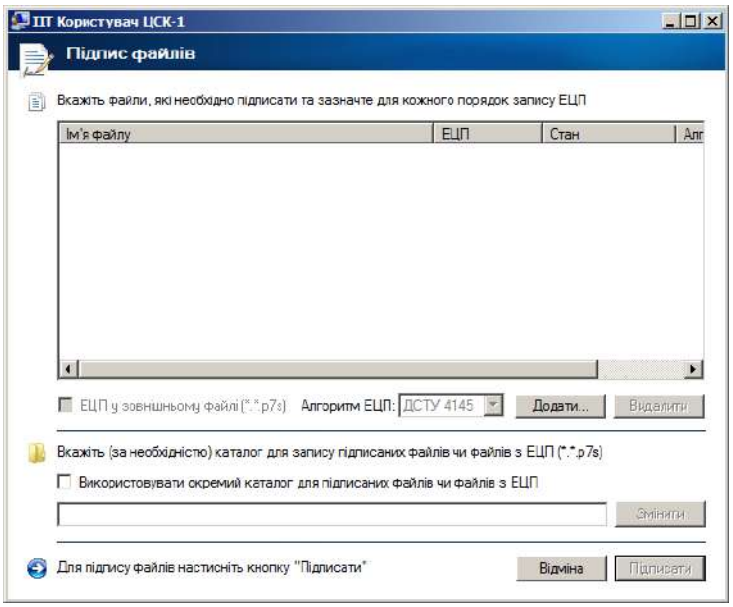


Рисунок 7.1

Після встановлення значень параметрів вікно може мати вигляд як наведено на рис. 7.2.

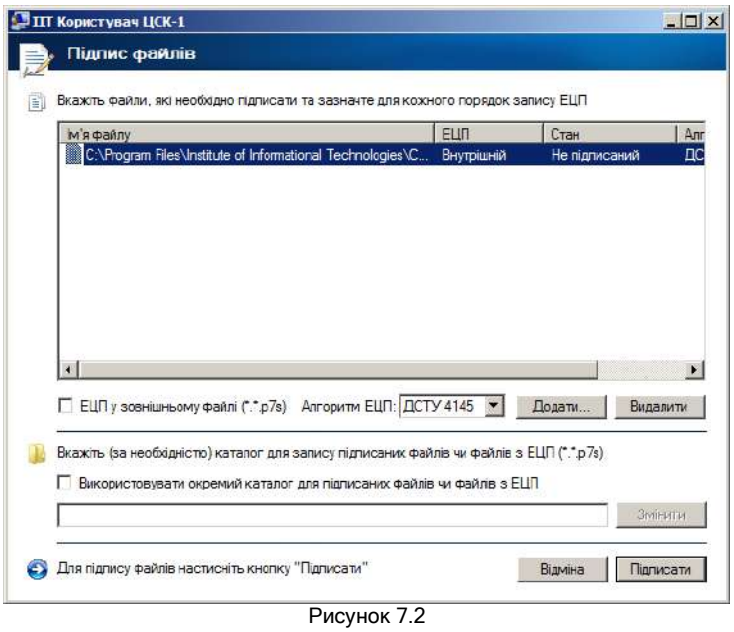


Рисунок 7.2

Для підпису файлів необхідно натиснути кнопку “Підписати”.

Після здійснення підпису файлів вікно буде містити інформацію про результати підпису (рис. 7.3).

