Прим. №__

ЗАТВЕРДЖЕНО

UA. 35363887.00002-01 34 02-ЛЗ

НАСТАНОВА ОПЕРАТОРА

“ПРОГРАМНИЙ КОМПЛЕКС КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ «КРИПТОСЕРВЕР». ЦЕНТР РОЗПОДІЛУ КЛЮЧІВ”

UA. 35363887.00002-01 34 02

на 37 аркушах

Київ – 2010

Інв. №	
Підпис та дата	
Інв. № копії	
Підпис та дата	

ЗМІСТ

ТЕРМІНИ ТА СКОРОЧЕННЯ

Комплекс	-	програмний комплекс криптографічного захисту інформації «Криптосервер»
Асиметричний ключ	-	ключ, що використовується в асиметричних алгоритмах (шифрування, ЕЦП) та створюється з пари *закритий ключ + відкритий ключ*.
Закритий ключ	-	параметр криптографічного алгоритму, доступний тільки підписувачу.
Відкритий ключ	-	параметр криптографічного алгоритму, доступний всім компонентам Комплексу, якій використовується для перевірки достовірності одержаного повідомлення.
Сеансовий ключ	-	ключ, що створюється між двома компонентами Комплексу та використовується для захисту каналу зв'язку шляхом шифрування інформації, що передається.
Сертифікат відкритого ключа (сертифікат)	-	дані, які підтверджує відповідність між відкритим ключем та інформацією, яка ідентифікує компонент Комплексу.
ЦГК	-	компонент Комплексу Центр генерації ключів.
ЦРК	-	компонент Комплексу Центр розподілу ключів.
МШ	-	компонент Модуль шифрування.
МК	-	компонент Комплексу Модуль керування.

1. ВСТУП

В даному документі наведена настанова оператора програмного модуля «Центр розподілу ключів», який є складовою частиною програмного комплексу криптографічного захисту інформації «Криптосервер» (далі – Комплекс) та призначений для зберігання і видачі мережевими каналами довіреним компонентам програмного комплексу криптографічного захисту інформації «Криптосервер» (далі – Комплекс) сертифікатів відкритих ключів, інформації про контур безпеки, що визначає учасників захищеної мережі, та іншої службової інформації

Максимальний гриф обмеження доступу інформації, яка циркулює в межах Комплексу – конфіденційна, що не є власністю держави.

Оформлення програмного документа «Настанова оператору» виконано відповідно до вимог ЕСПД (ГОСТ 19.101-77 [1], ГОСТ 19.103-77 [2], ГОСТ 19.104-78* [3], ГОСТ 19.105-78* [4], ГОСТ 19.106-78* [5], ГОСТ 19.401-78 [6], ГОСТ 19.604-78* [7]).

[1] ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов
[2] ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов
[3] ГОСТ 19.104-78* ЕСПД. Основные надписи
[4] ГОСТ 19.105-78* ЕСПД. Общие требования к программным документам
[5] ГОСТ 19.106-78* ЕСПД. Общие требования к программным документам, выполненным печатным способом
[6] ГОСТ 19.401-78 ЕСПД. Текст программы. Требования к содержанию и оформлению
[7] ГОСТ 19.604-78* ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом

2. ЗАГАЛЬНІ ВІДОМОСТІ

2.1 Позначення та назва програми

Програмний модуль «Центр розподілу ключів» має наступні атрибути:

- Версія продукту - v. 1.0
- Назва продукту - Програмний модуль «Центр розподілу ключів»
- Розробник - ТОВ НВП «Безпека інформаційно-телекомунікаційних систем»
- Найменування файлу, що виконується - KeyDistributionCentre.exe

2.2 Програмне забезпечення, необхідне для функціонування ЦРК

Функціонування Центру розподілу ключів здійснюється під керуванням операційних систем Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Vista.

2.3 Мова програмування

Центр розподілу ключів написано мовою програмування C++. У якості компілятору використовується CodeGear C++Builder 2007 компанії Borland.

3. ФУНКЦІОНАЛЬНЕ ПРИЗНАЧЕННЯ

Центр розподілу ключів є програмним засобом зберігання та видачі мережевими каналами довіреним компонентам програмного комплексу криптографічного захисту інформації «Криптосервер» (далі – Комплекс) сертифікатів відкритих ключів, інформації про контур безпеки, що визначає учасників захищеної мережі, та іншої службової інформації

4. ОПИС ЛОГІЧНОЇ СТРУКТУРИ

4.1 Перелік програмних модулів (файлів)

ЦРК складається з наступних частин:

- робочий модуль (KeyDistributionCentre.exe): виконує операції перевірки статусу сертифікатів та надає необхідні відомості (статус сертифікатів, інформацію про контур безпеки) модулям шифрування, які встановлюють між собою захищений канал зв'язку.
- система керування базою даних MySQL: засіб зберігання інформації та реалізації механізмів розмежування доступу до інформації і функцій складових частин ЦРК;
- бібліотека функцій криптографічних перетворень "UaCrypto": забезпечує реалізацію механізмів криптографічних перетворень під час генерації та зберігання ключових даних.

4.2 Робота з компонентами ЦРК

4.2.1 Інсталяція компонентів

Система керування базами даних

Для забезпечення роботи ЦРК необхідно виконати інсталяцію бази данихMySQL v.3.28. Завдання розгортання та інсталяції СКБД покладається на адміністратора автоматизованої системи, в межах якої передбачено функціонування Комплексу.

Примітка:

Інсталяційний пакет СКБД в комплект поставки ЦРК не входить.

Інсталяція робочого модуля

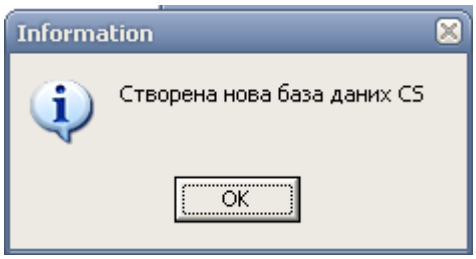
- виконати інсталяцію програмного забезпечення ЦРК (файл Setup KeyDistributionCentre _v1.exe);
- виконати налаштування параметрів ЦРК (в файлі KeyDistributionCentre.ini).

Бібліотека криптографічних перетворень буде скопійована каталог разом з файлами ЦРК під час його інсталяції.

Розгортання бази даних

Під час першого запуску ЦРК автоматично буде створено базу даних з назвою, що вказана у конфігураційному файлу (наприклад, CS).

Рис. 1 Повідомлення про створення бази даних



4.2.2 Налаштування параметрів робочого модуля

Налаштування параметрів виконуються у ручному режимі (безпосередньо на АРМ з встановленим ЦРК).

Параметри задаються у файлі KeyDistributionCentre.ini.

Існують наступні блоки параметрів:

Блок [DB] – описує налаштування, необхідні для з'єднання ЦРК з базою даних. У блоці задаються значення параметрів, таких як:

Host - IP-адреса АРМ, на якому встановлено базу даних.

Name - ім'я бази даних.

ReserveType - спосіб резервування даних. Приймає наступні значення: 0 – за командою адміністратора, 1 – під час запуску програми, 2 – під час завершення роботи програми, 3 – періодично (додатково вказується період резервування даних).

ReserveTime - дата та час створення останнього створення резервної копії даних (встановлюється автоматично).

ReserveDays - період резервування даних (діб, використовується, якщо параметр ReserveType встановлено у 3).

Приклад заповнення параметрів блоку:

```
[DB]
  Host=localhost
  Name=CS
  ReserveType=0
  ReserveDays=30
  ReserveTime=0
```

Блок [Server] – описує налаштування, необхідні для з'єднання ЦРК з іншими компонентами Комплексу. У блоці задаються значення параметрів, таких як:

Port - номер порту, по якому інші компоненти Комплексу будуть встановлювати з'єднання з ЦРК.

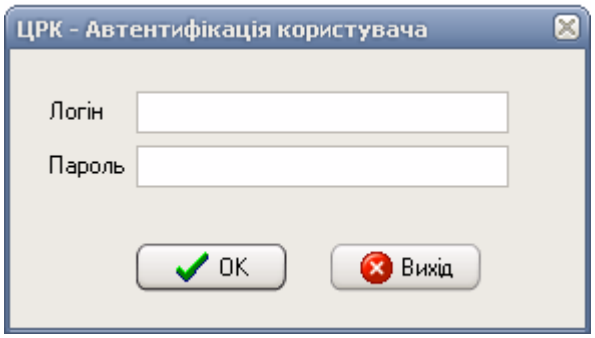
Приклад заповнення параметрів блоку:

[Server]
Port=10001

4.2.3 Запуск ЦРК

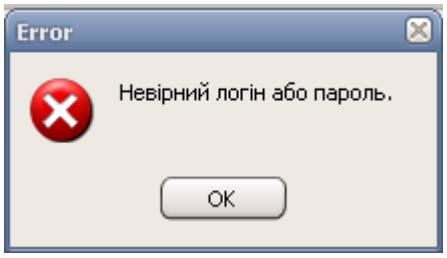
Для запуску ЦРК на виконання необхідно обрати файл KeyDistributionCentre.exe та виконати його запуск, після чого ввести атрибути доступу до ресурсів ЦРК (логін/пароль адміністратора бази даних).

Рис. 2 Вікно запиту паролю



У випадку введення невірного паролю користувач отримує повідомлення, наведене на рис. 3. Якщо невірний пароль буде вказано тричі поспіль ЦРК завершує свою роботу без попереджень.

Рис. 3 Попередження про введення невірного паролю



У випадку запуску ЦРК без завантажених ключових даних ЦРК та зареєстрованого сертифікату ЦГК користувач одержує повідомлення, які наведені на рис. 4.

