ПРАВЕКС БАНК

Інструкція

користувачеві програмного комплексу

Користувач ЦСК (версія 1.3.1)

АНОТАЦІЯ

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

Оглавление

ПЕРЕЛІК СКОРОЧЕНЬ

ОС	Операційна система
ЕОТ	Електронно-обчислювальна техніка
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

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;
  - визначення статусу сертифікатів за допомогою СВС;
  - перевірку чинності та цілісності сертифікатів та ін.;
- захист файлів користувача:
  - підпис файлів;
  - перевірку файлів;
  - шифрування файлів;
  - розшифрування файлів.
  -

2 УМОВИ ВИКОНАННЯ ПРОГРАМИ

Програма може бути завантажена та виконана на ПЕОМ під керуванням ОС Microsoft Windows версій 7, 8 або 10.

3 ІНСТАЛЯЦІЯ ПРОГРАМИ

Для інсталяції програми необхідно скачати і потім запустити програму інсталяції (майстер інсталяції) EUPravexBankInstall.exe з одного із сайтів Банку:

https://www.pravex.com.ua/korporativnym-klientam-bankam/vsi-poslugi/groshovi-perekazi

https://ca.pravex.com.ua/user-downloads або з іншого інсталяційного носія.

Після запуску програми інсталяції на першій сторінці (рис. 3.2) виводиться інформація про початок інсталяції. Для продовження інсталяції необхідно натиснути кнопку “Далі”, а для завершення – “Скасувати”.

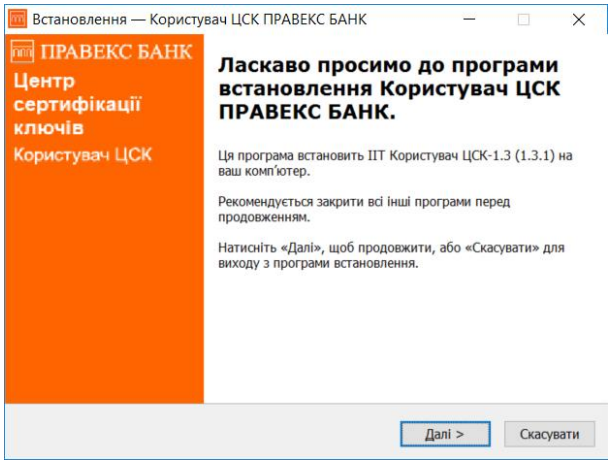


Рисунок 3.2

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”.

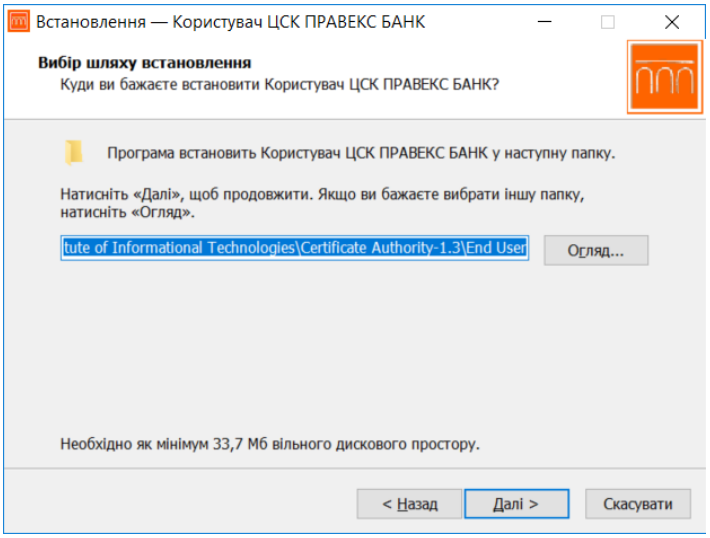


Рисунок 3.3

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”.

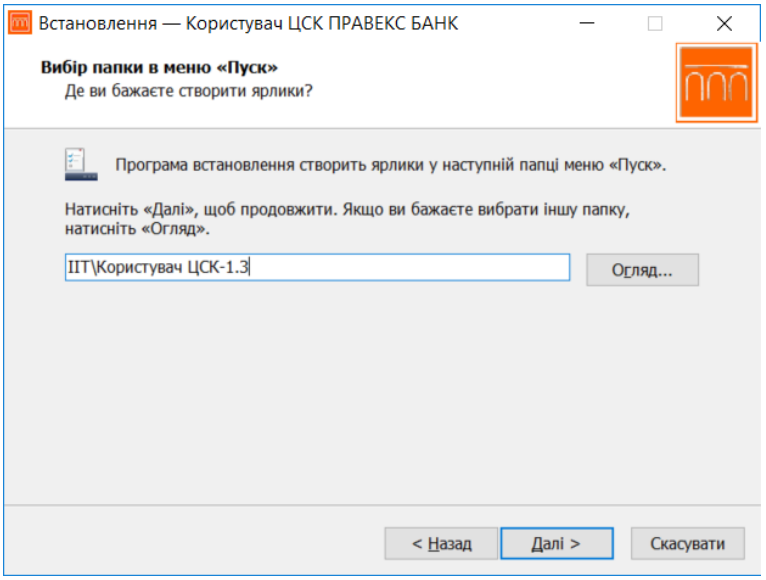


Рисунок 3.4

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”. Рекомендується залишити цей параметр без змін.

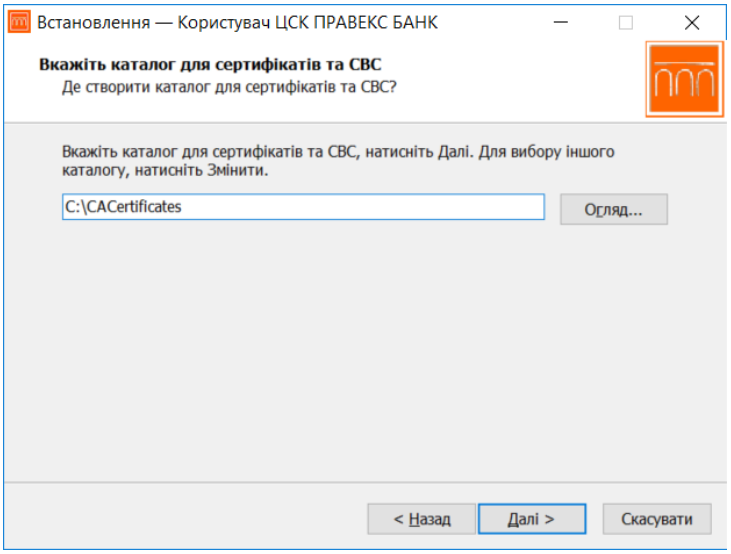


Рисунок 3.5

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”.

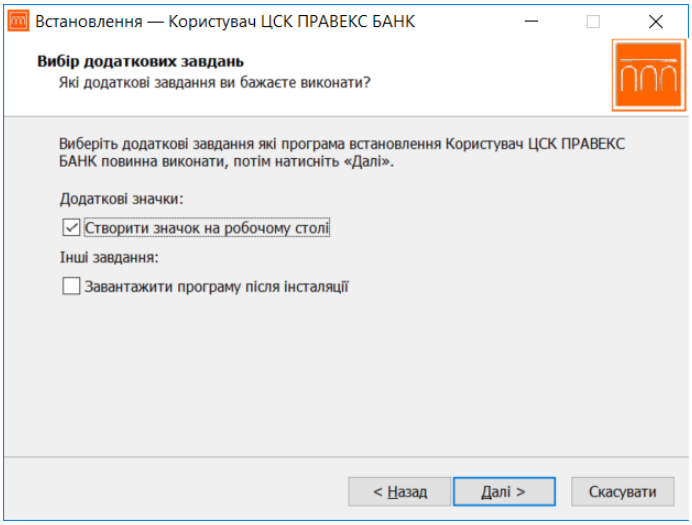


Рисунок 3.6

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

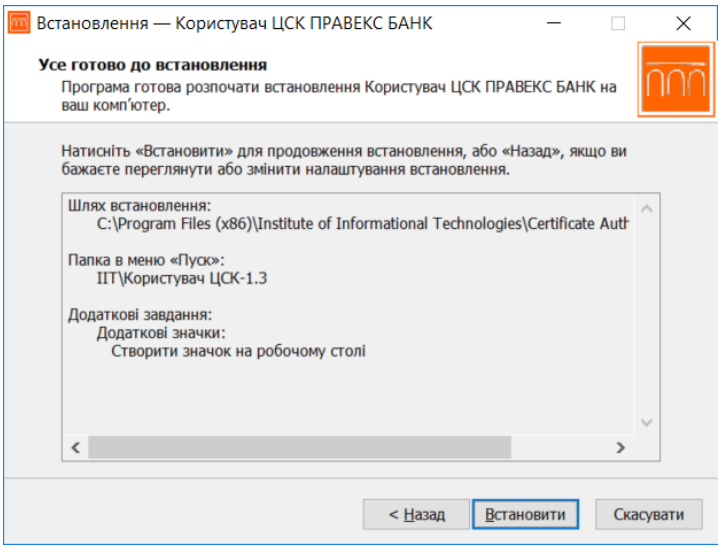


Рисунок 3.7

Після інсталяції програми, майстер завершує свою роботу.

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;
- діючі СВС.

Інформативно: сертифікати ЦСК, серверів ЦСК та СВС необхідно записати у відповідний каталог, отримавши їх від співробітників Банку разом з інсталяційним пакетом або завантажити з офіційного сайту ЦСК ca.pravex.com.ua.

Для завантаження програми необхідно запустити модуль EU.exe через файловий менеджер ОС або через меню “Пуск”, обравши у розділі “IIT\Користувач ЦСК-1” підпункт “Користувач ЦСК ПРАВЕКС БАНК” чи за допомогою значку на робочому столі. Після запуску на екрані буде відображене головне вікно програми, що наведене на рис. 4.1.

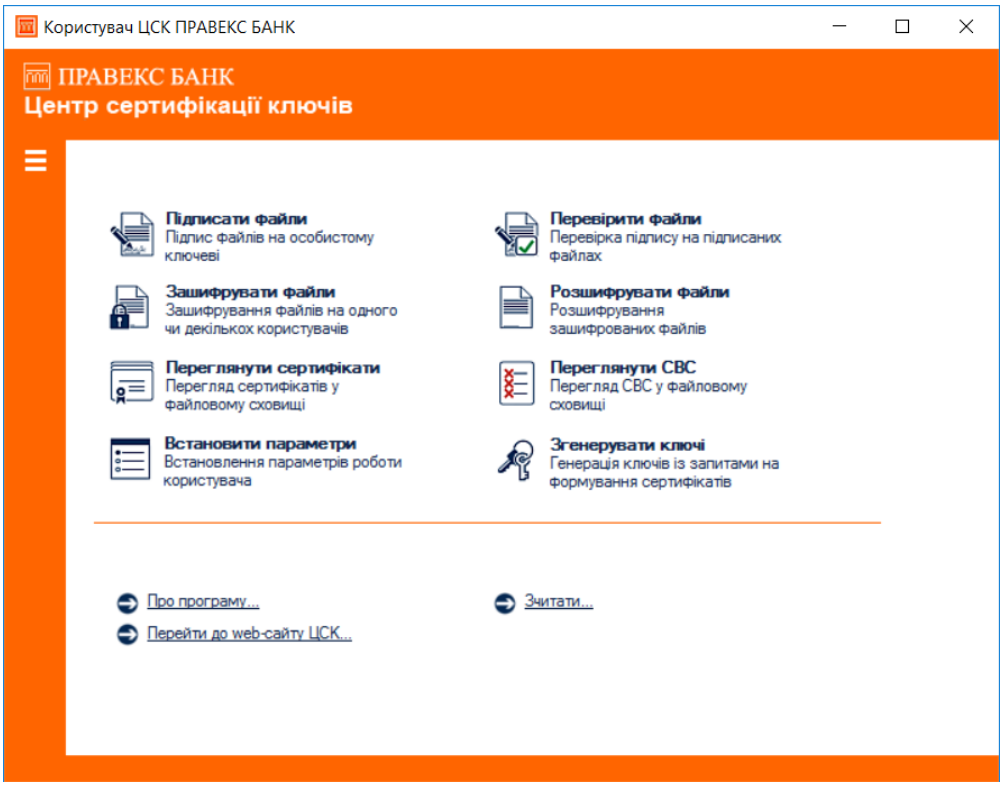


Рисунок 4.1

4.2 Встановлення параметрів роботи програми

Програма інсталяції під час свого виконання встановлює параметри роботи програми зазамовчанням. Параметри встановлені для онлайн режиму, тобто потребується доступ до сайту ca.pravex.com.ua.

Інформативно: для роботи в офф-лайн режимі (без взаємодії з ЦСК) необхідно в меню обрати пункт «Параметри», після чого натиснути «Перейти в режим off-line (не взаємодіяти з ЦСК)» або натиснути комбінаціію клавіш Ctrl+O. Для роботи в off-line режимі у файловому сховищі повинні бути сертифікати ЦСК, користувача та списки відкликаних сертифікатів (СВС, або CRL). Усе це можна завантажити з веб-сайту ЦСК.

Для встановлення чи зміни параметрів роботи програми необхідно обрати підпункт “Встановити” впункті меню “Параметри” (рис. 4.1). Вікно встановлення параметрів наведене на рис. 4.2.