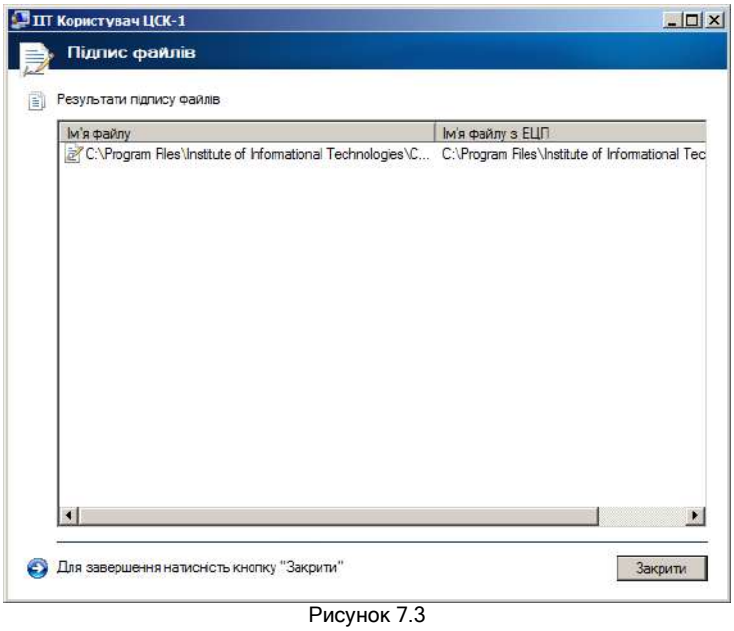


Рисунок 7.3

7.2 Перевірка файлів

Для перевірки підпису (ЕЦП) файлів необхідно натиснути на панелі “Перевірити файли” у головному вікні програми, або обрати підпункт “Перевірити підпис” у пункті меню “Файли”, або натиснути клавішу F6.

Вікно перевірки файлів наведене на рис. 7.4. Вікно містить наступні параметри:

- список файлів, які необхідно перевірити;
- признак запису файлів без ЕЦП у окремий каталог;
- ім’я каталогу для запису файлів без ЕЦП.

Список файлів містить імена файлів що необхідно перевірити. Файли додаються до списку за допомогою кнопки “Додати” та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку “Видалити”.

Признак запису файлів без ЕЦП у окремий каталог встановлює необхідність запису файлів після зняття ЕЦП у окремий каталог що задається параметром “Каталог для запису файлів без ЕЦП ”. Якщо признак не встановлено файли без ЕЦП будуть записуватися у каталог з підписаними файлами.

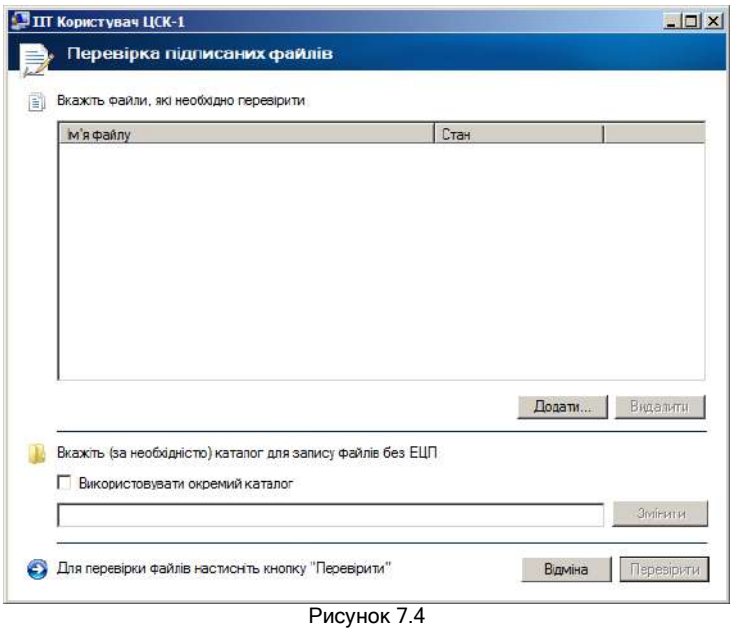


Рисунок 7.4

Після встановлення значень параметрів вікно може мати вигляд як наведено на рис. 7.5.

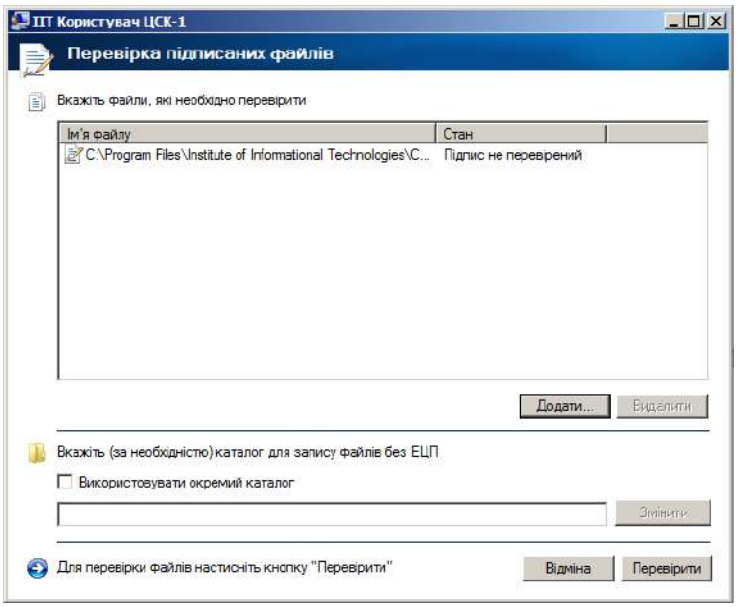


Рисунок 7.5

Для перевірки файлів необхідно натиснути кнопку “Перевірити”.

