Інструкція з інсталяції та налаштування програмного комплекса КЗІ «Криптосервер»

v1.4

Зміст

Загальна інформація і склад комплексу

Програмний комплекс КЗІ «Криптосервер» функціонує під керуванням наступних операційних систем виробництва Microsoft: Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2012 та вище.

Робота комплексу забезпечується СКБД MySQL v.3.28

Комплекс складається з наступних компонентів:

Центр генерації ключів (ЦГК, KGC) - програмний модуль, призначений для генерації закритих (особистих / приватних ключів) і відкритих ключів (ключових даних), а також для запису ключових носіїв інформації (ключових документів) для всіх компонентів Комплексу. Центр генерації ключів рекомендовано встановлювати на комп'ютері, що не має мережевих з'єднань.

Центр розподілу ключів (ЦРК, KDC) - програмний модуль, призначений для зберігання та видачі мережевими каналами довіреним компонентам Комплексу сертифікатів відкритих ключів, інформації про контур безпеки, що визначає учасників захищеної мережі, та іншої службової інформації

Модуль керування (МК) - програмний модуль, призначений для дистанційного керування компонентами Комплексу, такими як ЦРК, МШ.

Модуль шифрування (МШ) - програмний модуль, призначений для побудови захищеної мережі шляхом створення захищених з'єднань із іншими довіреними модулями шифрування. В складі Комплексу передбачено наступні варіанти налаштування модулів шифрування:

- Модуль шифрування в режимі сервер (type=server) очікує підключення від МШ, що працюють в режимі клієнтів, дешифрує та перенаправляє запити від них до вказаного ресурсу
- Модуль шифрування в режимі клієнт (type=client) отримує нешифровані дані, шифрує і надсилає до МШ, що працює в режимі сервера
- Модуль шифрування модуля керування слугує проміжною ланкою між модулем керування та модулями шифрування. Захищає процес отримання налаштувань модулями шифрування від модуля керування

Опис інтерфейсу та конфігураційних файлів компонентів комплексу наведено нижче.

Для швидкого налаштування Комплексу можна одразу переходити до розділів «Інсталяція і налаштування серверної частини Комплексу» та «Створення клієнтських модулів шифрування»

Принцип дії Комплексу описано в розділі «Приклад схеми взаємодії компонентів Комплексу»

Центр генерації ключів

Найменування файлу, що виконується «KeyGenerationCentre.exe»

Параметри ЦГК задаються в файлі «KeyGenerationCentre.ini»

Опис параметрів:

[DB] – В цьому блоці описуються налаштування, необхідні для з`єднання ЦГК з базою даних

Host= IP адреса СКБД

Name= Назва бази даних

ReserveType= Спосіб резервування БД (допустимі значення: **0** – ручний режим, за командою користувача; **1** – під час запуску програми; **3** – періодично, виходячи з налаштувань параметру ReserveDays)

ReserveDays= Період резервування даних в добах (цей параметр використовується, якщо ReserveType=3)

ReserveTime= Дата та час створення останньої копії БД (встановлюється автоматично)

[DefParamsCA] – В цьому блоці задаються значення реквізитів ЦГК за замовченням

CommonName= Назва

StateOrProvinceName= Область

LocalityName=Місто

OrganizationName= Назва організації

OrganizationalUnitName= Підрозділ

[DefParamsKDC] – В цьому блоці задаються значення реквізитів ЦРК за замовченням

CommonName= Назва

StateOrProvinceName= Область

LocalityName= Місто

OrganizationName= Назва організації

OrganizationalUnitName= Підрозділ

[DefParamsMK] – В цьому блоці задаються значення реквізитів МК за замовченням

CommonName= Назва

StateOrProvinceName= Область

LocalityName= Місто

OrganizationName= Назва організації

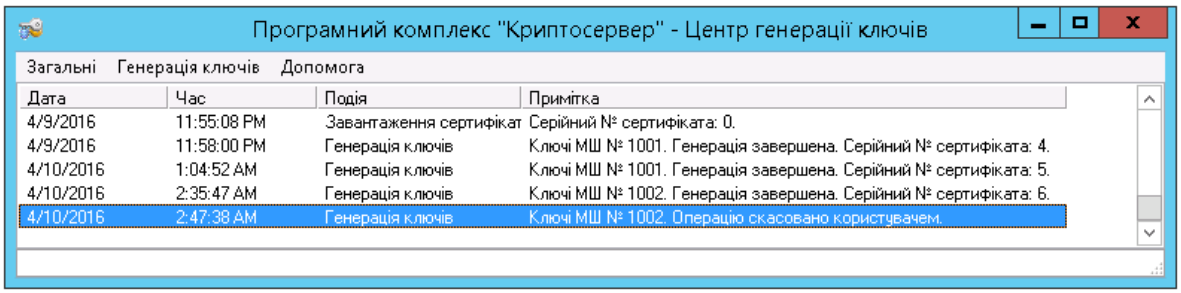
OrganizationalUnitName= Підрозділ

Приклад файлу «KeyDistributionCentre.ini» в разі, якщо СКБД розташована на тому самому ПК, що й ЦГК

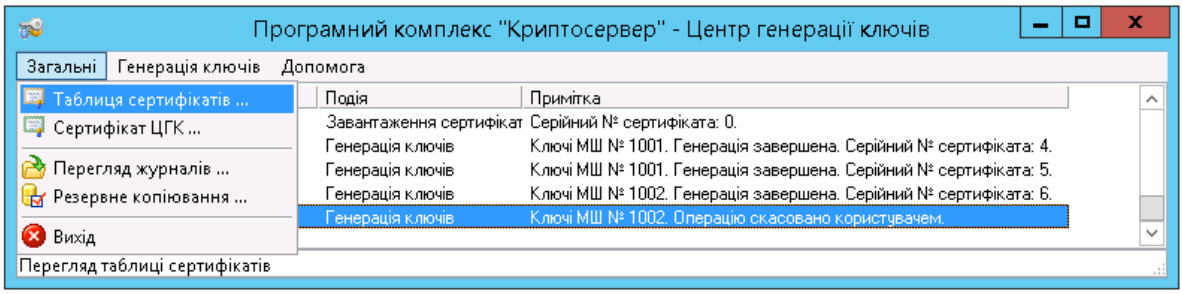
```
[DB]
Host=localhost
Name=CS_CGK
ReserveType=0
ReserveDays=30
ReserveTime=1290395772
[DefParamsCA]
CommonName=ЦГК
StateOrProvinceName=Київська
LocalityName=Київ
OrganizationName=Амбрелла
OrganizationalUnitName=Захист інформації
[DefParamsKDC]
CommonName=ЦРК
StateOrProvinceName=Київська
LocalityName=Київ
OrganizationName= Амбрелла
OrganizationalUnitName=Захист інформації
[DefParamsMK]
CommonName=МК
StateOrProvinceName=Київська
LocalityName=Київ
OrganizationName= Амбрелла
OrganizationalUnitName=Захист інформації
```

Опис інтерфейсу ЦГК

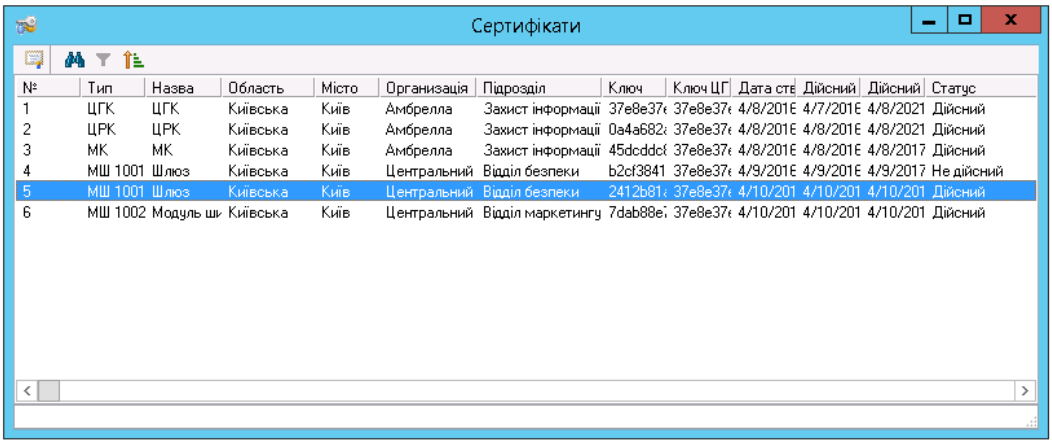
В головному вікні програми відображуються поточні події

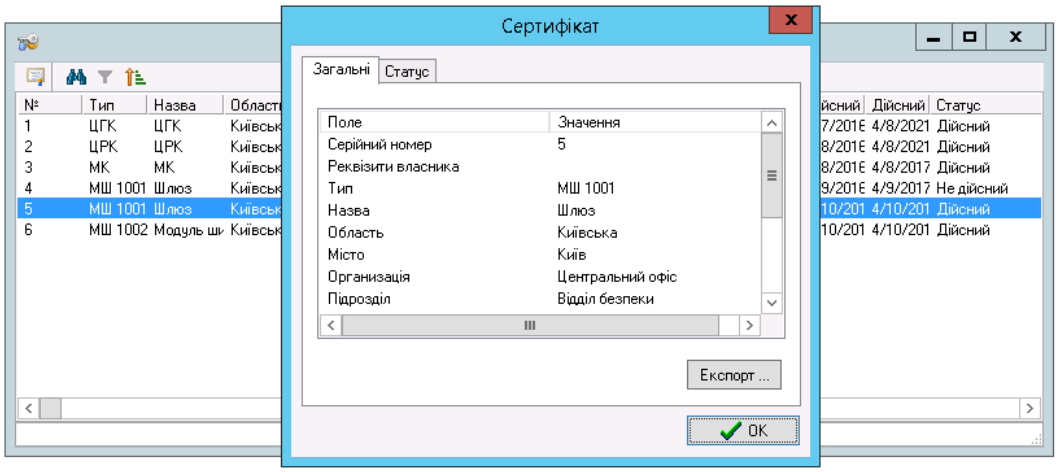


Пункт меню «Загальні», підпункт «Таблиця сертифікатів…» - перелік сертифікатів, згенерованих ЦГК

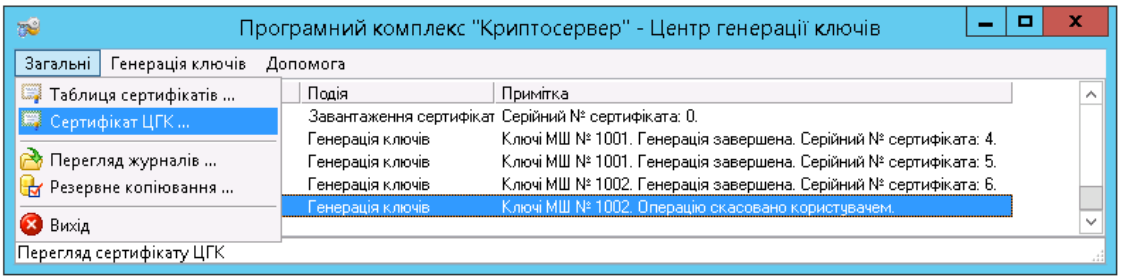


Вікно «Сертифікати» містить перелік сертифікатів і дозволяє здійснити пошук, сортування, отримати детальну інформацію по обраному сертифікату

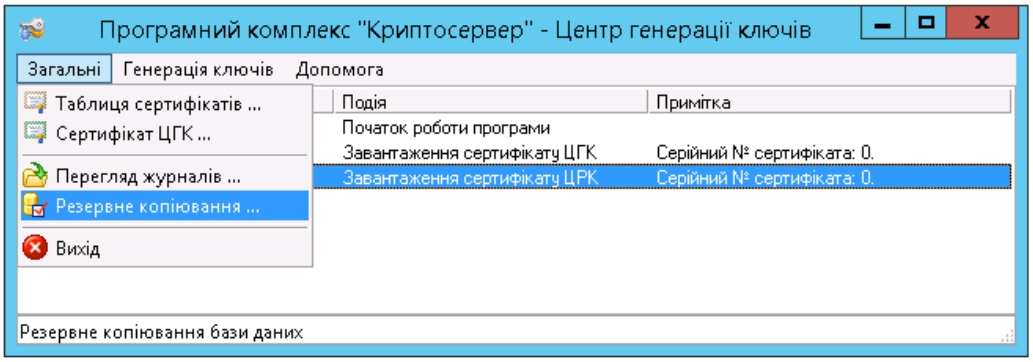


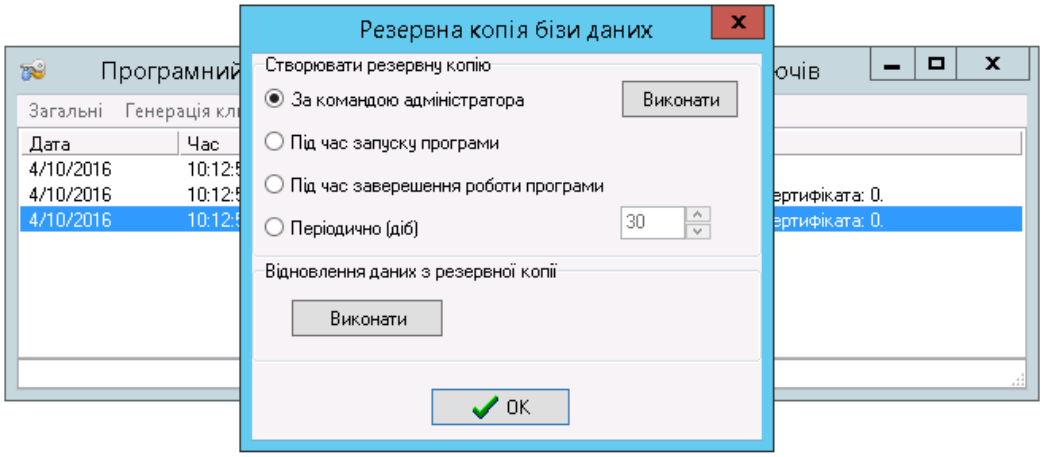


Пункт меню «Загальні», підпункт «Сертифікат ЦГК…» - детальна інформація про сертифікат ЦГК

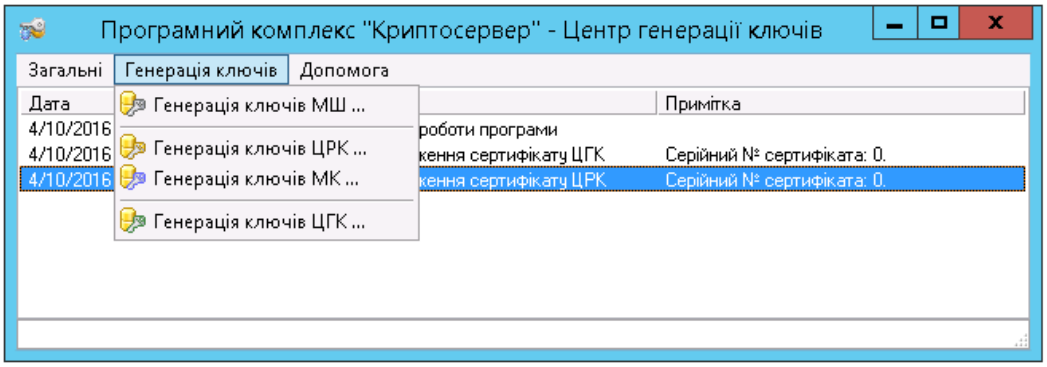


Пункт меню «Загальні», підпункт «Резервне копіювання…» - налаштування резервування бази даних





Пункт меню «Генерація ключів», підпункти «Генерація ключів ЦГК…», «Генерація ключів ЦРК…»,«Генерація ключів МК…»,«Генерація ключів МШ…» - опис буде наведено в розділі «Інсталяція і налаштування серверної частини Комплексу».



Центр розподілу ключів

Найменування файлу, що виконується «KeyDistributionCentre.exe»

Параметри ЦРК задаються в файлі «KeyDistributionCentre.ini»

Опис параметрів:

[DB] – В цьому блоці описуються налаштування, необхідні для з`єднання ЦРК з базою даних

Host= IP адреса СКБД

Name= Назва бази даних

ReserveType= Спосіб резервування БД (допустимі значення: **0** – ручний режим, за командою користувача; **1** – під час запуску програми; **3** – періодично, виходячи з налаштувань параметру ReserveDays)

ReserveDays= Період резервування даних в добах (цей параметр використовується, якщо ReserveType=3)

ReserveTime= Дата та час створення останньої копії БД (встановлюється автоматично)

[Server] – В цьому блоці описуються налаштування, необхідні для з`єднання ЦРК з іншими компонентами Комплексу

Port= Порт по якому буде проходити з`єднання ЦРК з іншими компонентами Комплексу

pass= Пароль до секретного ключа ЦРК

AutoStart= Стартувати сервер ЦРК після запуску модуля ЦРК (**0** – Ні; **1** – Так)

[Form] – В цьому блоці описується розташування та розмір вікна модуля ЦРК на робочому столі ПК, параметри змінюються програмою автоматично

Width=

Height=

Left=

Top=

Приклад файлу «KeyDistributionCentre.ini» в разі, якщо СКБД розташована на тому самому ПК, що й ЦРК

[DB]

Host=localhost

Name=CS

ReserveType=0

ReserveDays=30

ReserveTime=1303404912

[Server]

Port=10001

pass=

AutoStart=1

[Form]

Width=724

Height=415

Left=284

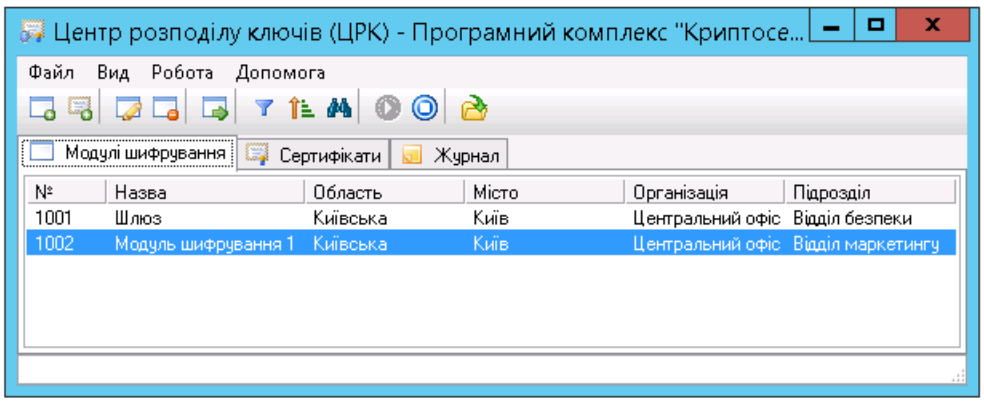
Top=376

Опис інтерфейсу ЦРК

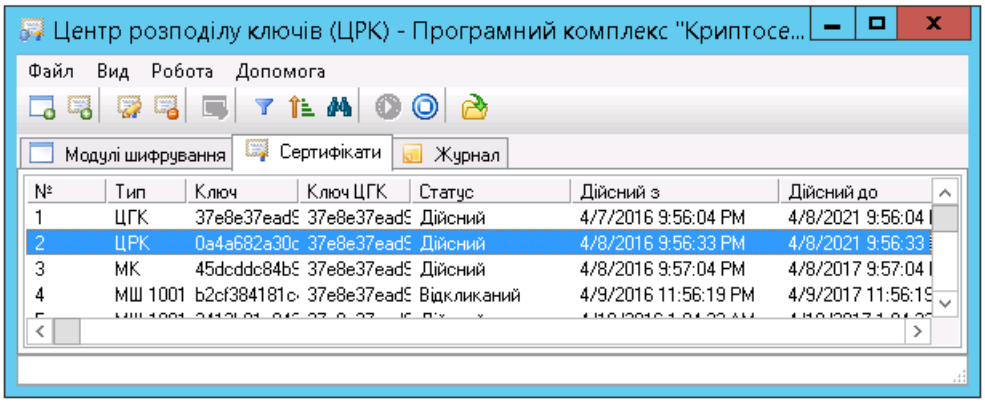
В головному вікні модуля відображуються :

- панель меню
- панель інструментів
- закладки: «Модулі шифрування», «Сертифікати», «Журнал».

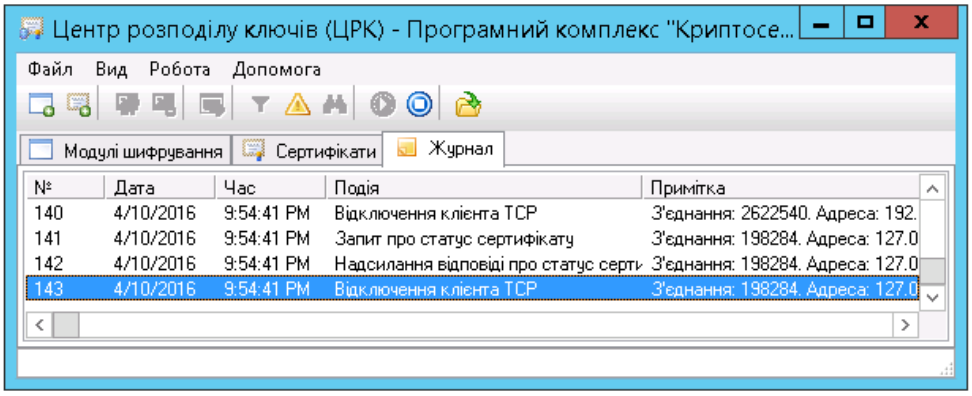
На закладці «Модулі шифрування» відображені модулі шифрування, налаштовані в ЦРК



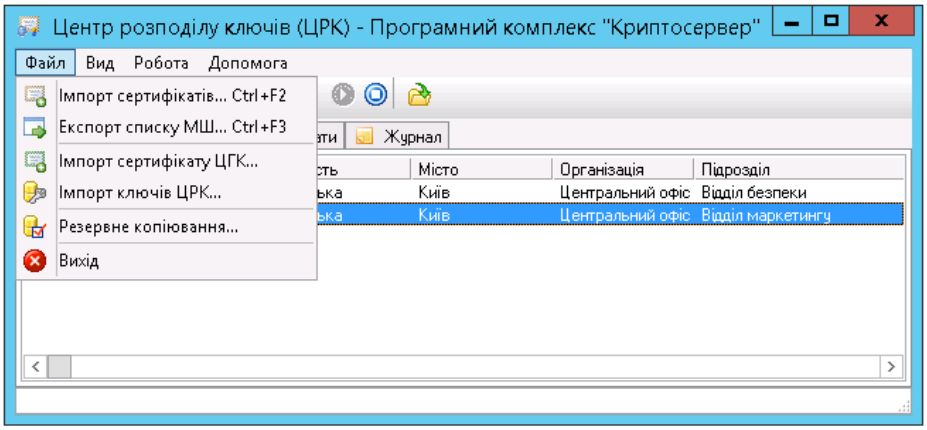
На закладці «Сертифікати» відображені сертифікати, що імпортовані до ЦРК



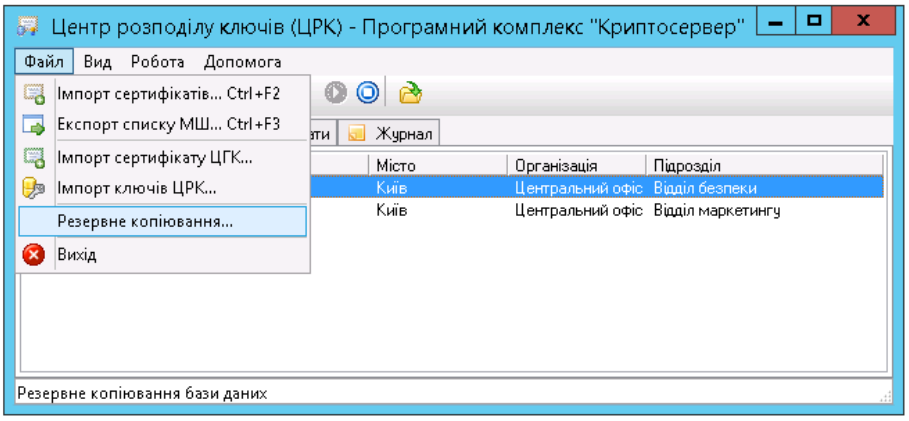
На закладці «Журнал» відображений журнал поточних подій

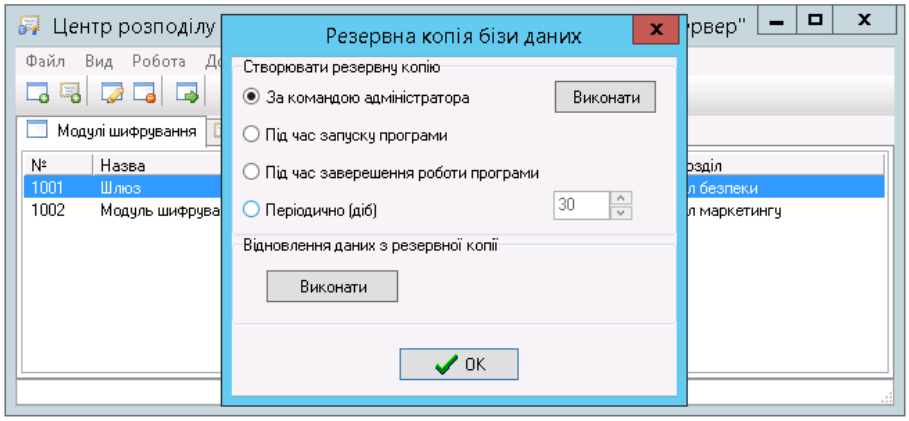


Пункт меню «Файл», підпункти «Імпорт сертифікатів…», «Експорт списку МШ…», «Імпорт сертифікату ЦГК…», «Імпорт ключів ЦРК…» - опис буде наведено в розділі «Інсталяція і налаштування серверної частини Комплексу».

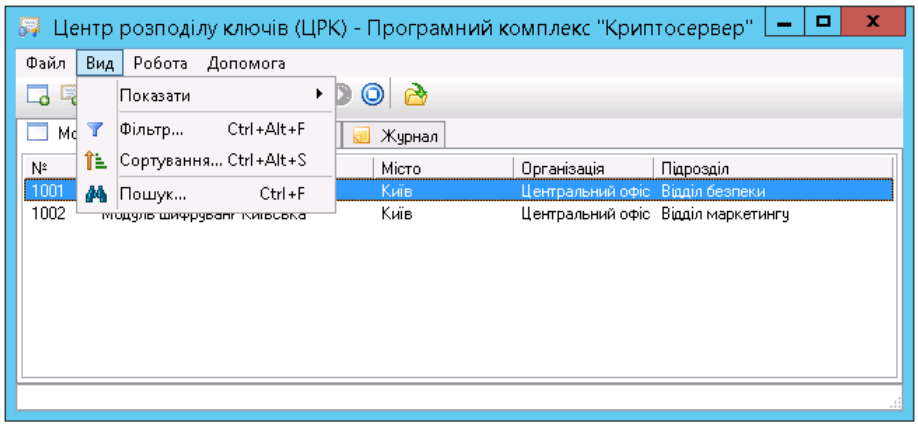


Пункт меню «Файл», підпункт «Резервне копіювання…» - налаштування резервування бази даних



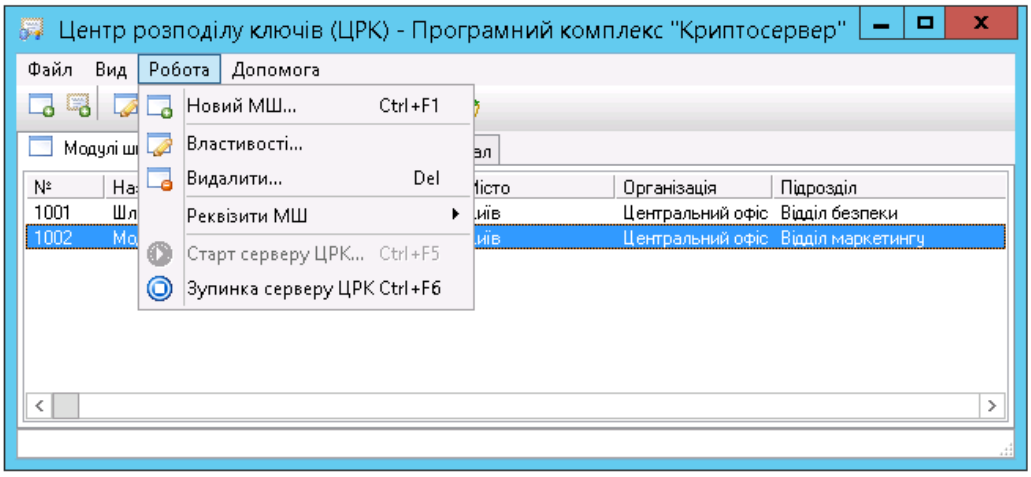


Пункт меню «Вид» - налаштування виду, фільтрація, сортування і пошук на активній закладці



Пункт меню «Робота»:

- Підпункт «Новий МШ…» - створення нового МШ
- Підпункт «Властивості…» - властивості виділеного на закладці МШ або сертифікату
- Підпункт «Видалити…» - видалення виділеного на закладці МШ або сертифікату
- Підпункт «Реквізити МШ» - словник реквізитів МШ
- Підпункти «Старт серверу ЦРК…»/«Зупинка серверу ЦРК» - відповідно старт/зупинка серверу ЦРК



Панель інструментів дублює функції, наявні в меню інструментів, окрім пункту «Відкрити файл журналу для перегляду»  -дозволяє завантажити файли журналів подій, що за замовченням зберігаються в каталозі «Logs»

Модуль керування

Модуль керування складається з двох частин:

- Модуль керування - МК (найменування файлу, що виконується «МК.exe») забезпечує реалізацію механізмів керування модулями шифрування Комплексу.

- Модуль шифрування модуля керування - МШМК(найменування файлу, що виконується «CryptoServer.exe») відповідає за реалізацію сеансів захищеного зв'язку модуля керування з модулями шифрування Комплексу.