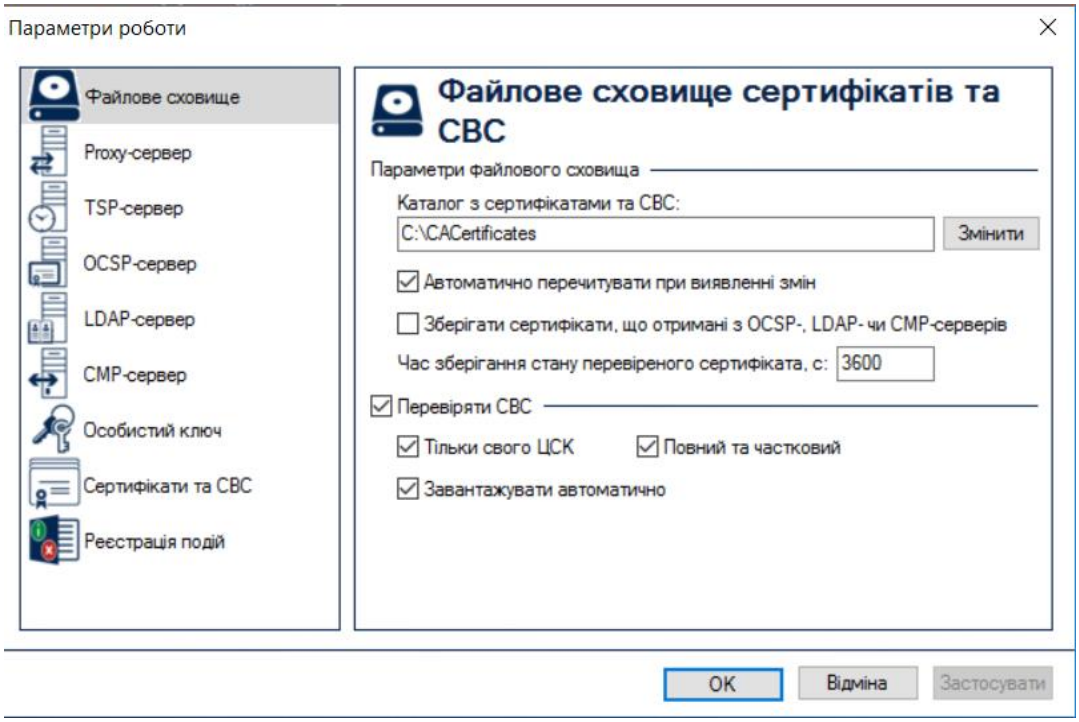


Рисунок 4.2

4.2.1 ФАЙЛОВЕ СХОВИЩЕ

Для настроювання параметрів файлового сховища сертифікатів та CBC необхідно перейти дозакладки “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 CBC”. Даний параметр встановлює каталог файлового сховища для зберігання сертифікатів та CBC. Всі сертифікати та CBC, що завантажуються не засобами програми повинні записуватися у даний каталог.

Інформативно: необхідно перевіряти правильність вказаного каталогу. Він повинен збігатися з тим, що був вказаний при інсталяції.

– “Автоматично перечитувати файлове сховище при виявлені змін”. Даний параметр визначає необхідність автоматичного перечитування каталогу файлового сховища програмою привнесенні будь-яких змін до цього каталогу (запису нового сертифіката чи CBC у каталог чи видалення файлу з сертифікатом або CBC). Якщо параметр не встановлено необхідно виконувати повторне зчитування файлового сховища після внесення змін. Для цього необхідно обрати підпункт “Зчитати сертифікати та CBC” в пункті меню “Сертифікати та CBC” або натиснути клавішу “F9” у головному вікні програми.
– “Використовувати CBC”. Параметр вказує на необхідність використання CBC в якості засобу перевірки статусу сертифікатів відкритих ключів що використовуються.
– “Тільки свого ЦСК”. Даний параметр визначає необхідність використовувати при перевірці сертифікатів CBC лише свого ЦСК у ланцюжку. Для цього повинен бути зчитаний особистий ключ користувача, оскільки ЦСК користувача визначається за допомогою параметрів особистого ключа.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

4.2.2 PROXY-СЕРВЕР

У випадку, якщо комп’ютер користувача підключений до мережі інтернет через proxy-сервер, то для настроювання параметрів необхідно перейти до закладки “Proxy-сервер” у вікні що наведене на рисунку 4.3. Поставити «галочку» навпроти пункту «Підключатися через proxy-сервер» та у відповідних полях прописати параметри цього сервера.

У випадку, якщо комп’ютер має пряме підключення до мережі інтернет, настроювати даний пунк не треба.

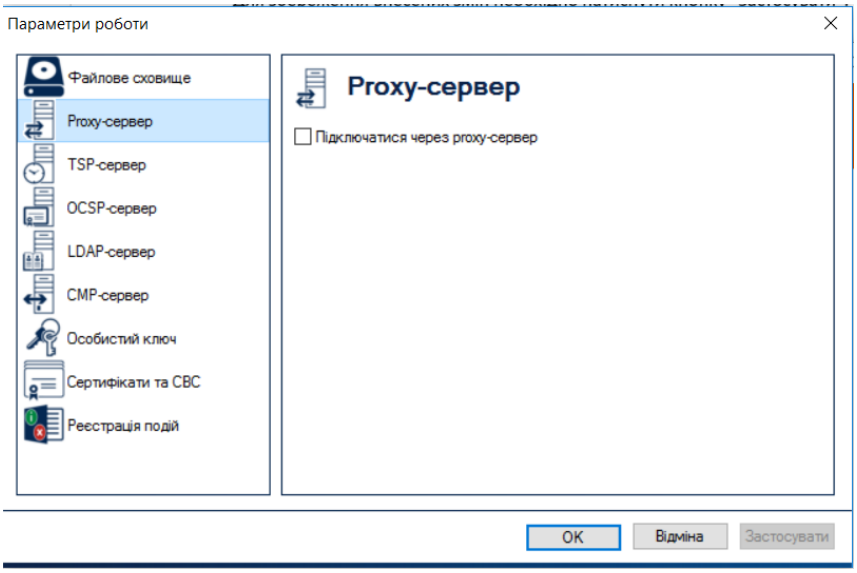


Рисунок 4.3

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 4.4.

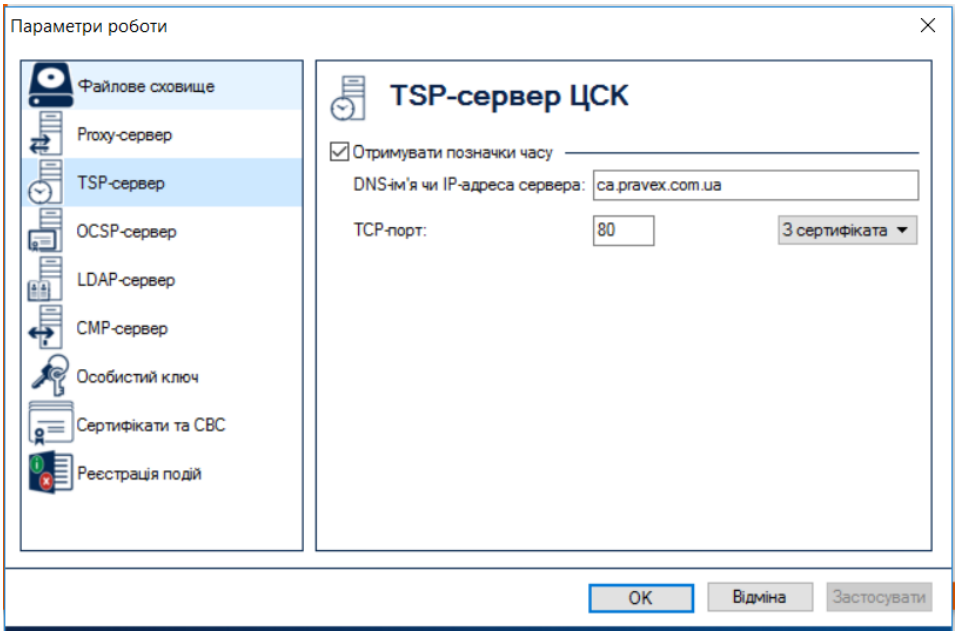


Рисунок 4.4

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 вікніщо наведене на рисунку 4.5.

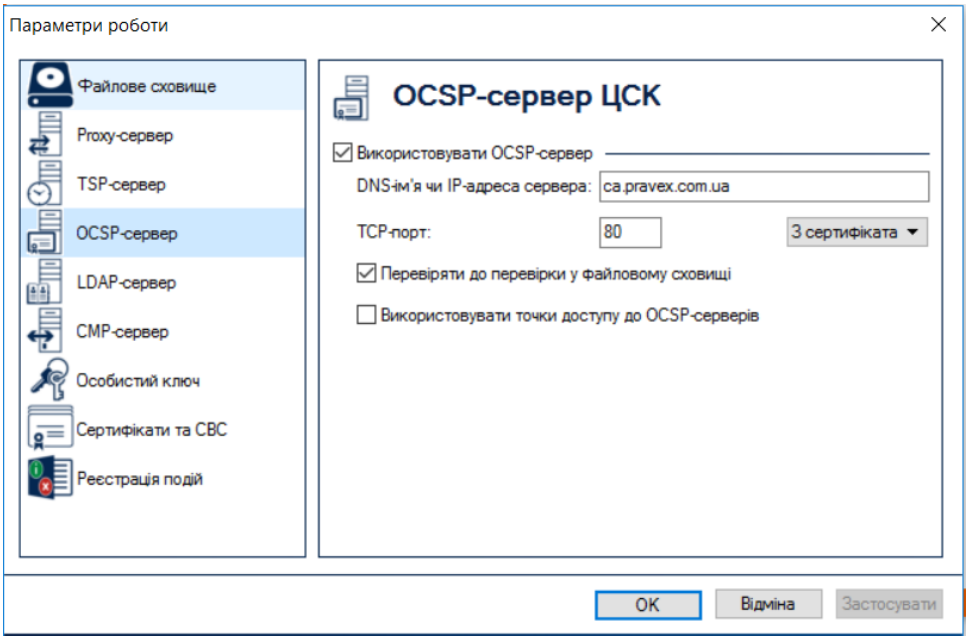


Рисунок 4.5

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 щонаведене на рисунку 4.6.

Зазвичай LDAP-сервер не використовується.

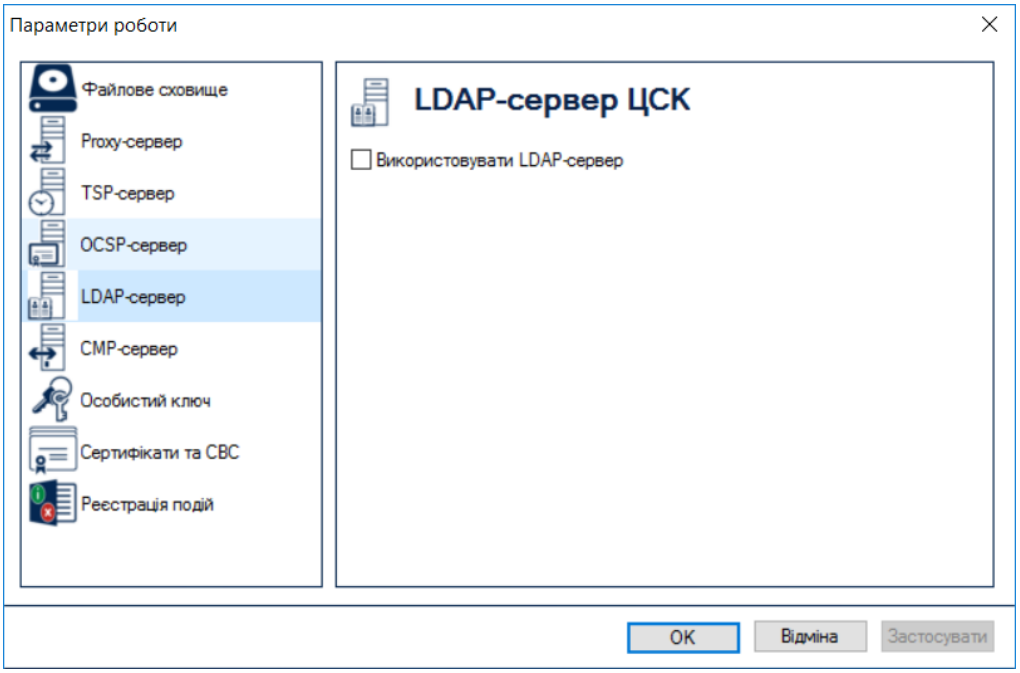


Рисунок 4.6

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

4.3 Режими роботи програми

Для встановлення режиму off-line роботи з ЦСК необхідно обрати підпункт меню “Перейти врежим 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 правої частини головного вікна програми (рис.4.7).

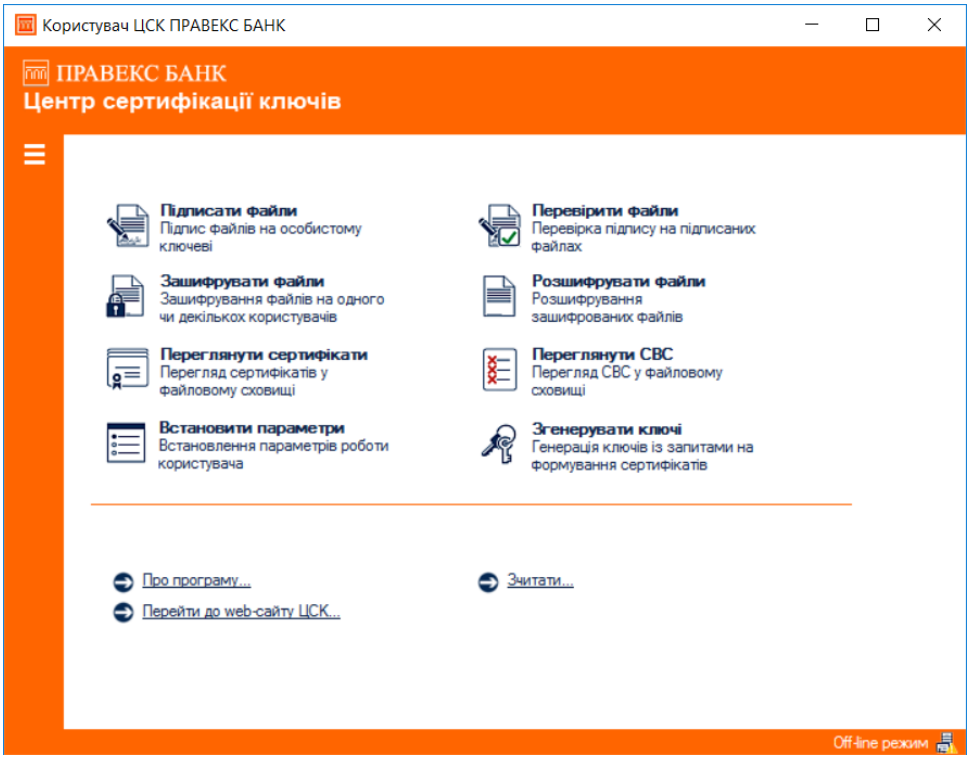


Рисунок 4.7

5 УПРАВЛІННЯ СЕРТИФІКАТАМИ ТА СВС

5.1 Отримання сертифікатів з ЦСК

Набір сертифікатів отримується разом з програмним забезпеченням Банком після укладання всіх необхідних договорів.