Після здійснення перевірки файлів вікно буде містити інформацію про результати підпису (рис. 7.6).

В разі вдалої перевірки можна також переглянути інформацію про підписаний файл (для цього необхідно натиснути на відповідний запис про файл). Вікно наведене на рис. 7.7.

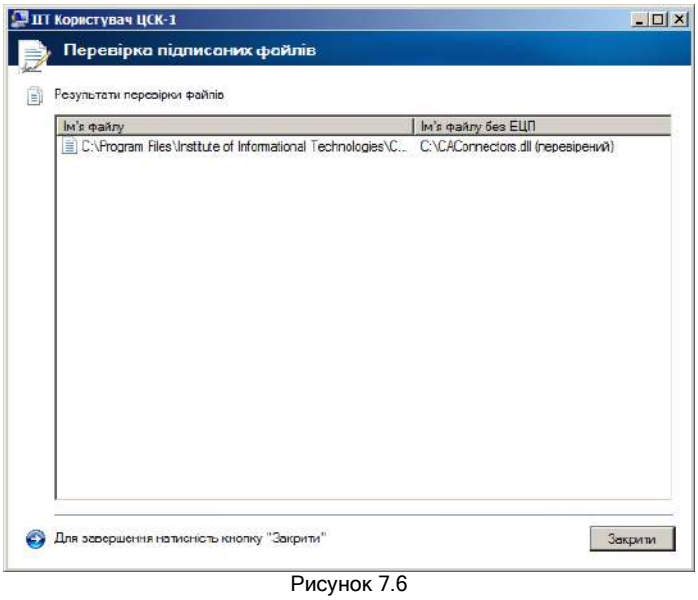


Рисунок 7.6

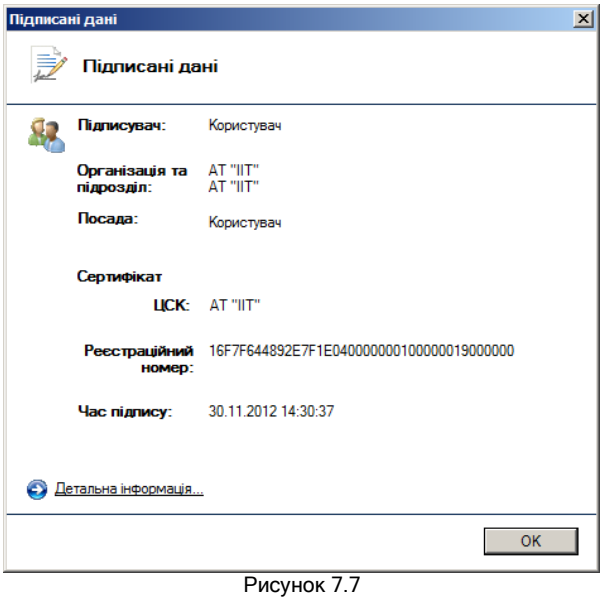


Рисунок 7.7

У детальній інформації наводиться сертифікат користувача що підписав файл.

Якщо ЕЦП містився в файлі з даними, при перевірці підпису буде створено копію файлу без підпису без розширення “.p7s”. За замовчанням (якщо не встановлено окремого каталогу для файлів без підпису) файл буде записаний до того ж каталогу у якому знаходився підписаний файл.

7.3 Зашифрування файлів

Для зашифрування файлу необхідно натиснути на панелі “Зашифрувати файли” у головному вікні програми, або обрати підпункт “Зашифрувати” у пункті меню “Файли”, або натиснути клавішу F7.

Вікно зашифрування файлів наведене на рис. 7.8. Вікно містить наступні параметри:

- список файлів, які необхідно зашифрувати;
- признак необхідності додаткового підпису файлу;
- признак запису зашифрованих файлів у окремий каталог;
- ім’я каталогу для запису зашифрованих файлів.

Список файлів містить імена файлів що необхідно зашифрувати. Файли додаються до списку за допомогою кнопки “Додати” та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку “Видалити”.