Налаштування модуля керування

Параметри МК задаються в файлі «МК.ini»

Опис параметрів:

[DB] – В цьому блоці описуються налаштування, необхідні для з`єднання МК з базою даних

Host= IP адреса СКБД

Name= Назва бази даних

ReserveType= Спосіб резервування БД (допустимі значення: **0** – ручний режим, за командою користувача; **1** – під час запуску програми; **3** – періодично, виходячи з налаштувань параметру ReserveDays)

ReserveDays= Період резервування даних в добах (цей параметр використовується, якщо ReserveType=3)

ReserveTime= Дата та час створення останньої копії БД (встановлюється автоматично)

CleanupLogExpireDays=

CleanupLogMsgCodes=

ReloadAll= час синхронізації МК с СКБД (значення вказується у секундах)

[Server] – В цьому блоці описуються налаштування, необхідні для з`єднання МК з іншими компонентами Комплексу

Port= Порт по якому буде проходити з`єднання модуля керування з робочим модулем шифрування

AutoStart= Стартувати сервер ЦРК після запуску модуля МК (**0** – Ні; **1** – Так)

[Info] – Блок налаштувань взаємодії МК з ЦРК та МШ

MKPort= номер порту, по якому забезпечується взаємодія модуля керування та модулів шифрування

OCSPPort= номер порту, по якому забезпечується взаємодія модуля керування та ЦРК

[Form] – В цьому блоці описується розташування та розмір вікна модуля ЦРК на робочому столі ПК, параметри змінюються програмою автоматично

Width=

Height=

Left=

Top=

Приклад файлу «МК.ini» в разі, якщо СКБД розташована на тому самому ПК, що й МК

[DB]

Host=localhost

Name=CS

ReserveDays=26

ReserveType=0

ReloadAll=5

ReserveTime=1318328114

CleanupLogExpireDays=1

CleanupLogMsgCodes=159;160;161;162;163;164;165;201;202;203;204

[Server]

Port=10003

AutoStart=1

[Info]

MKPort=10002

OCSPPort=10001

[Form]

Width=619

Height=463

Left=327

Top=354

Налаштування модуля шифрування модуля керування (МШ МК)

Параметри МШМК задаються в файлі «CryptoServer.ini»

Опис параметрів:

[common] – Блок загальних параметрів

cacertfile= Назва файлу, який містить сертифікат ЦГК

certdir= Найменування каталогу, який містить сертифікати (локальна база сертифікатів)

certfile=Назва файлу сертифіката МК

contfile= Назва файлу-контейнера МК

dkefile= Назва файлу, який містить довгостроковий ключовий елемент (ДКЕ) МК

keysdir= Найменування каталогу, в якому зберігаються ключові дані

sid= Ідентифікаційний номер модуля шифрування модуля керування в структурі комплексу (значення за замовченням «**3**»)

pass= Пароль до секретного ключа МК

logdir= Найменування каталогу, який містить журнали повідомлень

[ocsp] – В цьому блоці описуються налаштування, необхідні для з`єднання МШМК з сервером ЦРК

certfile= назва файлу, який містить сертифікат ЦРК

addr= IP адреса ПК, на якому встановлено ЦРК

port= номер порту, по якому забезпечується взаємодія МШМК з сервером ЦРК

[link1] – В цьому блоці задаються параметри відкритого з`єднання МШМК з МК, та захищених з`єднань МШМК з іншими модулями шифрування

id= ідентифікаційний номер з`єднання (значення за замовченням «**1**», не рекомендується змінювати)

inp_port= номер порту для створення захищених з`єднань МШМК з іншими модулями шифрування

out_addr= IP адреса ПК, на якому встановлений МК

out_port= номер порту для створення відкритих з`єднань МШМК з МК

sid= ідентифікаційний номер МШМК (значення за замовченням «**3**», не рекомендується змінювати)

type= тип з`єднання (в нашому випадку значення цього параметру - «**server**»)

Приклад файлу «CryptoServer.ini»

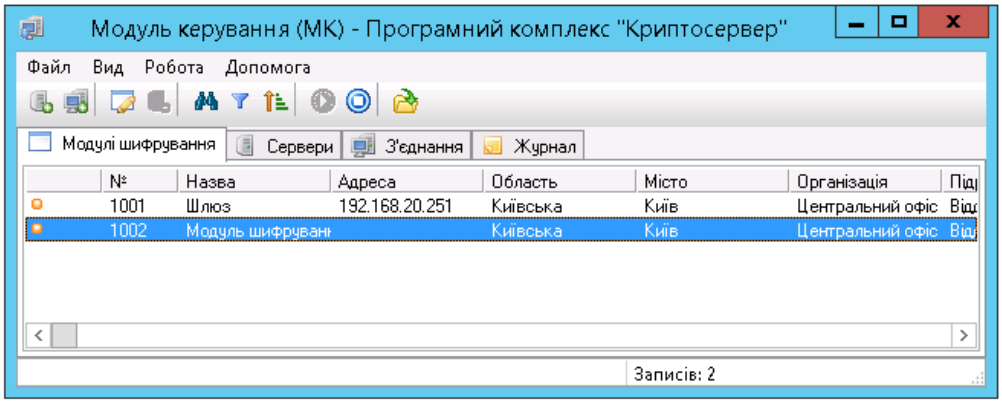
```
[common]
cacertfile=ca.edbca3977ab695494f8ab67fa7e73ea7e4ce33250d7616f8e7a72ca4458348be.crt
certdir=cert_db
certfile=mk.24c47cfec47e90ae9ea5d7891016269f20398ebdb87d9785df553e3367d3818d.crt
contfile=mk.24c47cfec47e90ae9ea5d7891016269f20398ebdb87d9785df553e3367d3818d.cnt
dkefile=mk.24c47cfec47e90ae9ea5d7891016269f20398ebdb87d9785df553e3367d3818d.dke
keysdir=keys
sid=3
pass=
logdir=LogsCS

[ocsp]
certfile=ocsp.39e44d852b55cfe64b922373c05df35a7995ab8600bd720810f8bcfcd6385953.crt
addr=127.0.0.1
port=10001

[link1]
id=1
inp_port=10002
out_addr=127.0.0.1
out_port=10003
sid=3
type=server
```

Опис інтерфейсу модуля керування

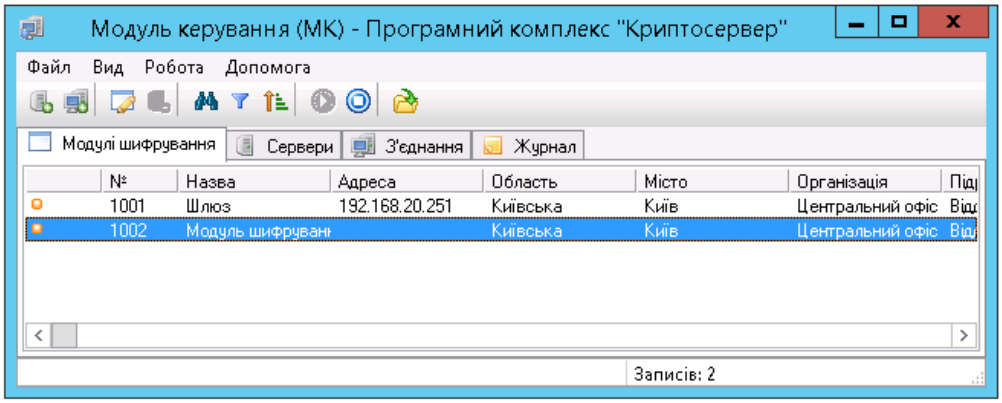
В головному вікні модуля відображуються :

- панель меню
- панель інструментів

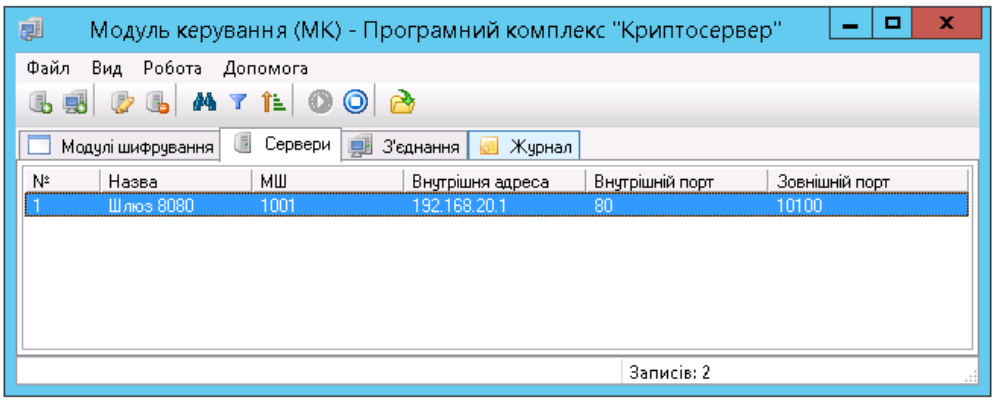
- закладки: «Модулі шифрування», «Сервери», «З`єднання», «Журнал».



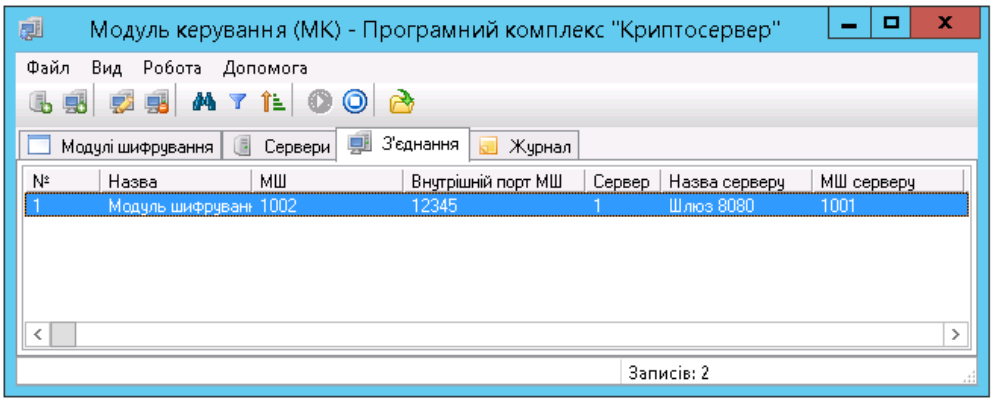
На закладці «Модулі шифрування» відображуються модулі шифрування. Активні модулі шифрування позначаються -



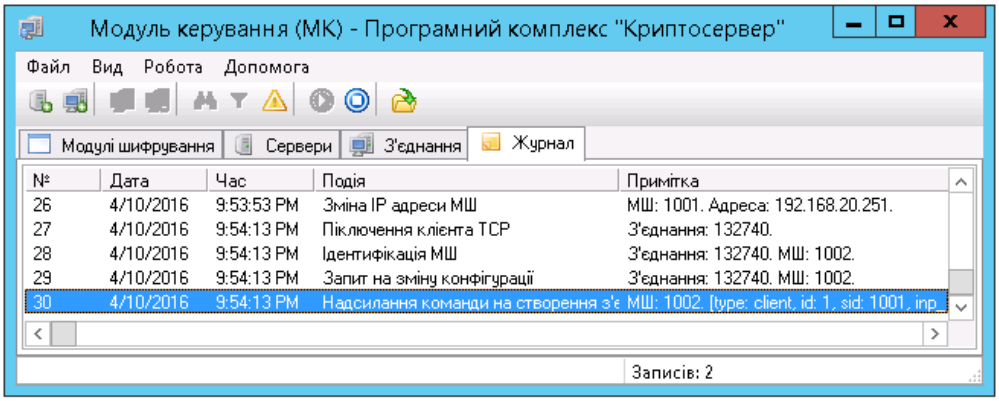
На закладці «Сервери» відображується налаштування серверів МШ



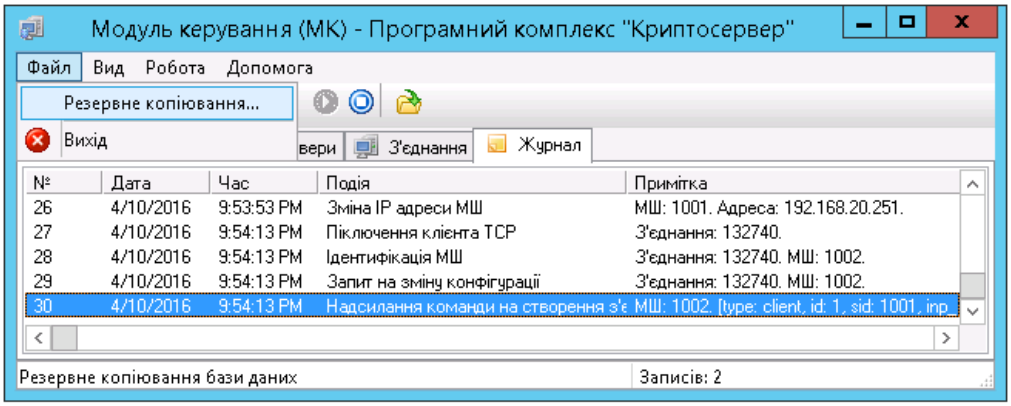
На закладці «З`єднання» відображується налаштування клієнтських МШ

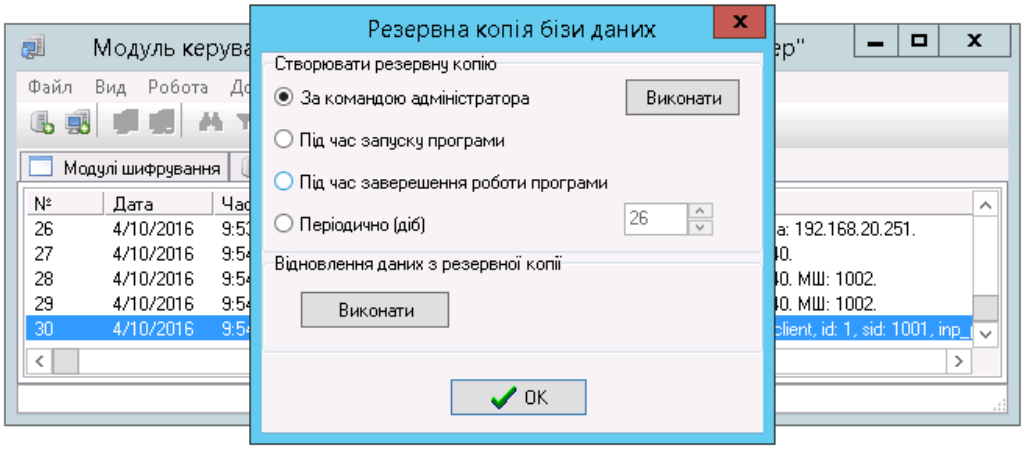


На закладці «Журнал» відображений журнал поточних подій

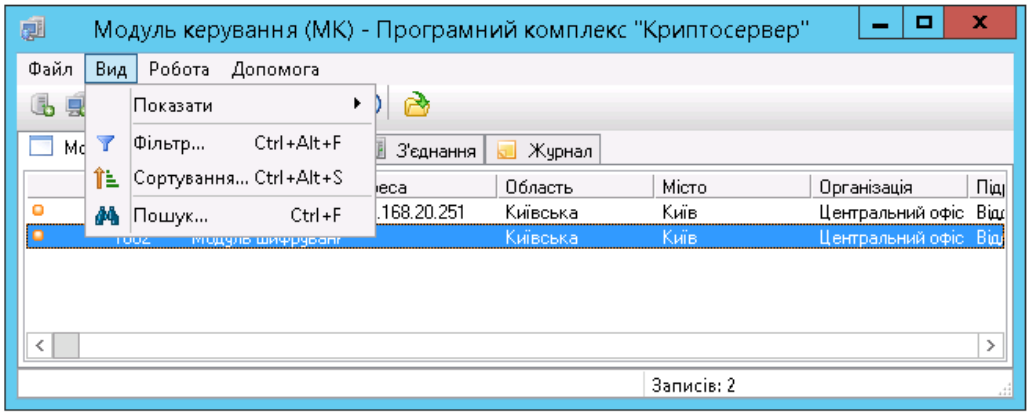


Пункт меню «Файл» підпункт «Резервне копіювання…» - налаштування резервування бази даних



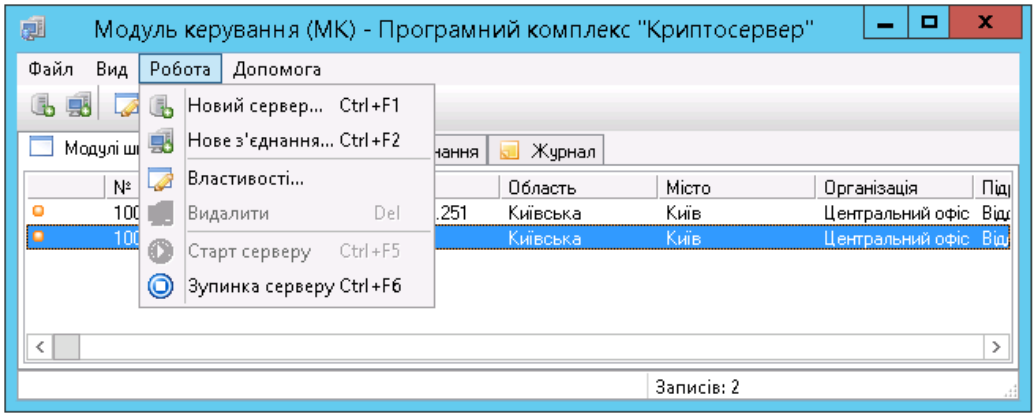


Пункт меню «Вид» - налаштування виду, фільтрація, сортування і пошук на активній закладці



Пункт меню «Робота»:

- Підпункт «Новий сервер…» - створення нового сервера
- Підпункт «нове з`єднання…» - створення нового з`єднання
- Підпункт «Властивості…» - властивості модуля шифрування, сервера або з`єднання
- Підпункт «Видалити» - видалення сервера або з`єднання
- Підпункти «Старт серверу» /«Зупинка серверу» - відповідно старт/зупинка серверу МК



Панель інструментів дублює функції, наявні в меню інструментів, окрім пункту «Відкрити файл журналу для перегляду»  -дозволяє завантажити файли журналів подій, що за замовченням зберігаються в каталозі «Logs»

Модуль шифрування

Найменування файлу, що виконується «CryptoServer.exe»

Параметри МШ задаються в файлі «CryptoServer.ini»

Опис параметрів:

[common] - В цьому блоці задаються значення загальних параметрів

cacertfile= Назва файлу, який містить сертифікат ЦГК

certdir= Найменування каталогу, який містить сертифікати (локальна база сертифікатів)

certfile=Назва файлу сертифіката МШ

contfile= Назва файлу-контейнера МШ

dkefile= Назва файлу, який містить довгостроковий ключовий елемент (ДКЕ) МК

keysdir= Найменування каталогу, в якому зберігаються ключові дані

sid= Ідентифікаційний номер модуля шифрування в структурі комплексу

logdir= Найменування каталогу, який містить журнали повідомлень

maxthreads= Максимальна кількість клієнтських підключень

pass= Пароль до секретного ключа МШ

[ocsp] – В цьому блоці описуються налаштування, необхідні для з`єднання МШ з сервером ЦРК

certfile= назва файлу, який містить сертифікат ЦРК

addr= адреса ПК, на якому встановлено ЦРК

port= номер порту, по якому забезпечується взаємодія МШ з сервером ЦРК

[mk] - В цьому блоці описуються налаштування, необхідні для з`єднання МШ з МК

addr= IP адреса ПК, на якому встановлено МК

port= номер порту, по якому забезпечується взаємодія МШ з МК

sid= ідентифікатор МК

restart= Періодичність спроб підключення до МК у мілісекундах (за замовченням дорівнює 20000мс)

[linkx] (x – ціле число) – блоки, що задають значення з`єднань, які необхідно захищати. ini-файл може містити декілька таких блоків, наприклад: [link1], [link2], [link3] **Важливо:** ці блоки формуються налаштуваннями серверів і з`єднань в модулі керування, тому нема потреби

заповнювати їх в ручному режимі. Після запуску модуль шифрування підключиться до модуля керування, завантажить ті налаштування, що відносяться до нього і збереже їх в файл конфігурації.

id= ідентифікаційний параметр з`єднання

sid = ідентифікаційний номер МШ, яким здійснюється з'єднання (використовується, якщо параметр **type= client**)

type= тип з`єднання (параметр може мати наступні значення: «**client**» - МШ виконує роль клієнта під час з`єднання, «**server**» - МШ виконує роль сервера під час з`єднання)

inp_port= номер порту, який «слухає» МШ: дані одержані з цього порту вважаються вхідними

out_addr= IP адреса, на яку будуть перенаправлені вхідні дані. В разі, якщо параметр **type= client**, це буде адреса модуля шифрування, до якого будуть надіслані зашифровані вхідні дані. В разі, якщо параметр **type= server**, це буде адреса на яку буде надіслано дешифровані вхідні дані (IP адреса ресурсу, до якого ми забезпечуємо захищений доступ).

out_port= номер порту, на який буде перенаправлено вхідні дані

Приклад файлу «CryptoServer.ini» МШ налаштованого як клієнт:

```
[common]
cacertfile=ca.9c73ea41ab4e9aab1ef124d5aeb4bee52887a8069a39fea7b7e7b70527332833.crt
certdir=cert_db
certfile=1003.b91dc99418a76c806a7dcdbbd5a7c7cd6f3c53b4e208acdffcf6bea7f77ec0f4.crt
contfile=1003.b91dc99418a76c806a7dcdbbd5a7c7cd6f3c53b4e208acdffcf6bea7f77ec0f4.cnt
dkefile=1003.b91dc99418a76c806a7dcdbbd5a7c7cd6f3c53b4e208acdffcf6bea7f77ec0f4.dke
keysdir=keys
pass=
sid=1003

[ocsp]
certfile=ocsp.39e44d852b55cfe64b922373c05df35a7995ab8600bd720810f8bcfcd6385953.crt
addr=192.168.20.251
port=10001

[mk]
addr=192.168.20.251
port=10002
```

sid=3

[link1]

id=1

inp_port=13128

out_addr=192.168.20.251

out_port=10011

sid=1002

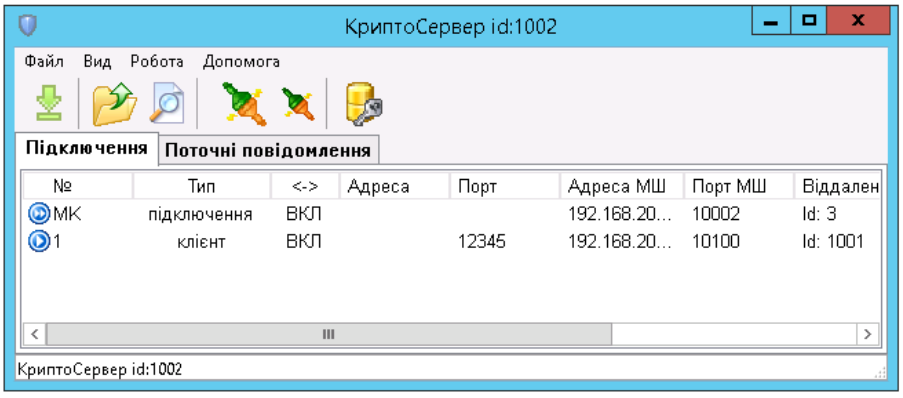
type=client

Опис інтерфейсу модуля шифрування

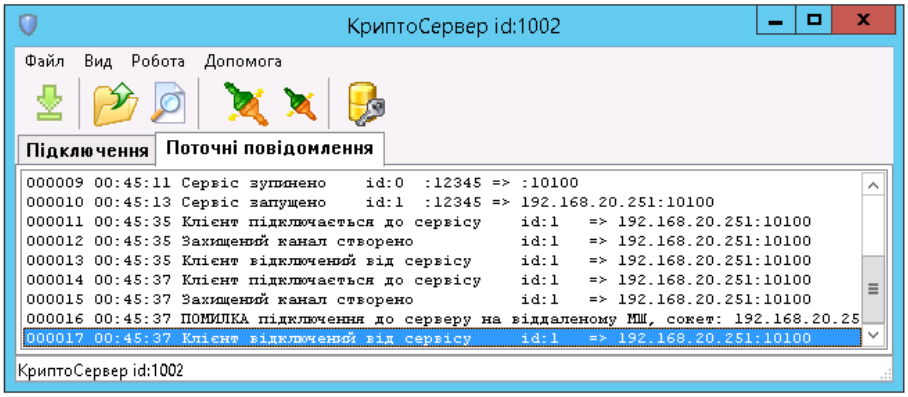
В головному вікні модуля відображуються :

- панель меню
- панель інструментів
- закладки: «Підключення», «Поточні повідомлення»

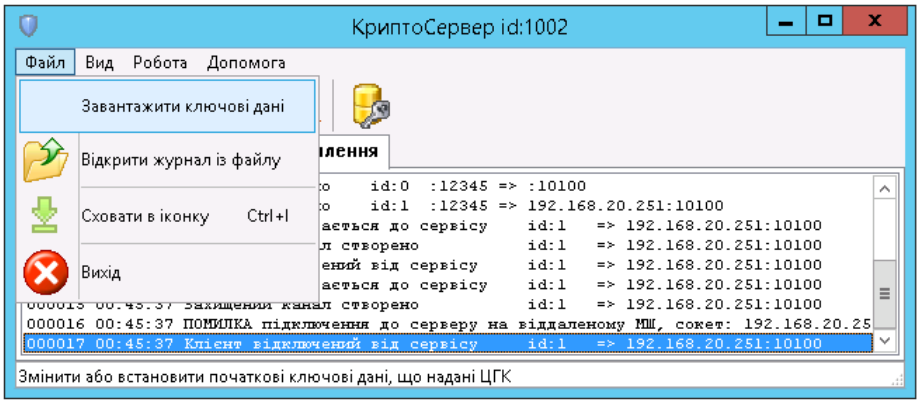
На закладці «Підключення» відображуються активні підключення



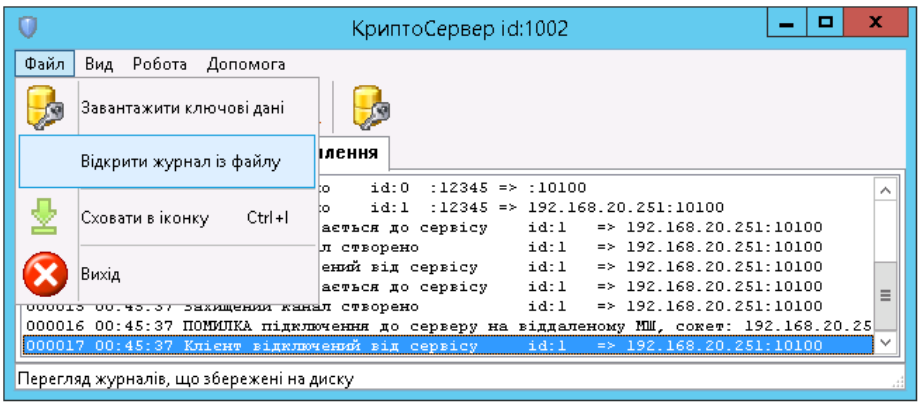
На закладці «Поточні повідомлення» відображуються поточні повідомлення МШ



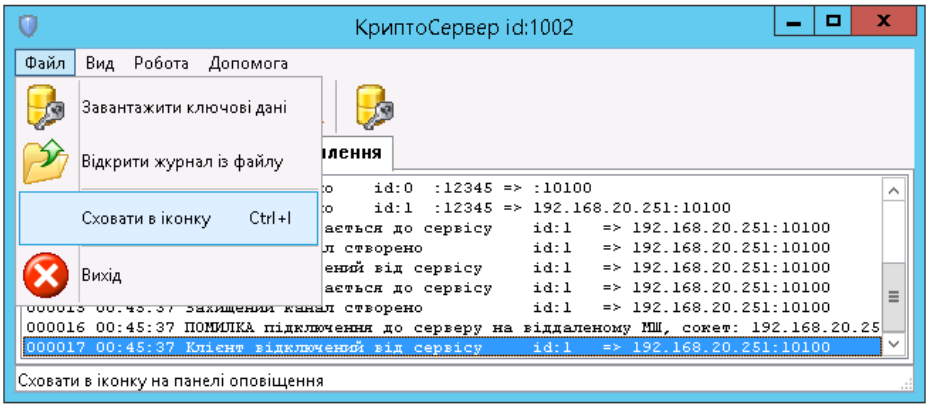
Пункт меню «Файл» підпункт «Завантажити ключові дані» - завантажує вказані ключові дані модуля шифрування



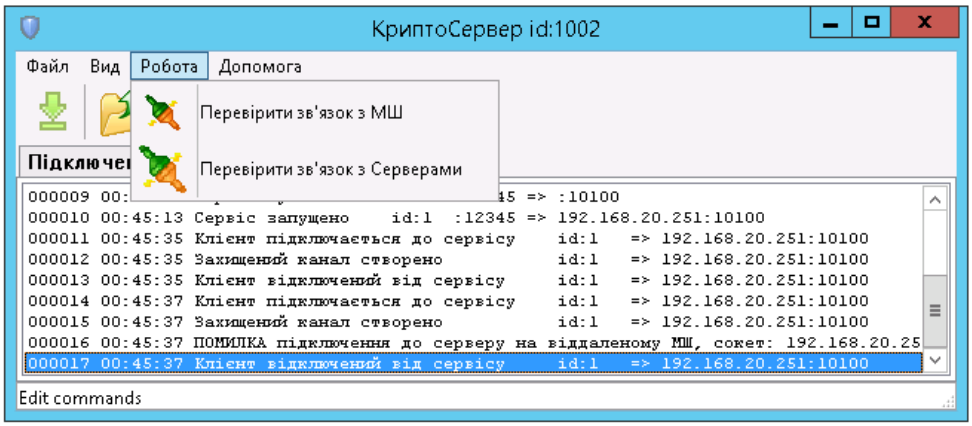
Пункт меню «Файл» підпункт «Відкрити журнал із файлу» - завантажує файли подій, що зберігаються в каталозі «Logs» (каталог можна змінити, вказавши шлях в параметрі «logdir» в ini-файлі)



Пункт меню «Файл» підпункт «Сховати в іконку» - згортає модуль в трей



Пункт меню «Файл» підпункти «Перевірити зв`язок з МШ» та «Перевірити зв`язок з Серверами» використовуються для перевірки зв`язку



Панель інструментів дублює функції, наявні в меню інструментів.

Приклад схеми взаємодії компонентів Комплексу

Нижче наведено схему взаємодії компонентів Комплексу для наступних вхідних даних:

Необхідно забезпечити доступ додатку користувача до Web-серверу, який має наступні параметри: IP-адреса 10.0.0.1, порт – 8080. IP-адреса сервера, на якому встановлено комплекс КЗІ «Криптосервер» - 192.168.0.1, IP-адреса АРМ користувача де встановлено додаток, якому потрібно отримати доступ до захищеного ресурсу - 192.168.0.2

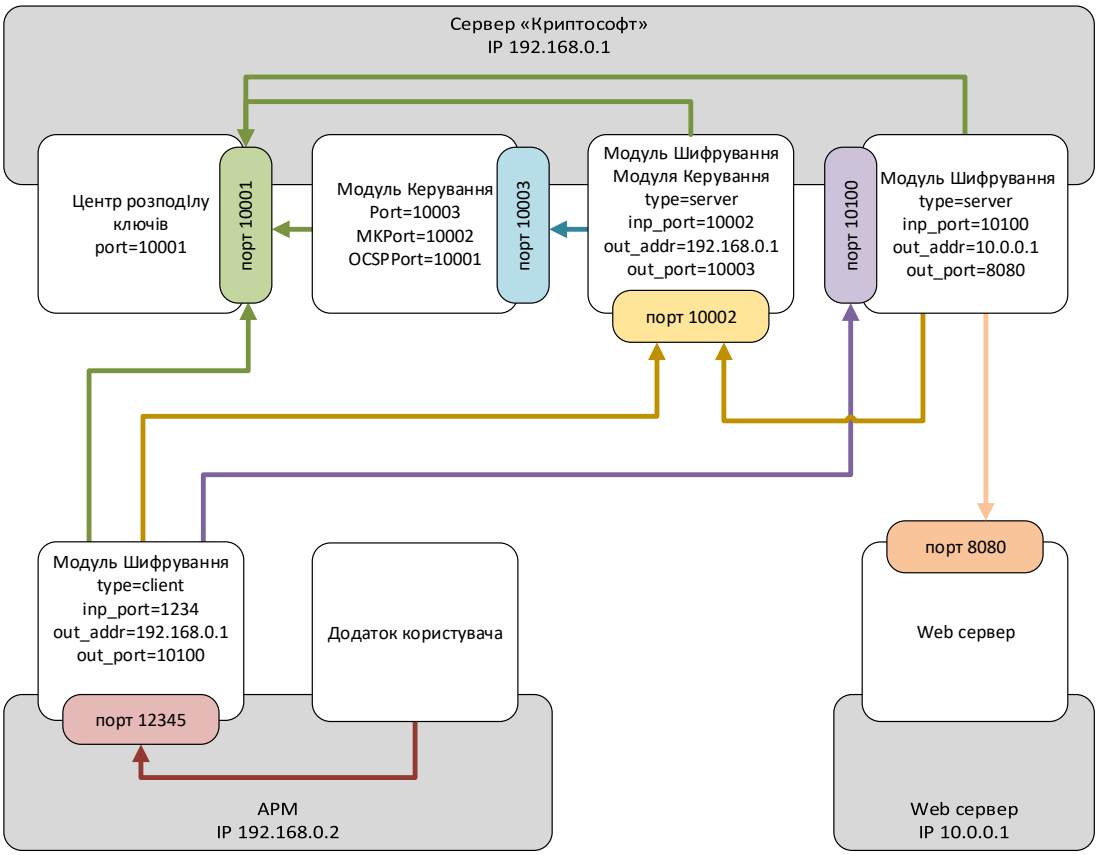


Схема роботи Комплексу наступна:

На сервері завантажено:

- модуль ЦРК (OCSP-сервер), порт 10001. Відповідає на запити модулів системи, щодо статусів сертифікатів Комплексу;
- модуль керування, порт 10003. По запиту надає конфігурацію модулям шифрування;
- модуль шифрування модуля керування, порт 10002. Шифрує\дешифрує дані між модулем керування та модулями шифрування;
- модуль шифрування, порт 10100. Працює в режимі сервера, очікує на захищені з`єднання від клієнтських модулів шифрування;

Після завантаження клієнтського модуля шифрування (IP-адреса 192.168.0.2), модуль відправляє запит на отримання статусів сертифікатів до сервера ЦРК (IP-адреса 192.168.0.1, порт 10001), потім запит на отримання конфігурації до МШМК (IP-адреса 192.168.0.1, порт 10002), який в свою чергу перенаправляє його до модуля керування (IP-адреса 192.168.0.1, порт 10003). Після цього

клієнтський модуль встановлює з`єднання з модулем шифрування, що працює в режимі серверу (IP-адреса 192.168.0.1, порт 10100) і готовий до роботи.