До пакету сертифікатів входять сертифікат ЦСК та сертифікат користувача.

Для встановлення сертифікатів необхідно скопіювати їх з носія в папку, що зазначається при інсталяції (рисунок 3.5.).

У режимі on-line можна отримати набір сертифікатів за власним ключем:

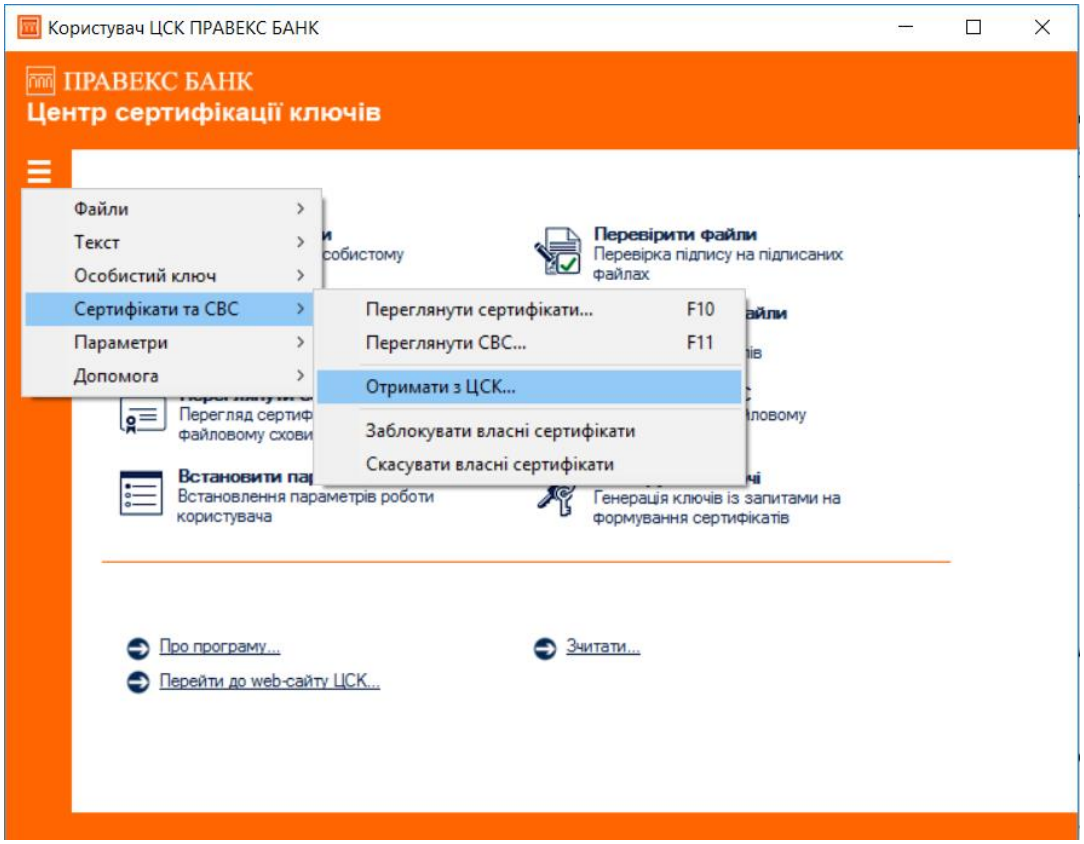


Рисунок 5.1

Потрібно зчитати власний ключ, після чого усі необхідні сертифікати будуть завантажені з веб-сайту ЦСК.

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 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 відображенийу 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.

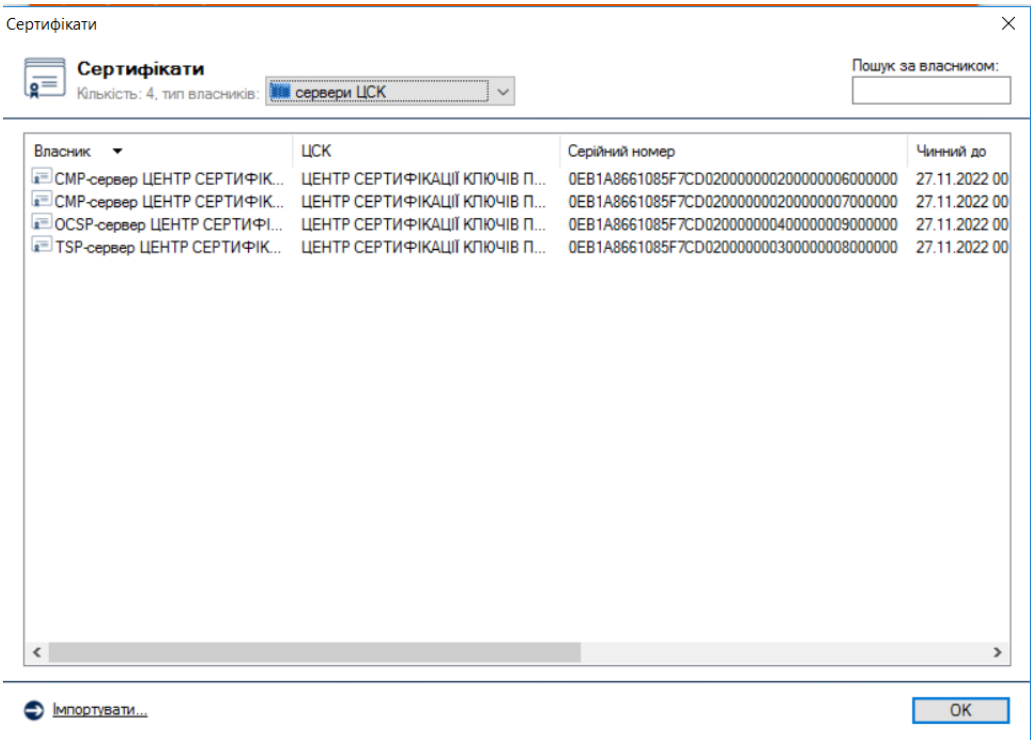


Рисунок 5.4

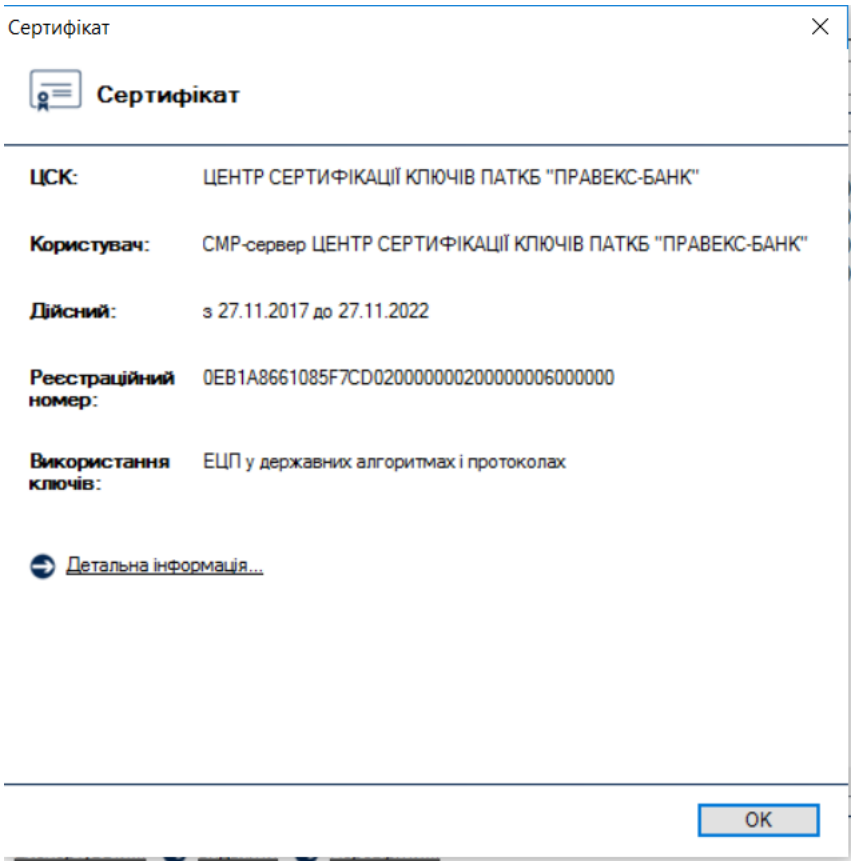


Рисунок 5.5

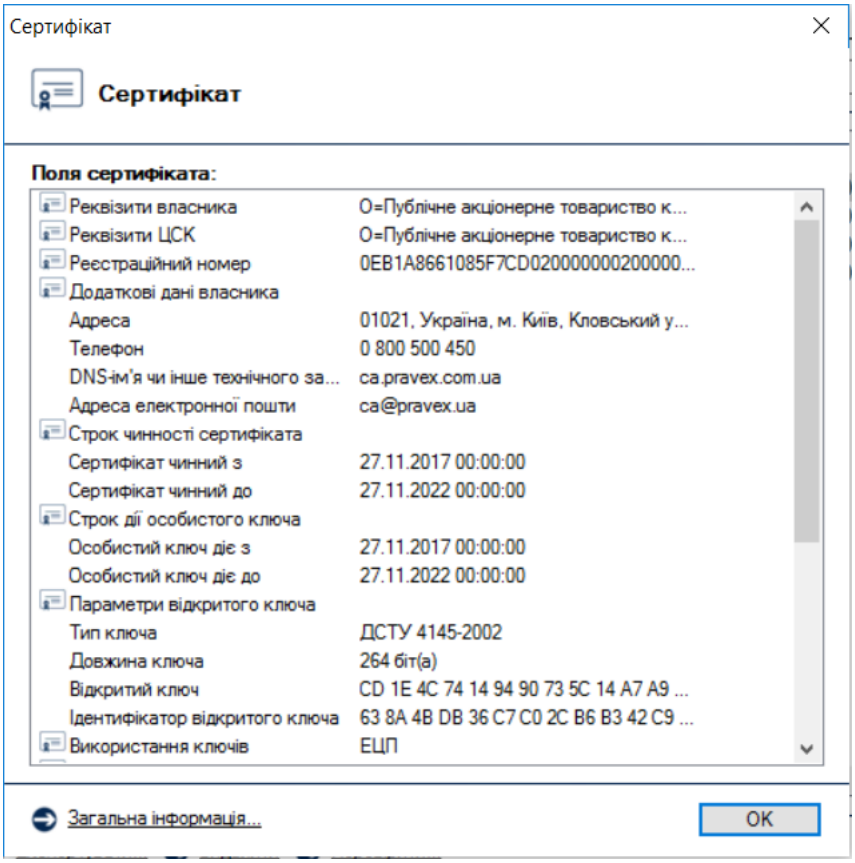


Рисунок 5.6

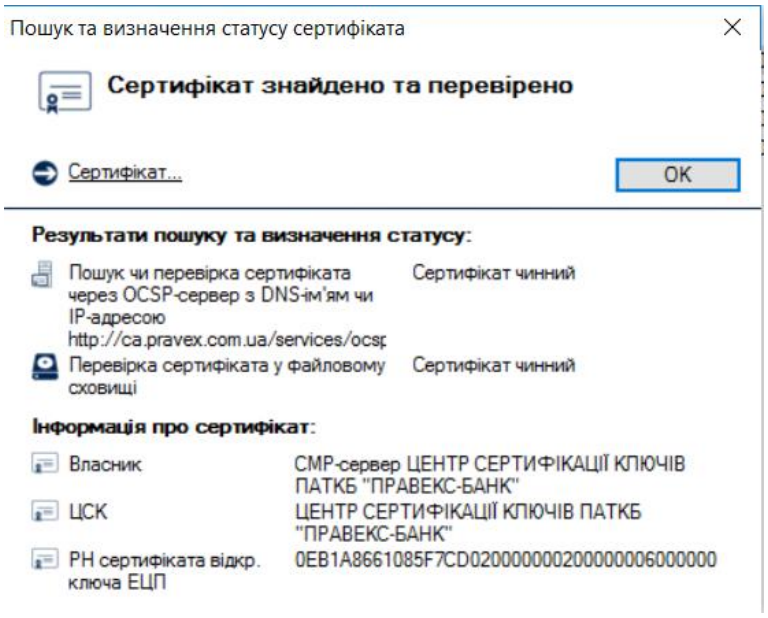


Рисунок 5.7

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.