Признак додаткового підпису файлів (“Додатково підписати”) встановлює необхідність підпису файлу. За замовчанням здійснюється лише зашифрування кожного файлу.

Вихідні зашифровані файли мають розширення “.p7e”.

Признак запису зашифрованих файлів у окремий каталог встановлює необхідність запису зашифрованих файлів до окремого каталогу що задається параметром “Каталог для запису зашифрованих файлів”.

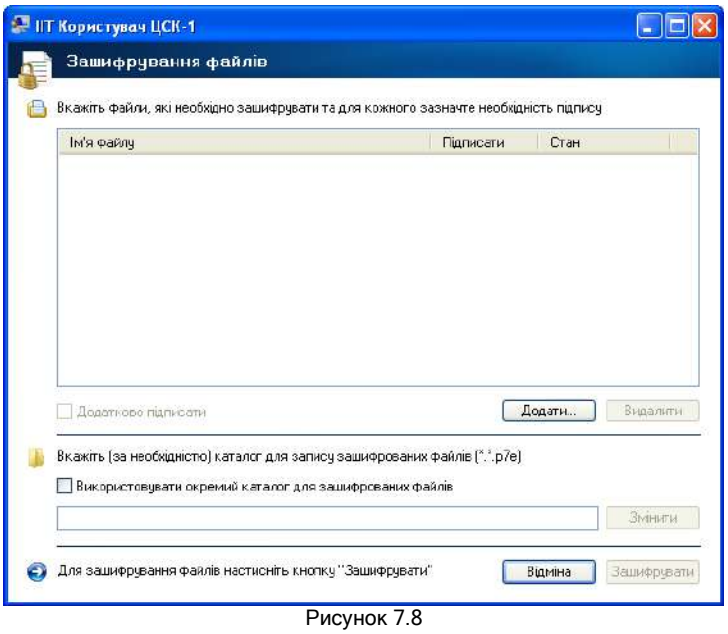


Рисунок 7.8

Після встановлення значень параметрів, вікно може мати вигляд як наведено на рис. 7.9. Для виконання зашифрування необхідно натиснути кнопку “Зашифрувати”.

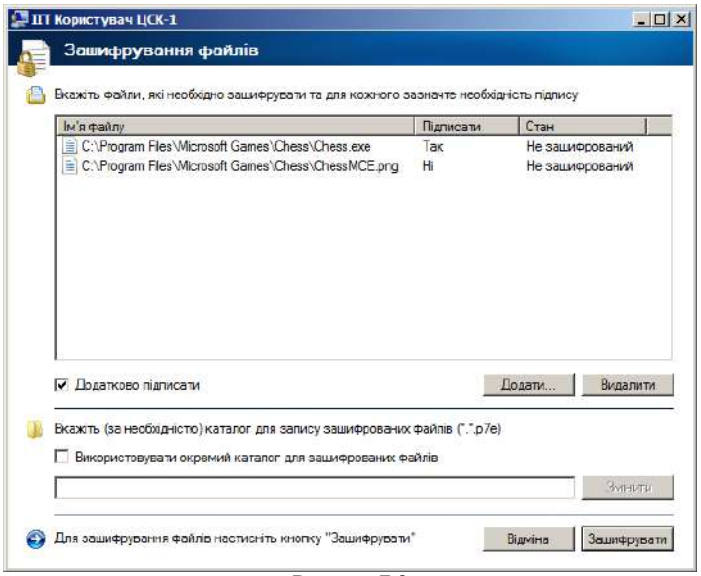


Рисунок 7.9

Для зашифрування файлів використовується особистий ключ користувача що виконує зашифрування та сертифікат(и) користувача(ів) для якого(их) зашифровується файл. Тому у вікні що наведене на рис. 7.10 необхідно обрати користувачів для яких виконується зашифрування файлу. Зашифрований файл може бути відкритим лише користувачем для якого виконувалось зашифрування.