Дані додатка користувача надсилаються до клієнтського модуля шифрування (IP-адреса 192.168.0.2, порт 12345), де шифруються і надсилаються до модуля шифрування, що розташований на сервері (IP-адреса 192.168.0.1, порт 10100), де дешифруються і надсилаються до Web сервера(IP-адреса 10.0.0.1, порт 8080).

Інсталяція і налаштування серверної частини Комплексу

Процес інсталяції комплексу «Криптосервер» наведено на прикладі встановленої ОС Microsoft Windows Server 2012 R2 Standart.

В разі, якщо інтерфейс операційної системи англомовний, для коректної роботи комплексу потрібно змінити мову програм, які не підтримують юнікод. Для цього в розділі «Control Panel\Language\Change date, time or number formats» на закладці «Administrative» натискаємо «Change system locale» і обираємо «Ukrainian (Ukraine)».

Інсталюємо СКБД MySQL v.3.28 в каталог за замовченням, «Setup Type» обираємо – «Typical».

Після закінчення інсталяції переходимо до каталогу «C:\mysql\bin» і запускаємо «winmysqladmin.exe» з правами адміністратора. Після цього буде створено службу в Windows і MySQL буде завантажуватись автоматично.

Копіюємо каталог з компонентами комплексу «Криптосервер» до місця розташування на сервері. В нашому випадку шлях розташування каталогу « C:\cryptoserver».

Структура каталогу:

C:\cryptoserver \KGC\ – Центр генерації ключів

C:\cryptoserver \KGC\CERT – Каталог, в якому будуть зберігатись згенеровані сертифікати

C:\cryptoserver \KGC\key – Каталог, в якому зберігається ключ ЦГК

C:\cryptoserver \KDC\ – Центр розповсюдження ключів

C:\cryptoserver \KDC\Keys – Каталог, в якому зберігається ключ ЦРК

C:\cryptoserver \MK\ – Модуль керування

C:\cryptoserver \MK\Keys – Каталог, в якому зберігається ключ МК

C:\cryptoserver \CS – Модуль шифрування, який працює в режимі серверу

Генерація ключів ЦГК, ЦРК, МК

Для початку роботи з комплексом нам потрібно згенерувати ключі для всіх компонентів комплексу. Для цього використовуємо модуль «Центр генерації ключів».

Спочатку перевіримо\налаштуємо конфігурацію центра генерації ключів, шляхом зміни параметрів в файлі «C:\cryptoserver\KGC\KeyGenerationCentre.ini»

[DB]

Host=localhost

Name=CS_CGK

ReserveType=0

ReserveDays=30

ReserveTime=1290395772

[DefParamsCA]

CommonName=ЦГК

StateOrProvinceName=Київська

LocalityName=Київ

OrganizationName=Амбрелла

OrganizationalUnitName=Захист інформації

[DefParamsKDC]

CommonName=ЦРК

StateOrProvinceName=Київська

LocalityName=Київ

OrganizationName= Амбрелла

OrganizationalUnitName=Захист інформації

[DefParamsMK]

CommonName=МК

StateOrProvinceName=Київська

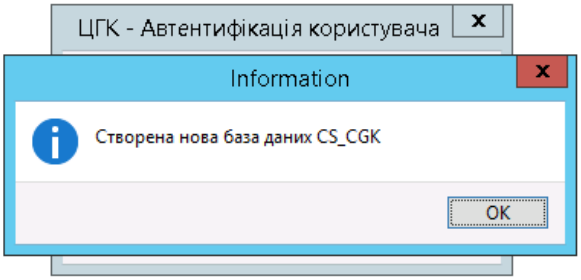
LocalityName=Київ

OrganizationName= Амбрелла

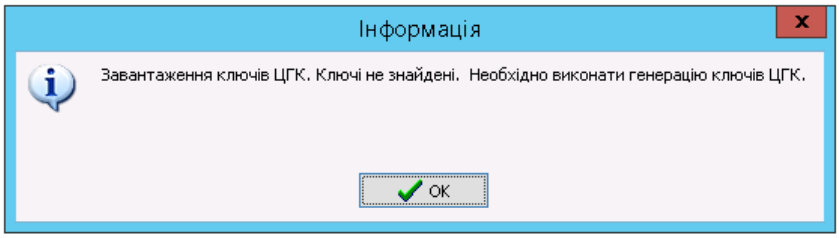
OrganizationalUnitName=Захист інформації

Запускаємо файл розташований по наступному шляху «C:\cryptoserver\KGC\KeyGenerationCentre.exe», та вводимо логін і пароль адміністратора бази даних MySQL (за замовченням логін: root, пароль відсутній). Так як це перший запуск модуля, то буде

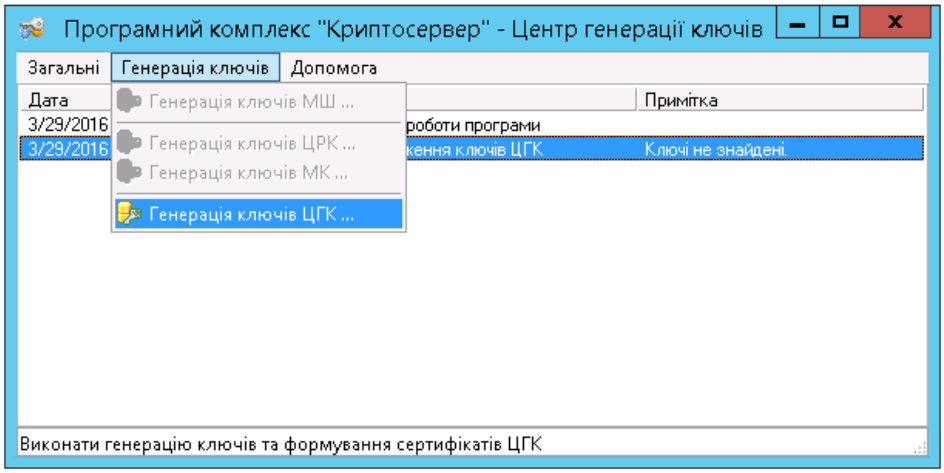
автоматично створена база даних з назвою вказаною в файлі налаштувань (в нашому випадку – CS_CGK)



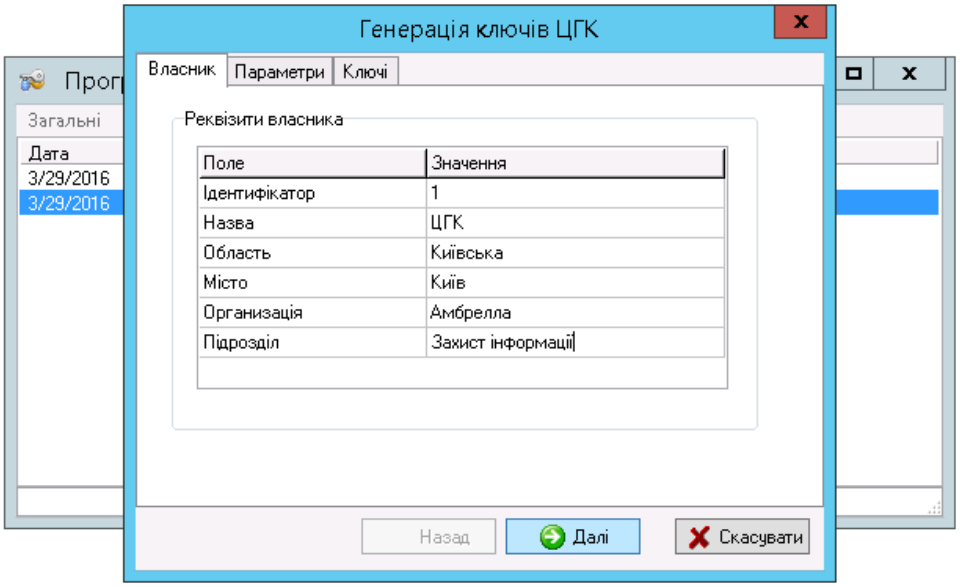
Після чого буде видано вікно з попередженням про відсутність завантажених ключів ЦГК.



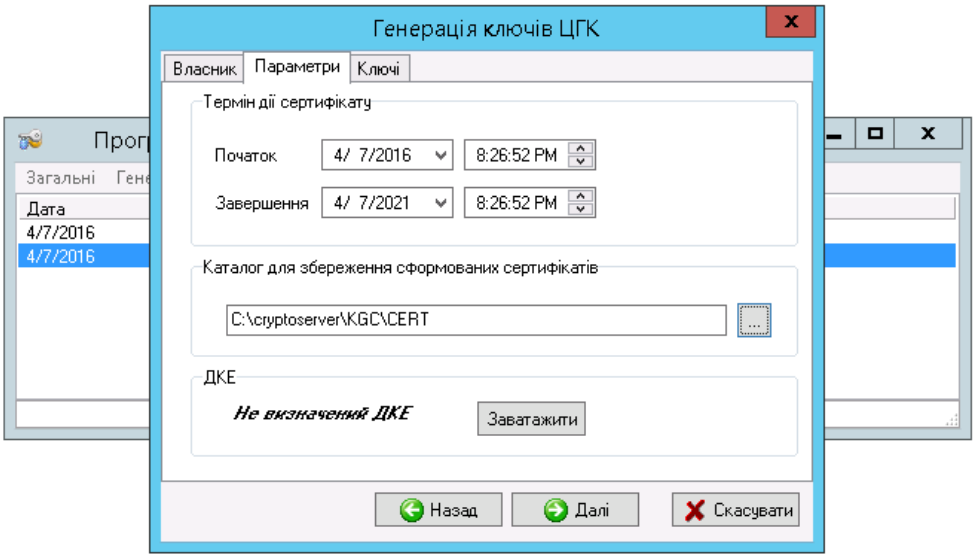
Для генерації ключів ЦГК натискаємо пункт меню «Генерація ключів» і вибираємо підпункт «Генерація ключів ЦГК»:



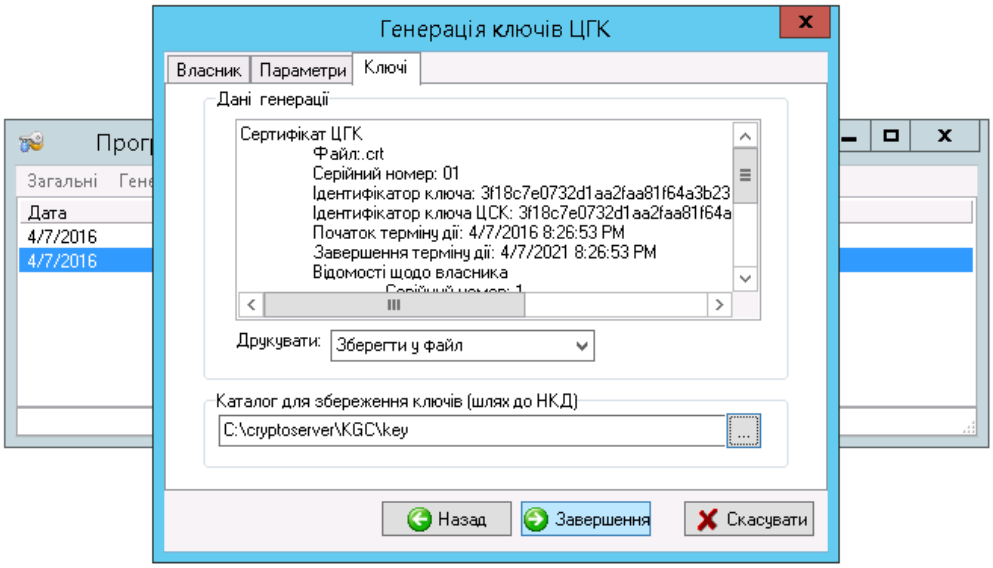
Якщо потрібно, то змінюємо/заповнюємо поля (значення за замовченням будуть взяті з ini-файлу, блок [DefParamsCA]) і натискаємо «Далі»



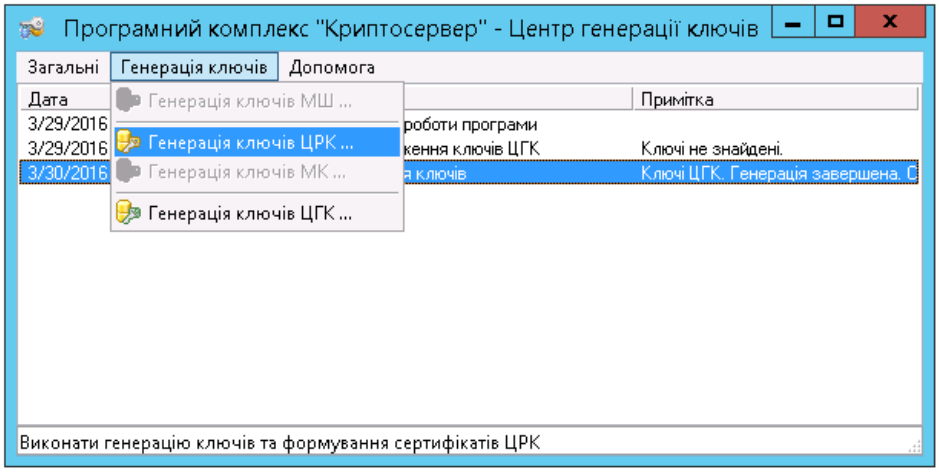
Обираємо термін дії сертифікату і каталог для збереження сформованих сертифікатів, натискаємо «Далі»



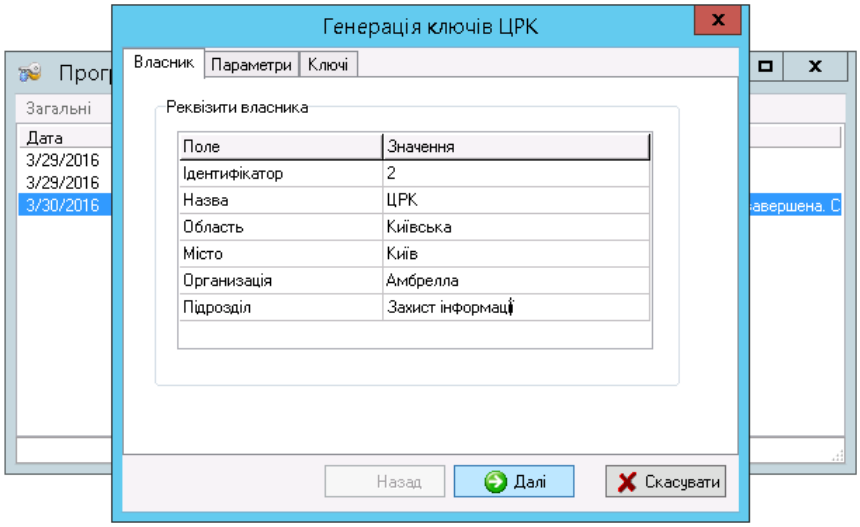
Обираємо каталог для збереження ключів - в нашому випадку це «C:\cryptoserver\KGC\key»



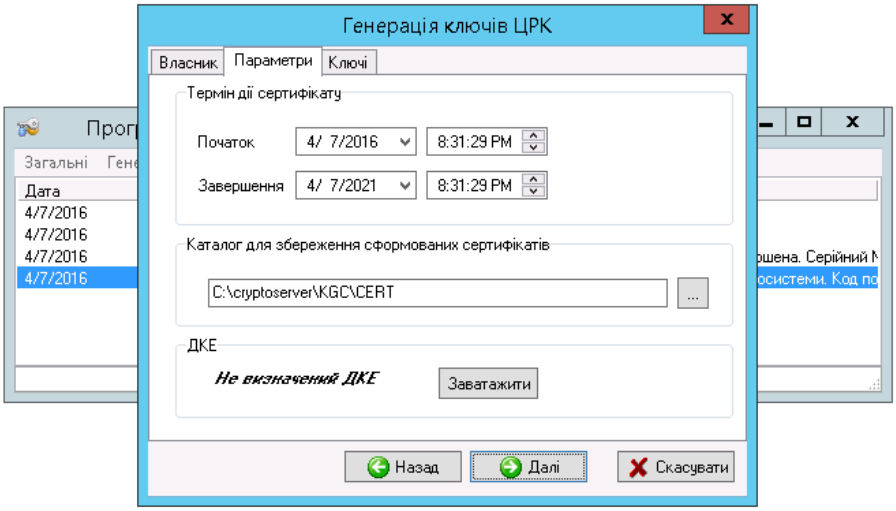
Завершуємо процес, після чого генеруємо ключі для модуля розподілу ключів (ЦРК)



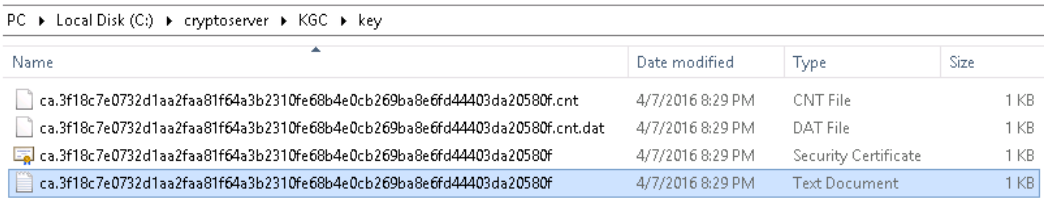
Якщо потрібно, то змінюємо/заповнюємо поля (значення за замовченням будуть взяті з ini-файлу, блок [DefParamsCA]), натискаємо «Далі»

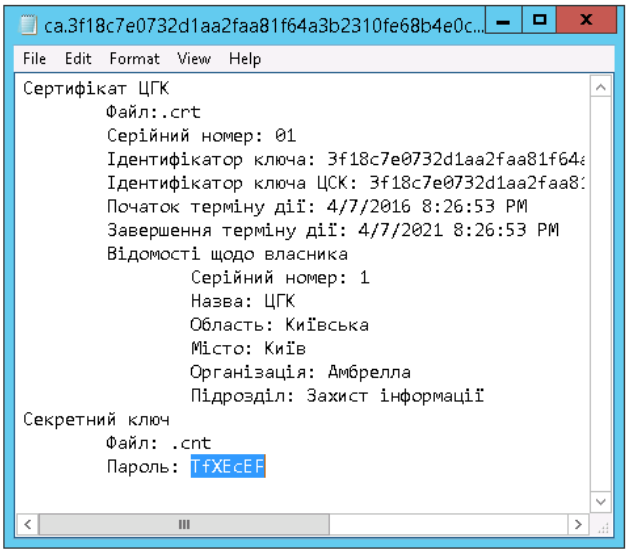


Обираємо термін дії сертифікату і каталог для збереження сформованих сертифікатів, натискаємо «Далі»

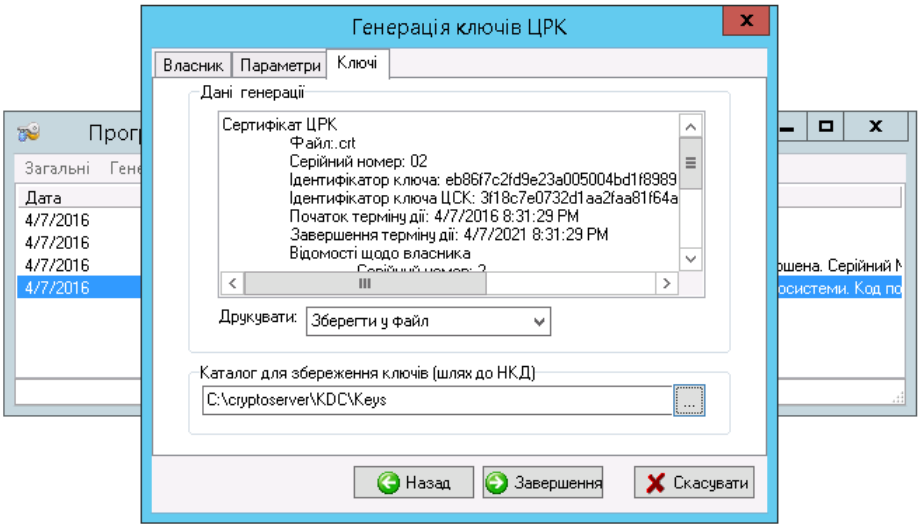


Вводимо пароль доступа до ключа ЦГК (пароль можна знайти в текстовому файлі, що знаходиться в каталозі, який ми обрали для збереження ключів в процесі генерації ключів ЦГК - в нашому випадку це «C:\cryptoserver\KGC\key»)

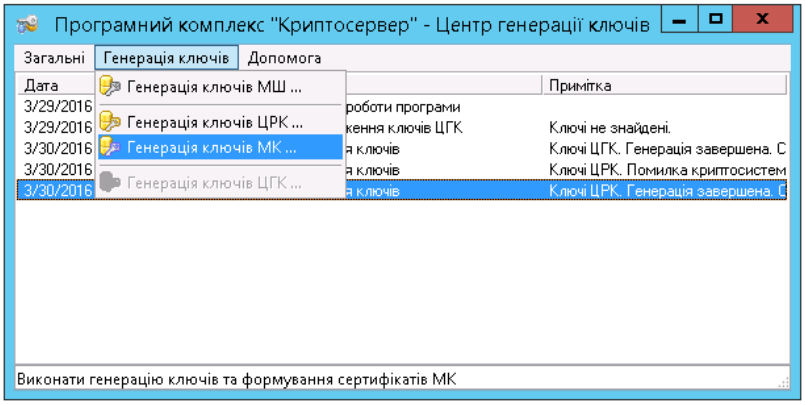




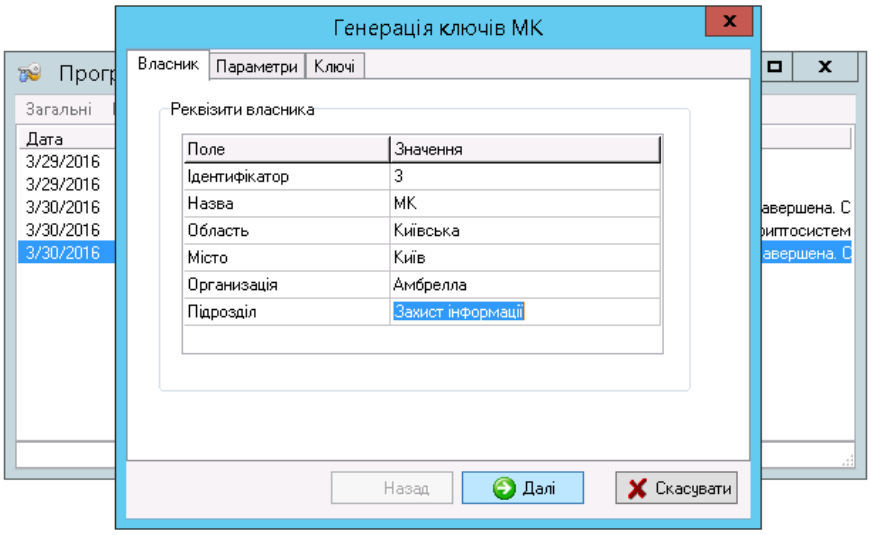
Обираємо каталог для збереження ключів - в нашому випадку це «C:\cryptoserver\KDC\Keys»



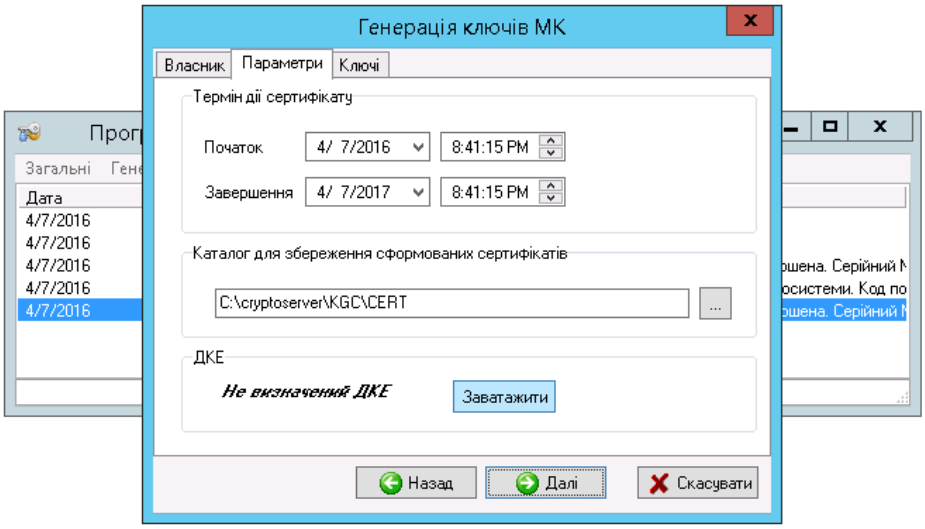
Генеруємо ключ для модуля керування - натискаємо пункт меню «Генерація ключів» і вибираємо підпункт «Генерація ключів МК»



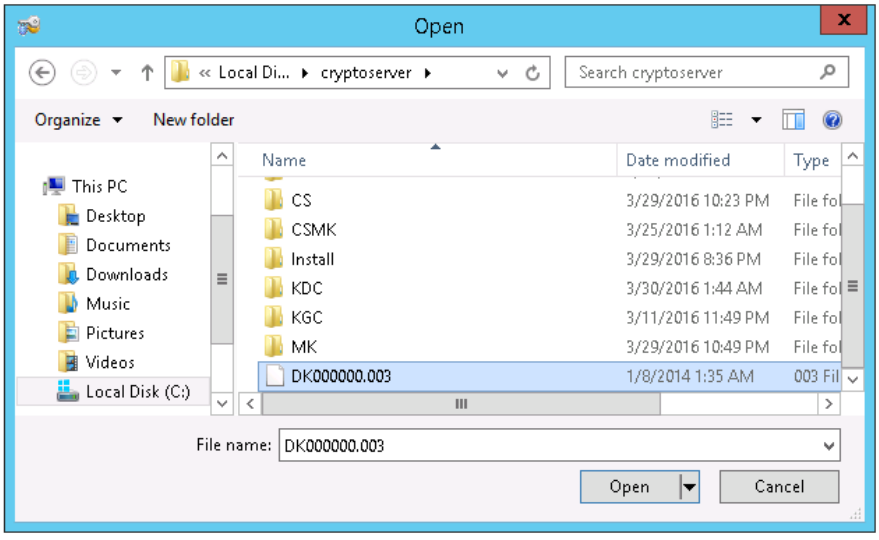
Якщо потрібно, то змінюємо/заповнюємо поля (значення за замовченням будуть взяті з ini-файлу, блок [DefParamsCA]), натискаємо «Далі»



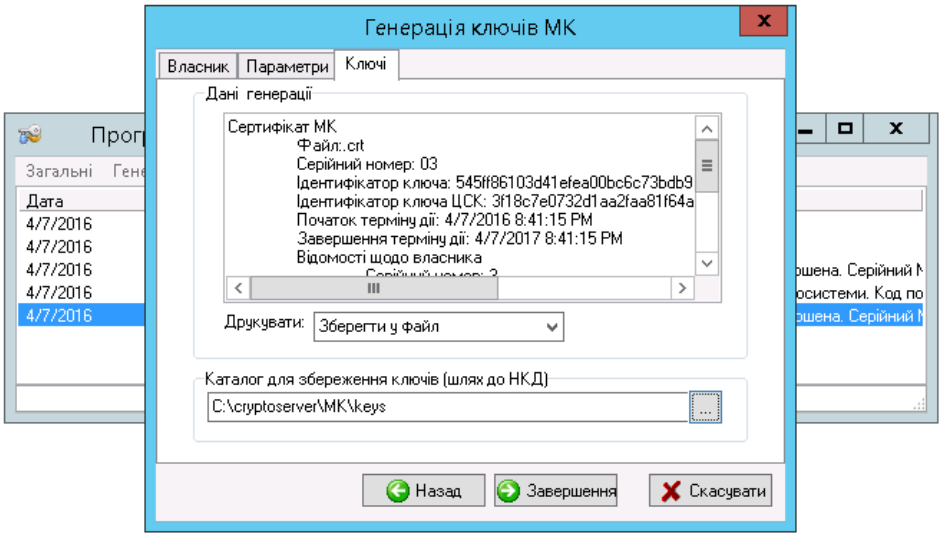
Обираємо термін дії сертифікату, каталог для збереження сформованих сертифікатів і завантажуємо файл довгострокового ключового елементу - ДКЕ (натискаємо «Завантажити»):



Обираємо файл ДКЕ (в нашому випадку він знаходиться «c:\cryptoserver\DK000000.003»)



Обираємо каталог для збереження ключів - в нашому випадку це «C:\cryptoserver\MK\Keys»



Ключі згенеровано.

Імпорт ключових даних в модуль ЦРК

Наступний крок – запуск модуля Центр розподілу ключів (ЦРК).