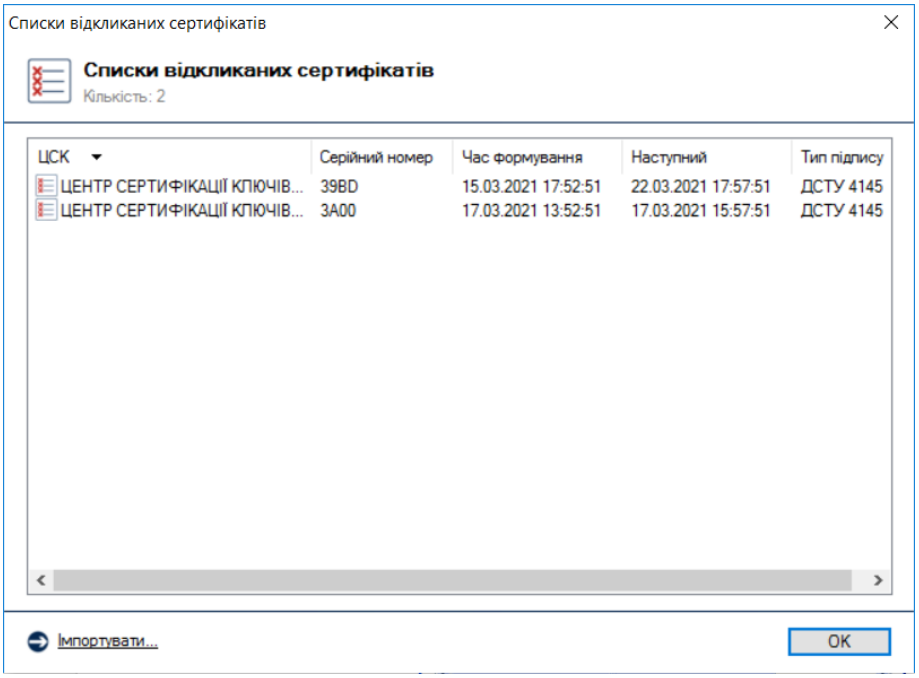


Рисунок 5.8

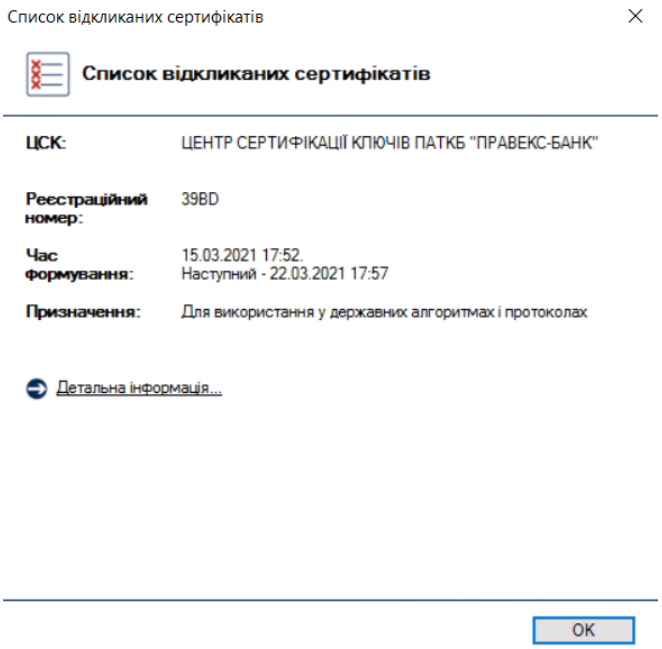


Рисунок 5.9

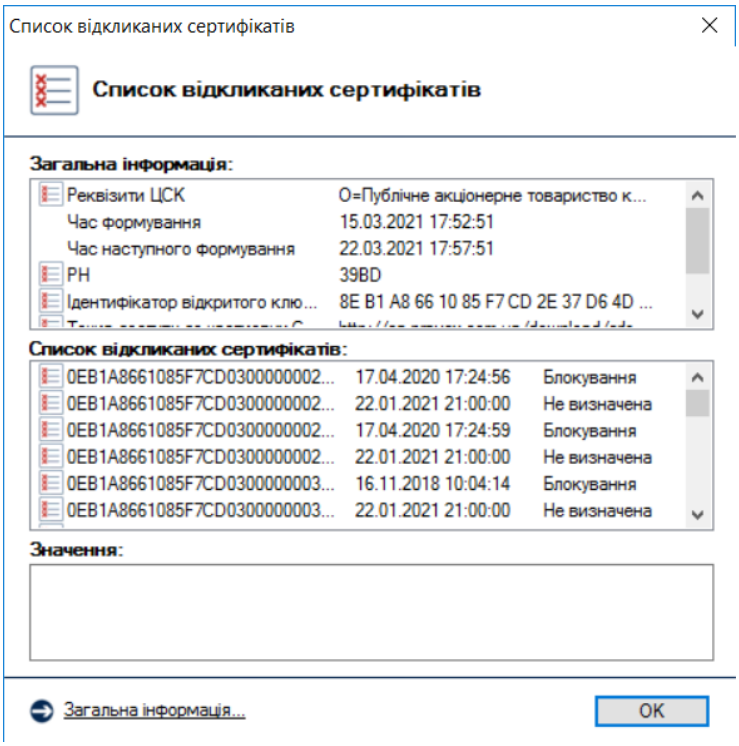


Рисунок 5.10

5.5 Завантаження СВС

Автоматичне завантаження списку відкликаних сертифікатів з web-сервера ЦСК в оффлайн-режимі необхідно відключати, знявши відповідну позначку (“Завантажувати автоматично”) у вікні параметрів, що наведене на рис. 4.2.

В онлайн-режимі СВС завантажуються автоматично.

6. УПРАВЛІННЯ КЛЮЧАМИ

6.1 Генерація ключів

1. На робочому столі необхідно знайти значок «Користувач ЦСК ПРАВЕКС БАНК» (Рис. 6.1):

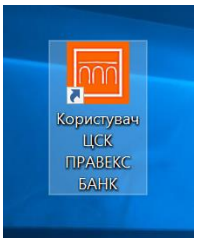


Рис. 6.1

2. Після запуску програми необхідно обрати підпункт “Згенерувати ключі” (Рис. 6.2).

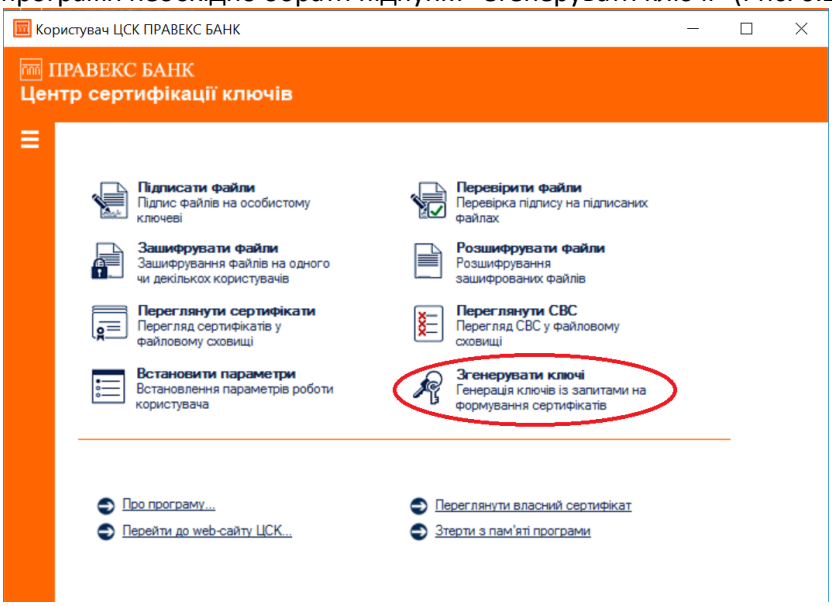


Рис. 6.2

3. На сторінці майстра (Рис. 6.3), що відкрилась, необхідно вибрати пункт «для державних алгоритмів і протоколів» і натиснути “Далі”.

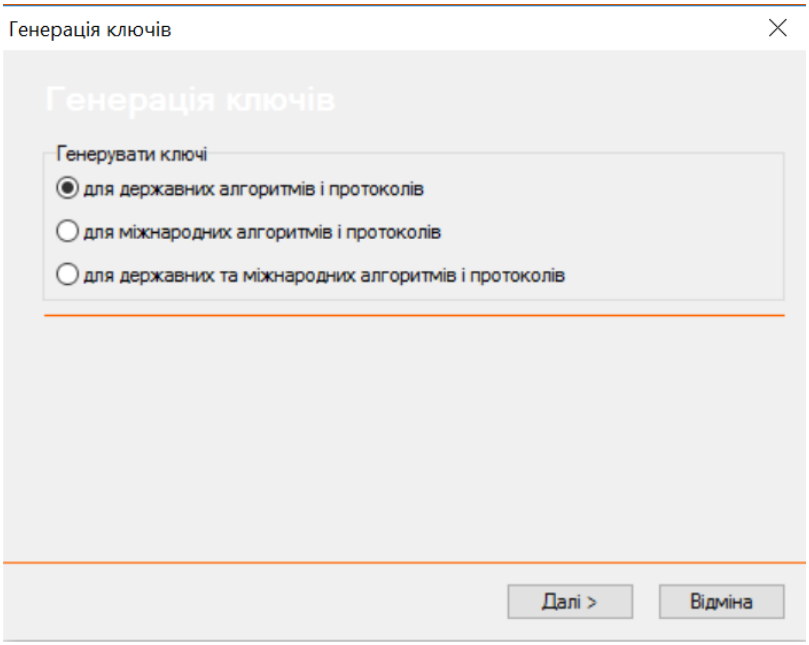


Рис. 6.3

4. На другій сторінці майстра за необхідністю можна вказати тип криптографічних алгоритмів та протоколів, та місце розміщення файлів з параметрами обраних криптографічних алгоритмів та протоколів.

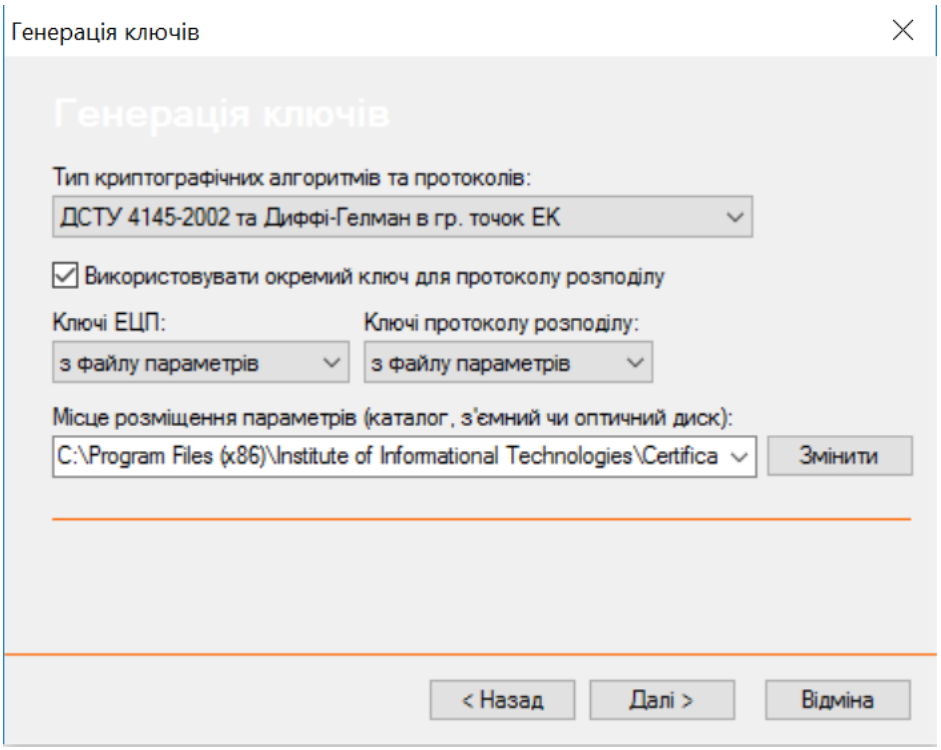


Рис. 6.4

Для переходу до наступної сторінки необхідно натиснути кнопку “Далі”.

5. На наступній сторінці майстра (Рис. 6.5) необхідно вказати тип носія -- як приклад, вказано токен Aladdin eToken Pro.
Пароль доступу до носія та захисту особистого ключа рекомендовано 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', '+', '-'.

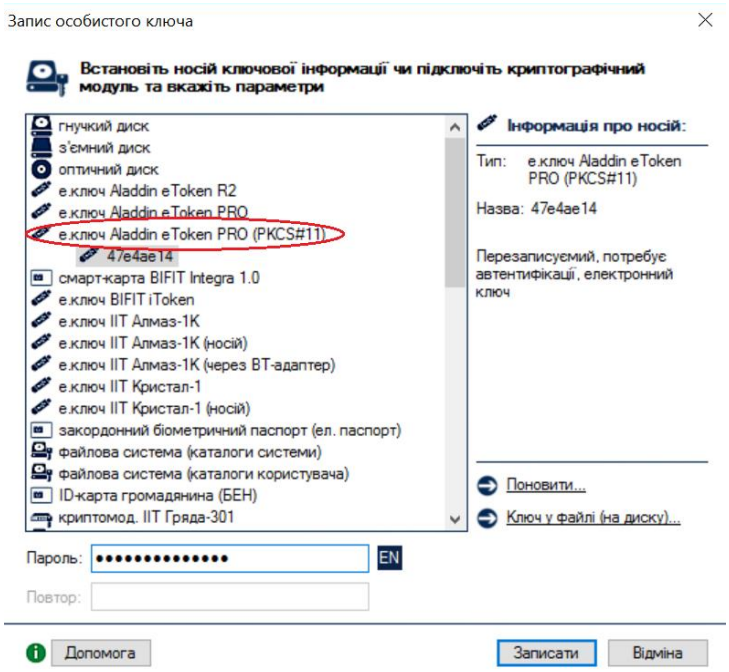


Рис. 6.5

6. Після введення паролю для запису особистого ключа необхідно натиснути кнопку «Записати».

Якщо на носії вже знаходиться попередньо отриманий електронний ключ, то з'явиться вікно (Рис. 6.6), в якому необхідно натиснути «Да».

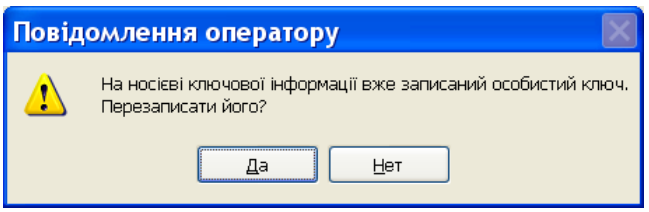


Рис. 6.6

7. На наступній сторінці майстра (Рис. 6.7) буде відображено два запити на формування сертифікату.