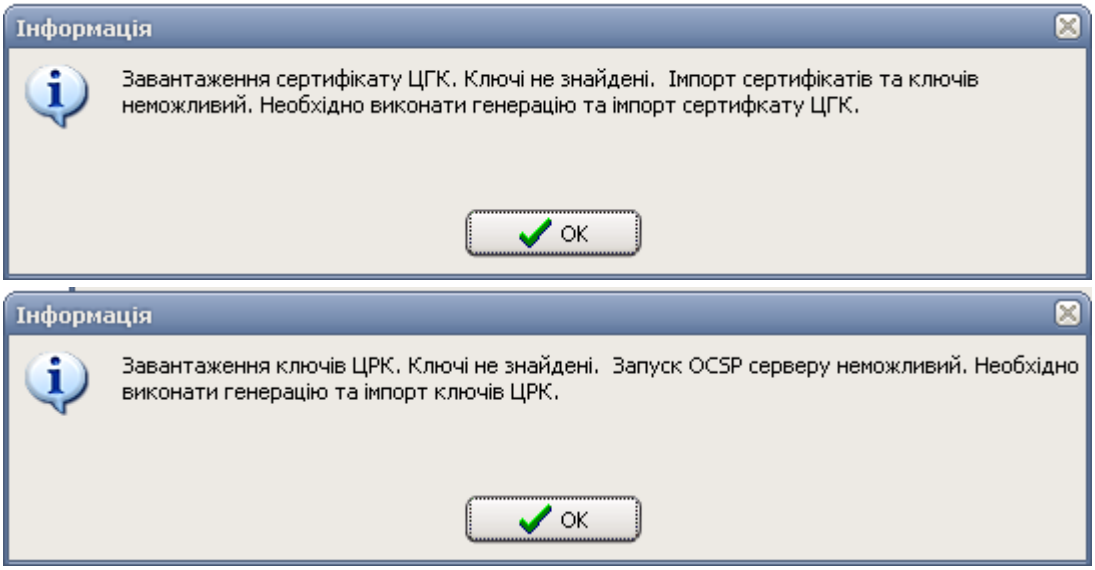


Рис. 4 Повідомлення про відсутність необхідних ключових даних

4.2.4 Інтерфейс користувача

Після запуску програмного модуля на виконання користувач отримує можливість працювати з графічним інтерфейсом, відображеним на рис. 5.

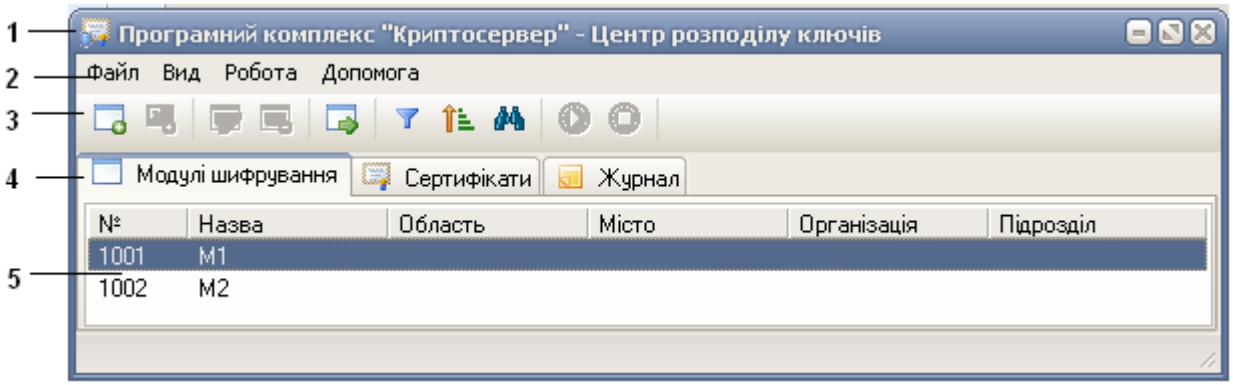


Рис. 5 Інтерфейс користувача

де,

1 - заголовок вікна: містить назву програми та кнопки керування;

2 - панель меню: призначена для забезпечення доступу до функцій програмного забезпечення.

Містить пункти меню *«Файл»*, *«Вид»*, *«Робота»* та *«Допомога»*.

2.1 Пункт меню *«Файл»* (рис. 6) надає користувачу можливість виконувати функції, що ініціюються наступними підпунктами:

- *«імпорт сертифікатів»*: дозволяє імпортувати сертифікати модулів шифрування та керування, які були сформовані ЦГК;

- *«експорт списку МШ»*: дозволяє сформувати «заявку на формування ключових даних МШ», яка використовується ЦГК під час формування ключових даних МШ;
- *«імпорт сертифікату ЦГК»*: дозволяє виконати імпорт сертифікату ЦГК;
- *«імпорт ключів OCSP»*: дозволяє імпортувати ключові дані ЦРК, які використовуються в процесі функціонування ЦРК;
- *«резервне копіювання»*: дозволяє виконати налаштування для резервного копіювання бази даних;
- *«сховати в іконку»*: дозволяє скрити програму в індикатор запущених програм («трей»);
- *«вихід»*: дозволяє завершити роботу програми.

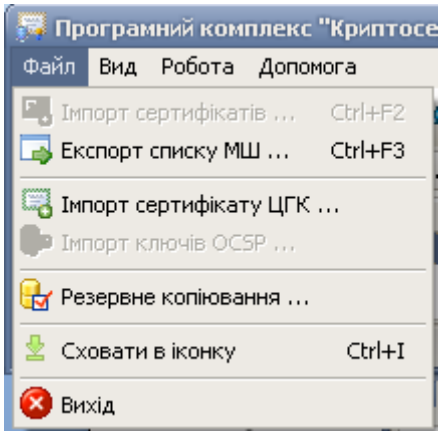
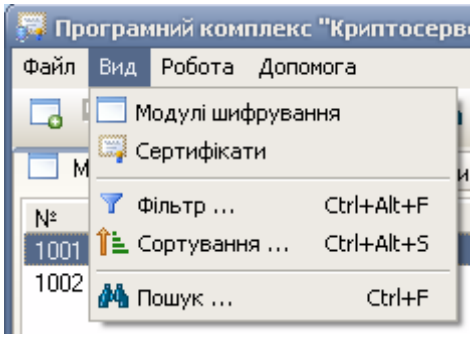


Рис. 6 Пункт меню *«Модулі шифрування»*

2.2 Пункт меню «*Вид*» (рис. 7) надає користувачу можливість роботи з даними та містить наступні підпункти:

- *«модулі шифрування»*: дозволяє відобразити або скрити вкладення «*Модулі шифрування*»;
- *«сертифікати»*: дозволяє відобразити або скрити вкладення «*Сертифікати*»;
- *«фільтр»*: дозволяє виконати фільтрацію інформації за вказаними параметрами в залежності від відкритого вкладення;
- *«сортування»*: дозволяє виконати сортування даних за обраними параметрами;
- *«пошук»*: дозволяє виконати пошук інформації за заданими критеріями.

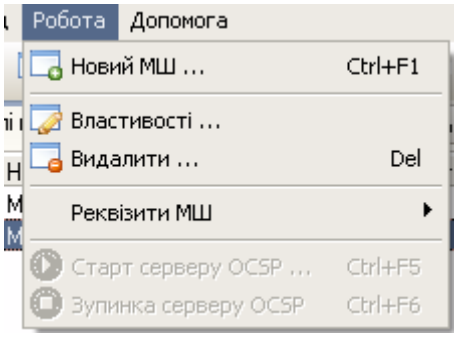
Рис. 7 Пункт меню *«Сертифікати»*



2.3 Пункт меню *«Робота»* надає користувачу можливість виконувати функції, що ініціюються наступними підпунктами:

- *«новий МШ»*: дозволяє створити запис про новий МШ;
- *«властивості»*: доза;
- *«імпорт ключів OCSP»*: завантажує ключові дані, необхідні для роботи ЦРК.

Рис. 8 Пункт меню *«Робота»*



2.4 Пункт меню *«Допомога»* надає довідкову інформацію.

3 - панель інструментів: призначена для забезпечення швидкого доступу до деяких функцій. У залежності від активної закладки змінюється набір інструментів.

Загальні для всіх закладок інструменти:

- реєстрація нового МШ, кнопка ;
- реєстрація нових сертифікатів, кнопка ;
- фільтрація записів за критеріями (критерії обираються залежно від активного вкладення), кнопка ;
- сортування записів (параметри сортування обираються залежно від активного вкладення), кнопка ;
- виконати старт роботи ЦРК у режимі «онлайн», кнопка ;
- завершити роботу ЦРК у режимі «онлайн», кнопка .

Інструменти, що доступні при активній закладці «*Модулі шифрування*»:

- перегляд та редагування параметрів МШ, кнопка  ;
- видалення МШ, кнопка  ;
- формування списку МШ для ЦГК, кнопка  .

Інструменти, що доступні при активній закладці «*Сертифікати*»:

- перегляд та редагування параметрів сертифікату, кнопка  ;
- видалення сертифікату, кнопка  ;

4 - закладка сторінок блокноту: дозволяє виконати переключення між закладками з інформацією.

5 - область відображення інформації про МШ, сертифікати та записи журналу реєстрації повідомлень.

4.2.5 Порядок роботи з ЦРК

4.2.5.1 Алгоритм запуску ЦРК під час впровадження Комплексу в експлуатацію

Для того, щоб ЦРК був здатний виконувати свої функції у повному обсязі необхідно почергово виконати наступні кроки:

- наповнити даними довідники реквізитів МШ (область/підрозділ);
- створити перелік МШ із використанням заповнених довідників;
- сформувати заявку для генерації ключових даних МШ;
- виконати генерацію ключових даних всіх компонентів Комплексу: виконується Адміністратором за допомогою засобів ЦГК. Опис процедури наведено в документі «Настанова оператора. «Програмний комплекс криптографічного захисту інформації «КРИПТОСЕРВЕР». Центр генерації ключів»;
- імпортувати сертифікат ЦГК до бази даних ЦРК;
- імпортувати ключові дані ЦРК до бази даних;
- імпортувати сертифікати МШ та МК до бази даних ЦРК;
- виконати запуск роботи ЦРК у режимі «онлайн».

Після того, як всі наведені дії будуть виконані на Адміністратора покладається завдання підтримання бази даних ЦРК в актуальному стані.