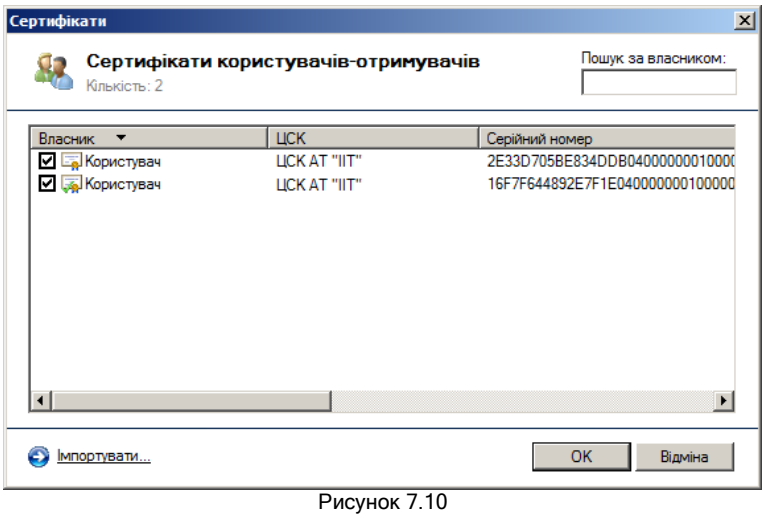


Рисунок 7.10

Під час шифрування здійснюється перевірка параметрів ключових даних користувачів що були обрані у списку (рис 7.10). Якщо параметри ключів користувачів для яких виконується шифрування будуть відрізнятись від параметрів ключів користувача що виконує шифрування, користувачу буде видане повідомлення про неможливість виконування шифрування у зв'язку з відмінністю параметрів та процес шифрування буде припинено. Для запобігання цього слід переглянути сертифікат користувача на адресу якого виконується шифрування та перевірити відповідність параметрів власних ключів параметрам ключів цього користувача.

Після здійснення зашифрування файлів буде виведене наступне вікно (рис. 7.11) з інформацією про результати зашифрування.

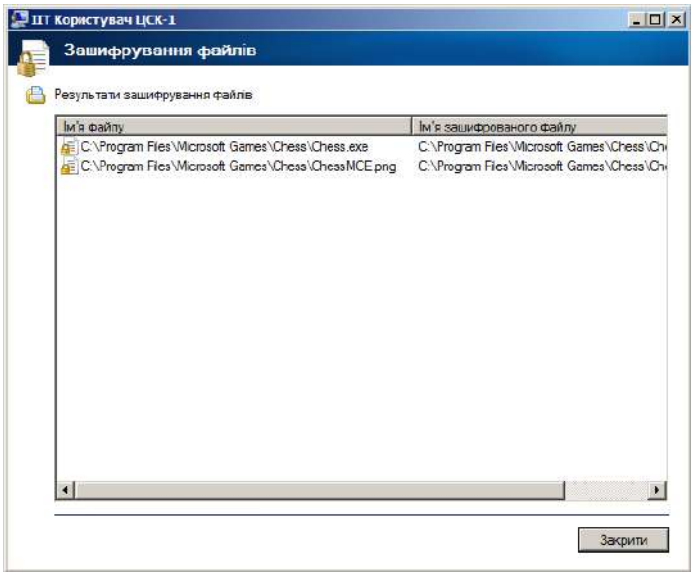


Рисунок 7.11

7.4 Розшифрування файлів

Для розшифрування файлів необхідно натиснути на панелі "Розшифрувати файли" у головному вікні програми, або пункт меню "Розшифрувати" у розділі меню "Файли", або натиснути клавішу F8. Вікно розшифрування файлів наведене на рис. 7.12. Форма містить наступні параметри:

- список зашифрованих файлів, які необхідно розшифрувати;
- признак запису розшифрованих файлів у окремий каталог;
- ім'я каталогу для запису розшифрованих файлів.

Список файлів містить імена файлів що необхідно розшифрувати. Файли додаються до списку за допомогою кнопки "Додати" та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку "Видалити".

Признак запису розшифрованих файлів у окремий каталог встановлює необхідність запису розшифрованих файлів у окремий каталог що задається параметром “Каталог для запису розшифрованих файлів”.