Спочатку перевіримо\налаштуємо конфігурацію центра генерації ключів, шляхом зміни параметрів в файлі «C:\cryptoserver\ KDC\KeyDistributionCentre.ini»

[DB]

Host=localhost

Name=CS

ReserveType=0

ReserveDays=30

ReserveTime=1303404912

[Server]

Port=10001

pass=

AutoStart=1

[Form]

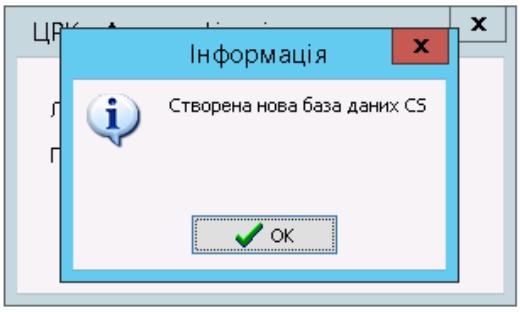
Width=724

Height=415

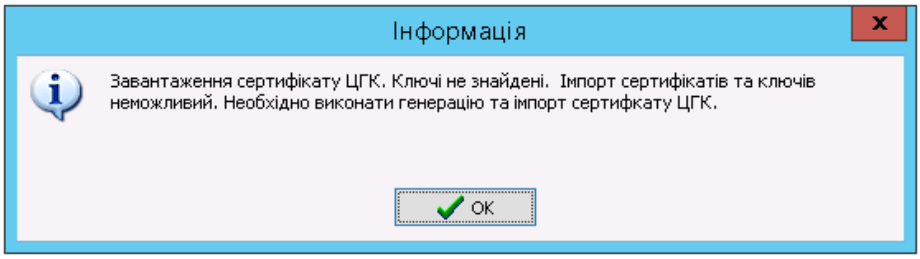
Left=284

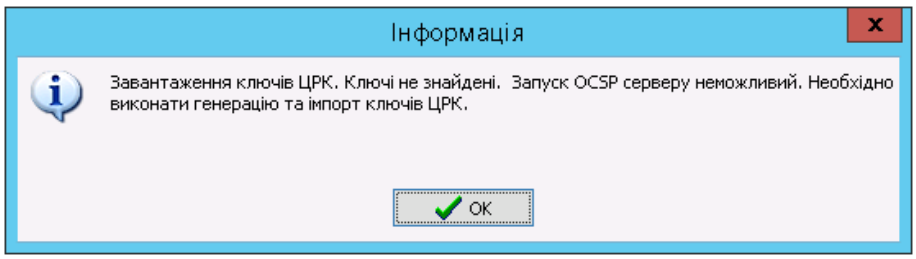
Top=376

Запускаємо файл розташований по наступному шляху «C:\cryptoserver\KDC\KeyDistributionCentre.exe», та вводимо ім`я логін і пароль адміністратора бази даних MySQL(за замовченням логін: root, пароль відсутній). Так як це перший запуск модуля, то буде автоматично створена база даних з назвою вказаною в файлі налаштувань (за замовченням – CS)

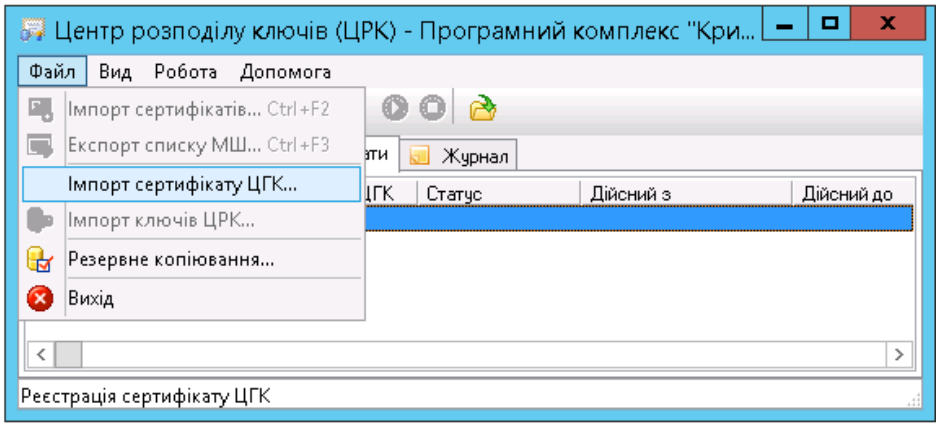


Після чого буде видано вікна з попередженням про відсутність завантажених ключів ЦРК та сертифікату ЦГК

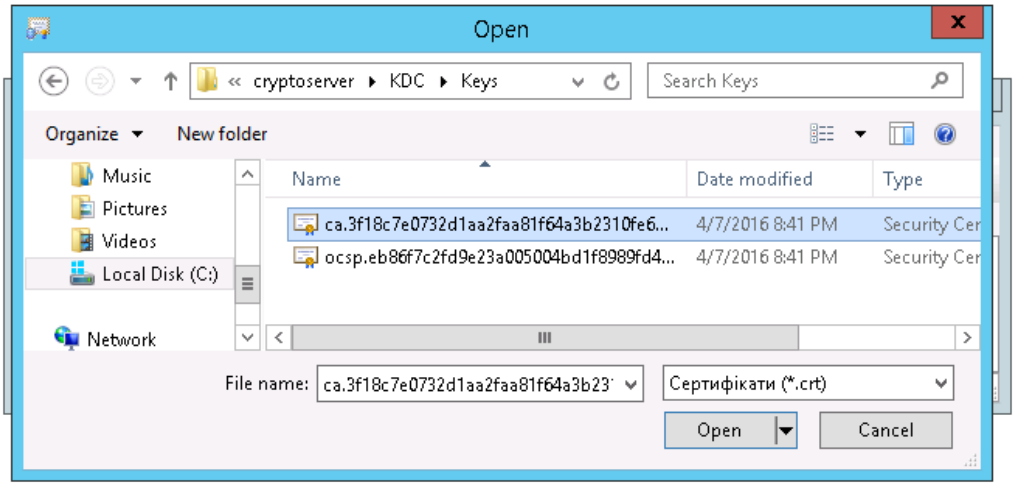




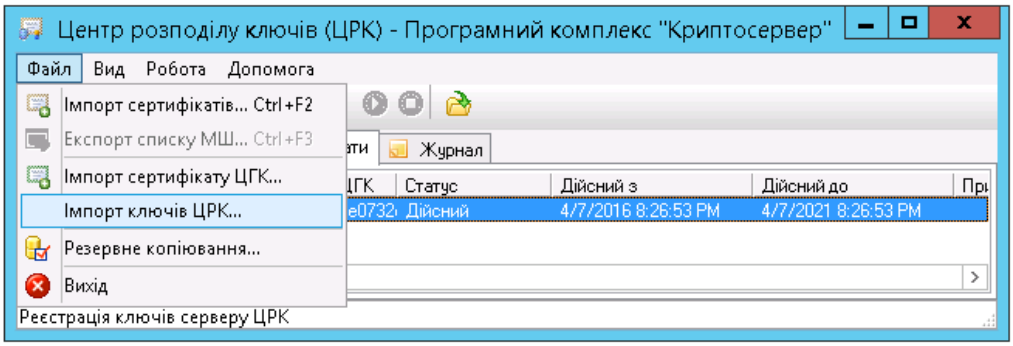
Імпортуємо в модуль ЦРК сертифікат ЦГК – пункт меню «Файл» підпункт меню «Імпорт сертифікату ЦГК…»



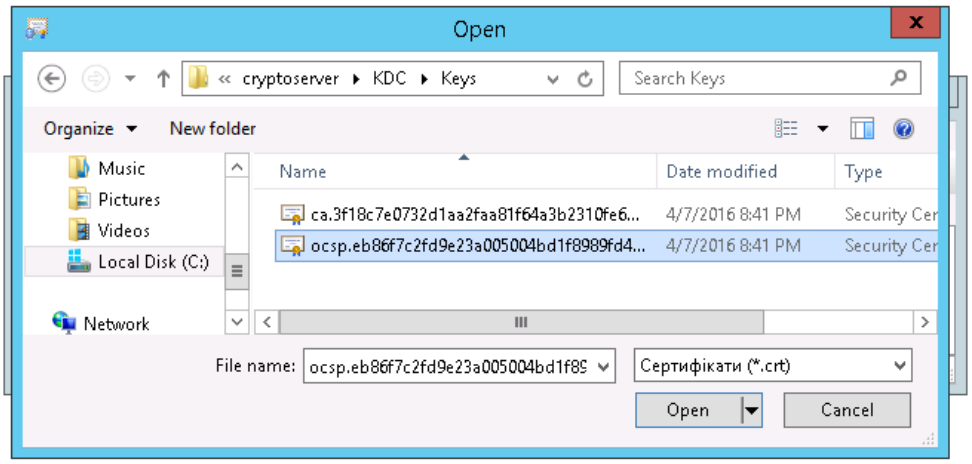
Обираємо файл сертифікату ЦГК. Назва файла буде починатися з ca. тип файлу .crt (в нашому випадку він знаходиться в каталозі «c:\cryptoserver\KDC\Keys\»)



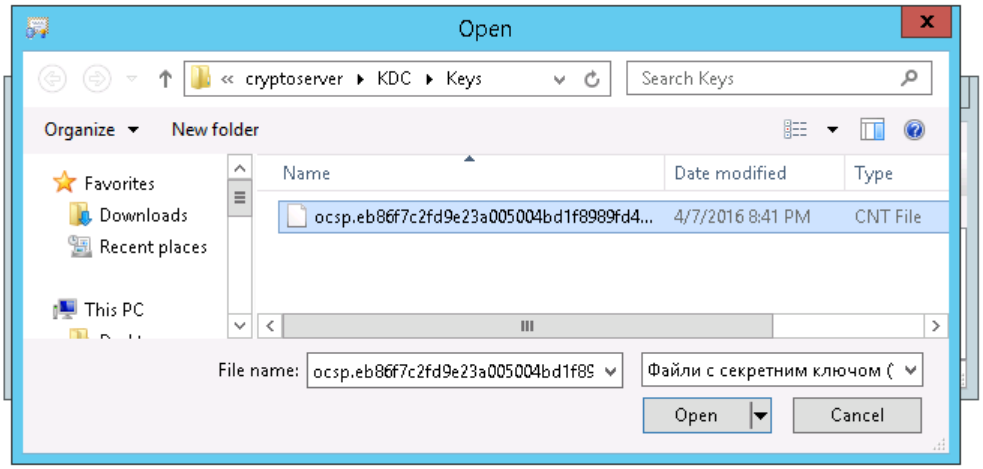
Імпортуємо в модуль ЦРК ключі ЦРК – пункт меню «Файл» підпункт меню «Імпорт ключів ЦРК…»



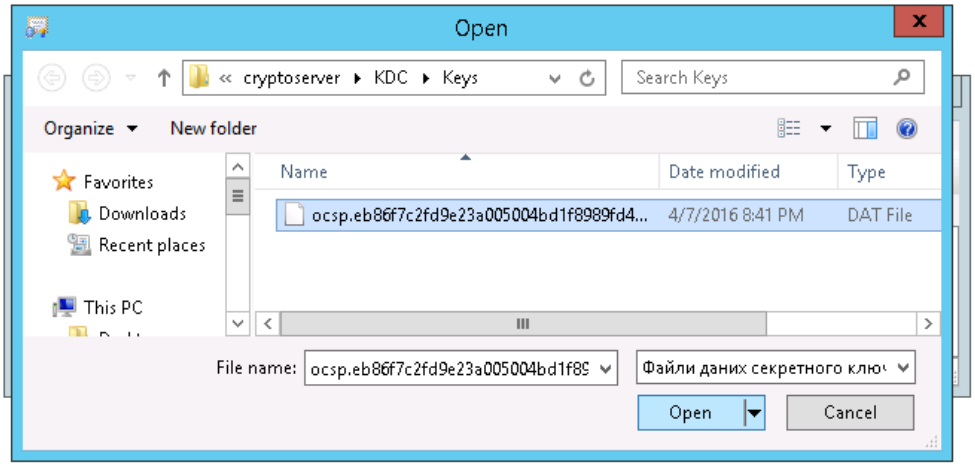
Обираємо файл сертифікату ЦРК. Назва файла буде починатися з ocsp. тип файлу .crt (в нашому випадку він знаходиться в каталозі «c:\cryptoserver\KDC\Keys\»)



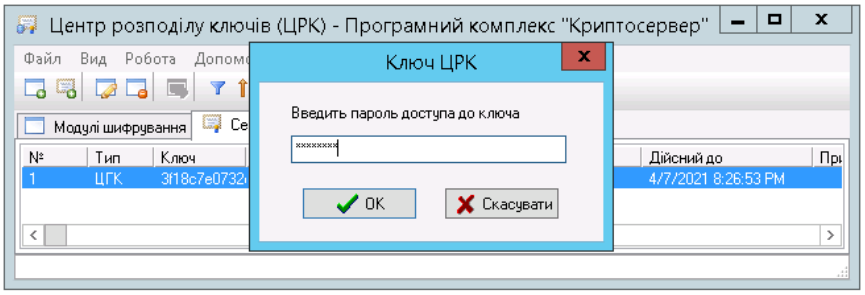
Обираємо файл з секретним ключом. Назва файла буде починатися з ocsp. тип файлу .cnt (в нашому випадку він знаходиться в каталозі «c:\cryptoserver\KDC\Keys\»)

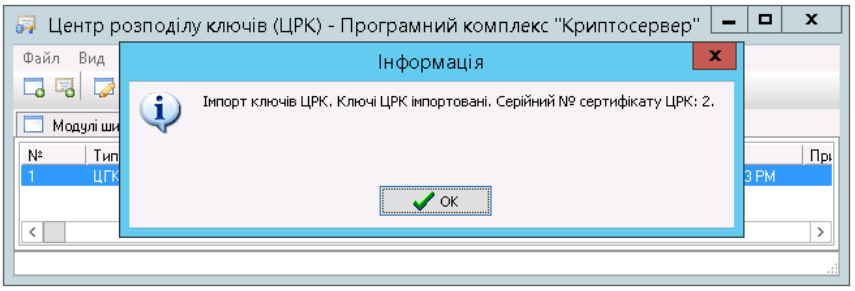


Обираємо файл даних секретного ключа. Назва файла буде починатися з ocsp. тип файлу .dat (в нашому випадку він знаходиться в каталозі «c:\cryptoserver\KDC\Keys\»)

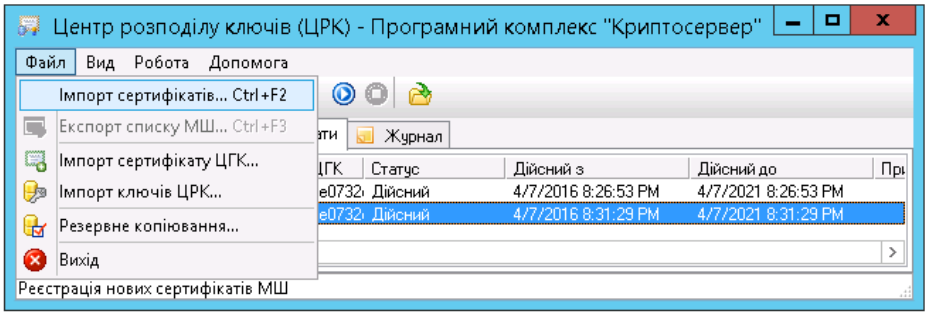


Вводимо пароль доступу до ключа ЦРК (пароль можна знайти в текстовому файлі, що знаходиться в каталозі, який ми обрали для збереження ключів в процесі генерації ключів ЦРК - в нашому випадку це «C:\cryptoserver\KDC\keys»)

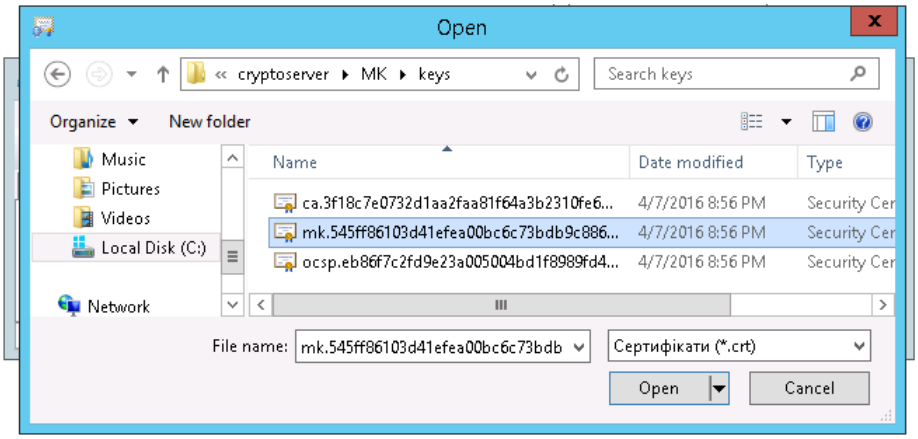




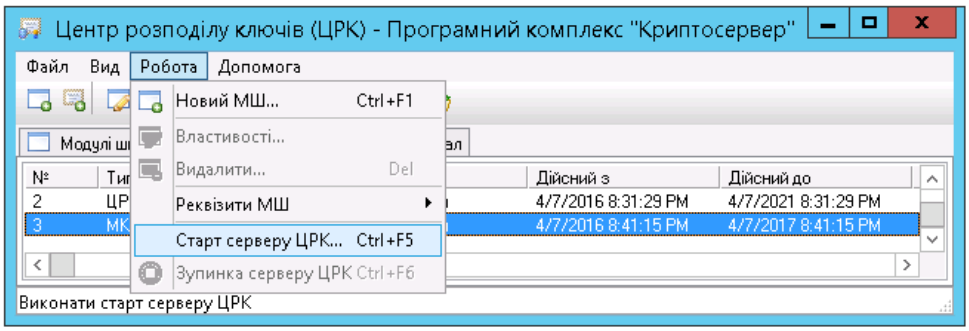
Імпортуємо до ЦРК сертифікат модуля керування (МК)– пункт меню «Файл» підпункт меню «Імпорт сертифікатів…»



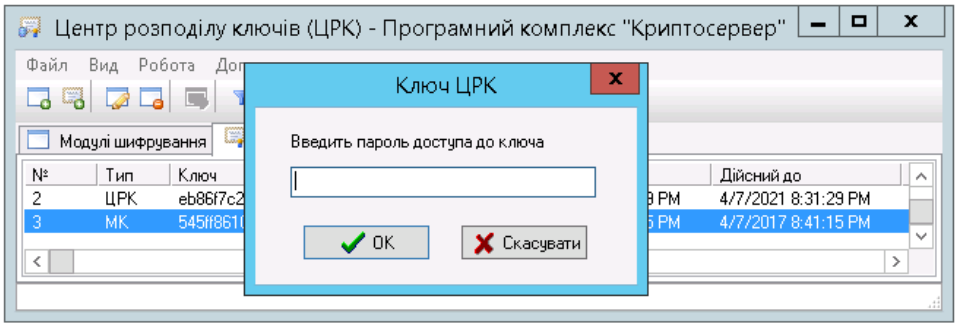
Обираємо файл сертифікату МК. Назва файла буде починатися з mk. тип файлу .crt (в нашому випадку він знаходиться в каталозі «c:\cryptoserver\MK\keys\»)



Запускаємо сервер ЦРК - пункт меню «Робота» підпункт меню «Старт серверу ЦРК…»



Вводимо пароль доступу до ключа ЦРК:



Налаштування і запуск модуля керування

Перевіримо\налаштуємо конфігурацію шифрування модуля керування, шляхом зміни параметрів в файлі «C:\cryptoserver\MK\CryptoServer.ini»

[common]

cacertfile=

certdir=cert_db

certfile=

contfile=

dkefile=

keysdir=keys

logdir=LogsCS

pass=

sid=3

[link1]

id=1

inp_port=10002

out_addr=127.0.0.1

out_port=10003

sid=3

type=server

[ocsp]

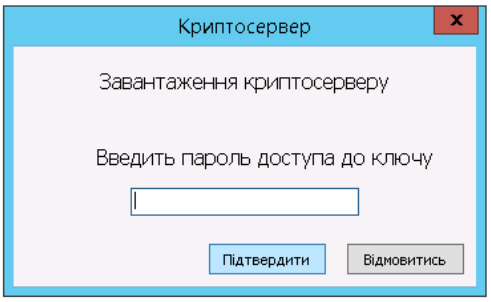
addr=127.0.0.1

certfile=

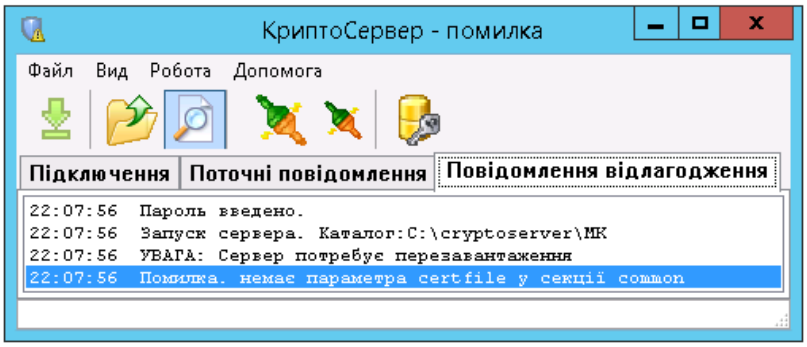
port=10001

Запускаємо файл розташований по наступному шляху «C:\cryptoserver\ MK\ CryptoServer.exe»

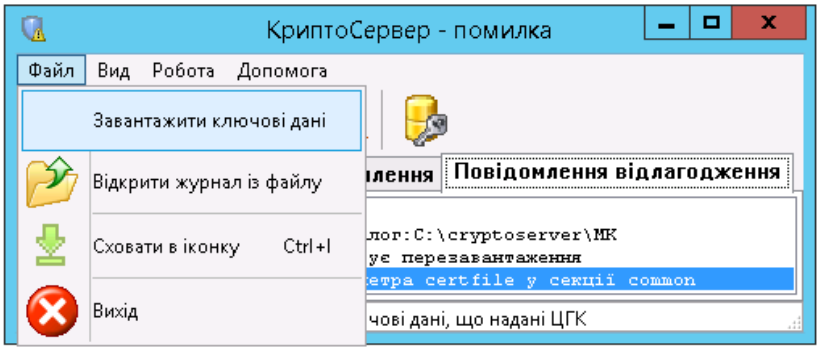
На запит паролю нічого не вводимо, натискаємо «Підтвердити»



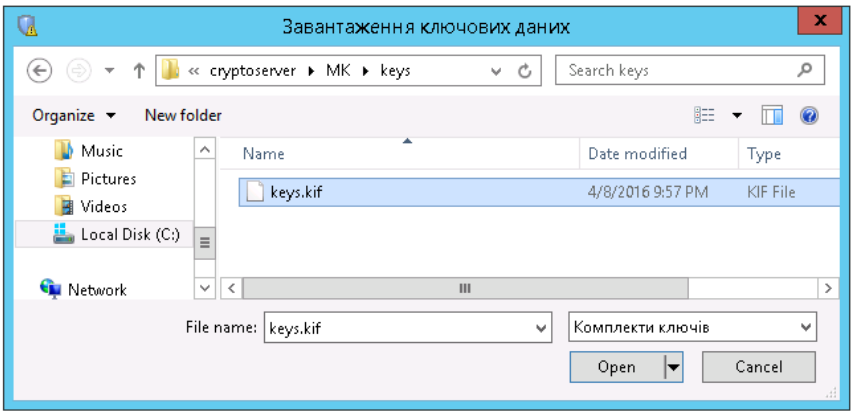
Буде видано повідомлення о помилці



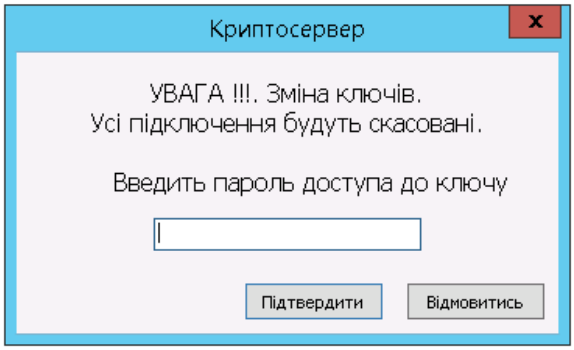
Завантажимо ключові дані - пункт меню «Файл» підпункт меню «Завантажити ключові дані»



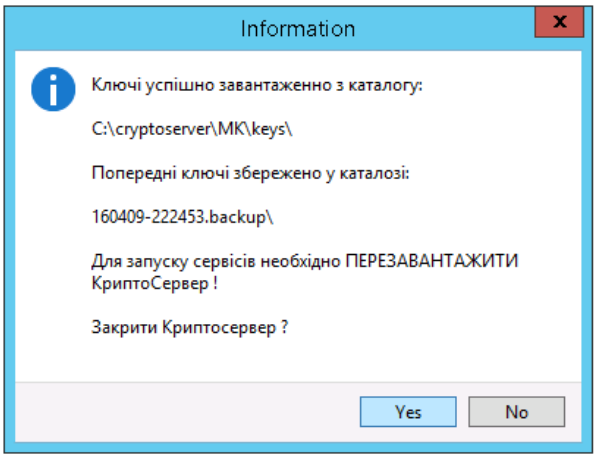
Ключові дані для модуля шифрування модуля керування знаходяться в каталозі, який ми обрали для збереження ключів в процесі генерації ключів МК - «C:\cryptoserver\MK\keys\», в файлі «keys.kif»



Вводимо пароль до ключових даних (пароль можна знайти в текстовому файлі, що знаходиться в каталозі, який ми обрали для збереження ключів в процесі генерації ключів МК - в нашому випадку це «C:\cryptoserver\MK\keys\»)



Закриваємо модуль шифрування:

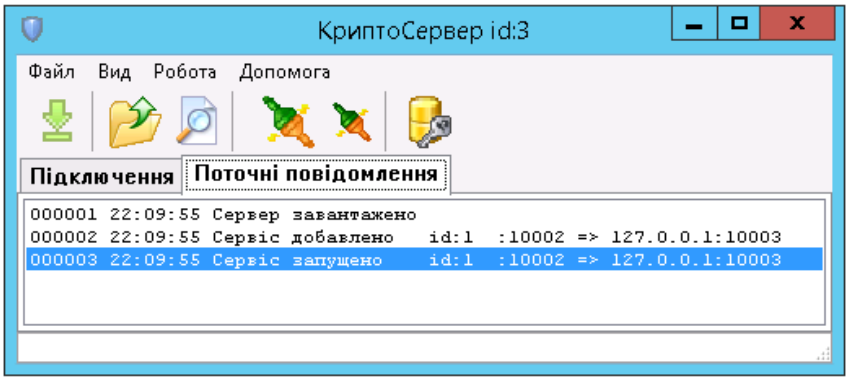


Для того, щоб не вводити пароль кожен раз при завантаженні модуля шифрування, можемо записати його в в файлі «C:\cryptoserver\MK\ CryptoServer.ini» блок [common], параметр «pass».

[common]

pass= iOz2Iv

Запускаємо модуль шифрування для модуля керування і перевіряємо статус:



Перевіримо\налаштуємо конфігурацію модуля керування, шляхом зміни параметрів в файлі «C:\cryptoserver\MK\MK.ini»

[DB]

Host=localhost

Name=CS

ReserveDays=26

ReserveType=0

ReserveTime=1318328114

CleanupLogExpireDays=1

CleanupLogMsgCodes=159;160;161;162;163;164;165;201;202;203;204

[Server]

Port=10003

AutoStart=1

[Info]

MKPort=10002

OCSPPort=10001

[Form]

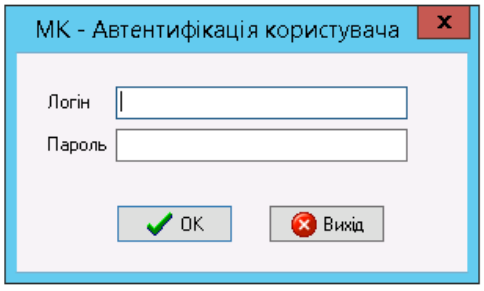
Width=1278

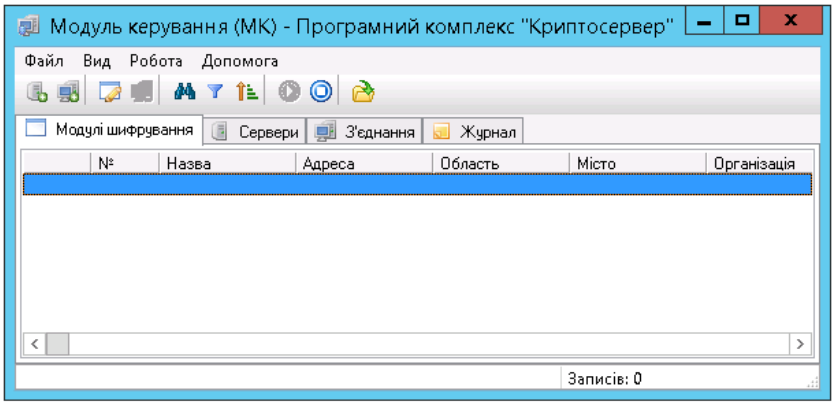
Height=982

Left=1

Top=1

Запускаємо файл розташований по наступному шляху «C:\cryptoserver\MK\MK.exe», та вводимо ім`я логін і пароль адміністратора бази даних MySQL(за замовченням логін: root, пароль відсутній).





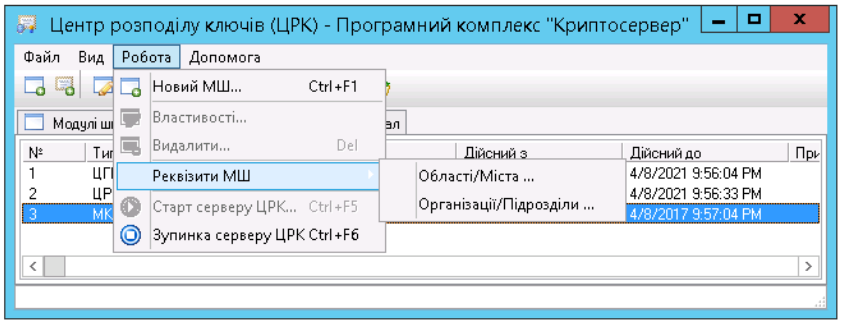
Налаштування модуля шифрування в режимі серверу

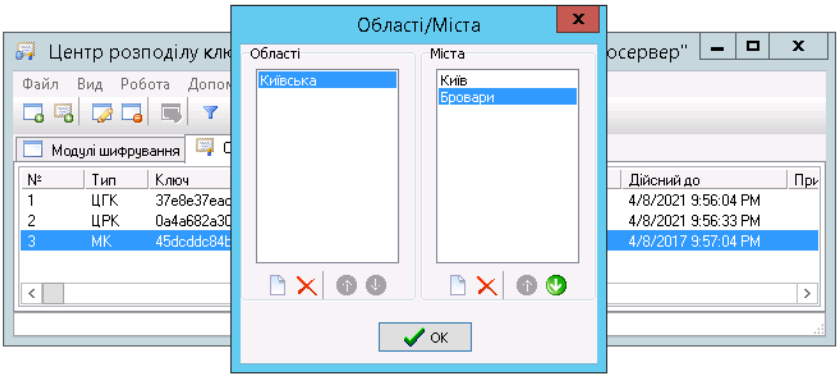
Модуль шифрування, що працює в режимі серверу, очікує підключень від модулів шифрування, що працюють в режимі клієнтів, дешифрує дані, отримані від інших МШ, та перенаправляє їх на вказаний порт і IP-адресу.

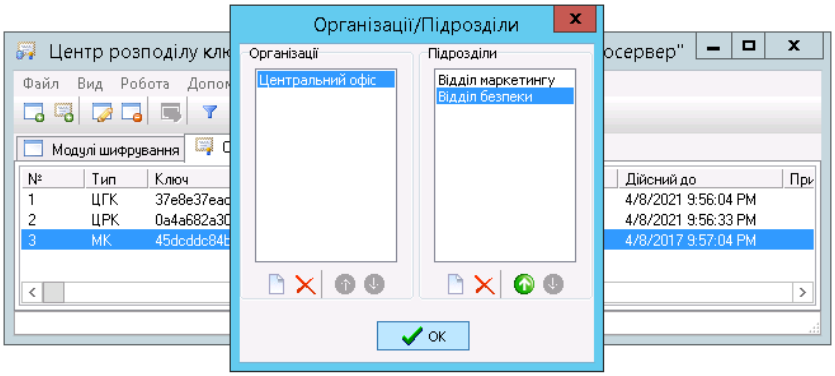
Важливо! Один модуль шифрування, що працює в режимі сервера, здатен обробляти підключення понад 1000 МШ-клієнтів. В разі, якщо кількість МШ-клієнтів більша – рекомендується створювати додаткові МШ сервери і розподіляти МШ-клієнти між ними.