4.2.5.2 Робота с записами МШ

Для перегляду переліку МШ необхідно відкрити закладку *«Модулі шифрування»*. Закладка надає наступну інформацію:

- номер МШ в складі Комплексу;
- назва МШ;
- область, де встановлено МШ;
- місто, де встановлено МШ;
- організація, яка експлуатує МШ;
- підрозділ вищевказаної інформації.

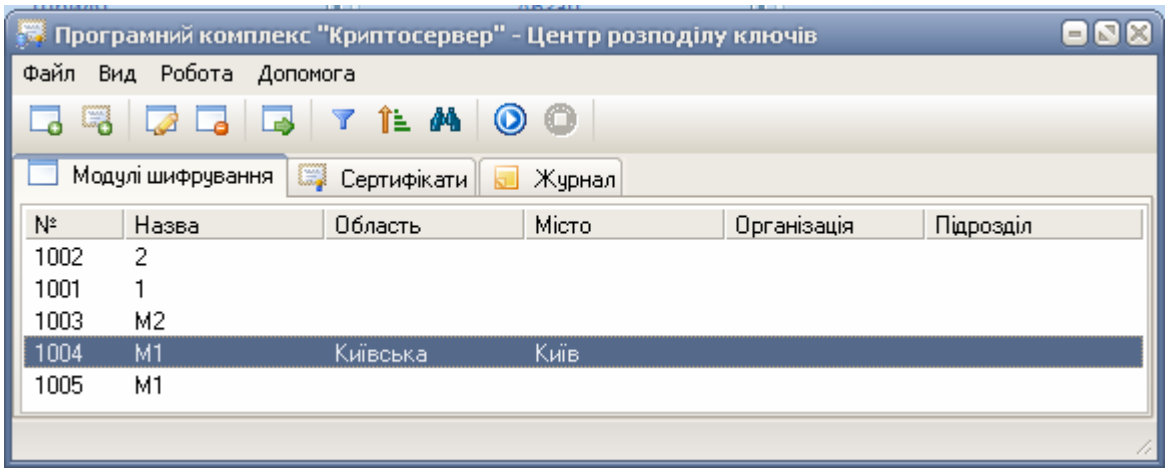


Рис. 9 Закладка *«Модулі шифрування»*

Заповнення довідників

Для того, щоб існувала можливість заповнення полів з допоміжною інформацією (також використовуються під час генерації ключових даних для МШ) під час створення запису МШ необхідно виконати заповнення довідників ЦРК.

Існує два типа довідників:

- географічний довідник: надає інформацію щодо розташування МШ (область, місто);
- довідник підрозділів: надає інформацію щодо установи, яка експлуатує МШ, та її підрозділів.

Для того, щоб ініціювати процедуру заповнення довідників необхідно обрати підпункт меню *«Робота»* > *«Реквізити МШ»* > *«Області / міста»* або *«Робота»* > *«Реквізити МШ»* > *«Організації / підрозділи»*. За результатами операції користувач одержує можливість заповнення даних у вікні, що зображено на рис. 10.

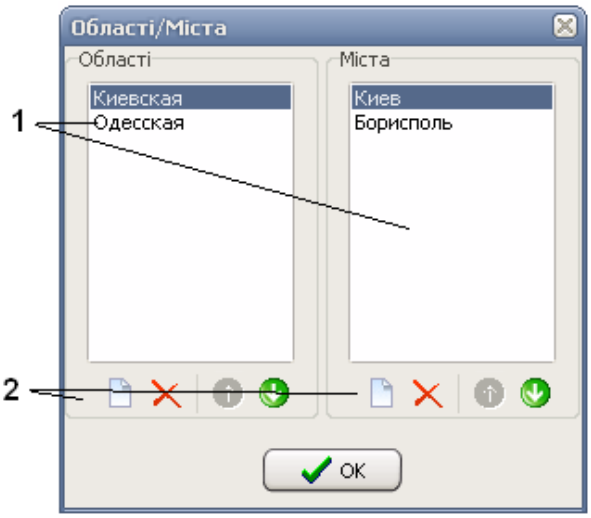


Рис. 10 Вікно заповнення довідника

Рис. 11 Панель інструментів довідника

Вікна довідників ідентичні один одному. В області 1, рис. 10, знаходяться інформаційні зони: в даному випадку *зона Області* та *зона Міста*. В них відображається відповідно інформація про області, та міста. При цьому слід зазначити, що перелік міст жорстко пов'язаний з областю. Наприклад, міста Київ та Бориспіль будуть відображатись лише у тому випадку, якщо буде обрана Київська область.

В області 2, рис. 10, розташовані дві інструментальні панелі, які дають можливість виконувати операції з даними, що знаходяться у *зоні Області* та *зоні Міста*.

Перелік операцій:

- додати інформацію про нову область/місто, кнопка 1, рис. 11;
- видалити інформацію про обрану область/місто, кнопка 2, рис. 11;
- виконати перехід на запис вверх/вниз у межах обраної зони, кнопка 3, рис. 11.

Слід зазначити, що у випадку видалення інформації про область також буде видалена інформація про всі міста, що їй відповідають.

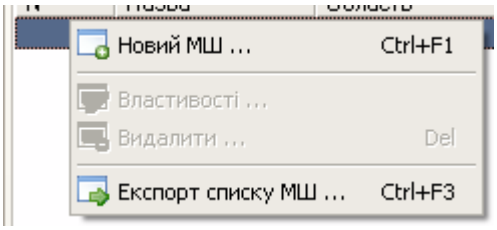
Створення записів про МШ

Для того, щоб створити в базі даних запис, який буде описувати МШ, необхідно скористатись:

- або підпунктом меню *«Робота» > «Новий МШ»;*

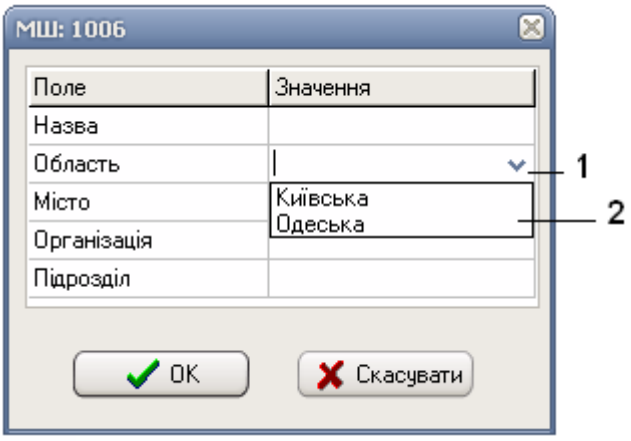
- або інструментом *«Реєстрація нового МШ»*;
- або комбінацією «гарячих» клавіш «Ctrl+F1»;
- або підпунктом *«Новий МШ»* меню, що «вспливає», рис. 12: «клік» правою кнопкою маніпуляторі типу «миша» на області відображення інформації про МШ, сертифікати та записи журналу реєстрації повідомлень (рис. 5).

Рис. 12 Підпункти меню, що «вспливає»



Після одержання вікна введення інформації про МШ необхідно заповнити дані у відповідних полях.

Рис. 13 Вікно введення інформації про МШ



Поля «область», «місто», «організація», «підрозділ» заповнюються даними з довідників. Для введення інформації необхідно обрати потрібне поле та одержати можливість перегляду переліку даних 2 (рис 13) за допомогою кнопки 1 (рис. 13).

Генерація «заявки на формування ключових даних»

Для генерації зазначеного запиту, після формування необхідного переліку МШ, необхідно скористатись підпунктом меню «Файл» > «Експорт списку МШ». За результатами операції буде виконано збереження заявки у файл з розширенням exp. Зазначений файл використовується під час процедури формування ключових документів модулів шифрування, детальний опис якої наведено в п. 4.2.5.1 «Генерація ключових даних» документу «Настанова оператора. «Програмний комплекс криптографічного захисту інформації «КРИПТОСЕРВЕР». Центр генерації ключів».

Перегляд та редагування записів МШ

Для перегляду даних або їх редагування необхідно відкрити закладку *«Модулі шифрування»*, обрати потрібний запис МШ та скористатись:

- або підпунктом меню *«Робота» > «Властивості»;*
- або інструментом *«Перегляд та редагування параметрів МШ»*;
- або двічі натиснути лівою кнопку маніпулятору на запису;
- або підпунктом *«Властивості»* меню, що «вспливає», рис. 12: «клік» правою кнопкою маніпулятору типу «миша» на області відображення інформації про МШ, сертифікати та записи журналу реєстрації повідомлень (рис. 5).

Після одержання вікна введення інформації про МШ необхідно змінити потрібні дані у відповідних полях.

У випадку наявності зареєстрованого діючого сертифікату обраного МШ необхідно буде визначитись з питанням: або підтвердити виконані зміни та перевести сертифікат МШ до переліку відізваних, або скасувати зміни.

Видалення запису про МШ

Для видалення даних необхідно відкрити закладку *«Модулі шифрування»*, обрати потрібний запис МШ та скористатись:

- або підпунктом меню *«Робота» > «Видалити»;*
- або інструментом *«Видалення МШ»*;
- або «гарячою» клавішею *«Del»*;
- або підпунктом *«Видалити»* меню, що «вспливає», рис. 12: «клік» правою кнопкою маніпуляторі типу «миша» на області відображення інформації про МШ, сертифікати та записи журналу реєстрації повідомлень (рис. 5).

Після чого необхідно підтвердити факт видалення.

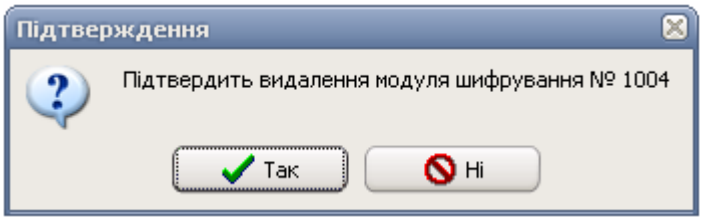


Рис. 14 Запит на підтвердження видалення МШ

Аналіз інформації, що описує МШ

ЦРК надає можливість користувачу виконати наступні операції з даними, що зберігаються в базі даних та описують МШ:

- фільтрування даних за вказаними параметрами;
- сортування даних за вказаними параметрами;
- пошук даних за заданими критеріями.