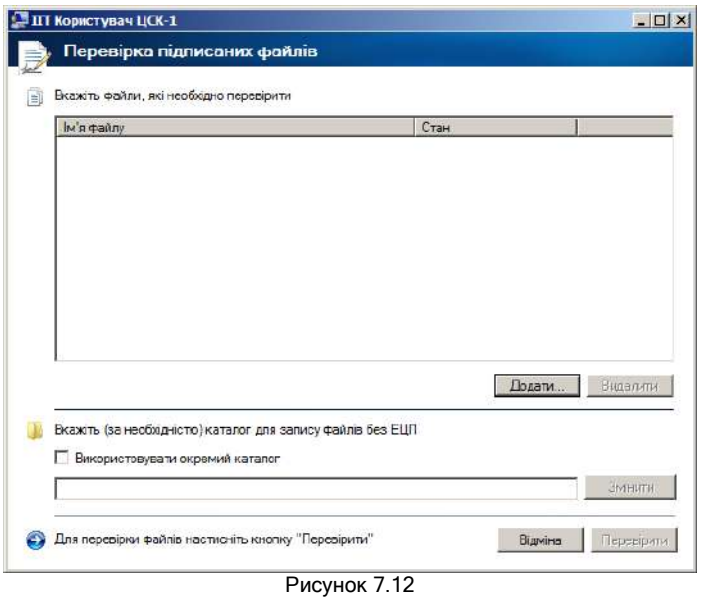


Рисунок 7.12

Після встановлення значень параметрів, вікно розшифрування файлів може мати вигляд як наведено на рис. 7.13.

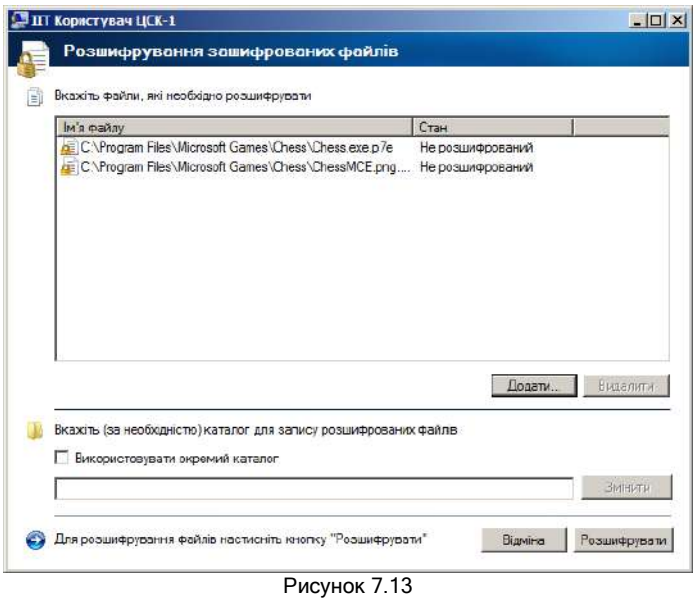


Рисунок 7.13

Для розшифрування файлів необхідно натиснути кнопку “Розшифрувати”. Після розшифрування буде виведено інформацію про результати розшифрування (рис. 7.14).

В разі вдалого розшифрування є можливість переглянути інформацію про розшифровані файли (рис. 7.15), для чого необхідно натиснути на запис про відповідний файл.

За замовчанням (якщо не встановлено окремого каталогу для розшифрованих файлів) розшифровані файли будуть записані до того ж каталогу у якому знаходилися зашифровані.