Для створення нового МШ-сервера треба виконати наступні кроки:

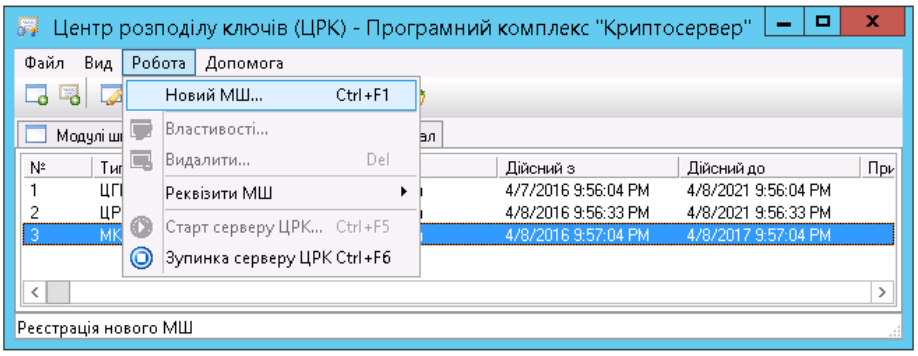
Запускаємо Центр розподілу ключів і заповнюємо реквізити МШ - пункт меню «Робота» підпункт меню «Реквізити МШ» підпункти «Області/Міста», «Організації/Підрозділи»:



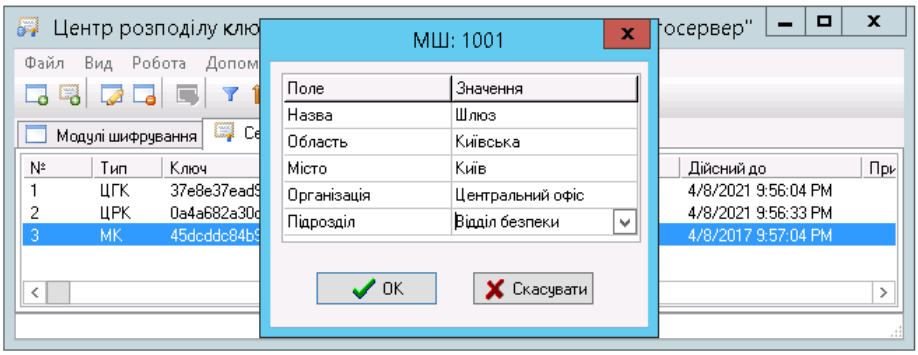




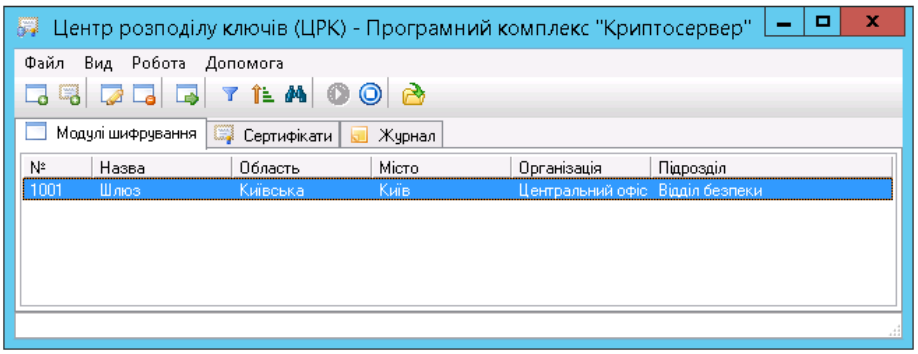
Обираємо пункт меню «Робота» підпункт меню «Новий МШ»:



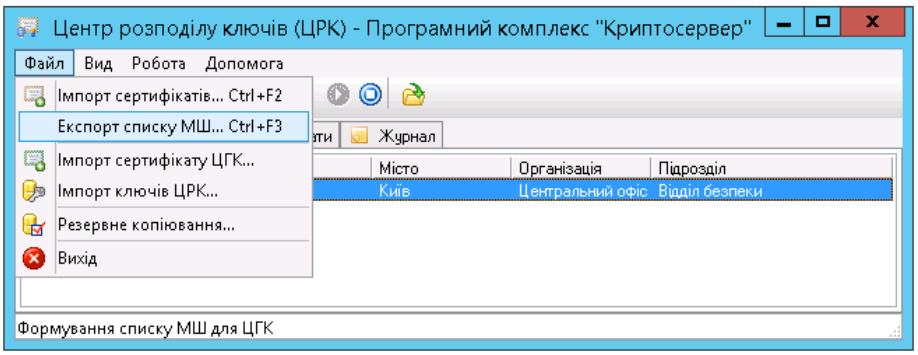
Заповнюємо поля:



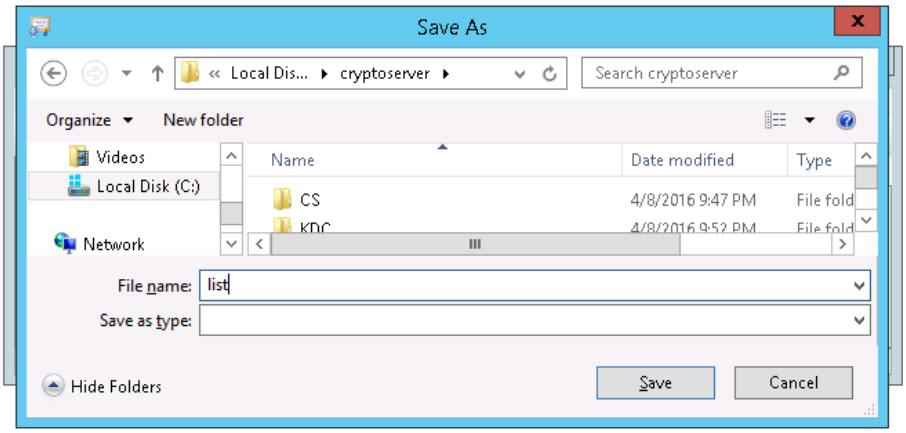
В закладці «Модулі шифрування» з`явиться новий МШ:

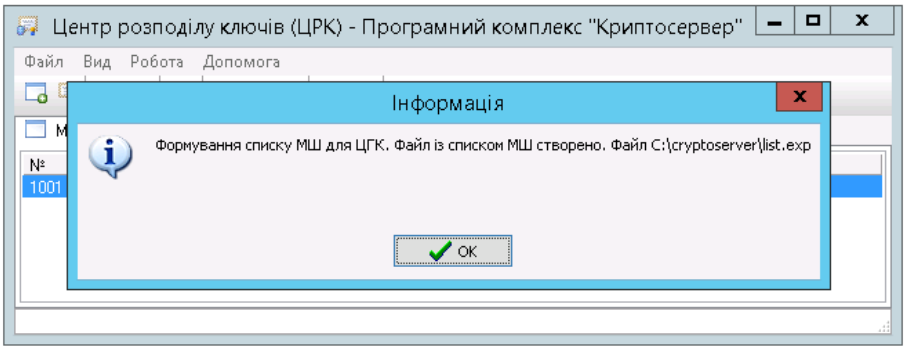


Обираємо пункт меню «Файл» підпункт меню «Експорт списку МШ»:

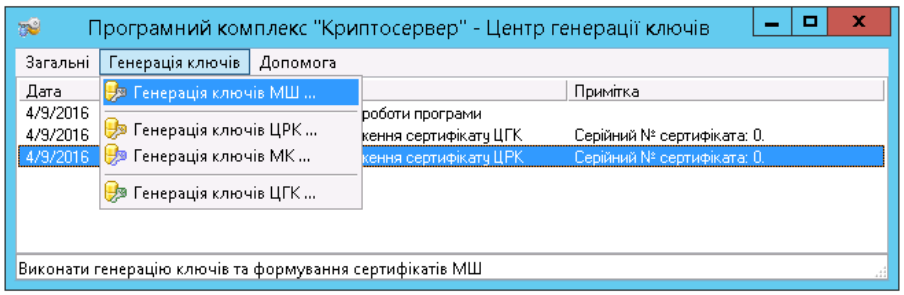


Зберігаємо під обраною назвою:

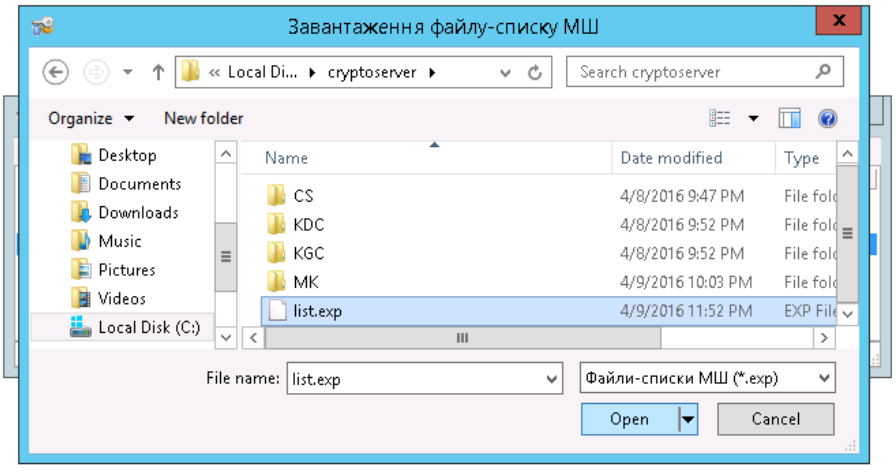




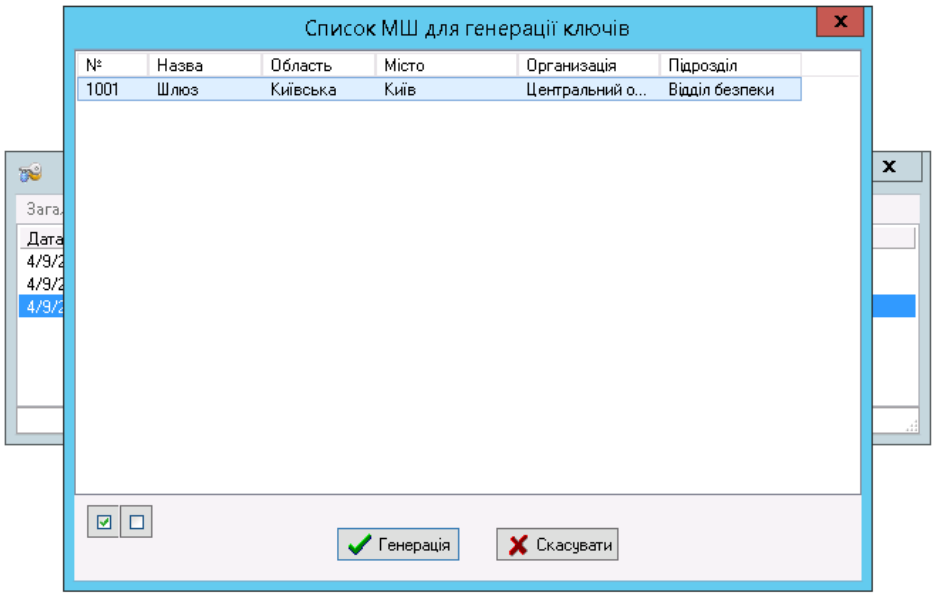
Запускаємо Центр генерації ключів, обираємо пункт меню «Генерація ключів» підпункт меню «Генерація ключів МШ …»:



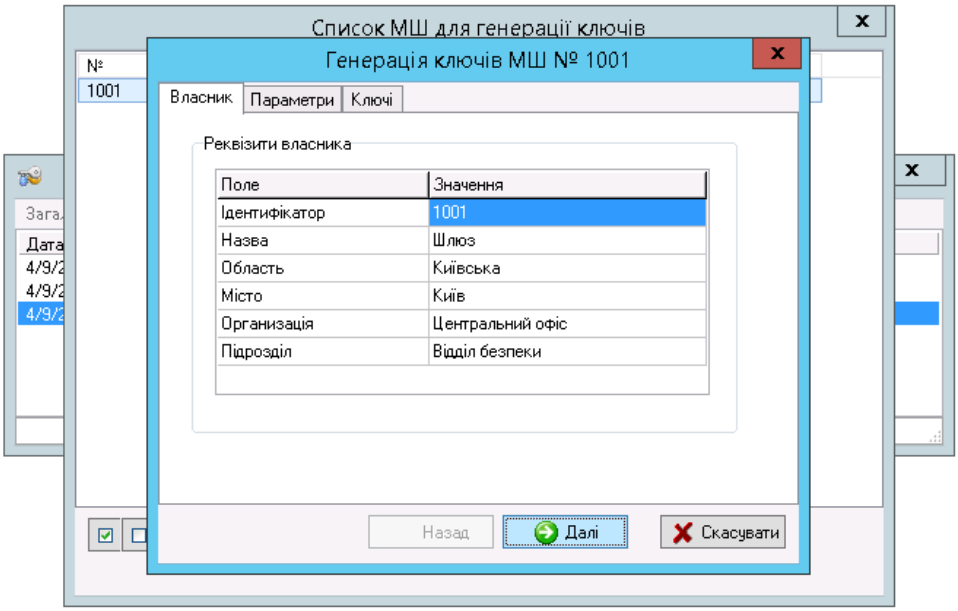
Знаходимо файл зі списком МШ, який ми імпортували з ЦРК:



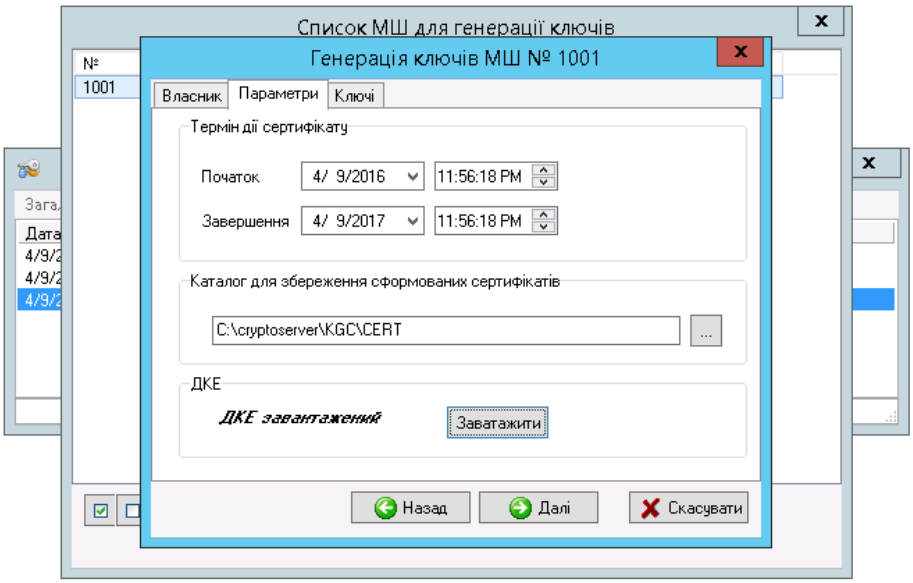
Обираємо МШ для якого нам потрібно згенерувати ключі (в даному випадку МШ в нас один) і натискаємо кнопку «Генерація»:



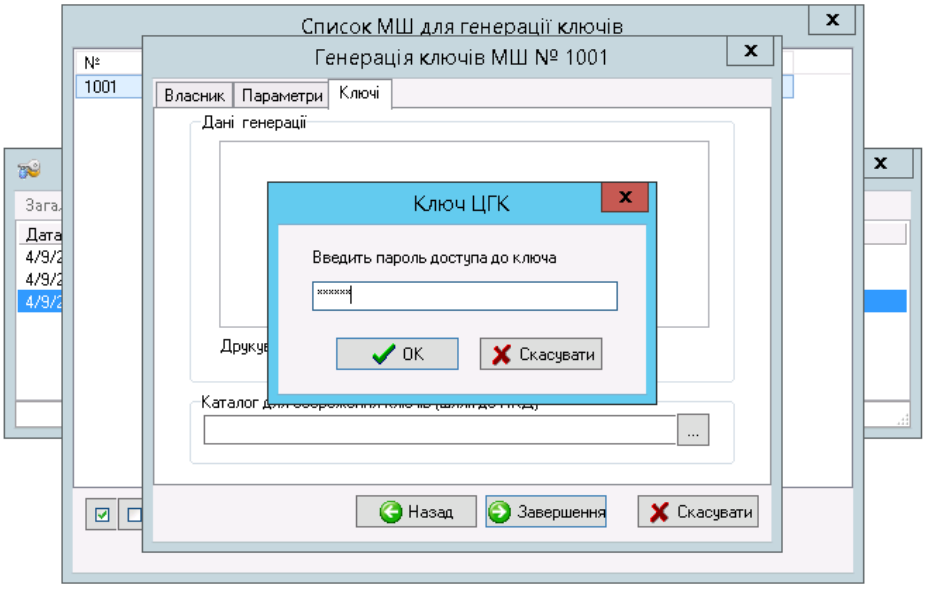
Змінити параметри власника МШ в даному вікні ми вже не можемо, натискаємо «Далі»:



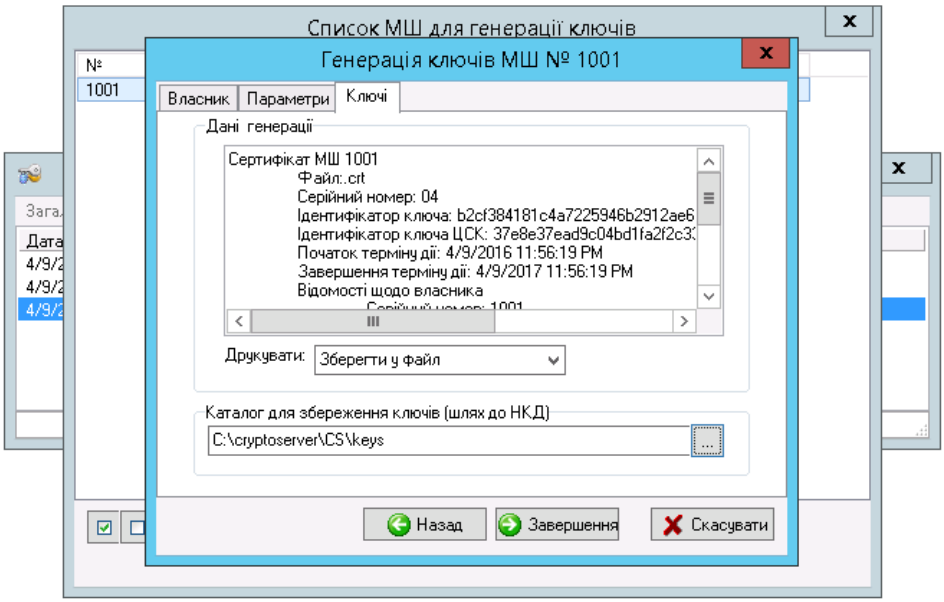
Обираємо термін дії сертифікату, каталог для збереження сертифікатів, та завантажуємо файл ДКЕ:



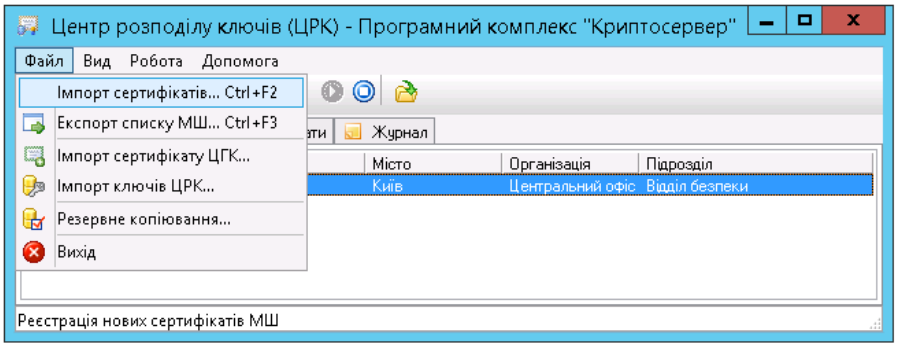
Вводимо пароль доступу до ключа ЦГК



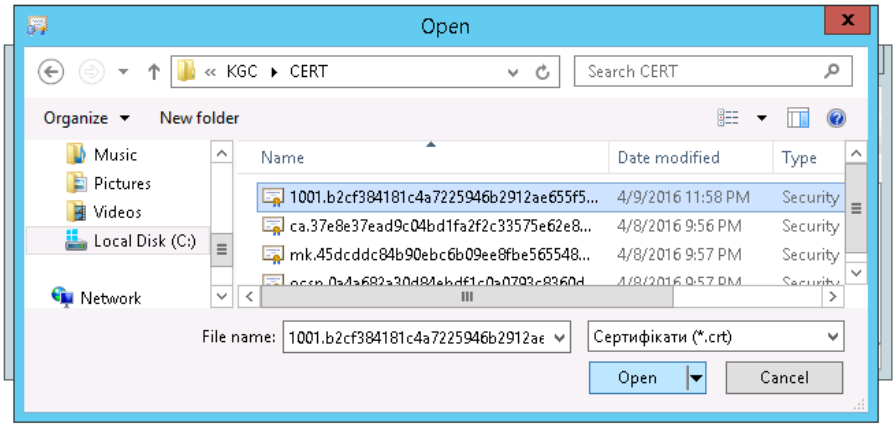
Обираємо каталог для збереження ключа і завершуємо генерацію

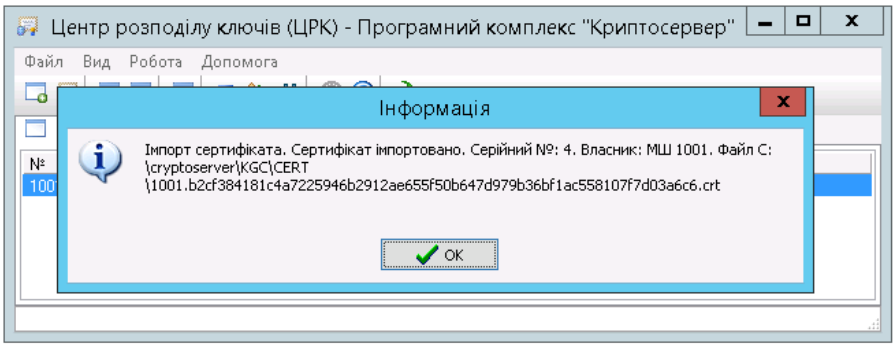


Повертаємось до ЦРК і імпортуємо створений сертифікат - пункт меню «Файл» підпункт меню «Імпорт сертифікатів…»



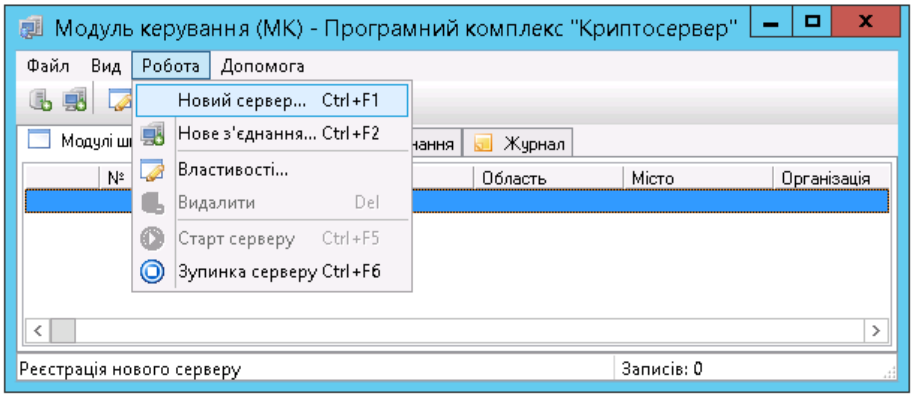
Обираємо сертифікат з каталогу, в який його зберігали під час генерації «C:\cryptoserver \KGC\CERT» (Увага! Назва файла сертифікату буде починатись з його порядкового номеру, що був присвоєний модулю шифрування під час створення нового МШ в ЦРК, в нашому випадку це - 1001)





Запускаємо модуль керування і налаштовуємо МШ:

Так як наш МШ буде працювати в режимі сервера, то обираємо пункт меню «Робота» підпункт меню «Новий сервер …»



Заповнюємо параметри нового сервера

Значення полей:

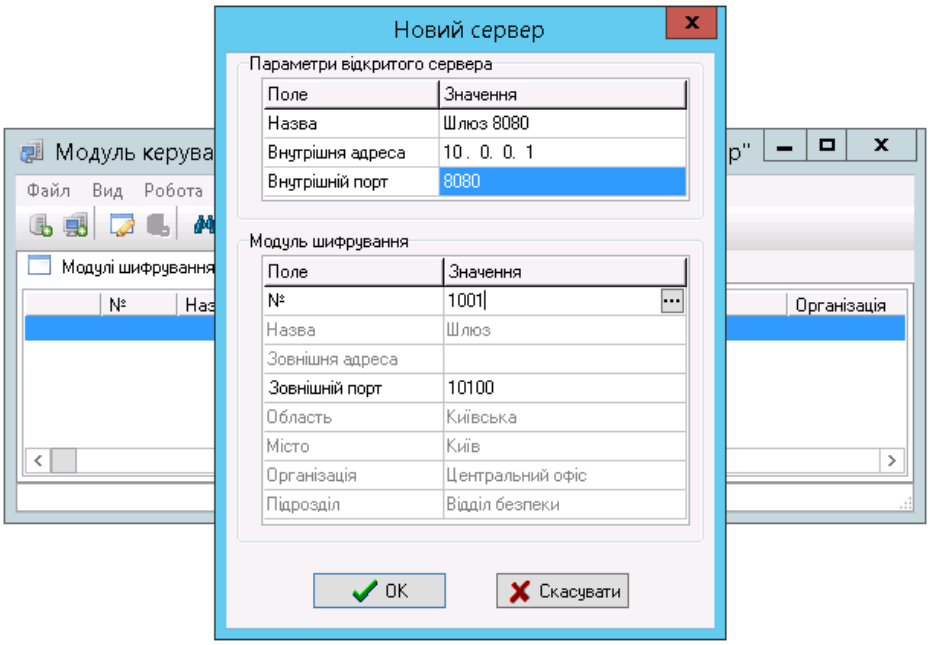
Назва – назва сервера в модулі керування

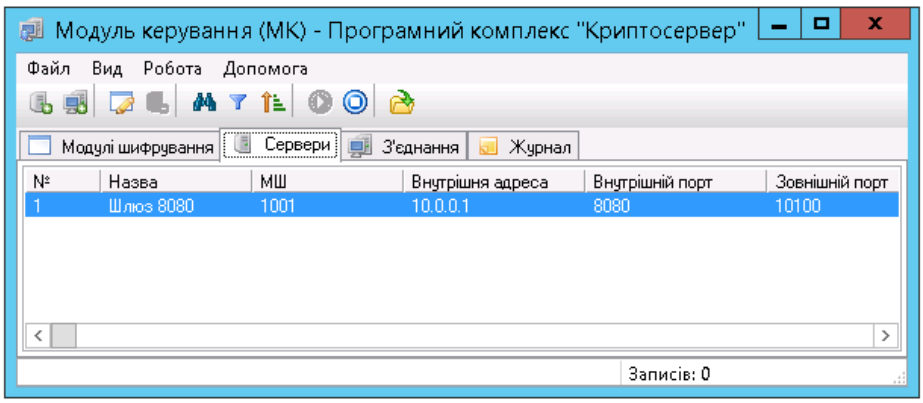
Внутрішня адреса – IP-адреса на яку будуть перенаправлятись дані від клієнтських МШ

Внутрішній порт - порт на який будуть перенаправлятись дані від клієнських МШ

№ - модуль шифрування, який буде виступати сервером

Зовнішній порт – порт, по якому до сервера будуть під`єднуватись клієнтські МШ





Перевіримо\налаштуємо конфігурацію модуля шифрування, шляхом зміни параметрів в файлі «C:\cryptoserver\CS\CryptoServer.ini»

[common]

cacertfile=

certdir=cert_db

certfile=

contfile=

dkefile=

keysdir=keys

pass=

sid=

[ocsp]

certfile=

addr=127.0.0.1

port=10001

[mk]

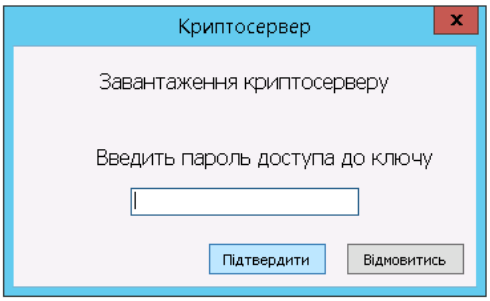
addr=127.0.0.1

port=10002

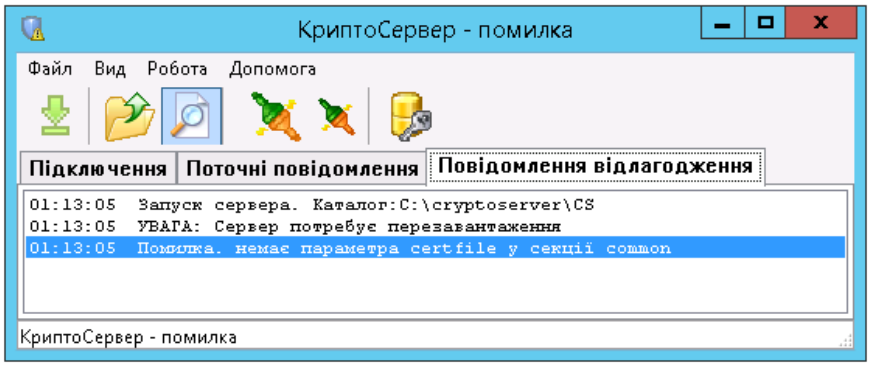
sid=3

Запускаємо файл розташований по наступному шляху «C:\cryptoserver\CS\ CryptoServer.exe»

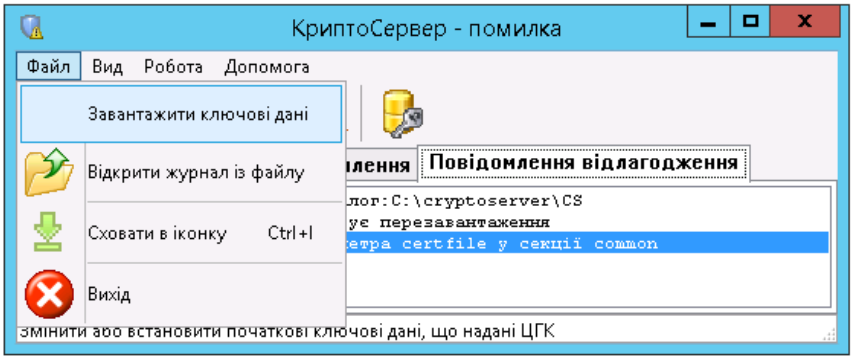
На запит паролю нічого не вводимо, натискаємо «Підтвердити»



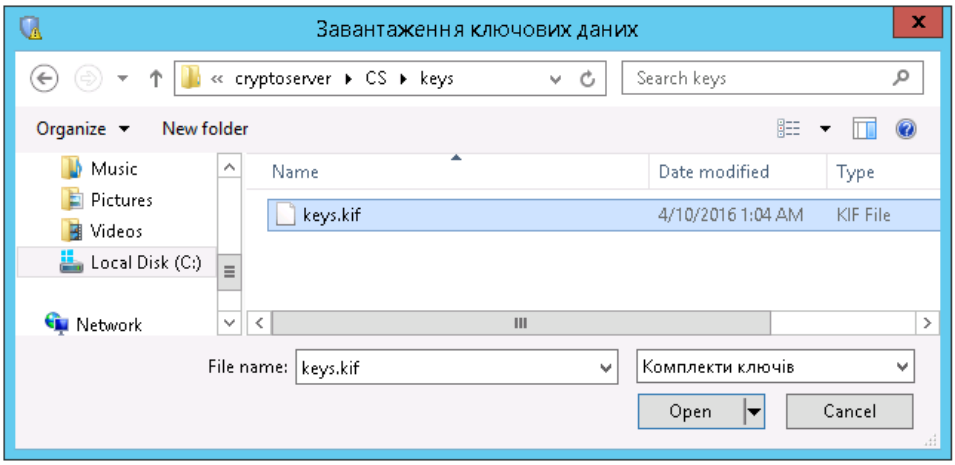
Буде видано повідомлення о помилці:



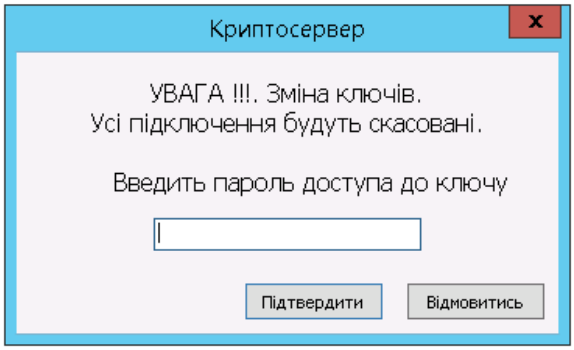
Завантажимо ключові дані - пункт меню «Файл» підпункт меню «Завантажити ключові дані»:



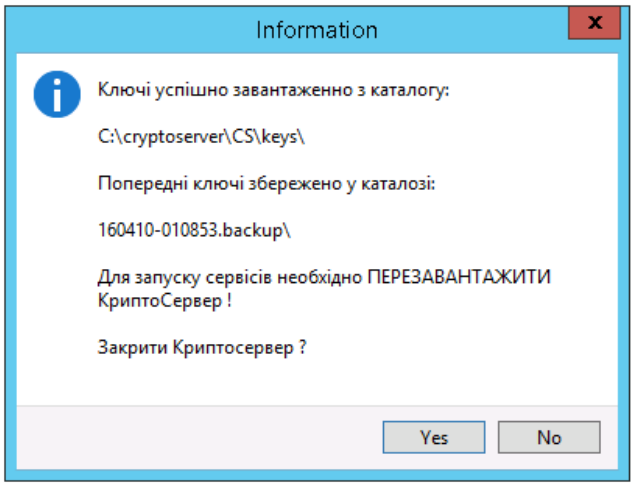
Ключові дані для модуля шифрування модуля керування знаходяться в каталозі, який ми обрали для збереження ключів в процесі генерації ключів МШ - «C:\cryptoserver\CS\keys\», в файлі «keys.kif»



Вводимо пароль до ключових даних (пароль можна знайти в текстовому файлі, що знаходиться в каталозі, який ми обрали для збереження ключів в процесі генерації ключів МШ - в нашому випадку це «C:\cryptoserver\CS\keys\»)



Закриваємо модуль шифрування:

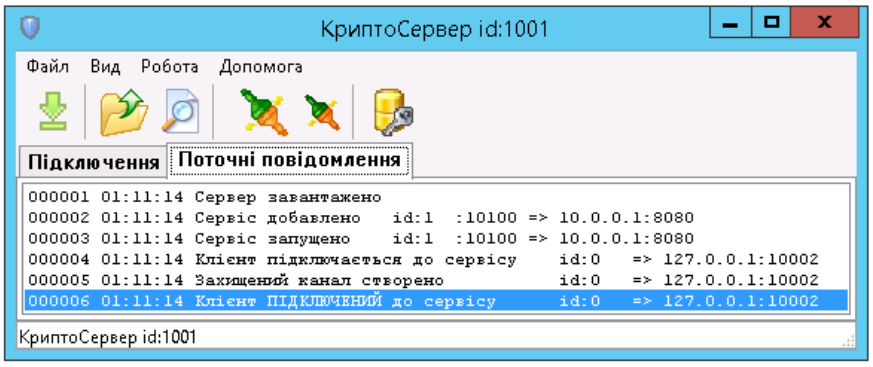


Для того, щоб не вводити пароль кожен раз при завантаженні модуля шифрування, можемо записати його в в файлі «C:\cryptoserver\ CS\ CryptoServer.ini» блок [common], параметр «pass».