Рис. 15 Інструменти, призначені для виконання операцій з даними

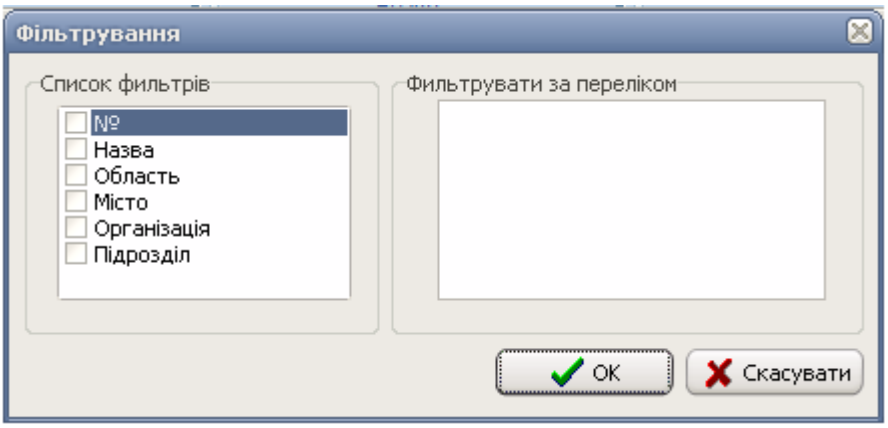
Для виконання всіх зазначених операцій необхідно відкрити закладку *«Модулі шифрування»*.

Фільтрація:

- необхідно відкрити закладку *«Модулі шифрування»*;
- за допомогою кнопки «*Фільтрування записів*» (1 на рис. 15) одержати вікно запиту, рис. 16;
- обрати з переліку один з наступних параметрів фільтрації:
  - *«номер»*: відображення переліку МШ, номери яких відповідають переліку та/або діапазону значень, що введені у полі фільтру;
  - *«назва»:* відображення переліку МШ, назви яких відповідають переліку та/або діапазону значень, що введені у полі фільтру;
  - *«область»:* відображення переліку МШ, що знаходяться в межах обраної області;
  - *«місто»:* відображення переліку МШ, що знаходяться в межах обраного міста;
  - *«організація»:* відображення переліку МШ, що експлуатуються обраною організацією;
  - *«підрозділ»:* відображення переліку МШ, що експлуатуються обраним підрозділом.

Слід зауважити, що фільтрація може бути складною: із використанням одночасно декількох параметрів.

Рис. 16 Вікно з параметрами фільтрації



Сортування:

- необхідно відкрити закладку «*Модулі шифрування*»;
- за допомогою кнопки «*Сортування записів*» (2 на рис. 15) одержати вікно запиту, рис. 17;
- обрати з переліку поле, за даними якого буде виконано сортування. Сортування виконується за наступними полями:
  - «*номер*»;
  - «*назва*»;
  - «*область*»;
  - «*місто*»;
  - «*організація*»;
  - «*підрозділ*».

Для того щоб обрати направлення сортування (за збільшення або за спаданням) необхідно натиснути лівою кнопкою маніпулятора на обраному параметрі. Як результат дії користувач отримує графічне зображення напрямку сортування(рис. 18). Після цієї операції необхідно підтвердити необхідність сортування шляхом натискання кнопки «*ОК*» у вікні (рис. 17).

Рис. 17 Вікно параметрів сортування

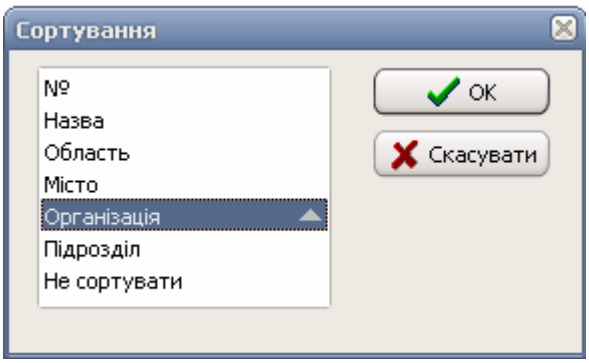
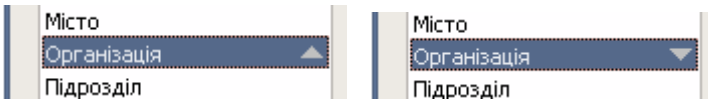


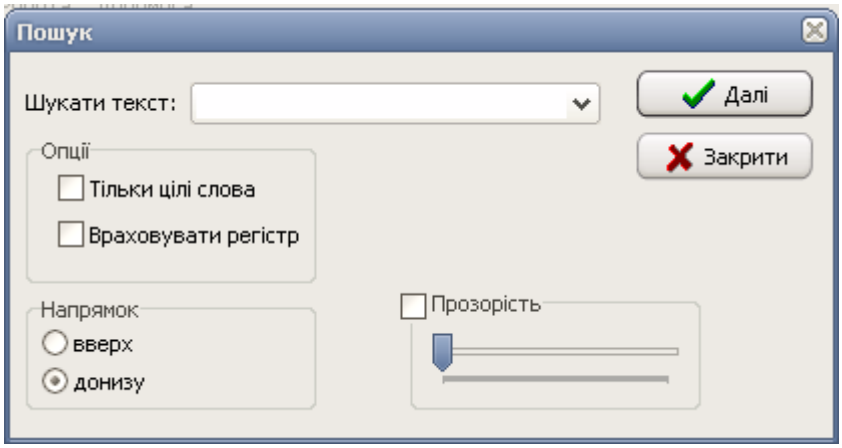
Рис. 18 Приклад напрямків сортування



Пошук виконується по всім інформаційним полям, які містять текстові дані. Для виконання пошуку необхідно

- відкрити закладку «*Модулі шифрування*»;
- за допомогою кнопки «*Пошук записів*» (3 на рис. 15) одержати вікно запиту, рис. 19;
- задати текст, пошук якого виконується в інформаційних полях, що описують сертифікати та натиснути кнопку «*Далі*».

Рис. 19 Вікно введення параметрів пошуку



4.2.5.3 Робота з ключовими даними

Для перегляду переліку зареєстрованих в базі даних ЦРК сертифікатів необхідно відкрити закладку *«Сертифікати».*

- ідентифікаційний номер сертифікату в базі: поле «*№*»;
- тип програмного модулю, для якого сертифікат було сформовано: поле «*Тип*»;
- ідентифікатор відкритого ключа: поле «*Ключ*»;
- ідентифікатор відкритого ключа ЦГК, який використовувався під час формування сертифікату програмного модуля: поле «*Ключ ЦГК*»;
- дата з якої сертифікат дійсний: поле «*Дійсний з*»;
- дата, до якої сертифікат дійсний: поле «*Дійсний до*»;
- поточний статус сертифікату: поле «*Статус*».

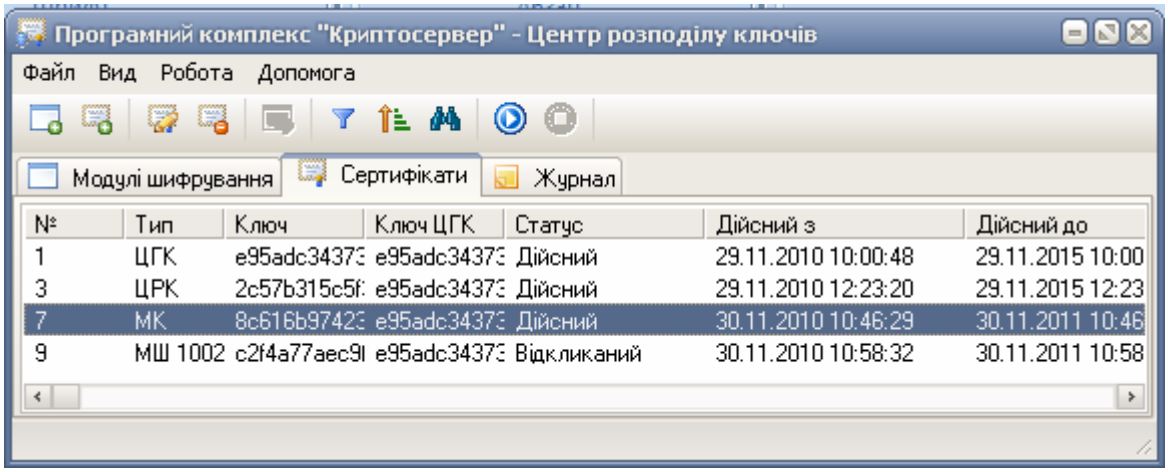


Рис. 20 Закладка *«Сертифікати»*

Імпорт сертифікату ЦГК

Для того, щоб запустити ЦРК до роботи необхідно виконати імпорт сертифікату ЦГК. Для цього потрібно скористатись підпунктом меню *«Файл» > «Імпорт сертифікату ЦГК»* та обрати файл із каталогу, в якому він зберігається. Після цього сертифікат ЦГК буде збережено у базі даних ЦРК.

Після імпорту сертифікату ЦГК стане доступним підпункт меню *«Файл» > «Імпорт ключів OCSP»*, рис. 22.