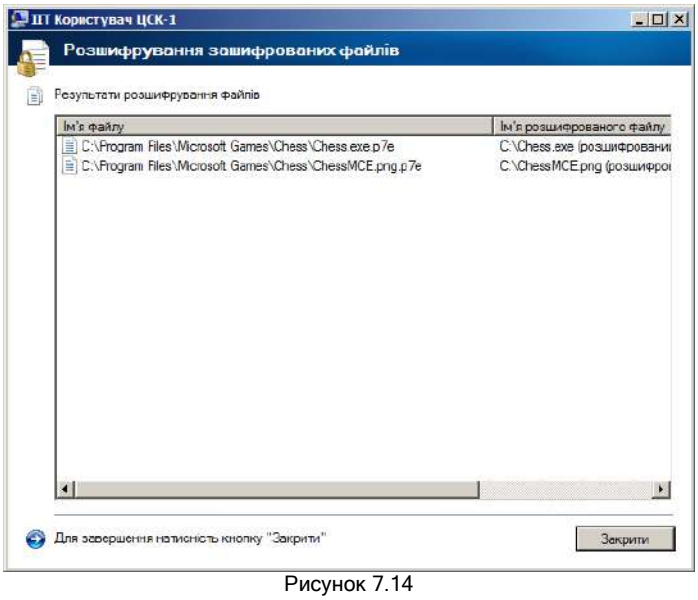


Рисунок 7.14

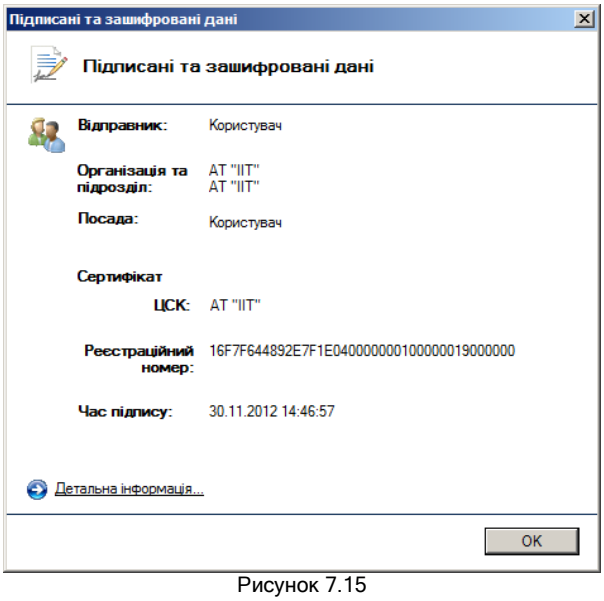


Рисунок 7.15

7.5 Помилки, що можуть виникати під час роботи програми

7.5.1 Помилка під час підпису, перевірці або шифруванні даних

Вікно з повідомленням про помилку наведене на рисунку 7.16.

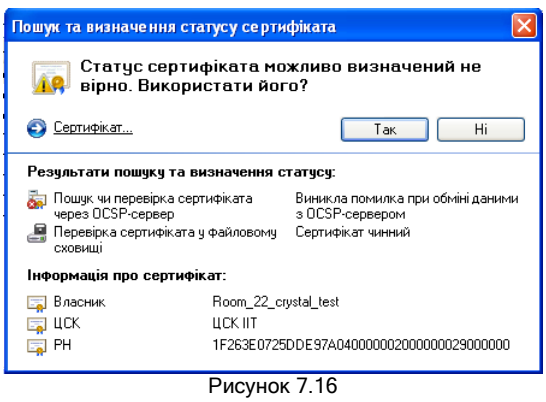


Рисунок 7.16

Опис: помилка може виникати як при обміні даними з OCSP сервером, так й при обміні даними з TSP або LDAP серверами.

Така помилка може виникати:

- якщо не вказано параметри (адреса, порт) proxy-сервера, а підключення до сервера обробки запитів ЦСК здійснюється за допомогою нього;
- якщо не вірно вказано параметри аутентифікації proxy-сервера;
- якщо особистий ключ користувача не є дійсним;
- якщо відсутній доступ до (TSP, OCSP або LDAP) сервера ЦСК.

7.5.2 Помилка під час шифрування у зв'язку з відмінністю параметрів ключів користувачів

Якщо параметри ключів користувачів для яких виконується шифрування будуть відрізнятись від параметрів ключів користувача що виконує шифрування, користувачу буде видане повідомлення про неможливість виконування шифрування у зв'язку з відмінністю параметрів та процес шифрування буде припинено. Для запобігання цього слід переглянути сертифікат користувача на адресу якого виконується шифрування та перевірити відповідність параметрів власних ключів параметрам ключів цього користувача.

8 ПОВІДОМЛЕННЯ ОПЕРАТОРУ ТА ДОВІДКОВА СИСТЕМА

8.1 Перехід до web-сайту центра сертифікації ключів

Для переходу до web-сайту центра сертифікації ключів необхідно натиснути посилання “Перейти до web-сайту ЦСК...” у головному вікні програми.

8.2 Перегляд настанови оператору

Для виведення настанови оператора необхідно обрати підпункт “Настанова оператору” в пункті меню “Допомога”, або натиснути клавішу F1, або натиснути посилання “Відкрити настанову оператору...” у головному вікні програми.

ПЕРЕЛІК СКОРОЧЕНЬ

ОС	Операційна система
ЕЦП	Електронний цифровий підпис
КЗІ	Криптографічний захист інформації
ДКЕ	Довгостроковий ключовий елемент
СВС	Список відкликаних сертифікатів
ЦСК	Центр сертифікації ключів
НКІ	Носій ключової інформації (особистого ключа)
ПЕОМ	Персональна електронно-обчислювальна машина
OCSP	Online Certificate Status Protocol (протокол визначення статусу сертифіката)
LDAP	Lightweight Directory Access Protocol (протокол доступу до каталогу)
TSP	Time-Stamp Protocol (протокол отримання позначок часу)
HTTP	Hyper Text Transfer Protocol