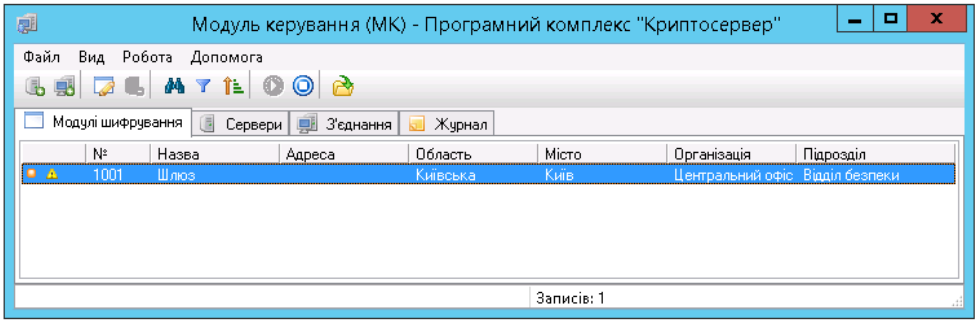
[common]

pass= 4EFMSOiR

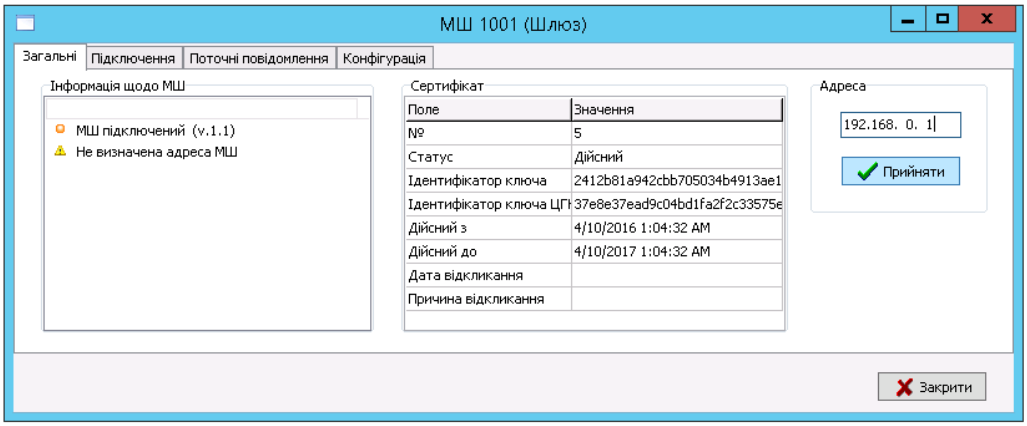
Запускаємо модуль шифрування і перевіряємо статус:

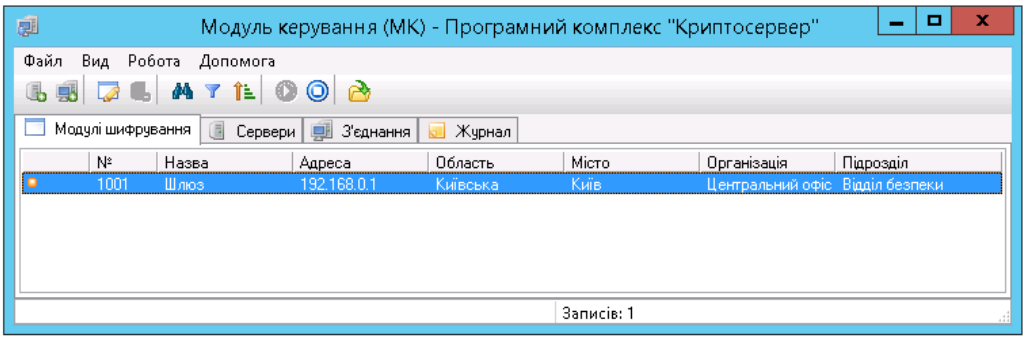


Повертаємось до МК, переходимо на закладку «Модулі шифрування». на ній повиннен бути відображений наш модуль шифрування 1001. В разі якщо МШ 1001 не відображується, перезавантажуємо модуль керування і модуль шифрування, який ми налаштовуємо



Подвійним клацанням відкриваємо властивості модуля шифрування і заповнюємо поле «Адреса» (Це IP-адреса, до якої будуть під`єднуватись клієнтські модулі шифрування)


МШ 1001 (Шлюз)
Загальні
Підключення
Поточні повідомлення
Конфігурація
Інформація щодо МШ
МШ підключений (v.1.1)
Не визначена адреса МШ
Сертифікат
Поле
Значення
№
5
Статус
Дійсний
Ідентифікатор ключа
2412b81a942cbb705034b4913ae1
Ідентифікатор ключа ЦГ
37e8e37ead9c04bd1fa2f2c33575e
Дійсний з
4/10/2016 1:04:32 AM
Дійсний до
4/10/2017 1:04:32 AM
Дата відкликання
Причина відкликання
Адреса
192.168. 0. 1
Прийняти
Закрити


Модуль керування (МК) - Програмний комплекс "Криптосервер"
Файл
Вид
Робота
Допомога
Модулі шифрування
Сервери
З'єднання
Журнал
№
Назва
Адреса
Область
Місто
Організація
Підрозділ
1001
Шлюз
192.168.0.1
Київська
Київ
Центральний офіс
Відділ безпеки
Записів: 1

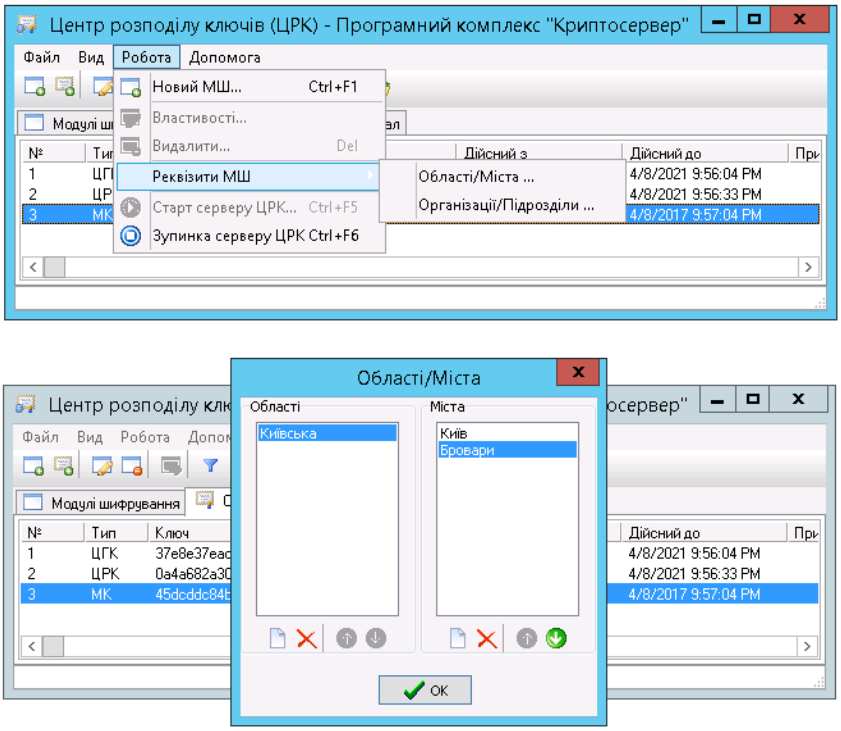
Створення клієнтських модулів шифрування

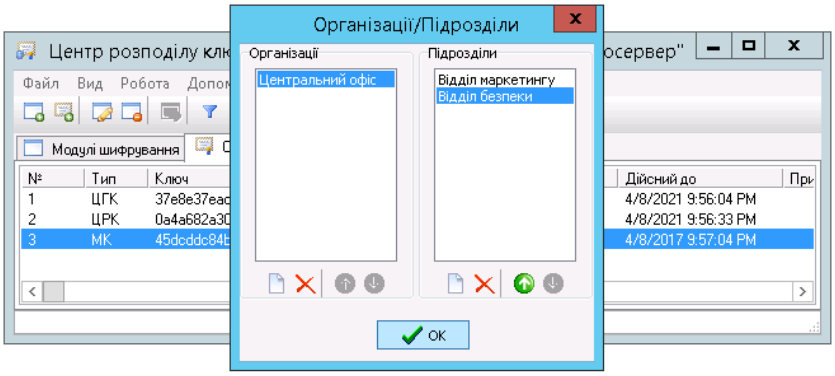
Процес створення модулів шифрування в комплексі «Криптосервер» виглядає наступним чином:

1. Реєстрація нових МШ в ЦРК (KDC)
2. Експорт списку МШ
3. Завантаження списку МШ в ЦГК (KGC)
4. Генерація ключових даних і сертифікатів в ЦГК (KGC)
5. Імпорт згенерованих сертифікатів в ЦРК (KDC)
6. Налаштування МШ в МК
7. Завантаження ключових даних в кожну окрему копію МШ

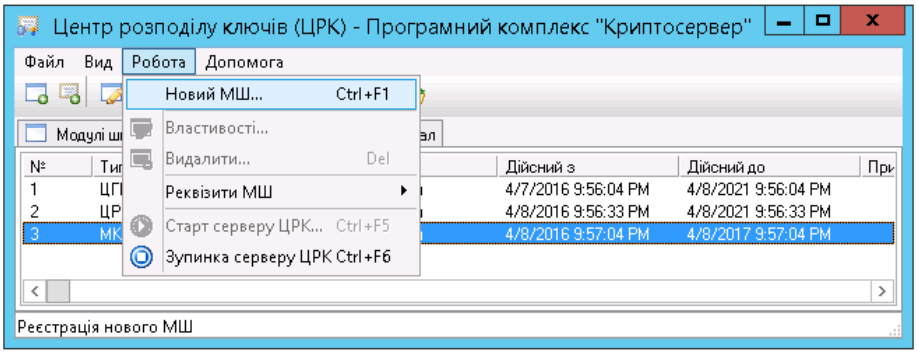
Створюємо каталог в який будемо зберігати ключову інформацію модуля шифрування (для кожного МШ – свій каталог), наприклад «C:\cryptoserver\keys\МШ1»

Запускаємо Центр розподілу ключів (KDC) і заповнюємо реквізити МШ (в разі, якщо вони ще не внесені до МК) - пункт меню «Робота» підпункт меню «Реквізити МШ» підпункти «Області/Міста», «Організації/Підрозділи»:

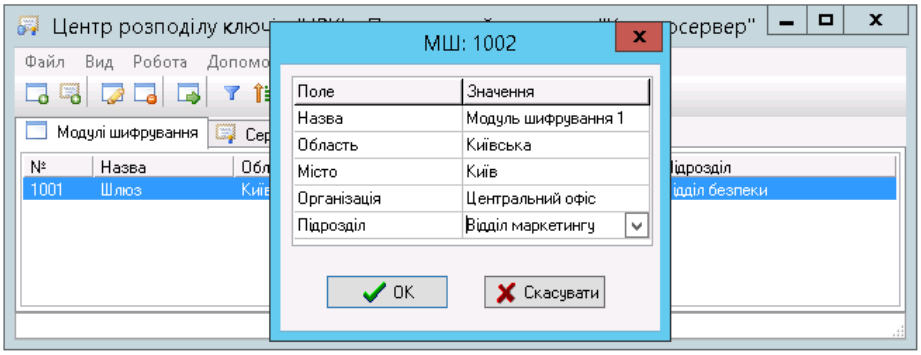




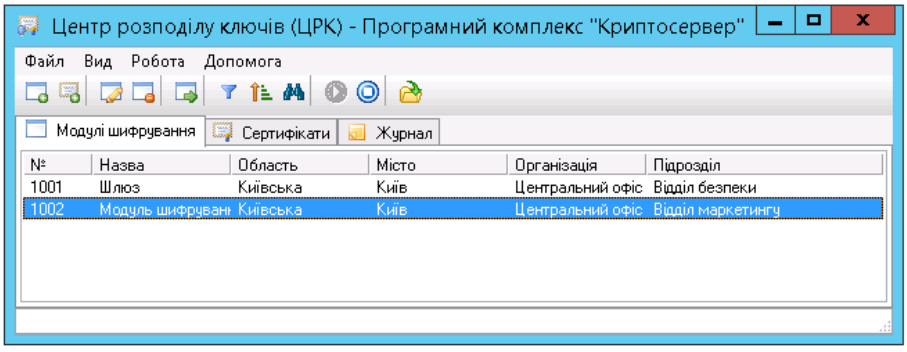
Обираємо пункт меню «Робота» підпункт меню «Новий МШ»



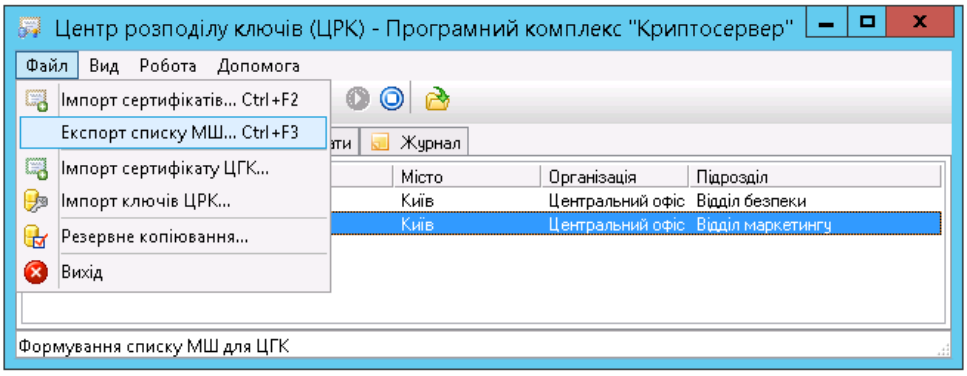
Заповнюємо поля



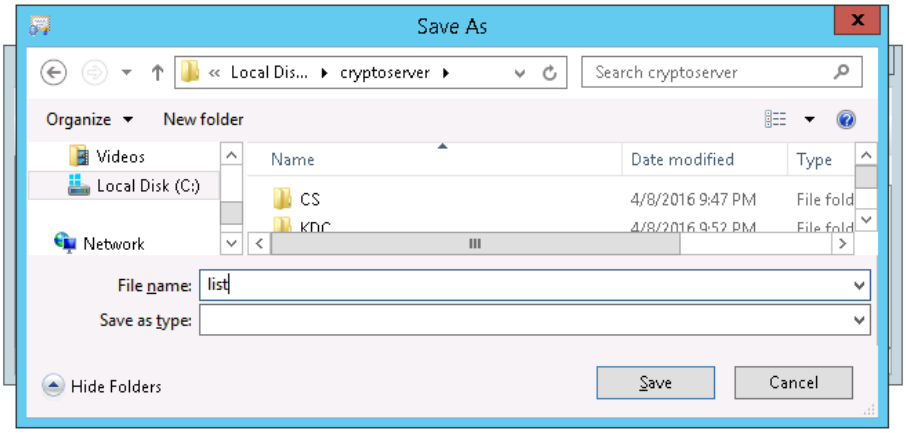
В закладці «Модулі шифрування» з`явиться новий МШ

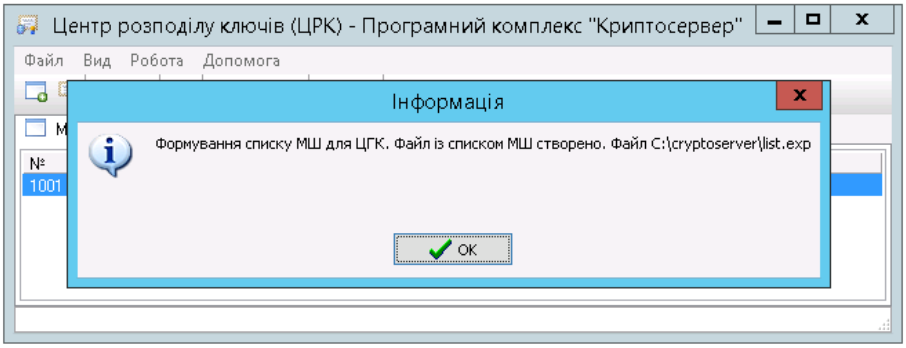


Обираємо пункт меню «Файл» підпункт меню «Експорт списку МШ»

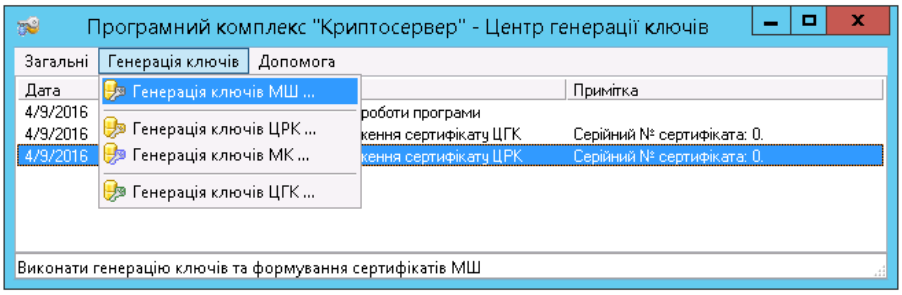


Зберігаємо під обраною назвою

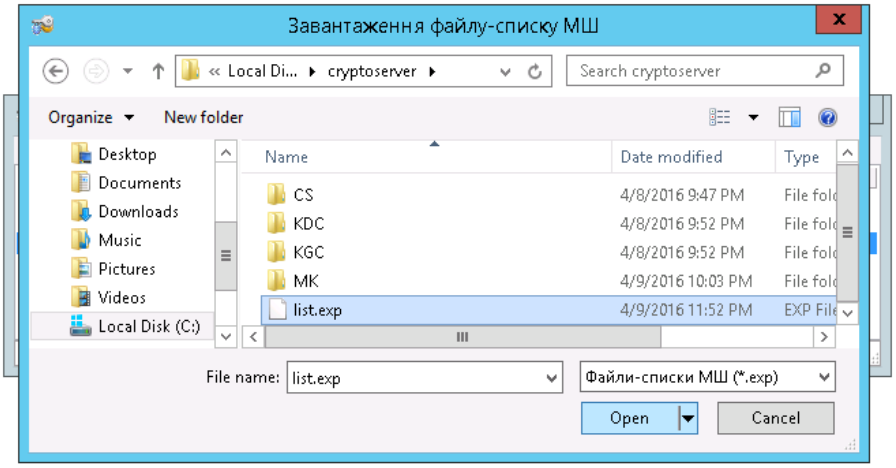




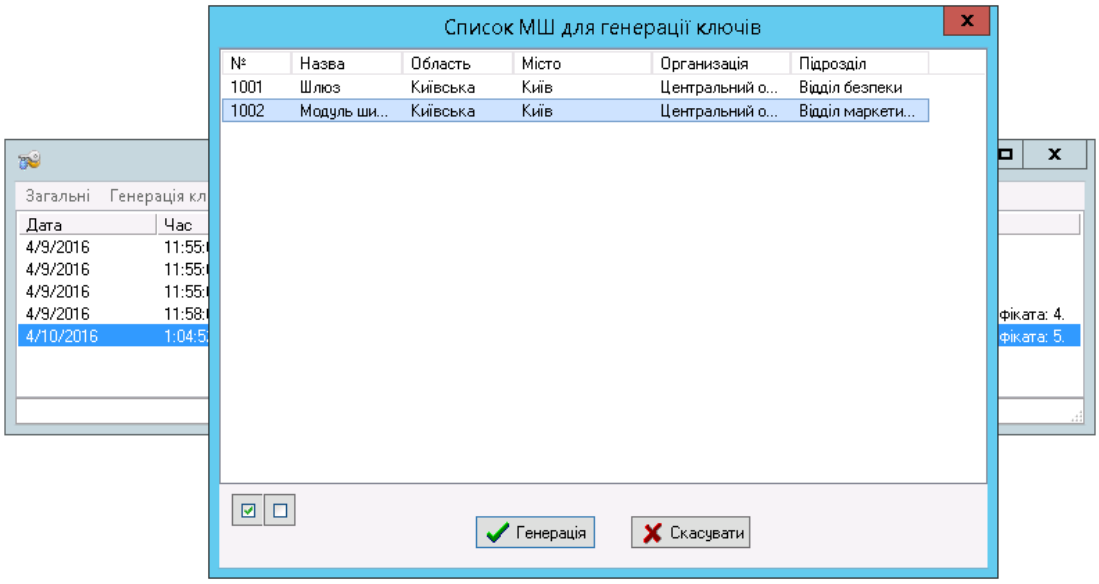
Запускаємо Центр генерації ключів (KGC), обираємо пункт меню «Генерація ключів» підпункт меню «Генерація ключів МШ …»



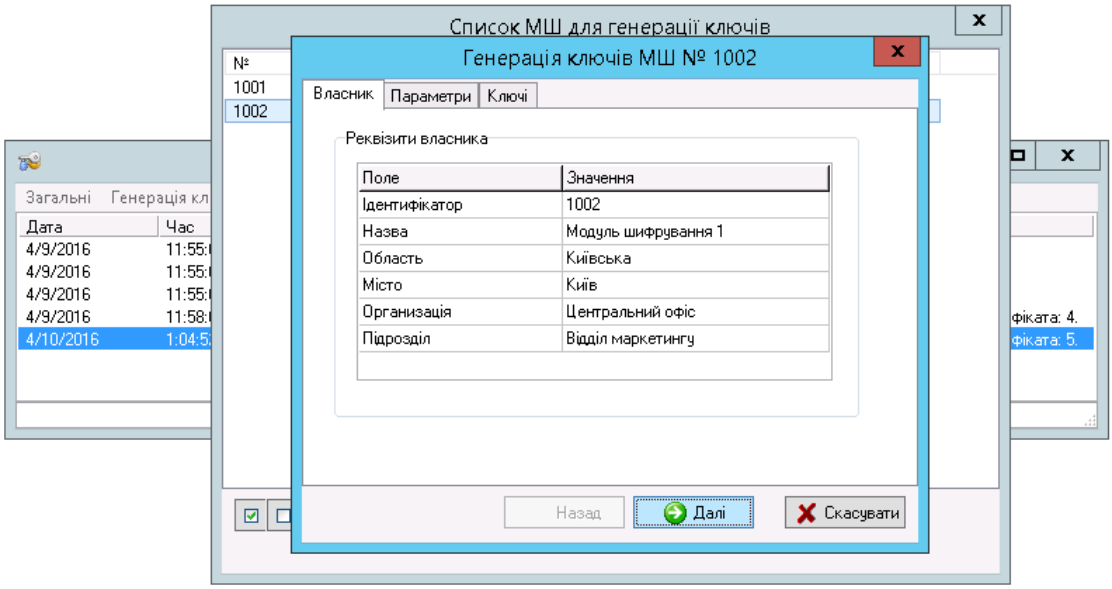
Знаходимо файл зі списком МШ, який ми імпортували з ЦРК (KDC)



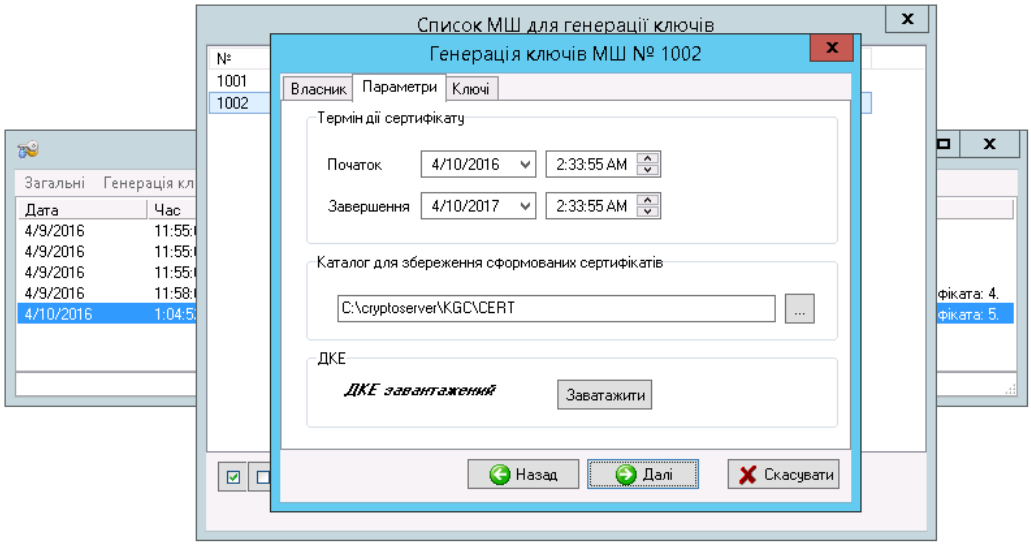
Обираємо МШ для якого нам потрібно згенерувати ключі і натискаємо кнопку «Генерація»:



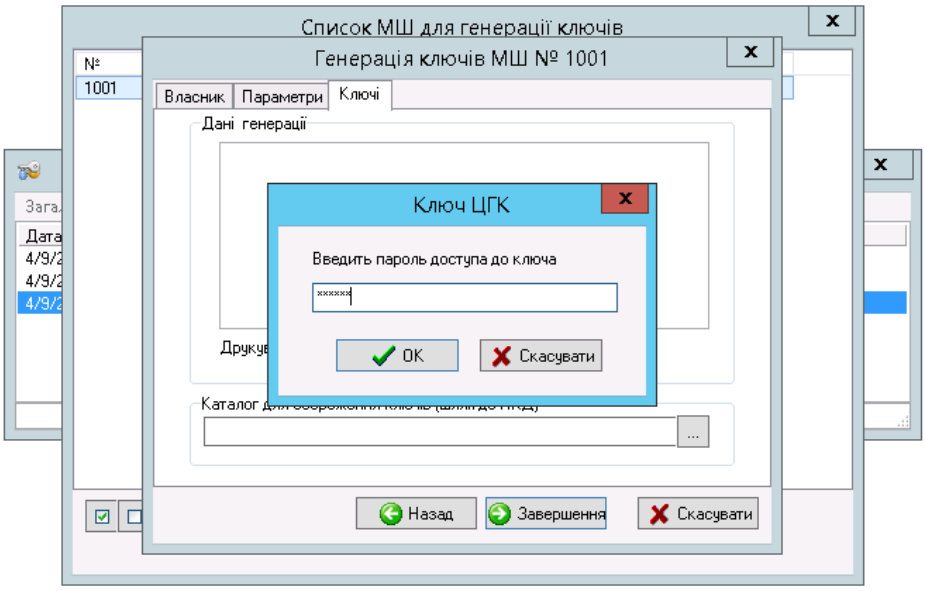
Змінити параметри власника МШ в даному вікні ми вже **не** можемо, натискаємо «Далі»



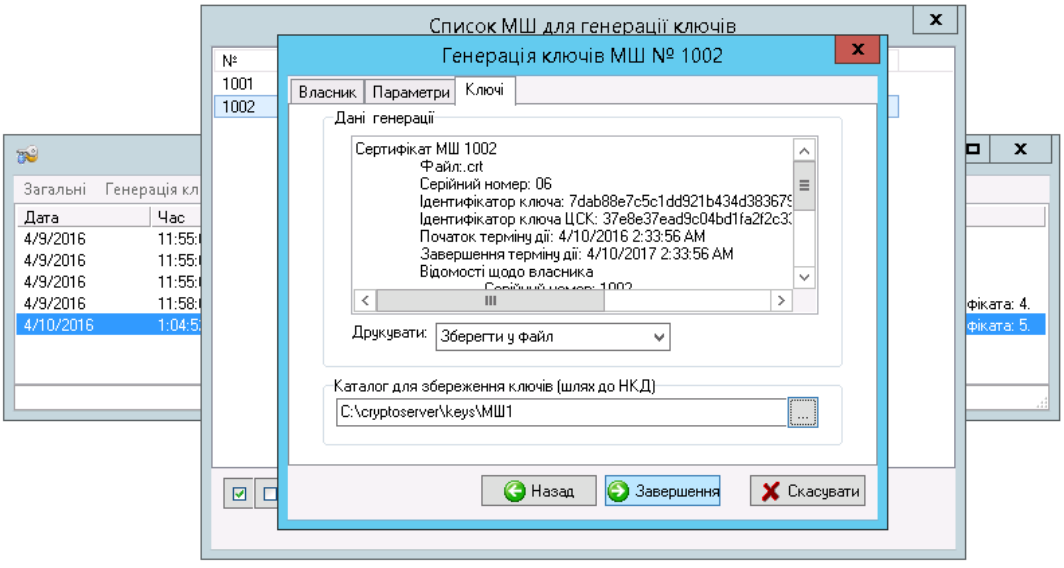
Обираємо термін дії сертифікату, каталог для збереження сертифікатів, та завантажуємо файл ДКЕ (якщо він ще не завантажений)



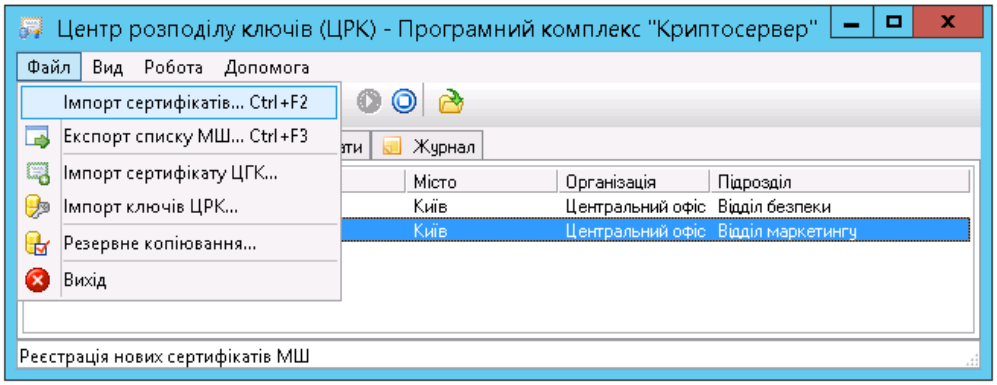
Вводимо пароль доступу до ключа ЦГК (KGC) (в разі, якщо ключі вже генерувались і модуль ЦГК не закривали, то запит пароля ЦГК відбуватись не буде)



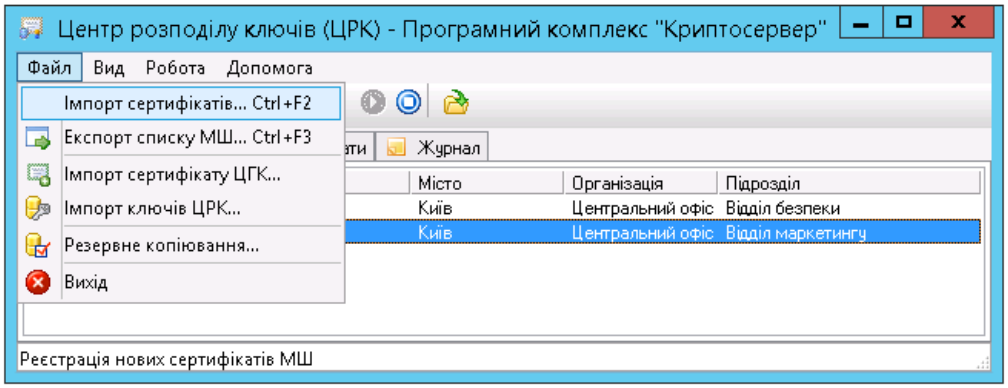
Обираємо каталог для збереження ключа і завершуємо генерацію:

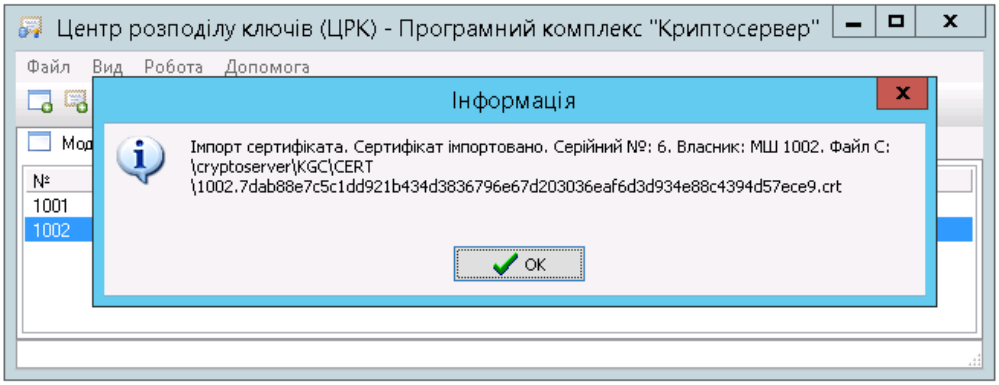


Повертаємось до ЦРК (KDC) і імпортуємо створений сертифікат - пункт меню «Файл» підпункт меню «Імпорт сертифікатів…»



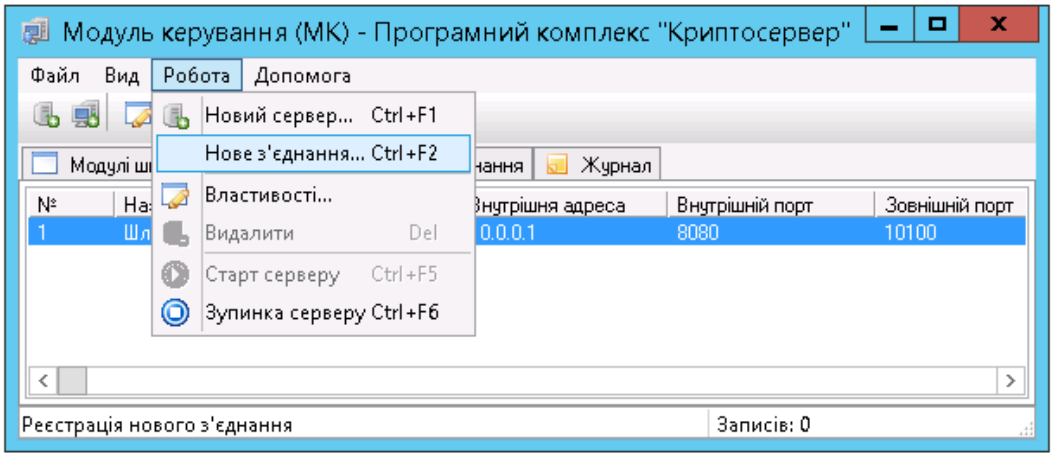
Обираємо сертифікат з каталогу, в який його зберігали під час генерації «C:\cryptoserver \KGC\CERT» (Увага! Назва файла сертифікату буде починатись з його порядкового номеру, що був присвоєний модулю шифрування під час створення нового МШ в ЦРК, в нашому випадку це - 1002)



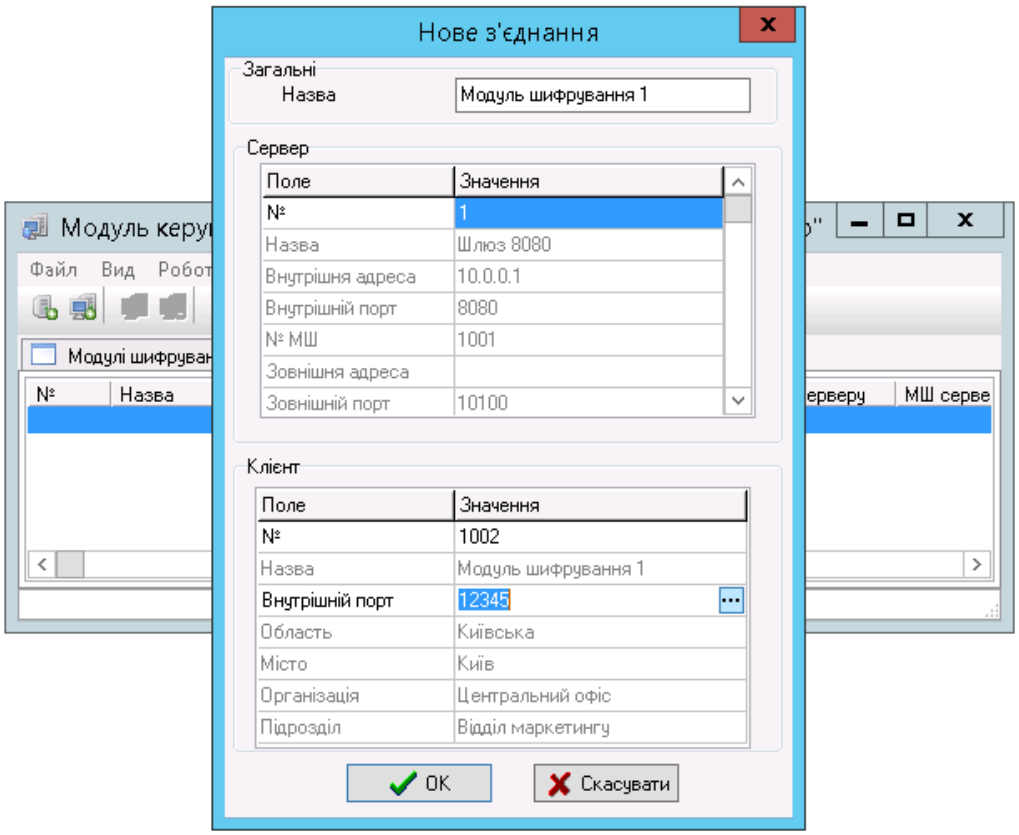


Запускаємо модуль керування і налаштовуємо конфігурацію МШ:

Так як наш МШ буде працювати в режимі клієнта, то обираємо пункт меню «Робота» підпункт меню «Нове з`єднання …»



Заповнюємо параметри нового з`єднання



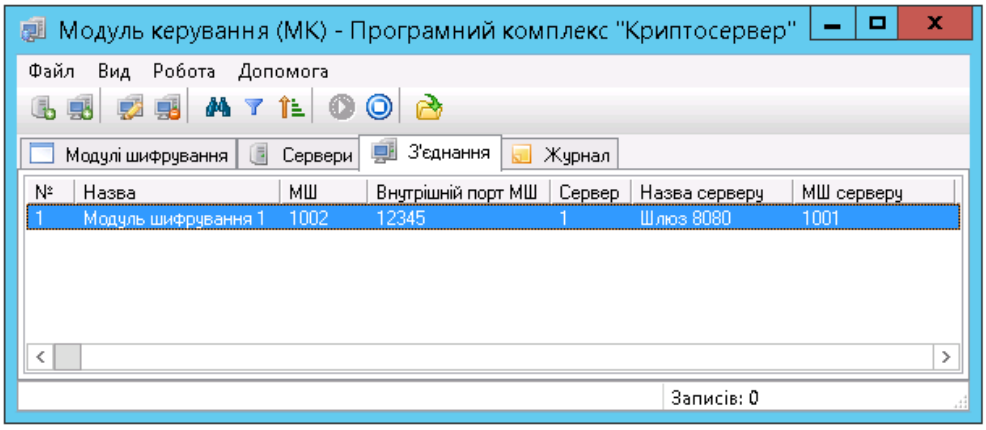
Значення полей:

Назва – назва з`єднання в модулі керування

Сервер № – МШ-сервер, до якого буде під`єднуватись даний МШ

Клієнт № - МШ, який буде виступати клієнтом

Внутрішній порт – порт, по якому до МШ буде під`єднуватись додаток користувача



Тепер створимо робочий клієнтський модуль шифрування:

Створимо каталог «C:\cryptoserver\CS1002\» (згідно з номером модуля шифрування, але назва не принципова, можна обирати такий принцип найменування, який буде зручніший вам)

До нього скопіюємо все з каталогу «C:\cryptoserver\CS\»

Видалимо всі файли з каталогів «C:\cryptoserver\CS1002\cert_db», «C:\cryptoserver\CS1002\keys», «C:\cryptoserver\CS1002\Logs».

Відредагуємо файл «C:\cryptoserver\CS1002\CryptoServer.ini»

(Видалимо з нього всі дані про сертифікати, ключові дані, налаштування з`єднань)

[common]

cacertfile=

certdir=cert_db

certfile=

contfile=

dkefile=

keysdir=keys

pass=

sid=

[ocsp]

certfile=

addr=192.168.0.1

port=10001

[mk]

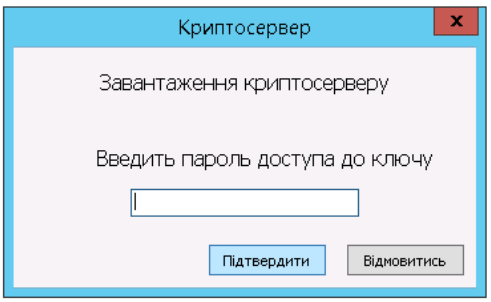
addr=192.168.0.1

port=10002

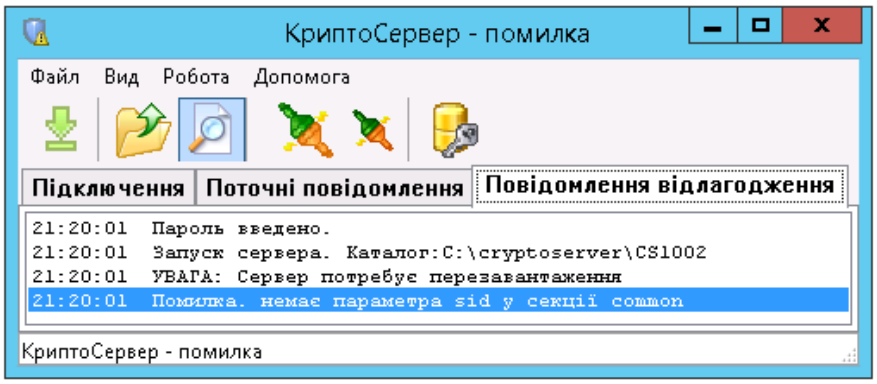
sid=3

Запускаємо файл розташований по наступному шляху «C:\cryptoserver\CS1002\ CryptoServer.exe»

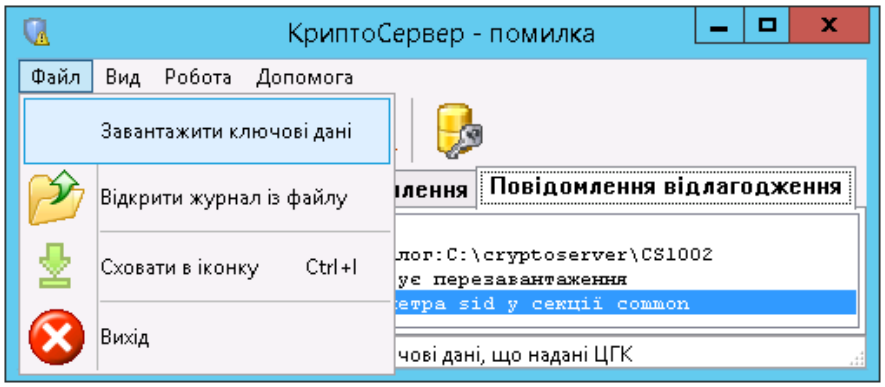
На запит паролю нічого не вводимо, натискаємо «Підтвердити»



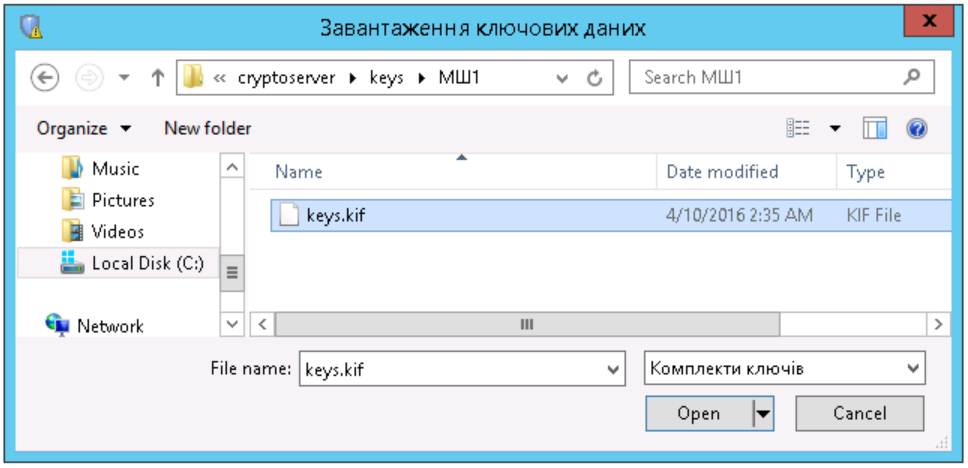
Буде видано повідомлення о помилці:



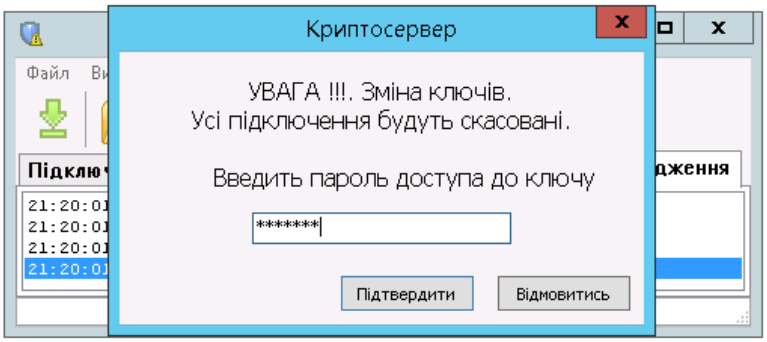
Завантажимо ключові дані - пункт меню «Файл» підпункт меню «Завантажити ключові дані»:



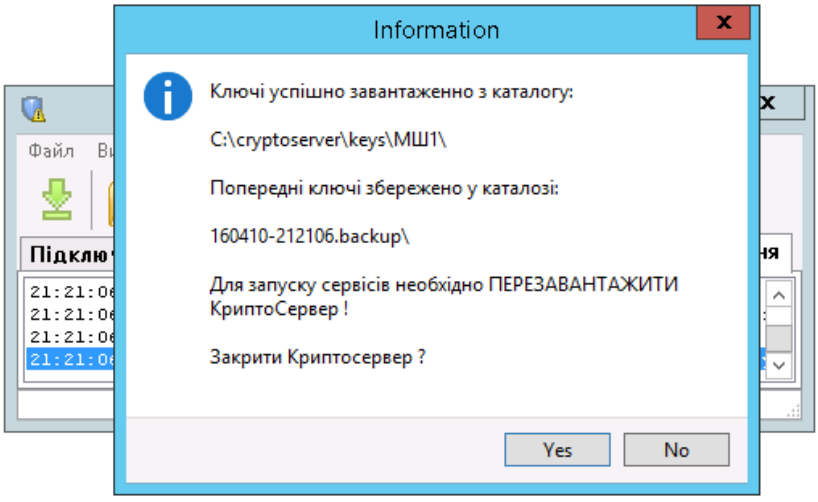
Ключові дані для модуля шифрування знаходяться в каталозі, який ми обрали для збереження ключів в процесі генерації ключів МШ - «C:\cryptoserver\keys\МШ1\», в файлі «keys.kif»



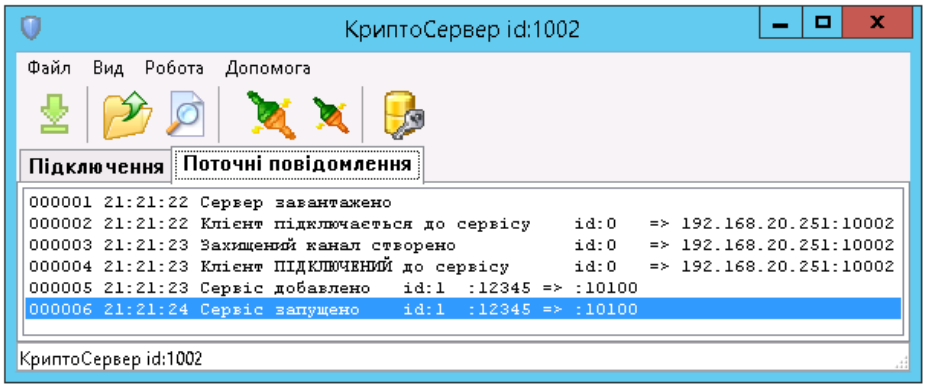
Введемо пароль до ключових даних (пароль можна знайти в текстовому файлі, що знаходиться в каталозі, який ми обрали для збереження ключів в процесі генерації ключів МШ - в нашому випадку це «C:\cryptoserver\keys\МШ1\»)



Закриваємо модуль шифрування:



Запускаємо модуль шифрування і перевіряємо статус:



Після того, як ми додали ключові дані і перезавантажили модуль шифрування, він підключиться до ЦРК і завантажить звідти сертифікати до каталогу «C:\cryptoserver\CS1002\cert_db», потім підключиться до модуля керування, завантажить звідти налаштування, що стосуються цього модуля шифрування і збереже їх в відповідних полях файла «C:\cryptoserver\ CS1002\ CryptoServer.ini»

В результаті ми отримаємо наступний файл «C:\cryptoserver\ CS1002\ CryptoServer.ini», в якому автоматично прописані дані щодо сертифікатів, ключової інформації, та налаштування з`єднання даного модуля шифрування:

[common]

cacertfile=ca.37e8e37ead9c04bd1fa2f2c33575e62e83067e6d4da759b544c8745628423fe8.crt

certdir=cert_db

certfile=1002.7dab88e7c5c1dd921b434d3836796e67d203036eaf6d3d934e88c4394d57ece9.crt

contfile=1002.7dab88e7c5c1dd921b434d3836796e67d203036eaf6d3d934e88c4394d57ece9.cnt

dkefile=1002.7dab88e7c5c1dd921b434d3836796e67d203036eaf6d3d934e88c4394d57ece9.dke

keysdir=keys

sid=1002

[ocsp]

addr=192.168.0.1

certfile=ocsp.0a4a682a30d84ebdf1c0a0793c8360dc6cb77e737c0de226cc450ca9d1e3f5b9.crt

port=10001

[mk]

addr=192.168.0.1

port=10002

sid=3

[link1]

id=1

inp_port=12345

out_addr=192.168.0.1

out_port=10100

sid=1001

type=client

Клієнтський модуль шифрування готовий до роботи, достатньо скопіювати каталог «CS1002» на потрібний ПК, та надати користувачу пароль до ключових даних. Аналогічним образом налаштовуються нові клієнтські модулі шифрування.

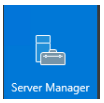
Автоматизація запуску програмного комплексу КЗІ «Криптосервер»

Для забезпечення автоматичного запуску програмного комплексу КЗІ «Криптосервер» під час планового або аварійного перезавантаження серверного обладнання рекомендується виконати наступні кроки.

1. Автоматичний запуск СКБД MySQL

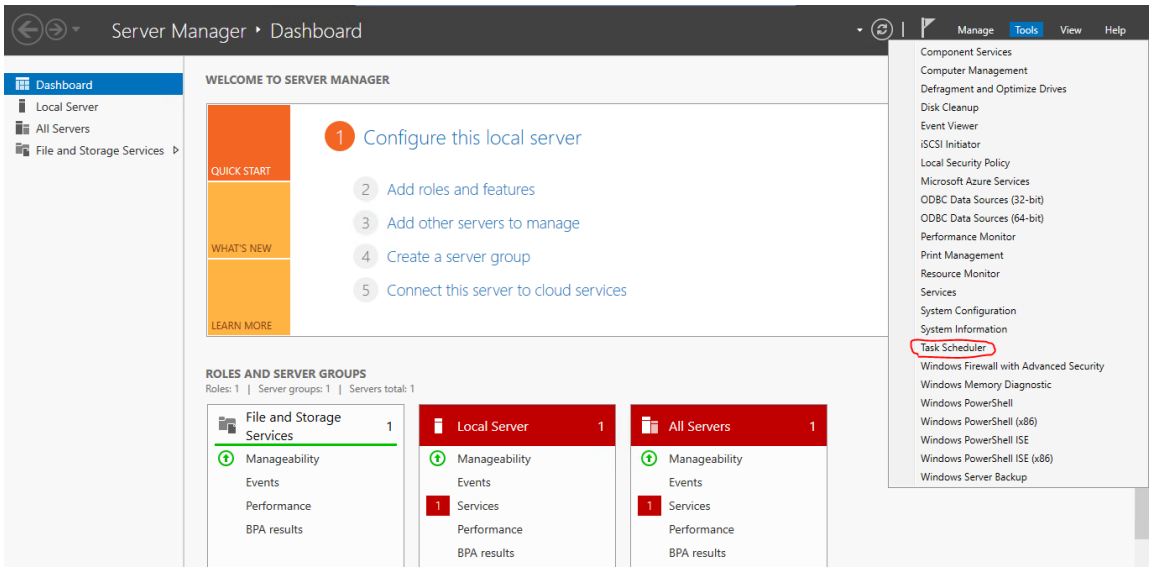
СКБД MySQL – це перший модуль програмного комплексу КЗІ «Криптосервер», що повинен бути завантажений. Усі інші модулі під час свого запуску повинні мати доступ до відповідних баз даних СКБД MySQL.

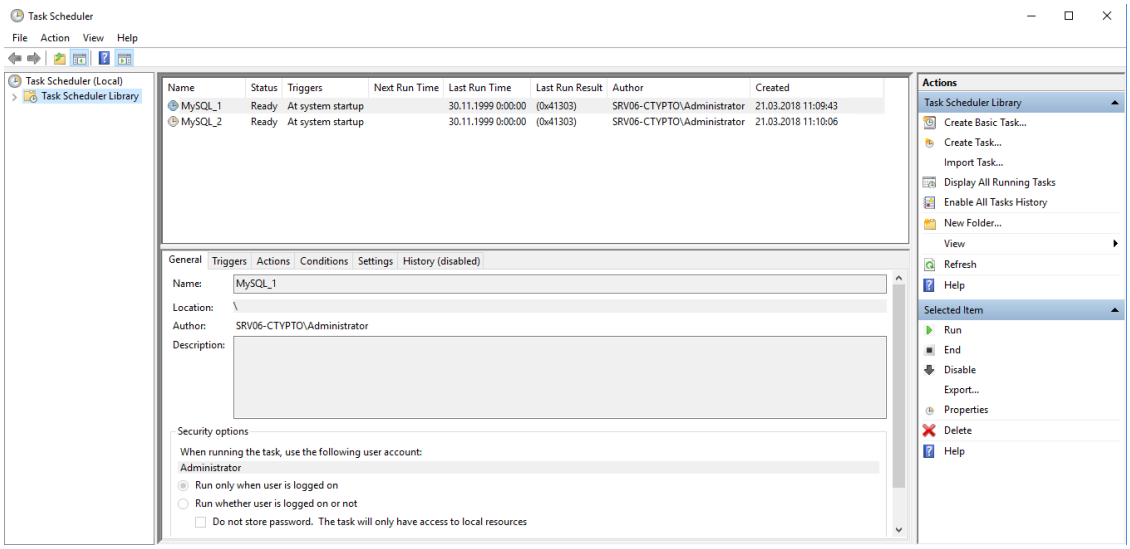
Рекомендовано запускати СКБД MySQL у фоновому режимі. Для цього необхідно виконати наступні кроки:

1.1 Завантажити *Server Manager: ПУСК- іконка* 

або ПУСК – Выполнить (Run) - ServerManager – клавіша Enter

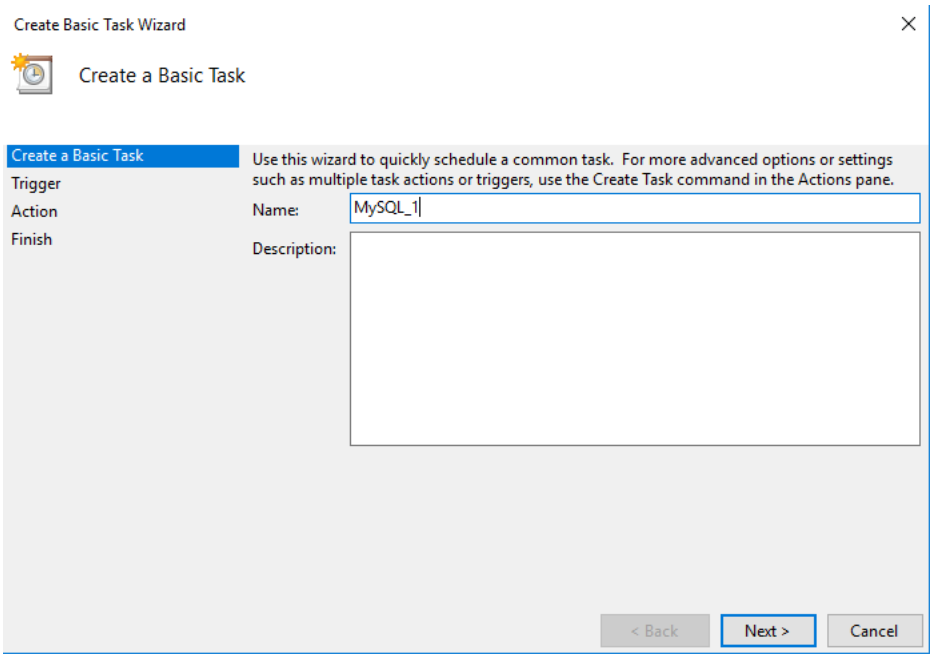
1.2 Завантажуємо Планувальник завдань (Task Scheduler)



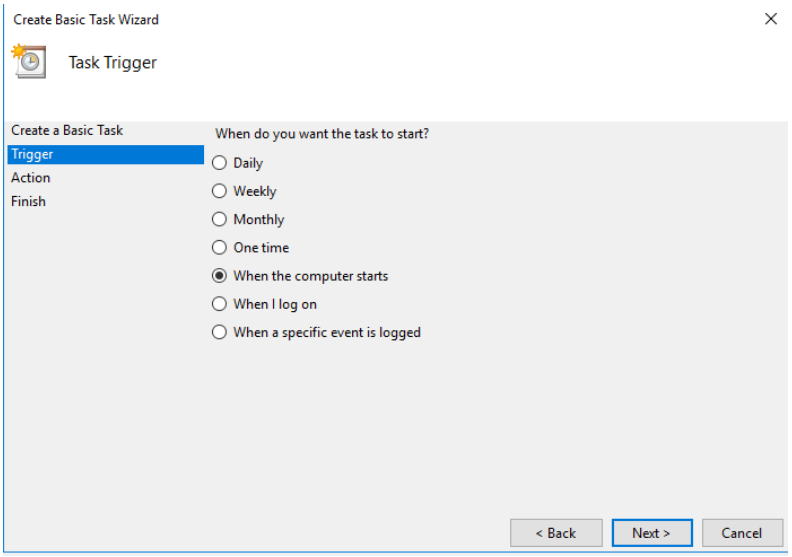


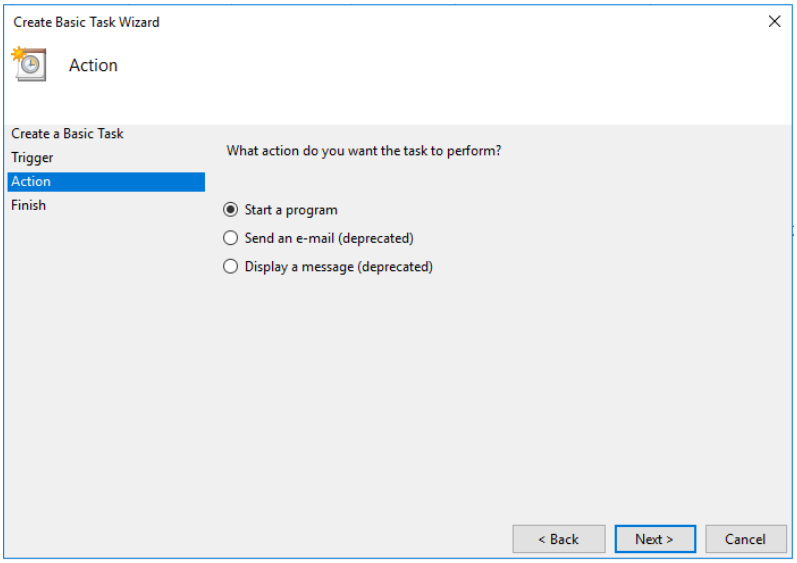
1.3 Створюємо просте завдання (Create Basic Task)

Ім’я завдання довільне, як приклад, MySQL_1

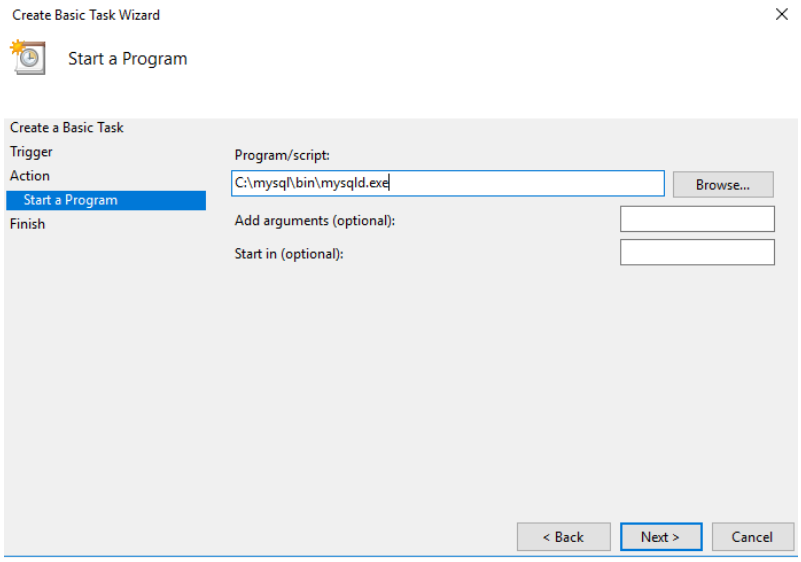


Сценарій запуску завдання - під час старту комп’ютера (When the computer starts)





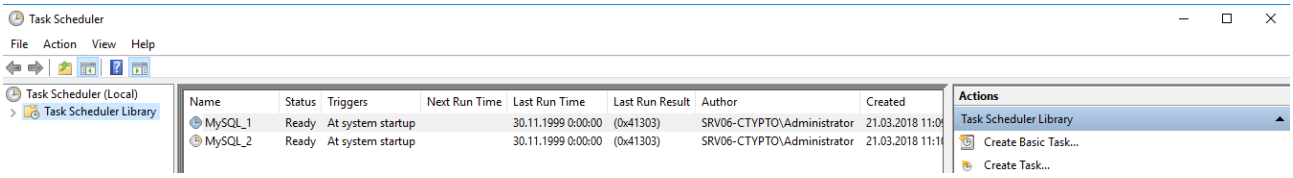
Вказуємо шлях до файлу mysqld.exe (C:\mysql\bin\mysqld.exe) СКБД MySQL



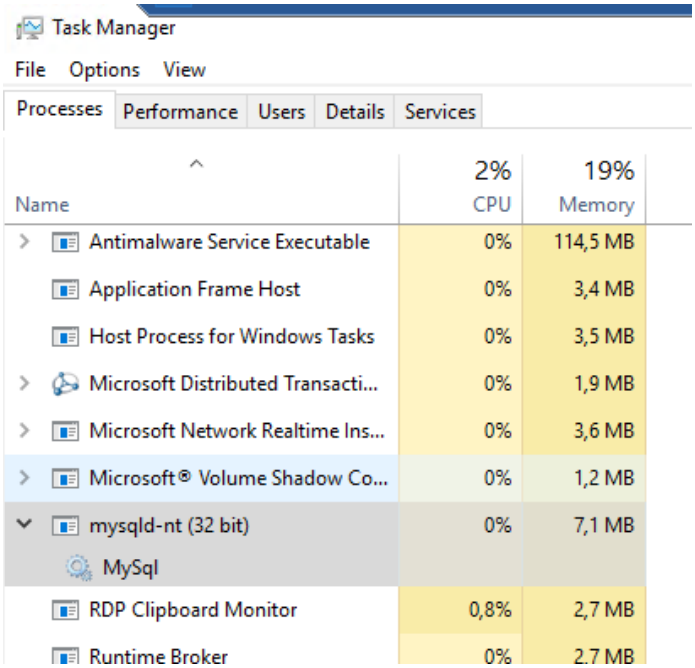
Завершуємо створення завдання кнопками Next - Finish

1.4 Створюємо нове завдання. Повторюємо пп 1.3. Ім’я завдання довільне, як приклад, MySQL_2.