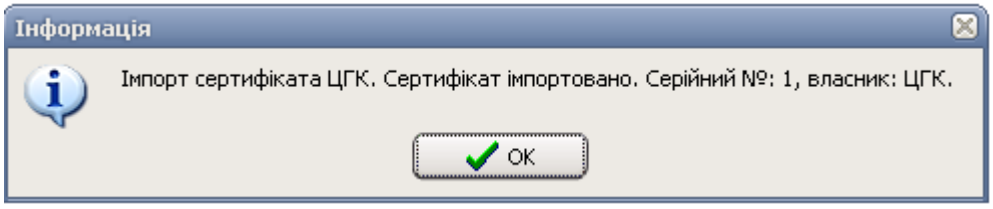


Рис. 21 Повідомлення про імпорт сертифікату ЦГК

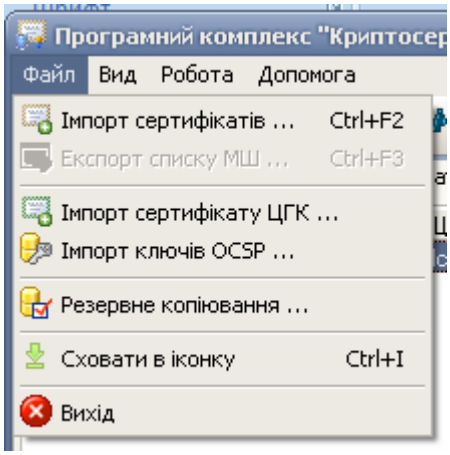


Рис. 22 Приклад пункту меню *«Файл»* після імпорту сертифікату ЦГК

Імпорт ключових даних ЦРК

Для імпорту ключових даних ЦРК необхідно скористатись підпунктом меню *«Файл» > «Імпорт ключів OCSP»* та почергово завантажити файли, які буде запитувати програма. А саме:

- сертифікат ЦРК, файл з розширенням “.crt”;
- файл з секретним ключем, розширення “c.nt”;
- файл даних секретного ключа, розширення “.dat”.

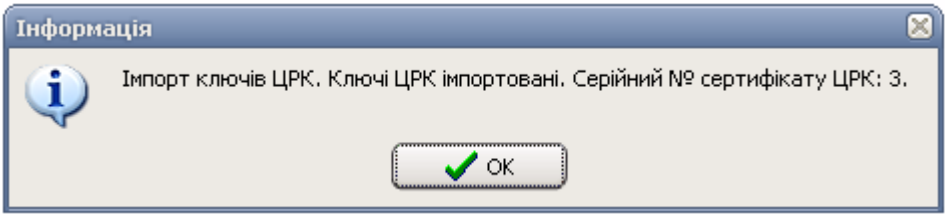


Рис. 23 Повідомлення про імпорт ключових даних ЦРК

Після імпорту ключових даних ЦРК стане доступним підпункт меню *«Файл» > «Імпорт сертифікатів»*, який дозволяє імпортувати сертифікати модулів шифрування та керування.

Імпорт сертифікатів МШ та МК

Для імпорту сертифікатів МШ / МК необхідно скористатись підпунктом меню *«Файл» > «Імпорт сертифікатів»* та почергово завантажити потрібні файли сертифікатів.

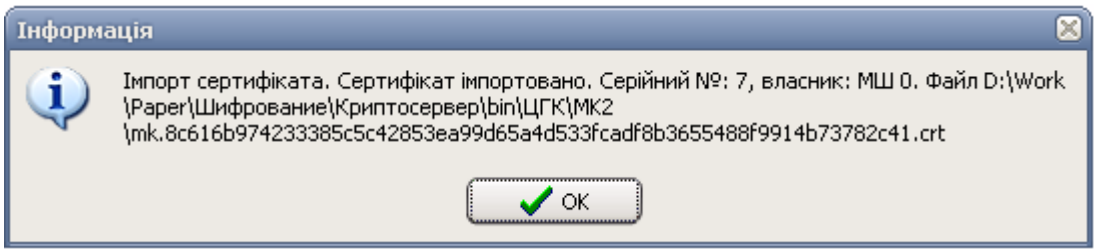


Рис. 24 Повідомлення про імпорт сертифікату МШ

Перегляд детальної інформації про сертифікати

Для перегляду інформації про сертифікат необхідно відкрити закладку *«Сертифікати»*, обрати потрібний запис сертифікат та скористатись:

- або підпунктом меню *«Робота» > «Властивості»;*
- або інструментом *«Перегляд та редагування параметрів сертифікату»*;
- або двічі натиснути лівою кнопку маніпулятору на запису;
- або підпунктом *«Властивості»* меню, що «вспливає».

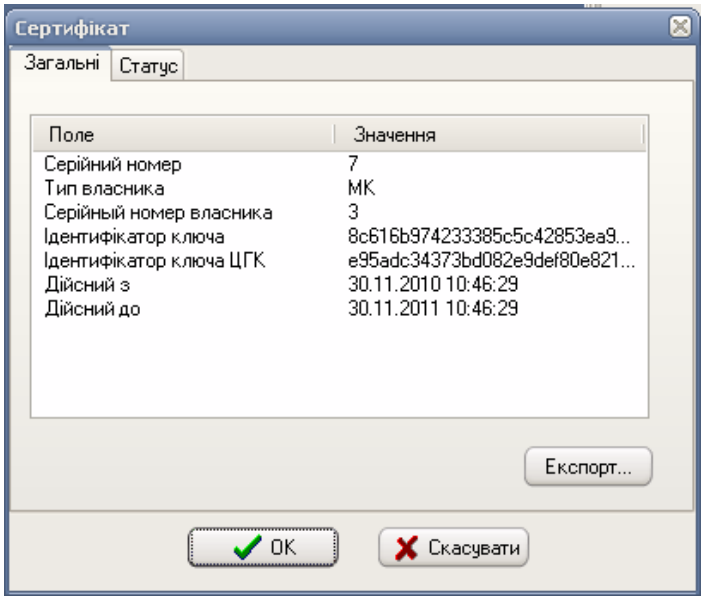


Рис. 25 Приклад вікна з детальною інформацією про сертифікат

Зміна статусу сертифікату

Сертифікат має три типу статусу:

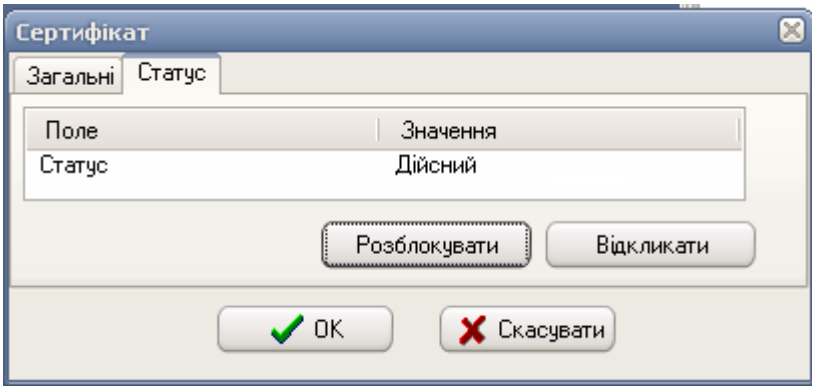
- *дійсний*: сертифікат може використовуватись в процесі створення захищеного зв'язку;
- *заблокований*: сертифікат тимчасово не може використовуватись в процесі створення захищеного зв'язку;
- *відкликаний*: сертифікат не може використовуватись в процесі створення захищеного зв'язку.

Після імпорту сертифікату до бази даних ЦРК він одержує статус «*дійсний*».

Для того, щоби перевести його до іншого статусу необхідно відкрити закладку *«Сертифікати»*, обрати потрібний запис сертифікат та скористатись:

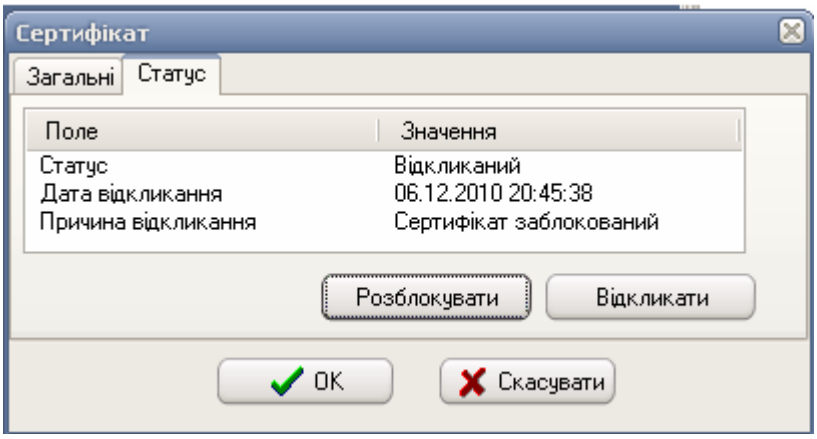
- або підпунктом меню *«Робота» > «Властивості»;*
- або інструментом *«Перегляд та редагування параметрів сертифікату»*;
- або двічі натиснути лівою кнопку маніпулятору на запису;
- або підпунктом *«Властивості»* меню, що «вспливає»;
- одержати доступ до вікна з детальною інформацією про сертифікат (рис. 25);
- відкрити закладку «Статус»;
- за допомогою кнопок «блокувати»/ «відкликати» змінити статус.

Рис. 26 Закладка «Статус»



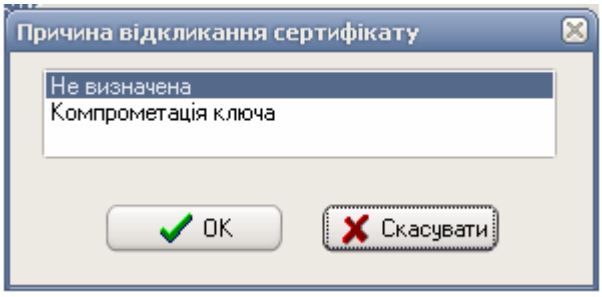
За результатами блокування користувач одержує повідомлення, наведене на рис. 22. Для розблокування сертифікату необхідно скористатись кнопкою «*Розблокувати*», рис. 27.

Рис. 27 Приклад повідомлення про блокування



У випадку відкликання сертифікату надається запит щодо причини такої дії, рис. 28.

Рис. 28 Запит щодо причини відкликання сертифікату



Після обрання причини надається попереднє повідомлення про відкликання сертифікату, а після закриття вікна надається запит про підтвердження виконаних змін.