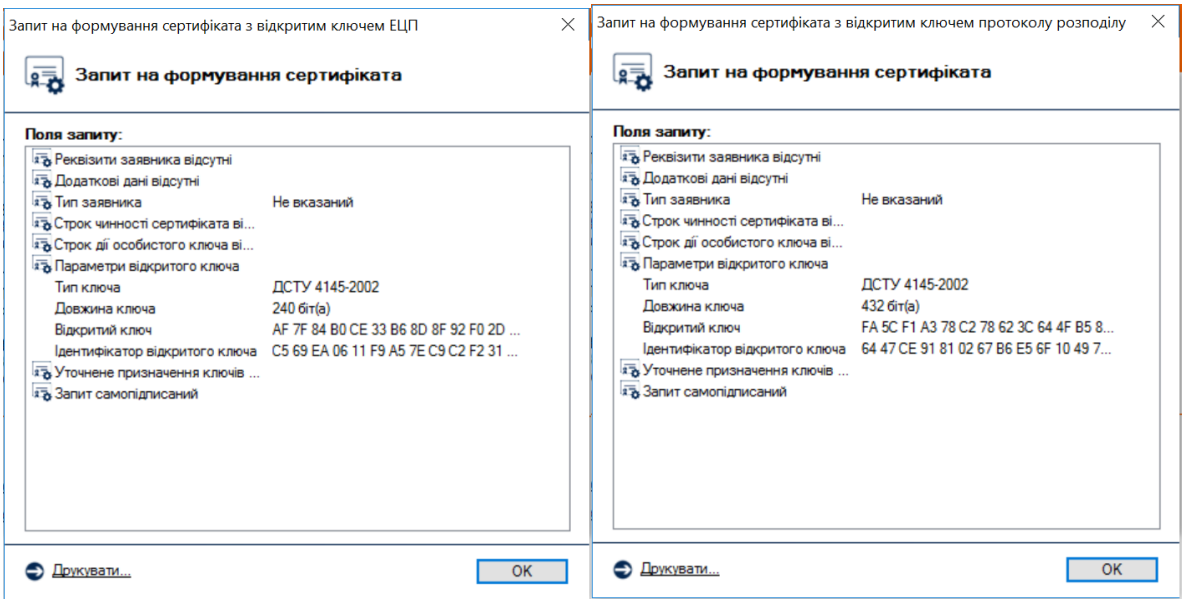


Рис. 6.7

8. На наступній сторінці майстра (Рис. 6.8) необхідно поставити позначку на «Зберегти у файл» та натиснути «Далі».

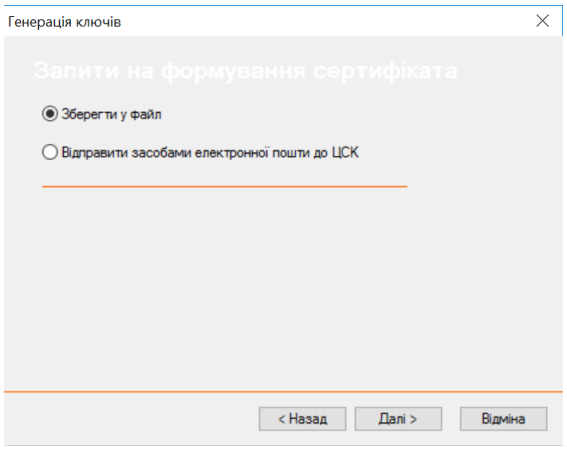


Рис. 6.8

9. На наступній сторінці майстра (Рис. 6.9) створюються два файли запиту на сертифікацію. Це файли, які згодом потрібно відправити в центр сертифікації.

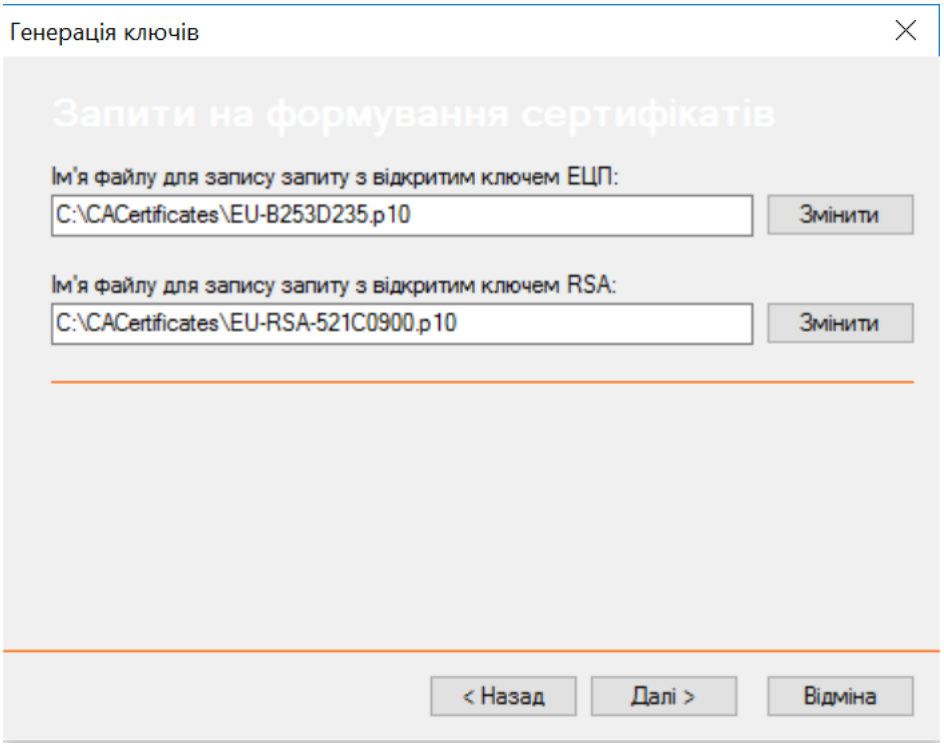


Рис. 6.9

10. Після виконання всіх дій майстер завершує свою роботу (Рис. 6.10).

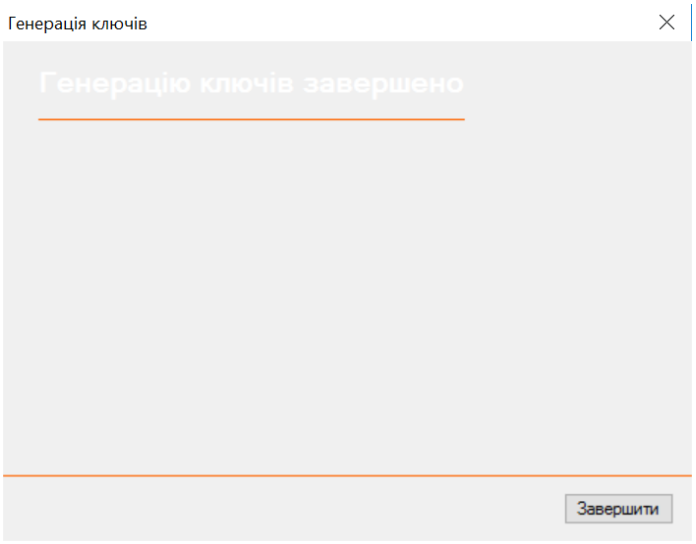


Рис. 6.10

Необхідно натиснути «Завершити».

11. Запити на формування сертифікатів сформовано, програму «Користувач ЦСК ПРАВЕКС БАНК» необхідно закрити.
12. Сформовані (згідно пункту 9) два файли запиту, що знаходяться у папці C:\CACertificates, з розширенням *.p10, необхідно засобами електронної пошти відправити адміністратору сертифікації (адреса вказана на офіційному сайті ЦСК у розділі «Контакти» -- https://ca.pravex.com.ua/contacts).
13. Після отримання письмової відповіді від адміністратора сертифікації, необхідно виконати наступний розділ даної інструкції (встановити сертифікати).

6.2 Встановлення сертифікатів особистого ключа ЕЦП

1. Сертифікати власного ключа ЕЦП встановлюються (копіюються в папку C:\CACertificates) на кожну робочу станцію, де буде працювати користувач і використовувати в своїй роботі ЕЦП.

2. Зазначена нижче процедура виконується на кожній робочій станції у повному обсязі один раз після проведення генерації особистого ключа ЕЦП користувача до наступного сеансу зміни особистого ключа ЕЦП.

3. Процедура проводиться особисто користувачем, якому був виданий особистий ключ ЕЦП.

4. На робочому столі своєї робочої станції знайти ярлик програми «Користувач ЦСК ПРАВЕКС БАНК» (Рис. 6.11):

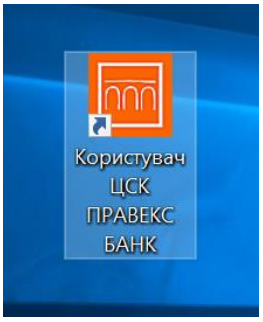


Рис. 6.11

5. Після запуску програми відкриється вікно, що зображене на Рис. 6.12

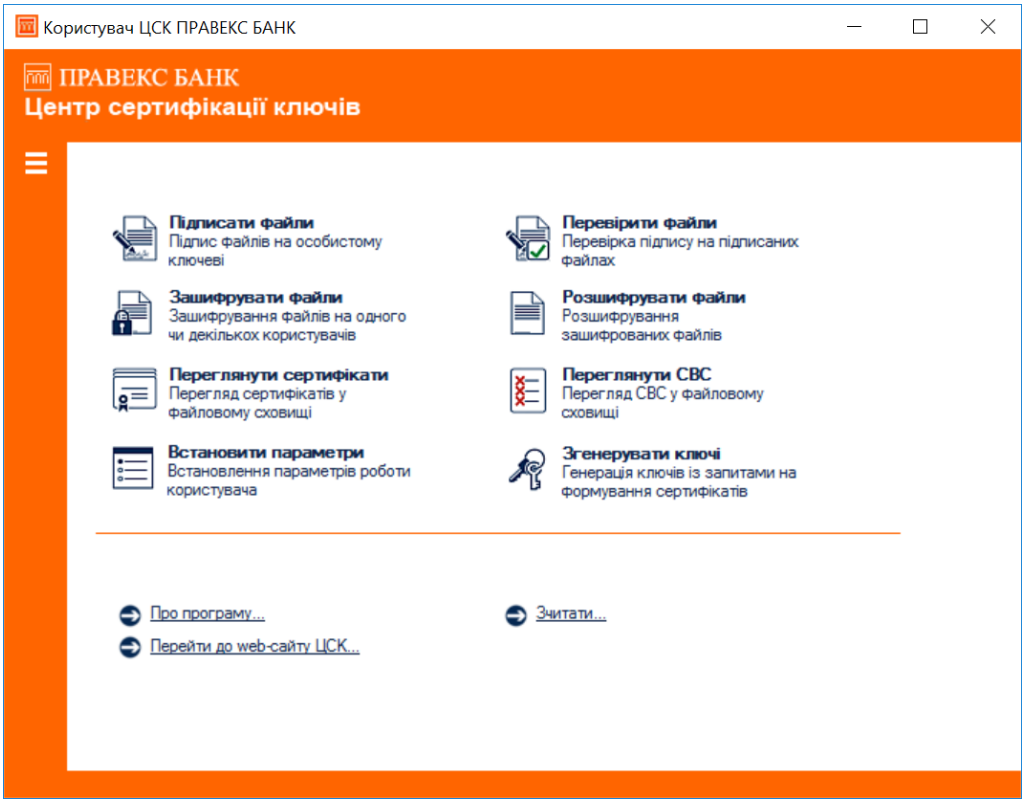


Рис. 6.12

6. У цьому вікні необхідно у меню обрати пункт «Сертифікати та СВС», далі з випадаючого меню обрати пункт «Отримати з ЦСК» (Рис. 6.13).

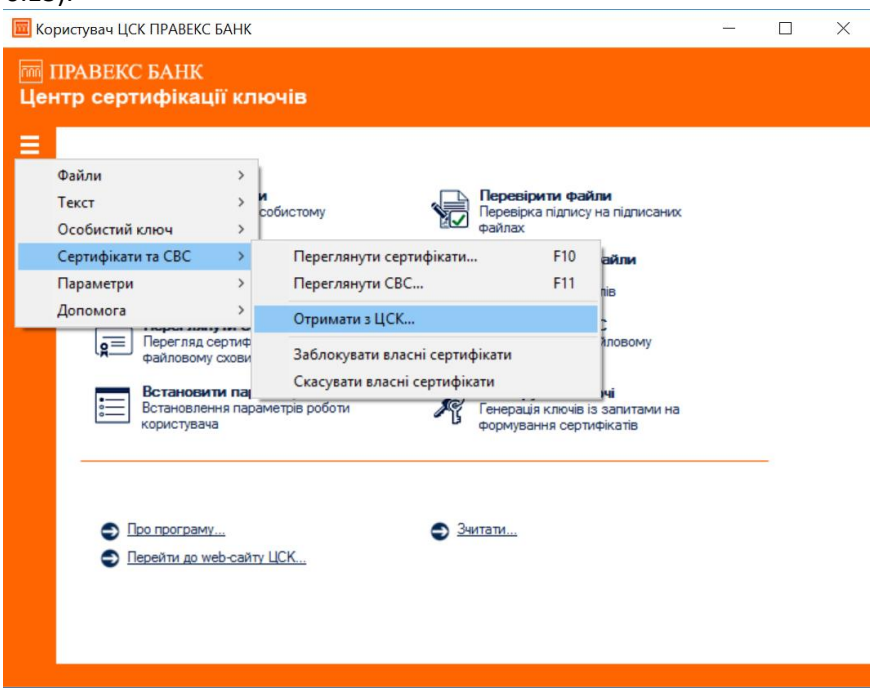


Рис. 6.13

7. У вікні «Повідомлення оператору» (Рис. 6.14) натиснути «Да».

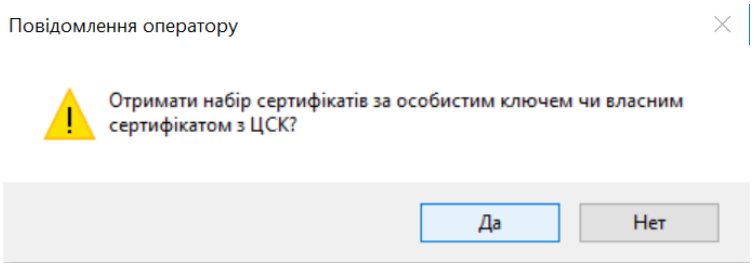


Рис. 6.14

8. Після цього з’являється вікно, що зображене на Рис. 6.15.