Вказуємо шлях до файлу winmysqladmin.exe (C:\mysql\bin\winmysqladmin.exe) СКБД MySQL



1.5 Після перезавантаження сервера СКБД MySQL запуститься автоматично у фоновому режимі. Перевірити запущений процес СКБД MySQL можна у Диспетчері завдань (Task Manager)



Важливо! Запуск у фоновому режимі СКБД MySQL не прив'язан до реєстрації користувачів у системі.

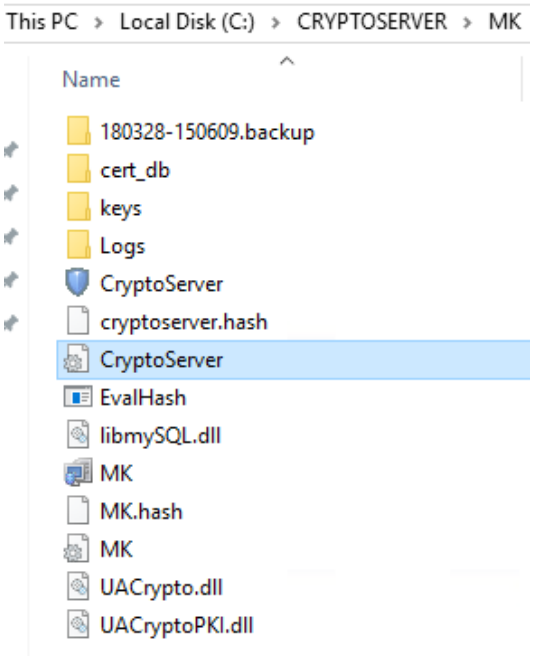
2. Автоматичний запуск модулів шифрування.

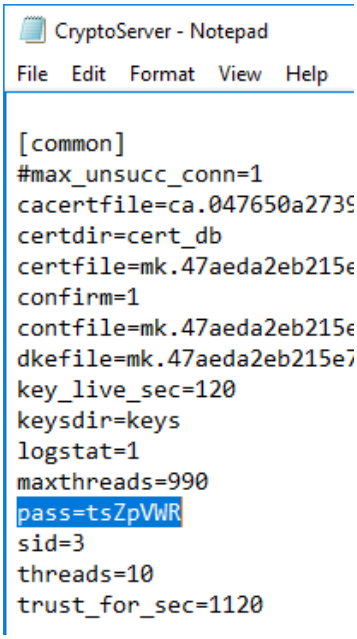
На сервері програмного комплексу КЗІ «Криптосервер», в залежності від схеми побудови, використовується, як мінімум два модулі шифрування: модуль шифрування модуля Керування (CS_MK) та модуль шифрування Сервера (CS_Server).

Важливо! Запуск модулів шифрування цьому пункті здійснюється тільки після реєстрації користувача у системі. Рішення дивись п.4

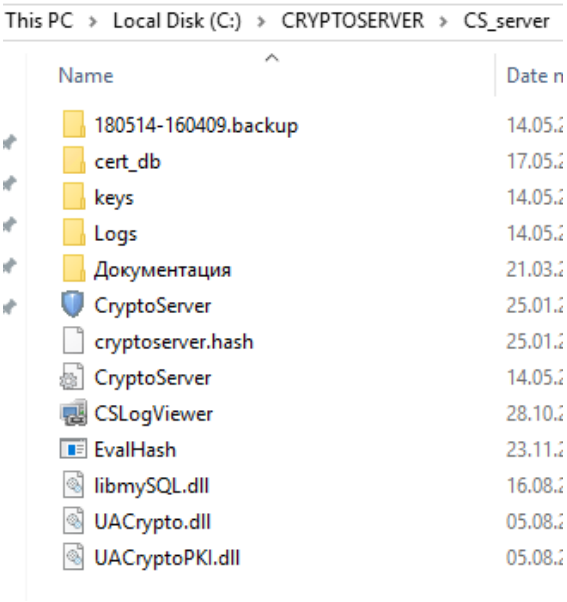
Для автоматичного запуску модулів шифрування рекомендовано виконати наступні кроки:

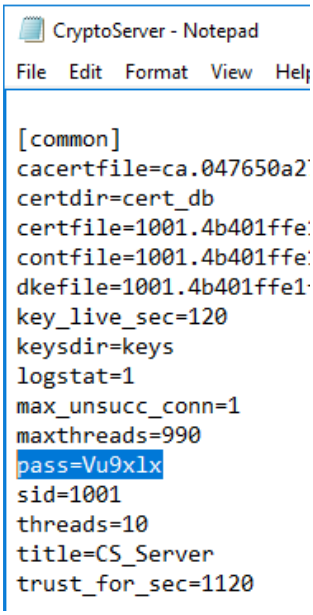
2.1 У конфігураційному файлі CryptoServer.ini модуля шифрування модуля Керування додати пароль авторизації, рядок "pass=пароль" в секції [common]:





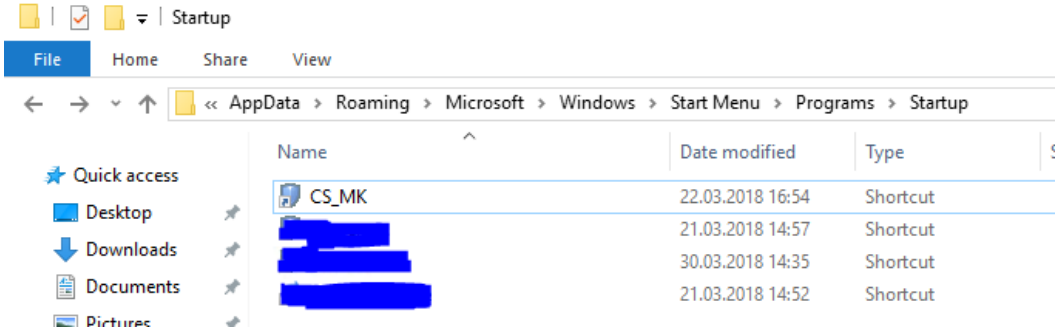
2.2 У конфігураційному файлі CryptoServer.ini модуля шифрування Сервера додати пароль авторизації, рядок "pass=пароль" в секції [common]:



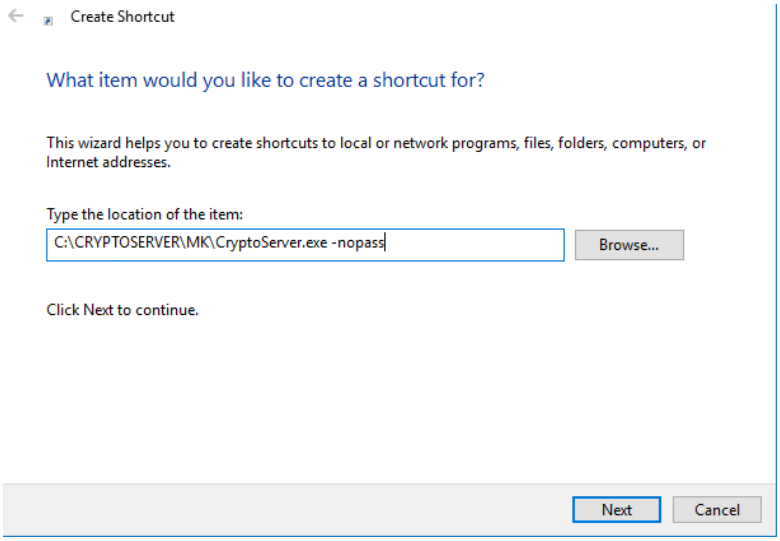


2.3 Створити ярлик автоматичного запуску модуля шифрування модуля Керування

У провіднику перейти до папки, яка зберігає ярлики автоматичного запуску додатків: C:\Users\UserName\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup, де UserName – ім'я користувача системи від якого необхідно запустити додаток



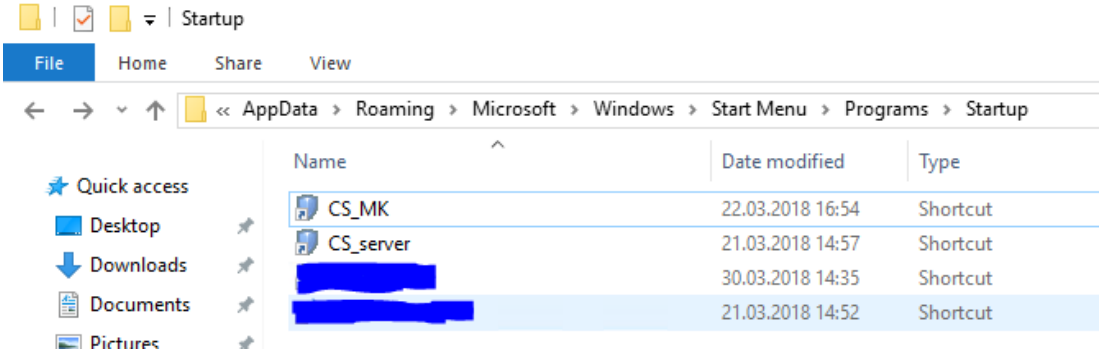
Створити ярлик запуску модуля шифрування модуля Керування з параметром "-nopass"



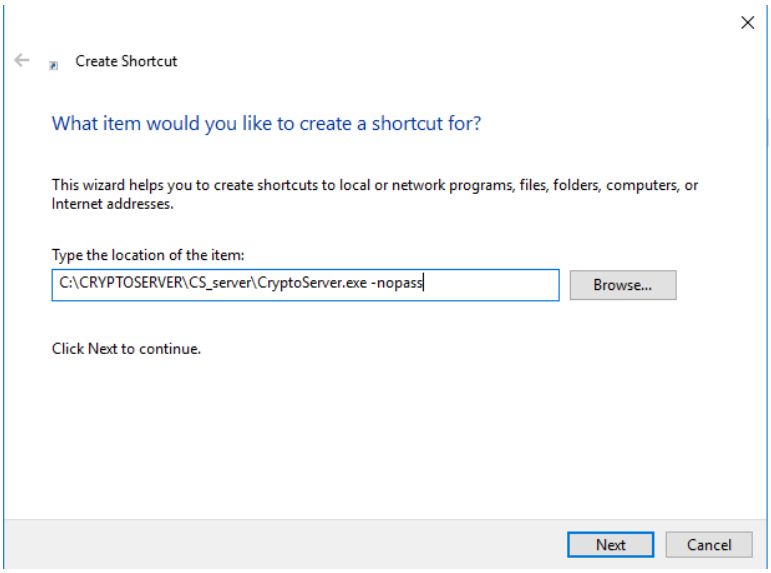
Завершити створення ярлика.

2.4 Створити ярлик автоматичного запуску модуля шифрування Сервера

У провіднику перейти до папки, яка зберігає ярлики автоматичного запуску додатків: C:\Users\UserName\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup, де UserName – ім'я користувача системи від якого необхідно запустити додаток



Створити ярлик запуску модуля шифрування Сервера з параметром "-nopass"

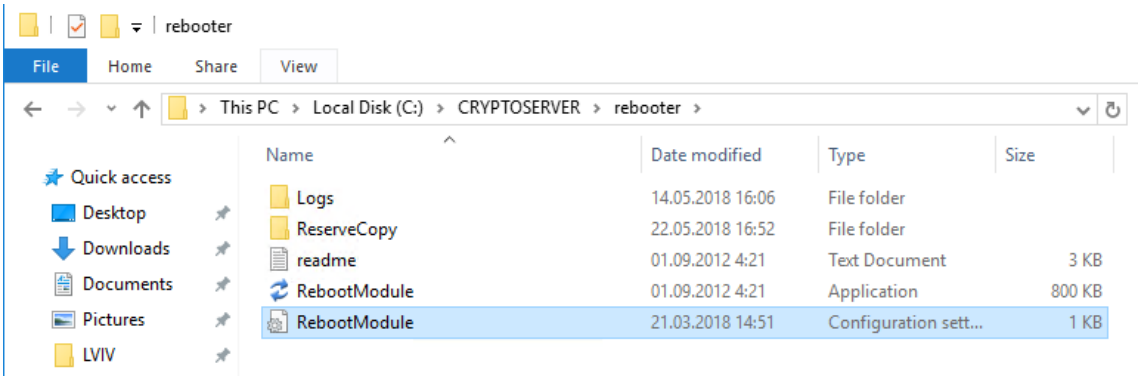


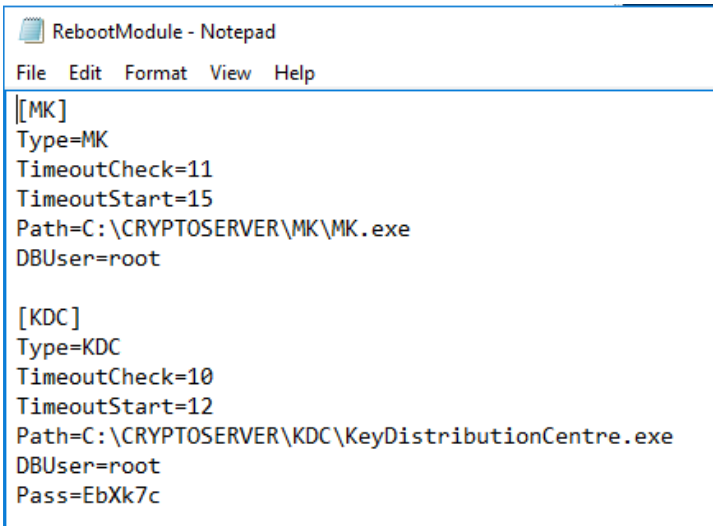
Завершити створення ярлика.

3. Автоматичний запуск модулів ЦРК та МК

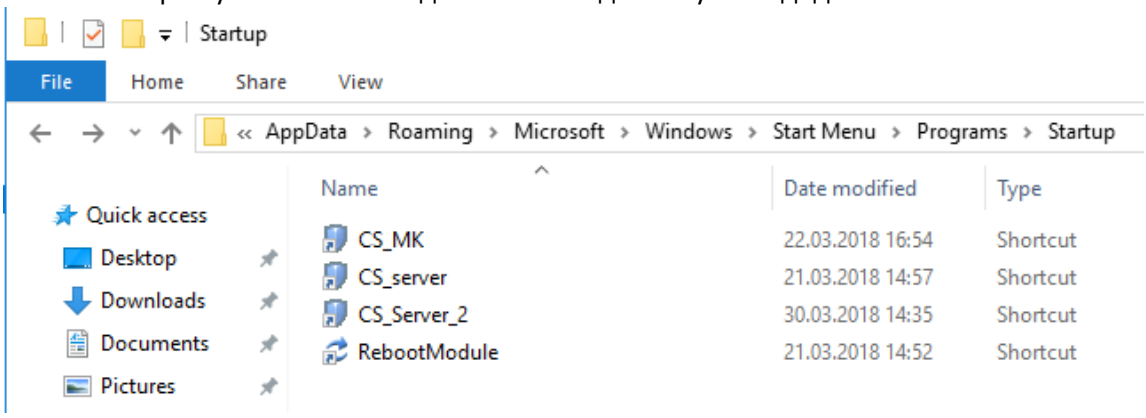
Важливо! Запуск модулів ЦРК та МК в цьому пункті здійснюється тільки після реєстрації користувача у системі. Рішення дивись п.4

3.1 За допомогою додаткового модуля RebootModule, у конфігураційному файлі RebootModule.ini опишемо модулі ЦРК та МК відповідними секціями [KDC] та [MK]

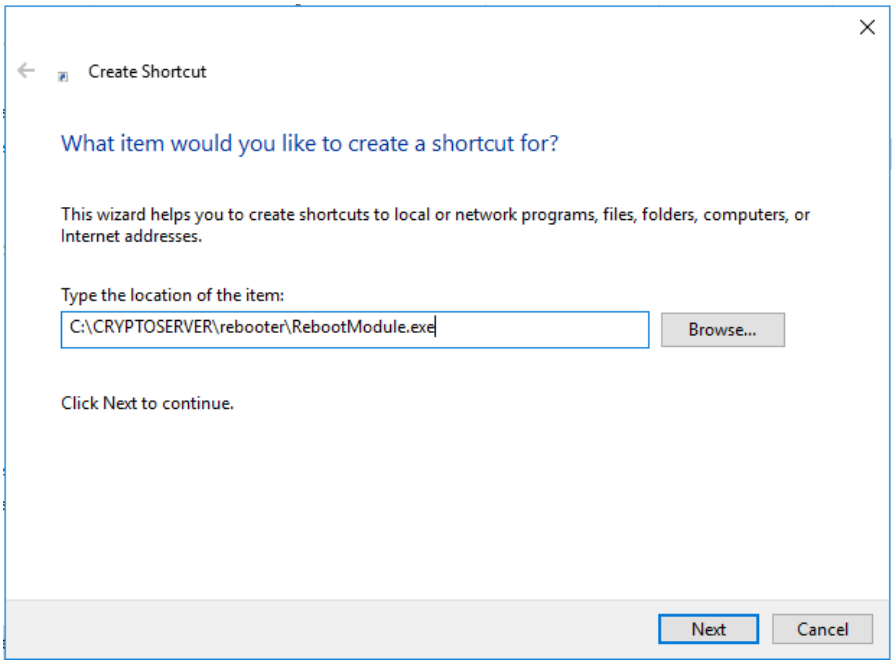




3.2 У провіднику перейти до папки, яка зберігає ярлики автоматичного запуску додатків: C:\Users\UserName\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup, де UserName – ім'я користувача системи від якого необхідно запустити додаток



Створити ярлик запуску модуля RebootModule



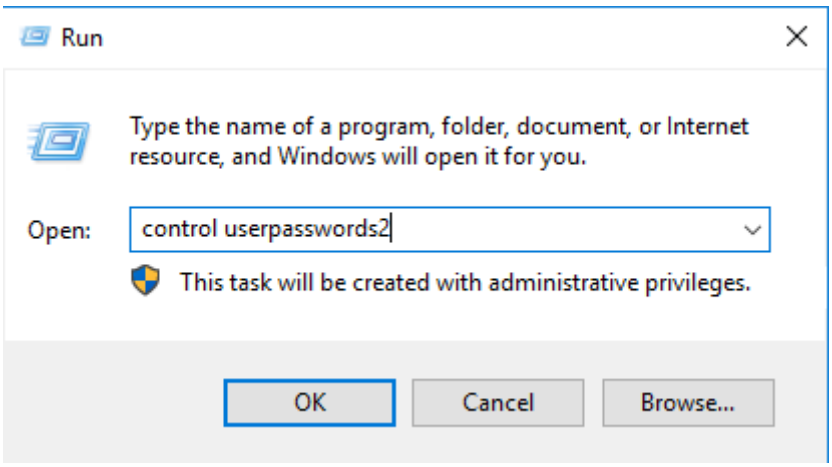
Завершити створення ярлика.

4. Автоматична реєстрація користувача у системі Widows Server – запуск термінальної сесії.

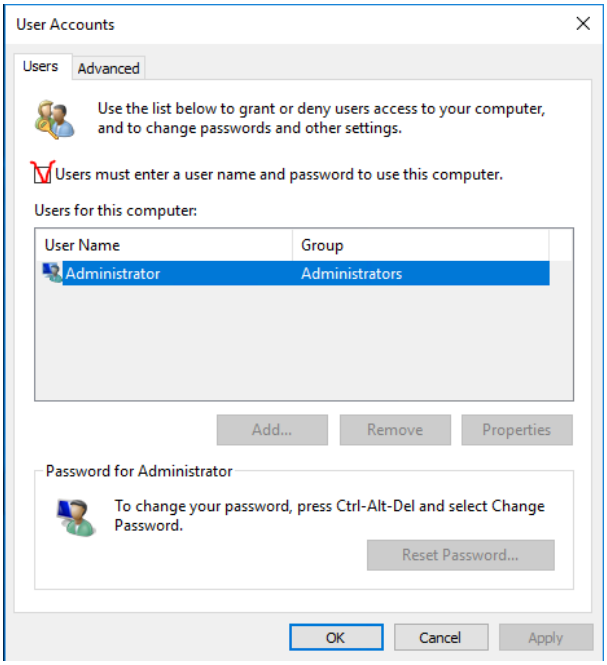
Для забезпечення автоматичного запуску вцілому програмного комплексу КЗІ «Криптосервер» під час планового або аварійного перезавантаження серверного обладнання без втручання адміністратора, необхідно забезпечити автоматичний запуск усіх модулів пп 2-3.

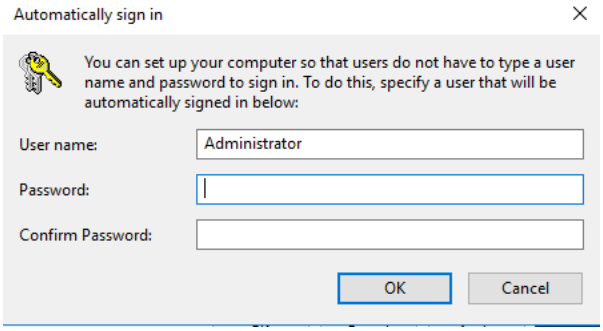
Враховуючи, що модулі пп.2-3 автоматично завантажуються тільки після реєстрації користувача у системі, рекомендується зробити автоматичний запуск термінальної сесії. Для цього необхідно здійснити наступні кроки:

4.1 ПУСК – Выполнить (Run) - control userpasswords2 -> OK

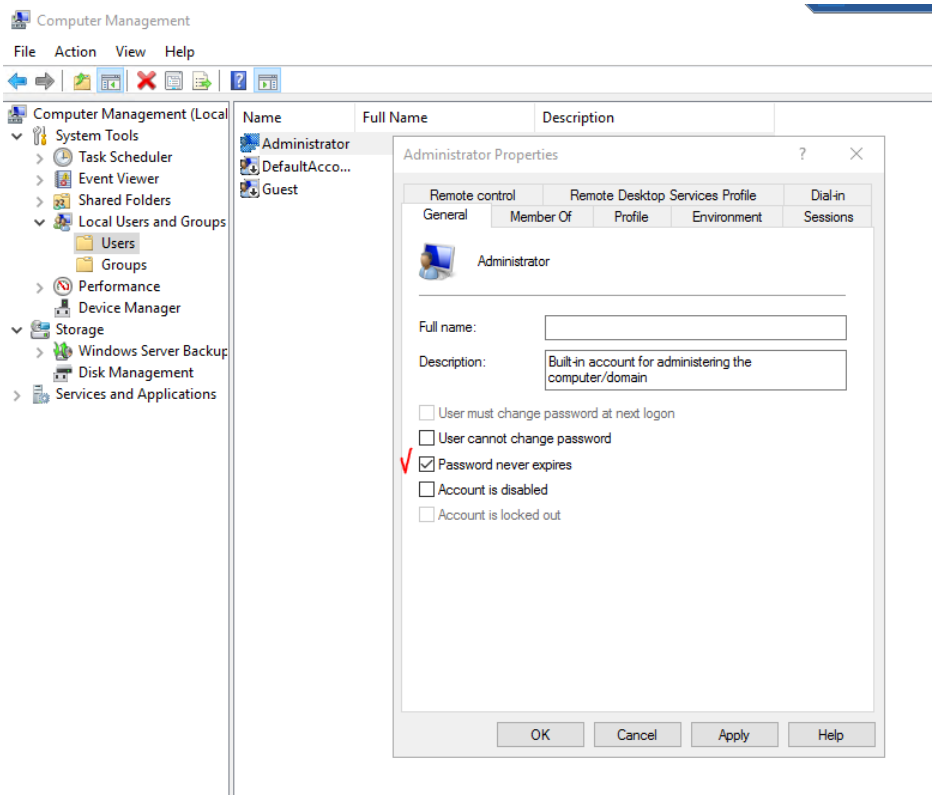


У новому вікні обрати користувача, як приклад Administrator, та зняти позначку «Вимагати введення ім'я користувача та пароля» (Users must enter a user name and password to use this computer). Натиснути кнопку ОК та підтвердити свої дії введенням пароля.

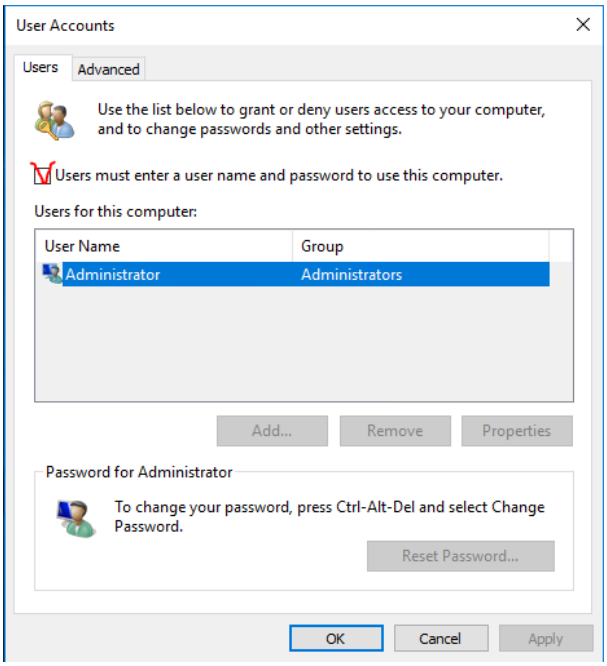




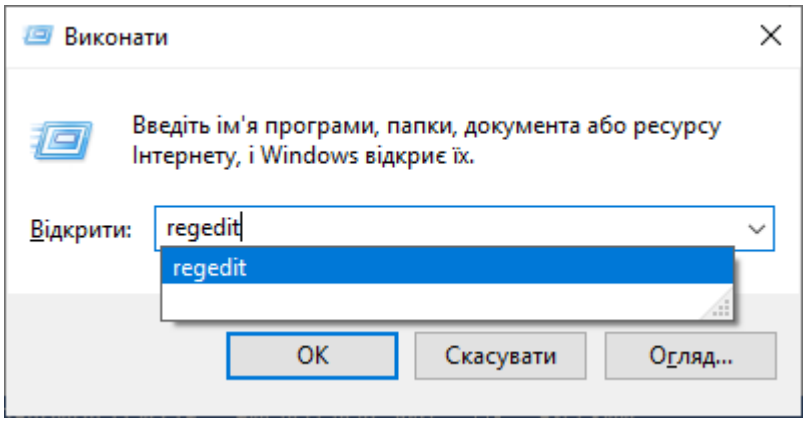
Важливо! Обліковий запис користувача, як приклад Administrator, повинен мати безстрокову дію пароля, та знята позначка на зміну пароля при реєстрації



4.2 У випадку, коли робоча станція знаходиться в домені, дана позначка буде відсутньою.



В такому випадку необхідно внести зміни в реєстр. Для цього введіть regedit у вікно «Виконати».



Перейдіть за шляхом: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon та додайте наступні значення параметрів реєстру (всі значення мають тип REG_SZ або String value):

- AutoAdminLogon зі значенням «1»;
- DefaultUserName з вказаним доменним ім'ям користувача, від імені якого буде відбуватися автоматичний вхід в систему;
- DefaultDomainName з вказаною назвою домену, в якому знаходиться робоча станція;
- DefaultPassword з вказаним паролем до облікового запису користувача, якого вказано в DefaultUserName. **ЗВЕРНІТЬ УВАГУ, ЩО В ТАКОМУ ВИПАДКУ ПАРОЛЬ БУДЕ ЗБЕРІГАТИСЯ В РЕЄСТРІ У ВІДКРИТОМУ ВИГЛЯДІ.**

Додаток 1

Опис параметрів конфігурації (файл - CryptoServer.ini)

Обов'язкові параметри основної конфігурації - секція [common]

Ім'я параметру	*Значення (за умовчанням)*	*Опис параметру*
sid	ціле число	Номер абоненту
certfile	Ім'я файлу	Файл з сертифікатом ключа абонента
cacertfile	Ім'я файлу	Файл з сертифікатом ключа ЦСК
contfile	Ім'я файлу	Файл з приватним ключом абонента
dkefile	Ім'я файлу	Файл з довгостроковим ключом абонента

Додаткові параметри основної конфігурації (секція [common])

Ім'я параметру	*Значення (за умовчанням)*	*Опис параметру*
pass	Стрічка у cp1251	Пароль доступу до приватного ключу за умовчанням
certdir	Шлях до каталогу (Certs)	Каталог з сертифікатами
logdir	Шлях до каталогу (Logs)	Каталог з журналами
keys	Шлях до каталогу (Keys)	Каталог з ключами
maxthreads	кількість потоків (990)	Максимальна кількість потоків
threads	кількість потоків (10)	Початкова кількість потоків після запуску
trust_for_sec	Секунди (60)	Час зберігання результату перевірки сертифіката
key_live_sec	Секунди (60)	Час використання сеансового ключа
title	Стрічка у cp1251	Альтернативний заголовок головного вікна
confirm	'0' | '1' ('1')	'0' – не запитувати підтвердження при виході та не запитувати пароль при наявності паролю за умовчанням
logstat	'0' | '1' ('0')	'1' – статистика у журналі відлагодження кожні 7 сек.

Параметри сервісу перевірки статусу сертифікатів - секція [ocsp]

Ім'я параметру	*Значення (за умовчанням)*	*Опис параметру*
port	Порт (0)	Номер порту OCSP. '0' = протокол OCSP не використовується для перевірки сертифікатів
addr	ip | dns-name	Адреса серверу OCSP
certfile	Ім'я файлу	Файл з сертифікатом ключа серверу OCSP
dbname	Ім'я бази даних mysql ('')	База даних ЦРК. Вказується у разі її безпосереднього використання для перевірки статусу сертифікатів
dbuser	Ім'я користувача бази даних mysql ('root')	Ім'я користувача бази даних ЦРК
dbpass	Пароль користувача ('')	Пароль користувача [ocsp].dbuser бази даних ЦРК
dbaddr	ip | dns-name ('localhost')	Адреса бази даних ЦРК
dbport	Порт ('0')	Порт підключення до бази даних ЦРК. '0' – підключатись до стандартного порту mysql

Параметри віддаленого підключення – секції виду [linkNNN]

Ім'я параметру	*Значення (за умовчанням)*	*Опис параметру*
id	ціле число >0	Локальний індекс підключення
type	'client' | 'server'	Тип підключення – клієнт або сервер
sid	ціле число	Для клієнта – номер абонента віддаленого МШ (типу 'сервер') Для сервера – не задано
inp_port	порт	Локальний порт. Для сервера – порт сервера, що захищається Для клієнта – порт, до якого підключатимуся клієнти
out_addr	ip | dns-name	Адреса віддаленого МШ
out_port	порт	Порт віддаленого МШ
max_conn	ціле число >0 ('1000')	Максимальна кількість одночасних підключень

Параметри підключення до МК – секція [mk]

Ім'я параметру	*Значення (за умовчанням)*	*Опис параметру*
port	порт (0)	Порт абонента віддаленого МШ, що захищає МК. Якщо не наведено або '0' – підключення до МК не здійснюється.
addr	ip | dns-name	Адреса віддаленого МШ, що захищає МК.
sid	ціле число	Номер абонента віддаленого МШ, що захищає МК
restart	Секунди (20)	Інтервал спроб підключення до МК

Параметри відображення головного вікна – секція [win]

Ім'я параметру	*Значення (за умовчанням)*	*Опис параметру*
tray	'0' | '1' ('0')	'1' – сховати вікно у трей (також параметр командної стрічки '–hidden')
left	ціле число	Координата x вікна
top	ціле число	Координата y вікна
width	ціле число	Ширина вікна
height	ціле число	Висота вікна

Параметри командної строки CryptoServer.exe

Ім'я параметру	*Опис параметру*
-nopass	не запитувати пароль при завантажуванні – використовувати пароль за умовчанням з конфігурації [common].pass
-hidden	при завантажуванні сховати вікно у трей (також [win].tray)