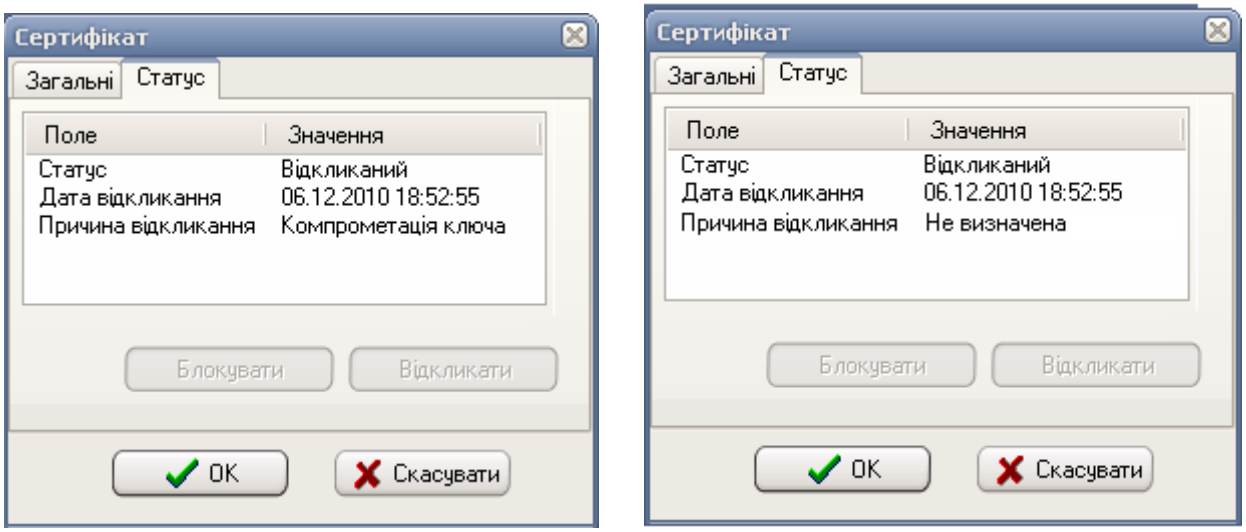


Рис. 29 Попереднє повідомлення про відкликання сертифікатів

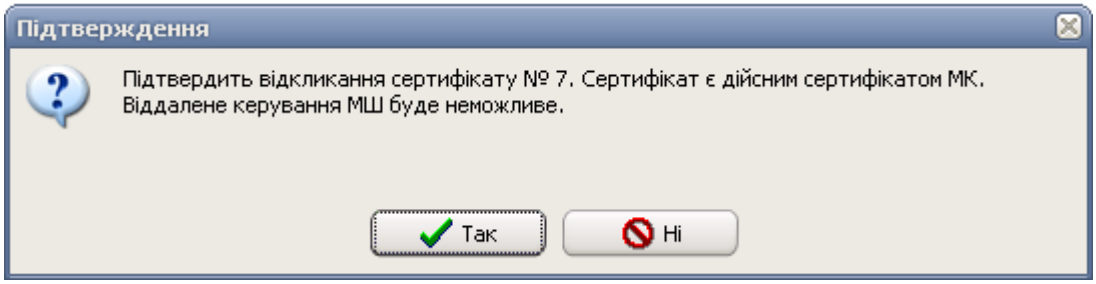


Рис. 30 Запит щодо підтвердження відкликання сертифікату

Крім того, статус сертифікату автоматично змінюється на «відкликаний» у випадку імпорту до бази даних нового сертифікату на один і той же компонент комплексу.

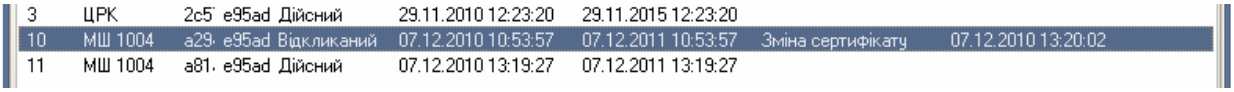


Рис. 31 Приклад повідомлення про зміну статусу сертифікату при імпорті нового сертифікату для цього же компоненту Комплексу

Видалення запису про сертифікат

Для видалення даних необхідно відкрити закладку *«Сертифікати»*, обрати потрібний запис сертифікату та скористатись:

- або підпунктом меню *«Робота» > «Видалити»;*
- або інструментом *«Видалення сертифікату»*;
- або «гарячою» клавішею *«Del»*;
- або підпунктом *«Видалити»* меню, що «вспливає», рис. 12: «клік» правою кнопкою маніпуляторі типу «миша» на області

відображення інформації про МШ, сертифікати та записи журналу реєстрації повідомлень (рис. 5).

Після чого необхідно підтвердити факт видалення.

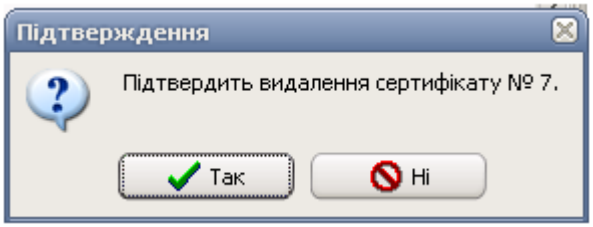


Рис. 32 Запит на підтвердження видалення сертифікату

Експорт сертифікату

Для експорту сертифікату необхідно відкрити закладку *«Сертифікати»*, обрати потрібний запис сертифікату та скористатись:

- або підпунктом меню *«Робота»* > *«Властивості»;*
- або інструментом *«Перегляд та редагування параметрів сертифікату»*;
- або двічі натиснути лівою кнопку маніпулятору на запису;
- або підпунктом *«Властивості»* меню, що «вспливає»;
- натиснути кнопку *«Експорт»* (рис. 25) та зберегти файл сертифікату у потрібне місце.

Аналіз інформації, що описує сертифікати

ЦРК надає можливість користувачу виконати наступні операції з даними, що зберігаються в базі даних та описують сертифікати:

- фільтрування даних за вказаними параметрами;
- сортування даних за вказаними параметрами;
- пошук даних за заданими критеріями.

Рис. 33 Інструменти, призначені для виконання операцій з даними

Для виконання всіх зазначених операцій необхідно відкрити закладку *«Сертифікати».*

Фільтрація:

- необхідно відкрити закладку *«Сертифікати»*;

- за допомогою кнопки «Фільтрування записів» (1 на рис. 33) одержати вікно запиту, рис. 34;
- обрати з переліку один з наступних параметрів фільтрації:
  - *«номер»*: відображення переліку сертифікатів, номери яких відповідають переліку та/або діапазону значень, що введені у полі фільтру;
  - *«тип»:* відображення переліку сертифікатів, які належать вказаному типу компонентів Комплексу (МШ, МК, ЦГК, ЦРК);
  - *«ключ»*: відображення переліку сертифікатів, ідентифікаторів ключа яких відповідають переліку та/або діапазону значень , що введені у полі фільтру;
  - *«ключ ЦГК»:* відображення переліку сертифікатів, для генерації яких використовувався вказаний ключ ЦГК;
  - *«дійсний з»:* відображення переліку сертифікатів початок дії яких попадає до вказаного часового діапазону;
  - *«дійсний до»:* відображення переліку сертифікатів, строк завершення дії яких попадає до вказаного часового діапазону;
  - *«статус»:* відображає перелік сертифікатів з вказаним статусом;
  - *«дата відкликання»*: відображає перелік сертифікатів, дата відкликання яких попадає до вказаного часового діапазону;
  - *«причина відкликання»:* відображає перелік відкликаних сертифікатів, причиною відкликання яких є вказана причина. Можлива фільтрація за наступними причинами:
    - не визначена;
    - компрометація ключа;
    - сертифікат ЦГК відкликаний;
    - зміна даних власника сертифікату;
    - зміна сертифікату;
    - термін дії сертифікату завершений;
    - сертифікат заблокований.
  - *«поточний МШ»:* відображає сертифікат МШ, запис якого на поточний момент обраний в переліку МШ на закладці *«Модулі шифрування».*

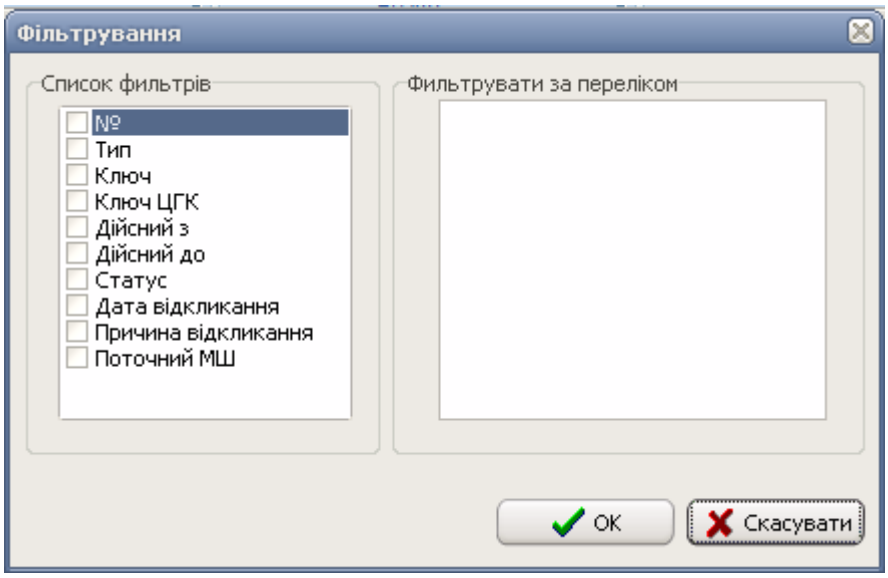


Рис. 34 Вікно з параметрами фільтрації

Сортування:

- необхідно відкрити закладку «*Сертифікати*»;
- за допомогою кнопки «*Сортування записів*» (2 на рис. 33) одержати вікно запиту, рис. 35;
- обрати з переліку поле, за даними якого буде виконано сортування. Сортування виконується за наступними полями:
  - «*номер*»;
  - «*тип*»;
  - «*ключ*»;
  - «*ключ ЦГК*»;
  - «*статус*»;
  - «*дійсний з*»;
  - «*дійсний до*»;
  - «*причина відкликання*»;
  - «*дата відкликання*».