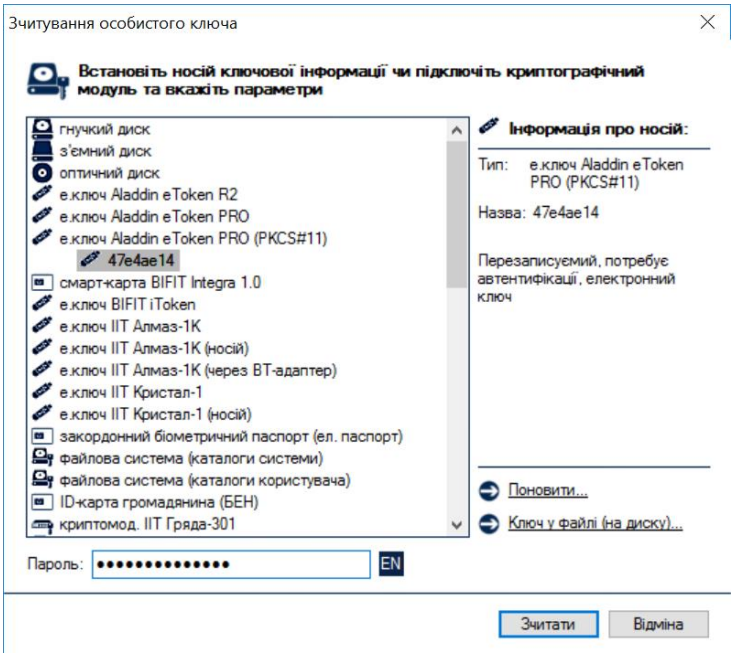


Рис. 6.15

10. Необхідно вказати тип носія, та у вікні «Пароль» ввести пароль носія.
Після введення паролю для запису особистого ключа необхідно натиснути кнопку «Зчитати».
11. У вікні «Завантажені сертифікати» (Рис. 6.22) натисніть «Да».

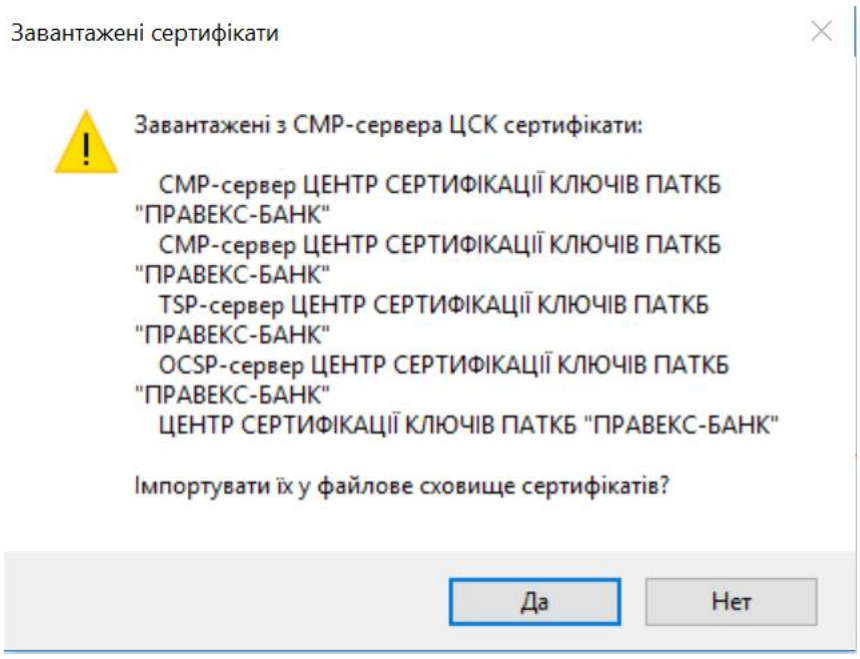


Рис. 6.22

15. Процедура встановлення сертифікатів особистого ключа ЕЦП на робочій станції завершена, програму «Користувач ЦСК ПРАВЕКС БАНК» необхідно закрити.

6.3 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. 6.7) необхідно вказати:

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

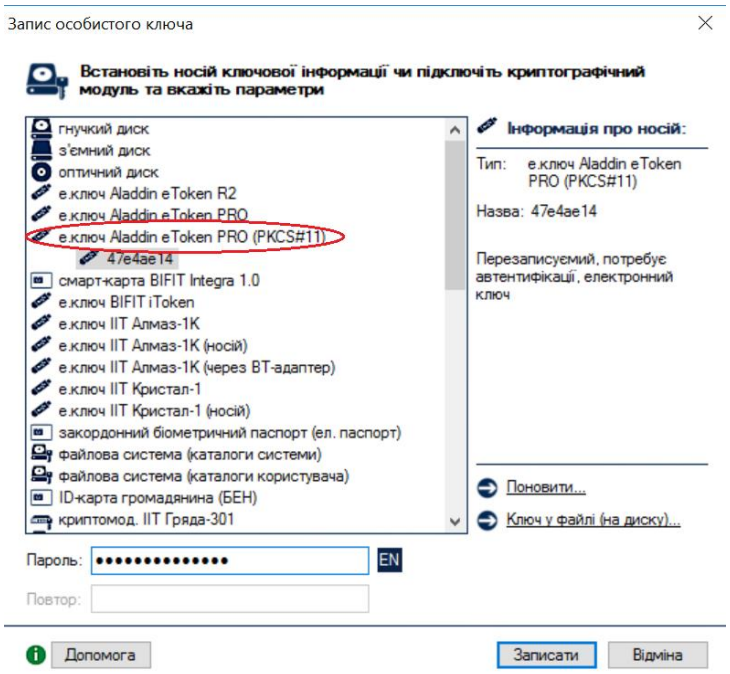


Рисунок 6.7

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 6.8.

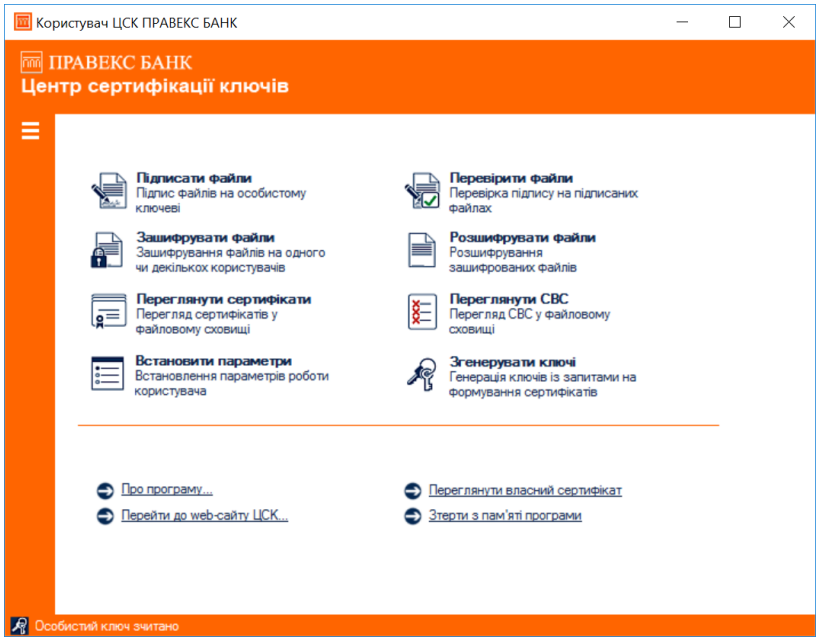


Рисунок 6.8

6.4 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 6.9. Під час резервного копіювання пароль захисту особистого ключа не вказується, та змінити його не можливо.

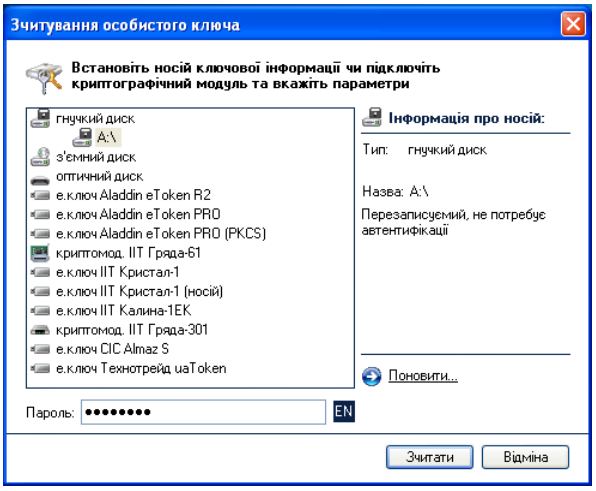


Рисунок 6.9

Після зчитування особистий ключ записується до резервного носія за допомогою вікна що наведене на рисунку 6.10.

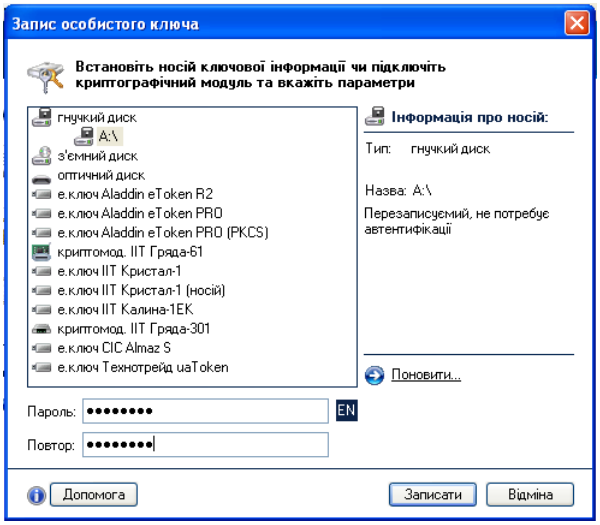


Рисунок 6.10

6.5 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 ключанаведене на рис. 6.11. У вікні необхідно вказати:

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

Після введення параметрів необхідно натиснути кнопку “Виконати”.

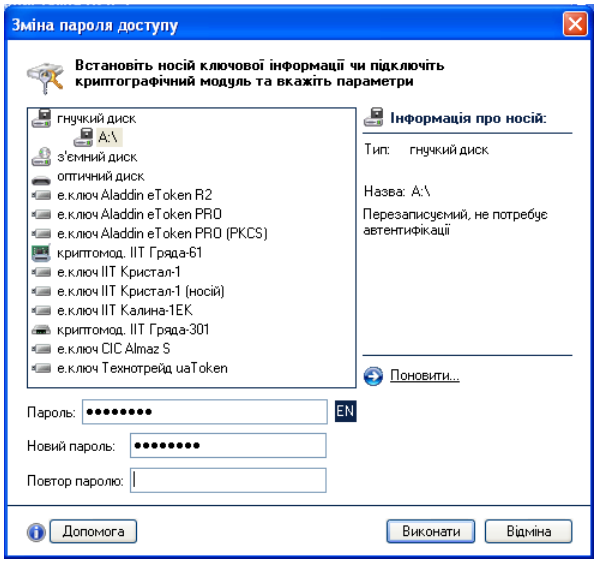


Рисунок 6.11

6 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 такі 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.

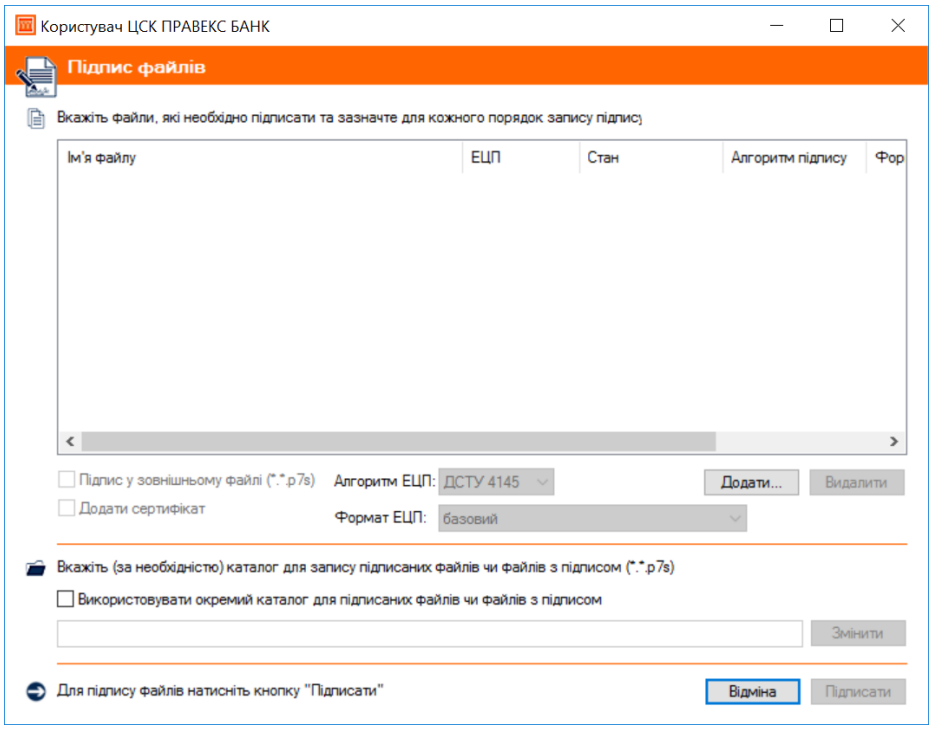


Рисунок 7.1

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

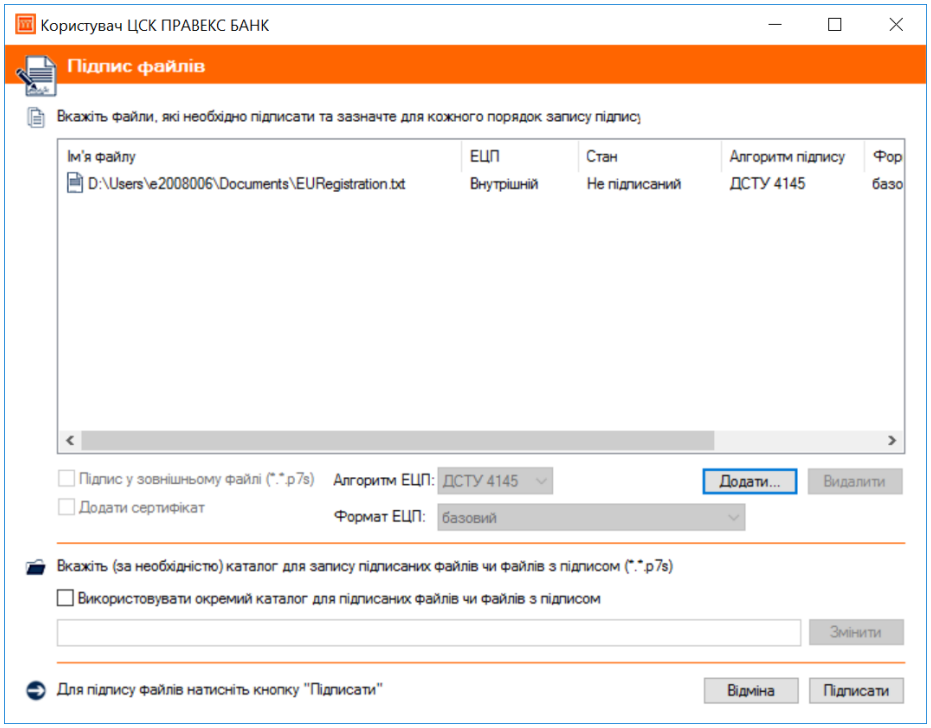


Рисунок 7.2

Для підпису файлів необхідно натиснути кнопку “Підписати”.

Після здійснення підпису файлів вікно буде містити інформацію про результати підпису.

7.2 Перевірка підпису 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 натиснутиклавішу 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.

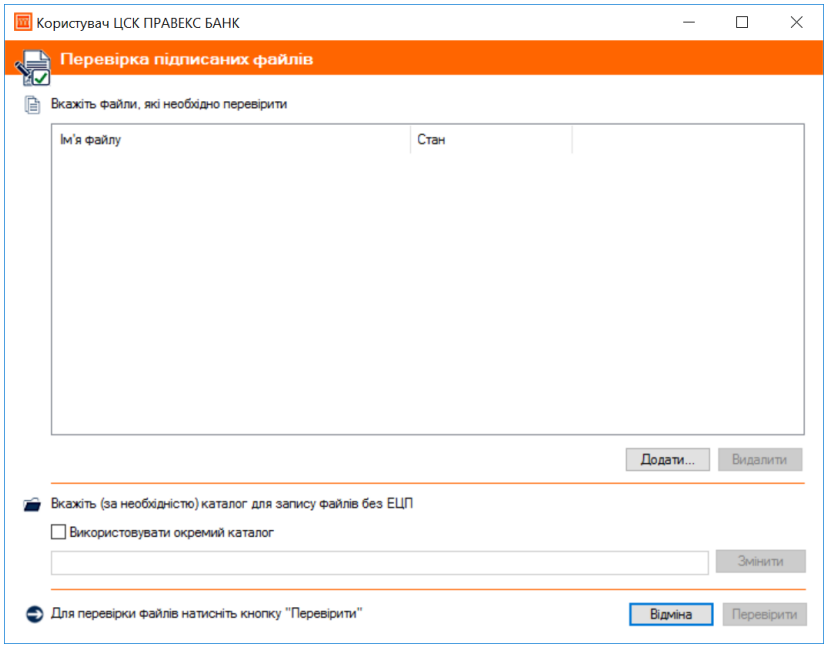


Рисунок 7.4

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

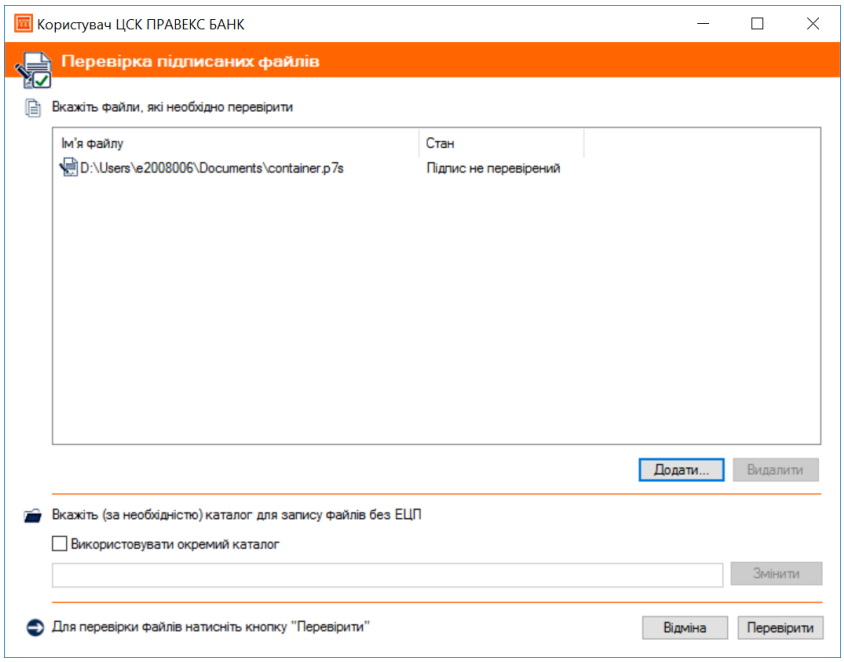
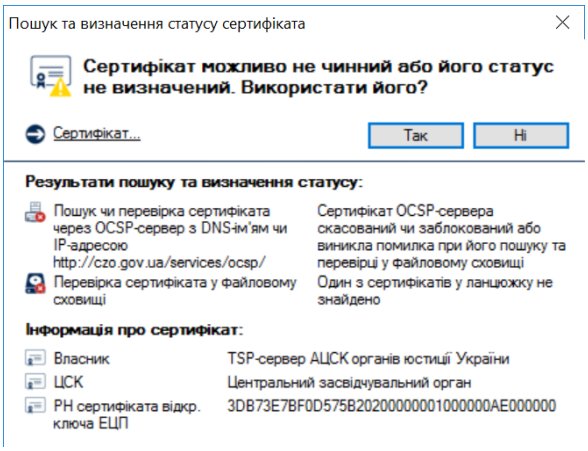


Рисунок 7.5

Для перевірки файлів необхідно натиснути кнопку “Перевірити”.

Якщо під час перевірки виникає помилка:



Це може означати, що у файловому сховищі відсутні необхідні сертифікати (підписувача, центру сертифікації або серверів центру сертифікації – зазвичай їх можна завантажити с офіційного сайту відповідного центру сертифікації) або відсутній мережевий доступ до веб-сайту центру сертифікації.

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.

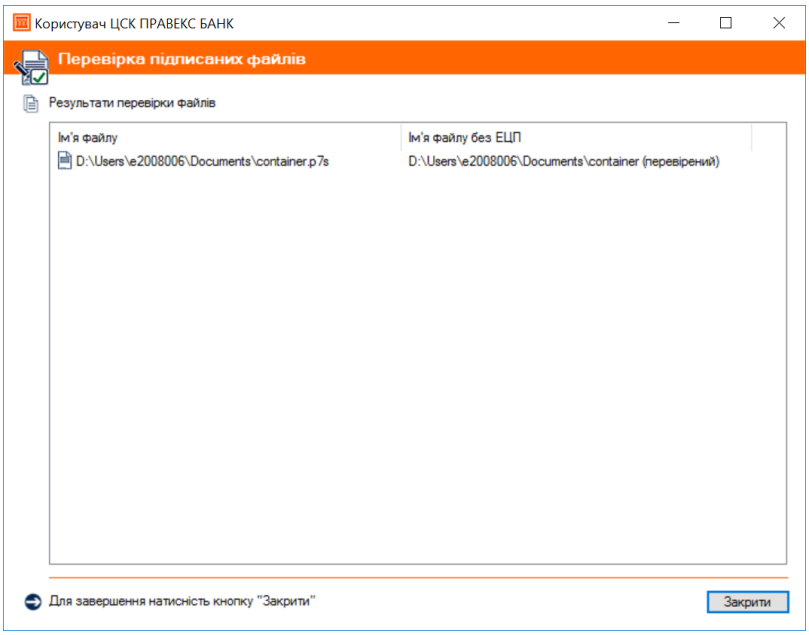


Рисунок 7.6

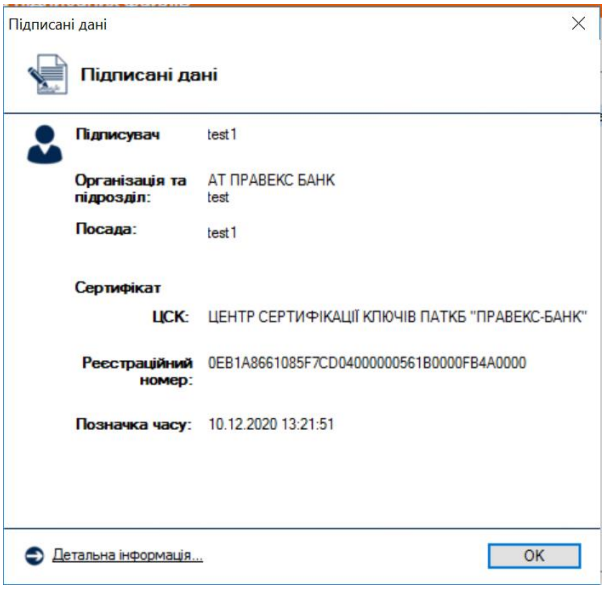


Рисунок 7.7

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.

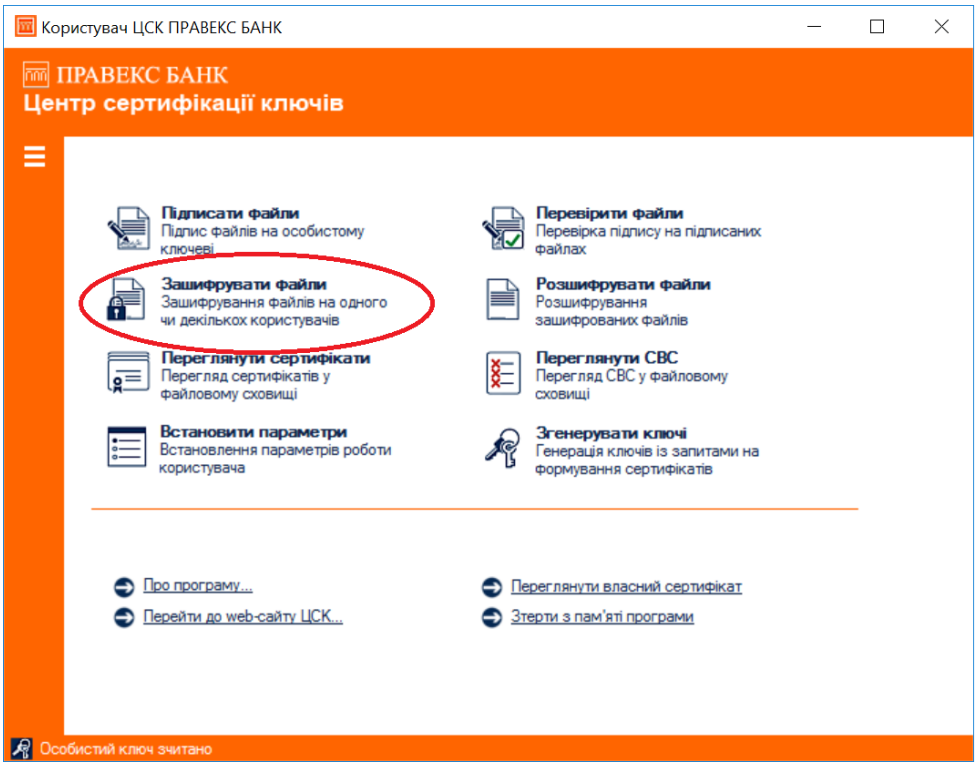


Рисунок 7.8

Вікно зашифрування файлів наведене на рис. 7.9. 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.

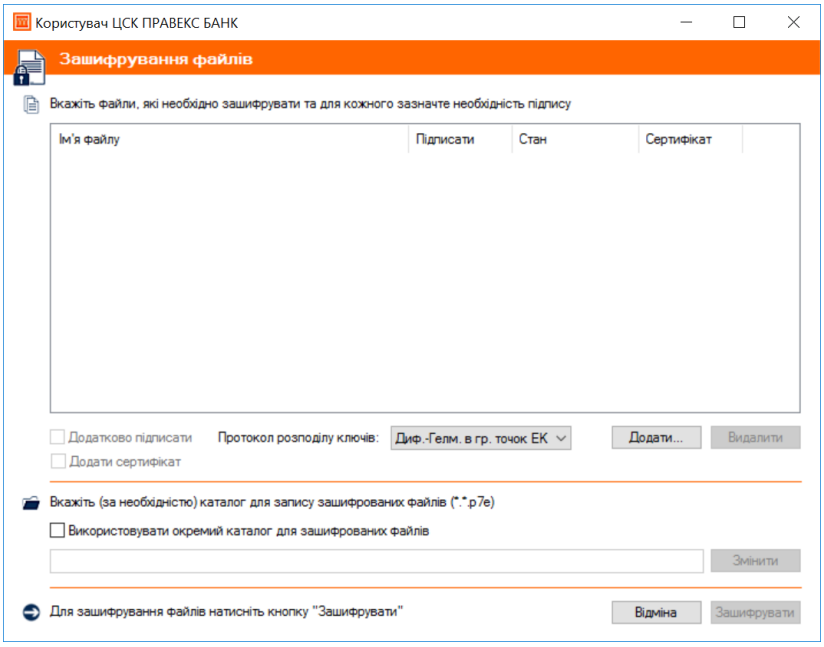


Рисунок 7.9

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. Для того, щоб пункт «додатково підписати» став активним, необхідно виділити файл лівою клавішою миші.

Інформативно: Для надання інформації в Банк необхідно **обов’язково** підписувати файли.