Для того щоб обрати направлення сортування (за збільшення або за спаданням) необхідно натиснути лівою кнопкою маніпулятора на обраному параметрі. Як результат дії користувач отримує графічне зображення напрямку сортування(рис. 36). Після цієї операції необхідно підтвердити необхідність сортування шляхом натискання кнопки «*ОК*» у вікні (рис. 35).

Рис. 35 Вікно параметрів сортування

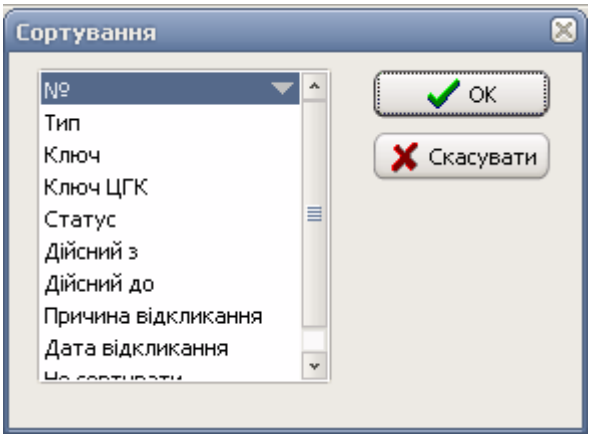
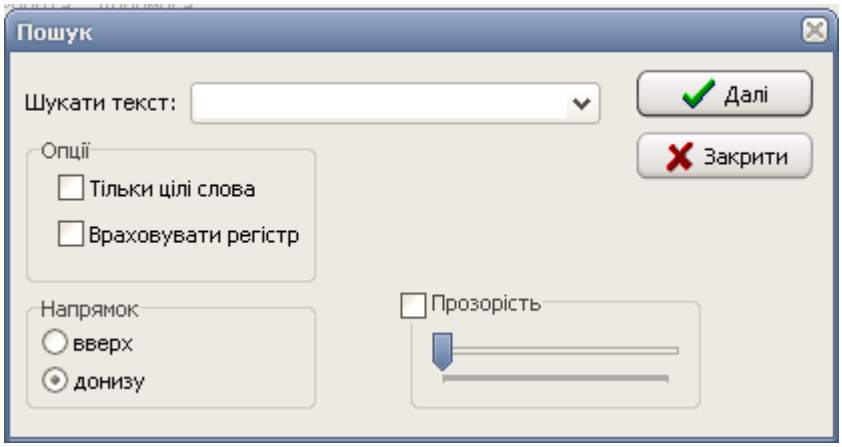


Рис. 36 Приклад напрямків сортування

Пошук виконується по всім інформаційним полям, які містять текстові дані. Для виконання пошуку необхідно

- відкрити закладку «*Сертифікати*»;
- за допомогою кнопки «*Пошук записів*» (3 на рис. 33) одержати вікно запиту, рис. 37;
- задати текст, пошук якого виконується в інформаційних полях, що описують сертифікати та натиснути кнопку «*Далі*».

Рис. 37 Вікно введення параметрів пошуку

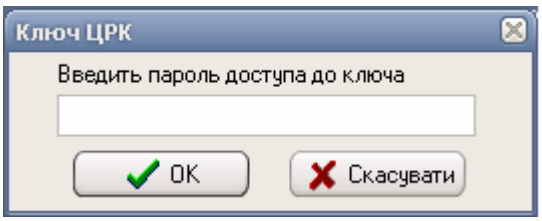


4.2.5.4 Робота ЦРК в режимі «онлайн»

Для того, щоб ЦРК виконував обробку запитів МШ щодо поточного стану сертифікатів, необхідно ініціювати запуск особового режиму роботи ЦРК – режиму роботи «онлайн». Для цього необхідно скористатись або підпунктом меню *«Робота» > «Старт серверу OCSP»*, або інструментом *«Виконати старт серверу»* (розташований на панелі 3, рис. 5).

Після цього необхідно буде ввести пароль доступу до закритого ключа ЦРК, рис. 38.

Рис. 38 Вікно запиту паролю доступу до закритого ключа ЦРК



Після успішного вводу пароля буде активовано заблоковані до цього часу інструмент *«Завершити роботу серверу OCSP»* та підпункт меню *«Робота»* > *«Зупинка серверу OCSP»*, які призначені для припинення роботи ЦРК у режимі «онлайн».

4.2.5.5 Робота з журналами ЦРК

Програма надає користувачу можливість виконати перегляд подій, які були зафіксовані у журналі реєстрації подій.

Перегляд переліку зареєстрованих подій в поточному сеансі роботи

Для того, щоб виконати перегляд подій, зареєстрованих в поточному сеансу програми необхідно відкрити закладку «*Журнали*».

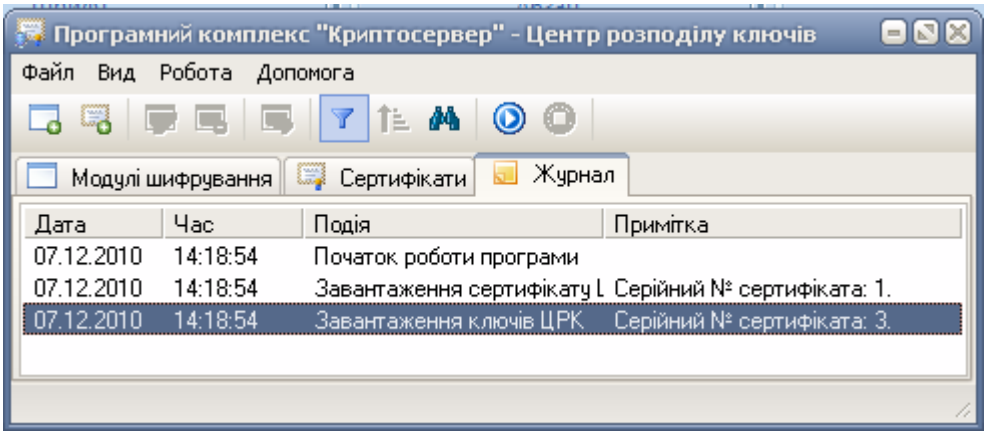


Рис. 39 Закладка «*Журнали*»

Журнал реєстрації подій надає інформацію щодо:

- дати реєстрації події;
- часу реєстрації події;
- опису безпосередньо події;
- примітка, що допомагає більш детально охарактеризувати подію.

Фільтрація подій

Для аналізу подій, що були зареєстровані у журналі необхідно скористатись:

- або підпунктом меню *«Вид»> «Фільтр»;*
- або «гарячими клавішами» Ctrl+Alt+F;
- або інструментом *«Фільтрування записів».*

Як результат користувач одержує доступ до вікна (рис. 40) з наступними параметрами фільтрації:

- «*тип повідомлення*»: дозволяє виконати перегляд подій, які мають один з наведених нижче типів повідомлення:
  - початок роботи програми;
  - завершення роботи програми;
  - збереження резервної копії бази даних;
  - відновлення бази даних з резервної копії;
  - завантаження сертифікату ЦГК;
  - завантаження ключів ЦРК;
  - імпорт ключів ЦРК;
  - старт серверу OCSP;
  - зупинка серверу OCSP;
  - підключення клієнта TCP;
  - відключення клієнта TCP;
  - запит про статус сертифікату;
  - надсилання відповіді про статус сертифікату;
  - реєстрація нового МШ;
  - зміна реквізитів МШ;
  - імпорт сертифікату ЦГК;
  - імпорт сертифікату;
  - формування списку МШ для ЦГК;
  - зміна статусу сертифіката;
  - видалення сертифікату
  - експорт сертифіката;
  - отримані помилкові дані від клієнта;
  - видалення ключів ЦРК.
- «*дата / час*»: відображаються всі події, час реєстрації яких потрапляє до вказаного періоду;

- «*поточний сеанс*»: відображає лише ті події, що були зареєстровані під час поточного сеансу роботи ЦРК. Слід зазначити, що ця опція фільтрації встановлена за замовченням і фільтрація працює з моменту запуску ЦРК.

Крім того, ЦРК надає можливість виконати фільтрацію подій, зареєстрованих в журналі, і комплексно, тобто з урахуванням одночасно обраних декількох параметрів фільтрації.

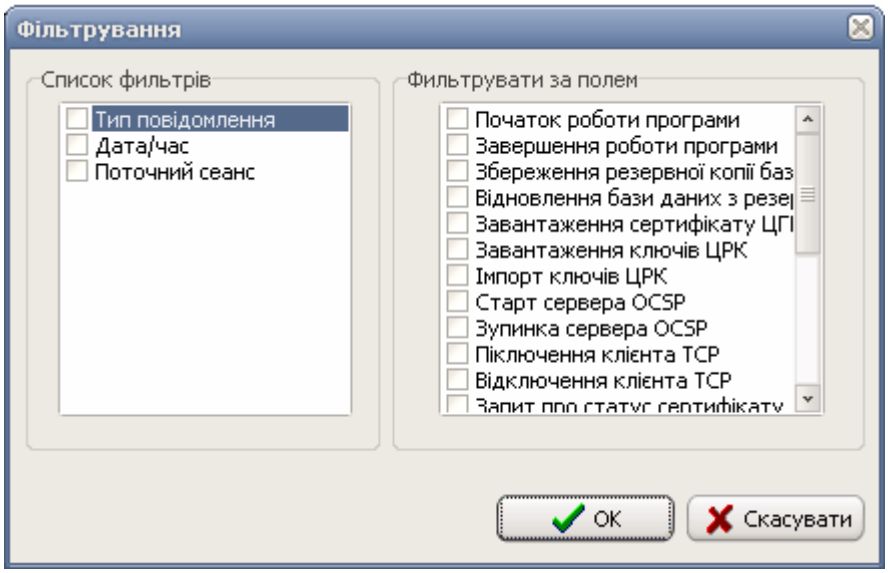


Рис. 40 Вікно з параметрами фільтрації журналу реєстрації подій

Пошук зареєстрованих подій за вказаними критеріями

Пошук виконується по всім інформаційним полям, які містять текстові дані. Для виконання пошуку необхідно

- відкрити закладку «*Журнал*»;
- одержати вікно запиту (рис. 41) за допомогою:
  - або інструменту «*Пошук записів*»;
  - або «гарячих клавіш» Ctrl+F;
  - або підпункту меню «*Вид*»> «*Пошук*»;
- задати текст, пошук якого виконується в інформаційних полях запису журналу реєстрації подій та натиснути кнопку «*Далі*».