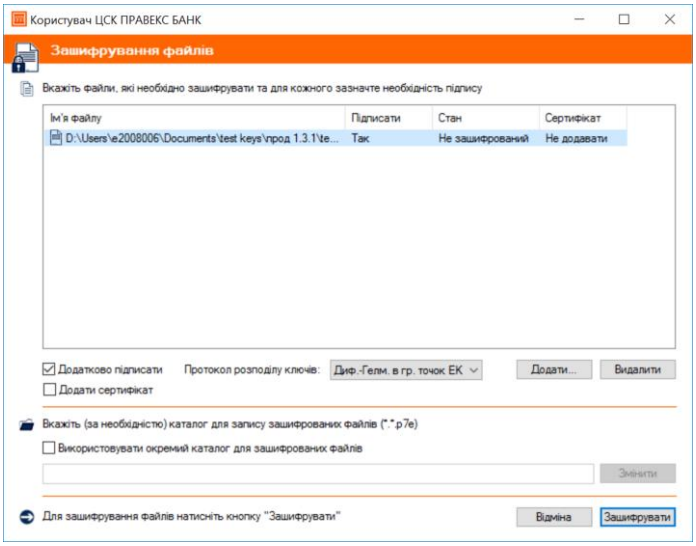


Рисунок 7.11

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”.

Після встановлення значень параметрів, вікно може мати вигляд як наведено на рис. 7.12. Для виконання зашифрування необхідно натиснути кнопку “Зашифрувати”.

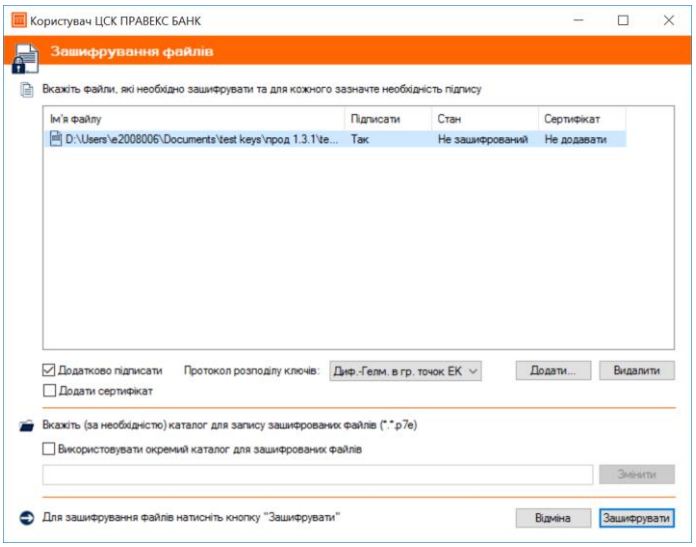


Рисунок 7.12

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. 7.13 необхідно обрати користувачів для яких виконується зашифрування файлу. Зашифрований файл може бути відкритим лише користувачем для якого виконувалось зашифрування.

Під час шифрування здійснюється перевірка параметрів ключових даних користувачів що були обрані у списку (рис 7.13). У списку присутні тільки ті користувачі, чиї сертифікати присутні у файловому сховищі, та параметри яких співпадають з параметрами ключа, яким шифруються файли (якщо шифрування ДСТУ, розшифрувати можна тільки ключем ДСТУ).

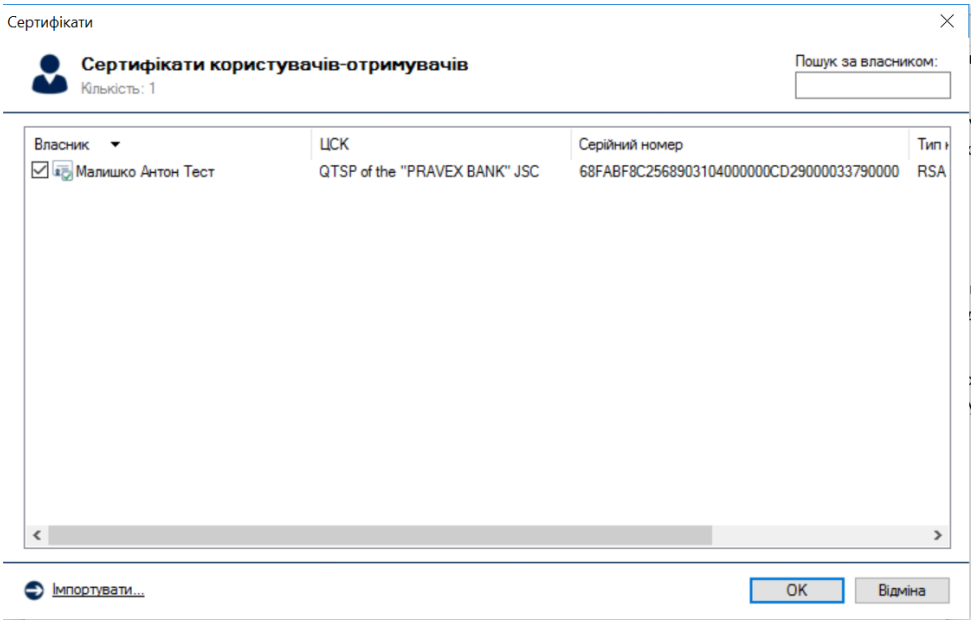


Рисунок 7.13

Після здійснення зашифрування файлів буде виведене наступне вікно (рис. 7.14) з інформацією про результати зашифрування.

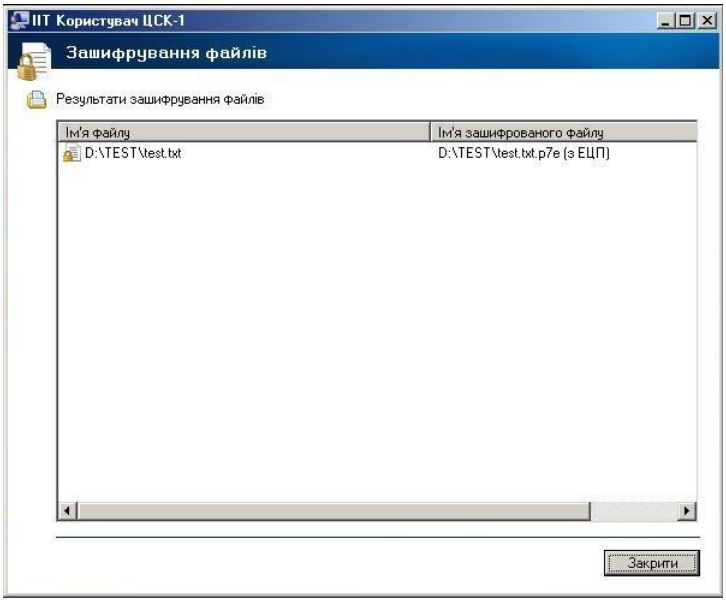


Рисунок 7.14

Інформативно: В колонці «Ім'я зашифрованого файлу» в дужках повинен обов'язково бути присутній напис «(з ЕЦП)», що свідчить про накладання на файл, що зашифрований, електронного цифрового підпису.

7.4 Розшифрування файлів

Перед розшифруванням файлів необхідно зчитати ключ, сертифікат якого було вказано у списку сертифікатів отримувачів зашифрованого файлу при зашифруванні (див. рис. 7.13).

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. 7.15. Форма містить такі 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".

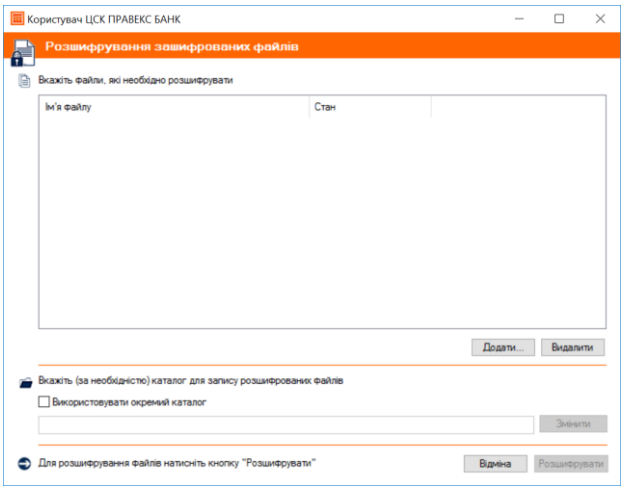


Рисунок 7.15

Після встановлення значень параметрів, вікно розшифрування файлів може мати вигляд, як наведено на рис. 7.16.

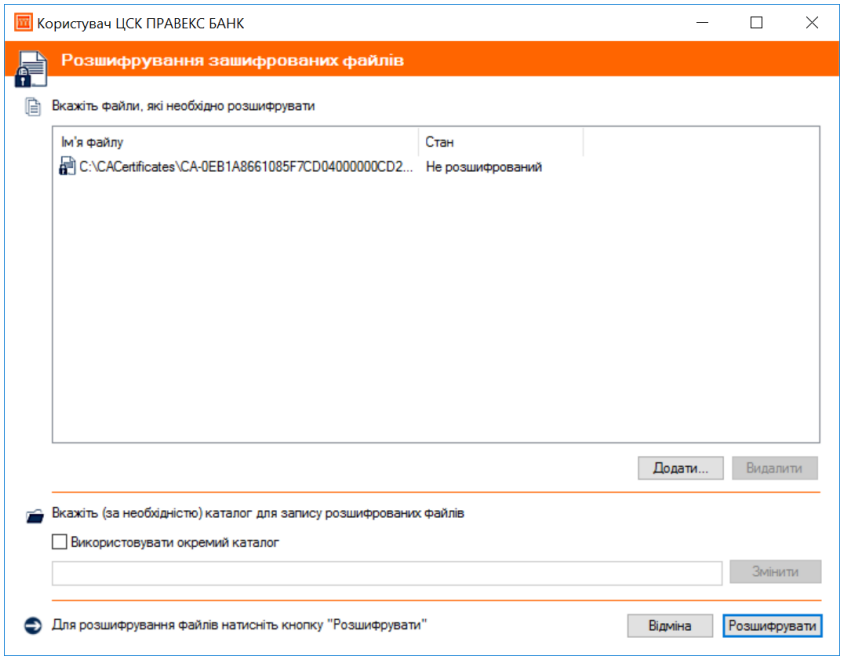


Рисунок 7.16

Для розшифрування файлів необхідно натиснути кнопку “Розшифрувати”. Після розшифрування буде виведено інформацію про результати розшифрування (рис. 7.17).

В разі вдалого розшифрування є можливість переглянути інформацію про розшифровані файли (рис. 7.18), для чого необхідно натиснути на запис про відповідний файл.

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

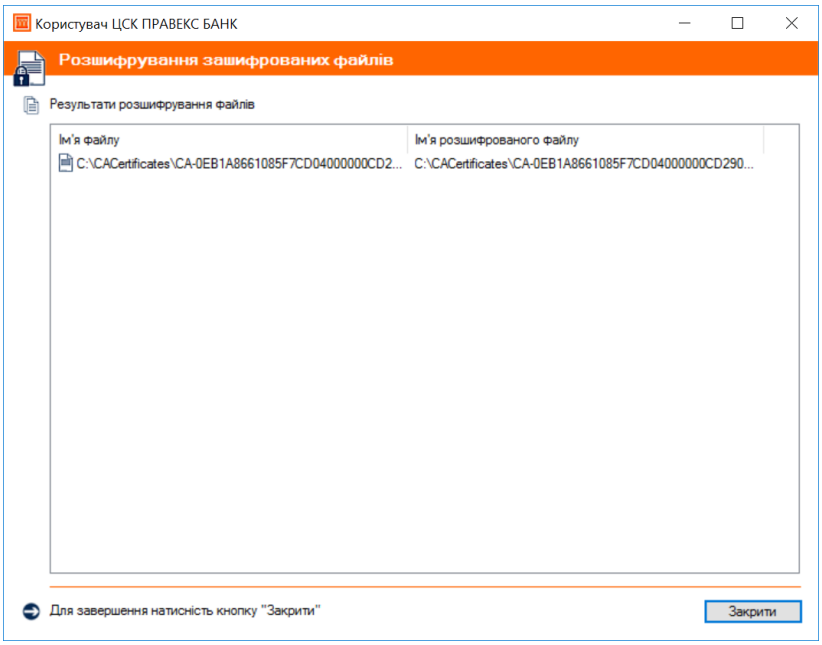


Рисунок 7.17

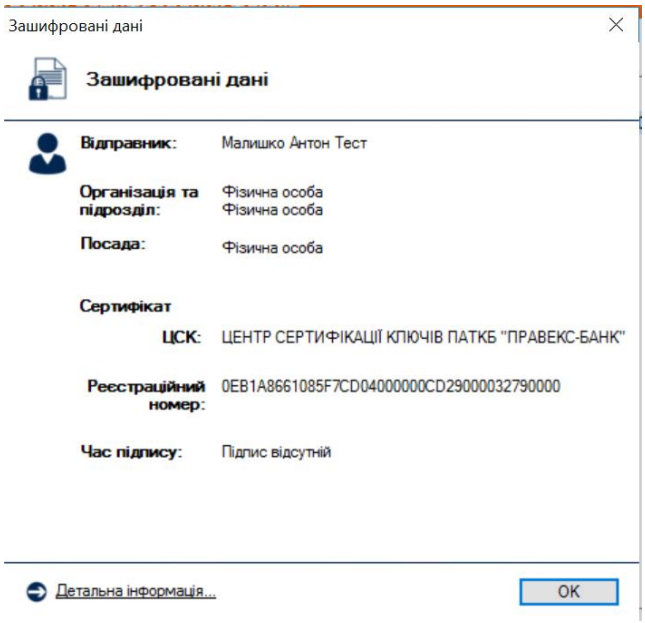


Рисунок 7.18

8 ДОВІДКОВА СИСТЕМА

8.1 Контактні відомості для зв'язку

Телефон, за яким необхідно звертатись в разі виникнення питань по ЦСК вказані на офіційному сайті ЦСК у розділі «Контакти» (https://ca.pravex.com.ua/contacts) або написавши листа на адресу ca@pravex.ua