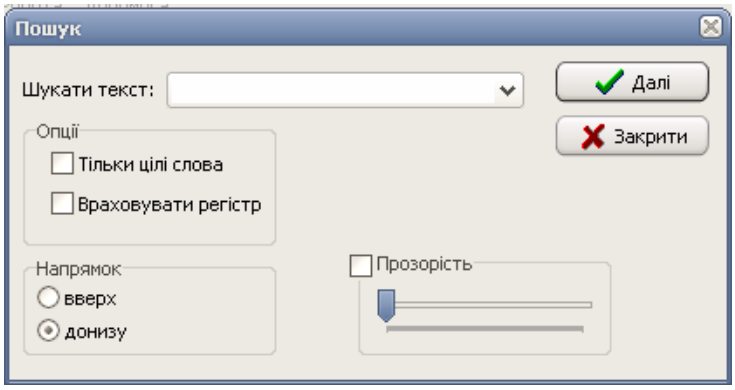


Рис. 41 Вікно введення параметрів пошуку

4.2.5.6 Резервування інформації

Створення резервної копії

Дана операція дозволяє виконати резервне копіювання інформації, яка зберігається у базі даних ЦРК

Для резервного збереження інформації необхідно виконати наступну послідовність дій:

- обрати підпункт меню *«Файл» > «Резервне копіювання»;*
- обрати у вікні, що зображено на рис. 42, необхідні параметри збереження. Надається можливість зберегти інформацію:
  - за командою адміністратора, натиснувши кнопку «*Виконати*», рис 42. За результатом виконання адміністратор одержує повідомлення, наведене на рис. 43;
  - під час запуску ЦРК на виконання;
  - одразу по завершенню роботи ЦРК;
  - за вказаною періодичністю.

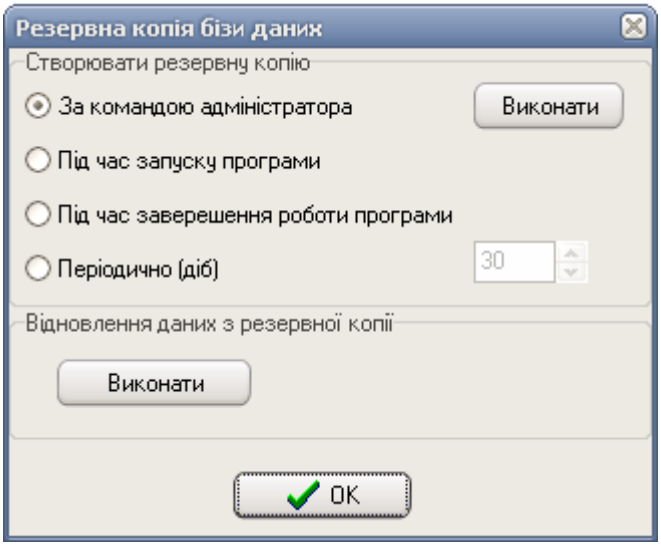


Рис. 42 Вікно вибору параметрів резервування

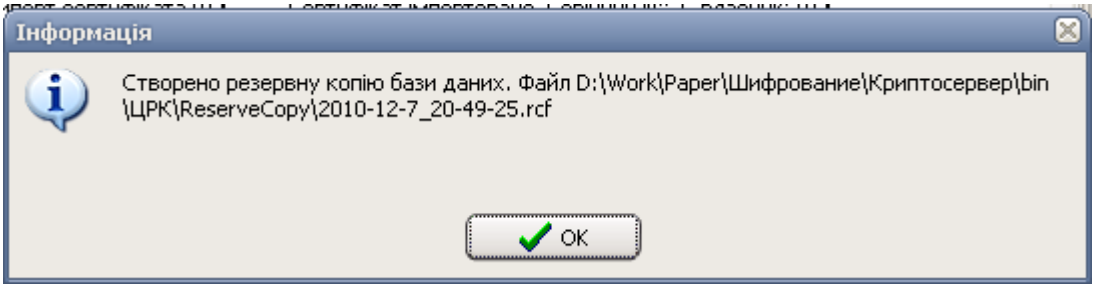


Рис. 43 Приклад повідомлення про створення резервної копії

Відновлення із резервної копії

Дана операція дозволяє виконати відновлення інформації, що зберігалась у базі даних ЦРК, із резервної копії.

Для відновлення інформації необхідно виконати наступну послідовність дій:

- обрати підпункт меню *«Файл» > «Резервне копіювання»;*
- обрати кнопку «*Виконати*» відновлення даних з резервної копії, рис. 42;
- обрати необхідний файл із наданого переліку, рис. 44;
- за результатами операції отримати повідомлення, вказане на рис. 45.

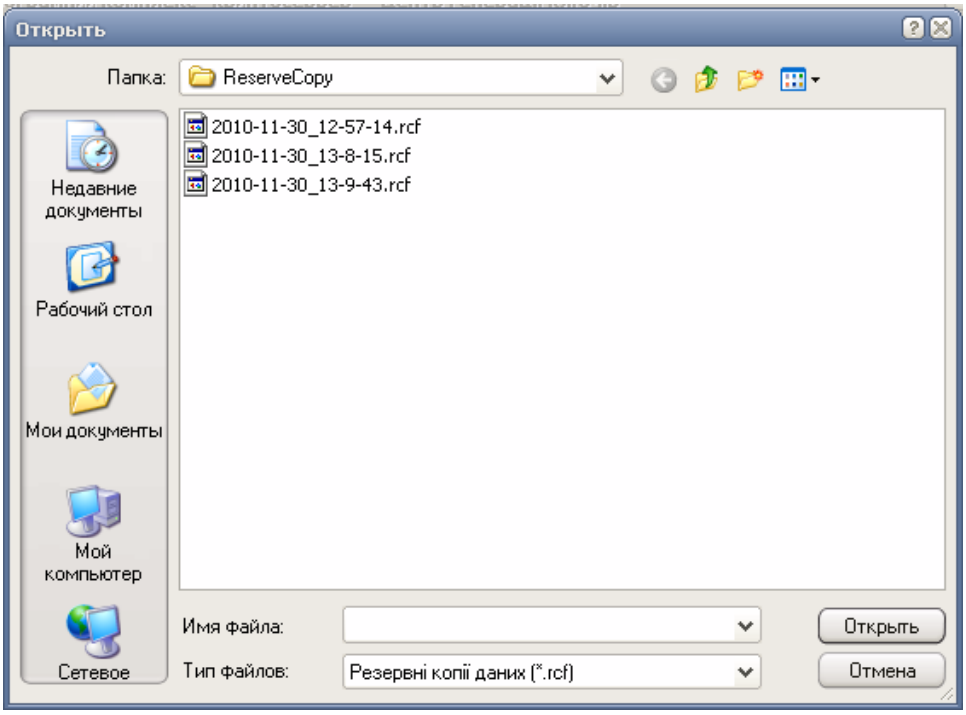


Рис. 44 Вибір файлу, що містить резервну копію даних

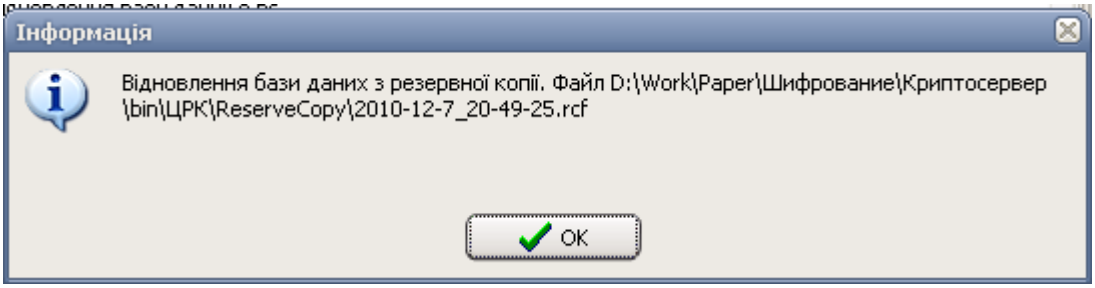


Рис. 45 Повідомлення про відновлення даних

4.2.5.7 Завершення роботи

Для завершення роботи необхідно обрати підменю *«Файл»* > *«Вихід»* після чого необхідно підтвердити запит на завершення роботи.

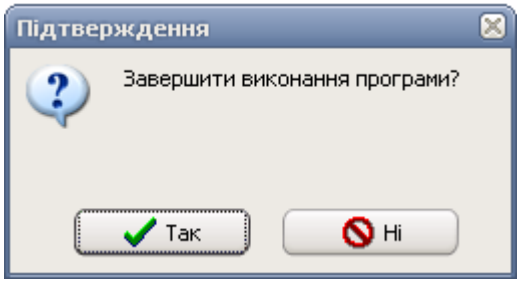


Рис. 46 Запит при завершенні роботи ЦРК

5. УМОВИ ВИКОНАНЯ ПРОГРАМИ

Центр розподілу ключів функціонує на ПЕОМ під керуванням операційних систем Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Vista.

Склад технічних засобів визначається вимогами зазначеної операційної системи.

Вимоги до персоналу не висуваються.

Аркуш реєстрації змін

Номер зміни	Номери сторінок				Усього сторінок після внесення змін	Інформація про знаходження зміни (номер супровідного листа)	Підпис особи, що внесла зміну	Прізвище цієї особи і дата внесення зміни
	замінених	долучених	вилучених	змінених				