Прим. №__

ЗАТВЕРДЖЕНО

UA. 35363887.00002-01 34 04-ЛЗ

НАСТАНОВА ОПЕРАТОРА

“ПРОГРАМНИЙ КОМПЛЕКС КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ «КРИПТОСЕРВЕР». МОДУЛЬ КЕРУВАННЯ”

UA. 35363887.00002-01 34 04

на 41 аркуші

Київ – 2010

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

ЗМІСТ

1. ВСТУП

В даному документі наведена настанова оператора модуля «Модуль керування», який є складовою частиною програмного комплексу криптографічного захисту інформації «Криптосервер» (далі – Комплекс) та призначений для дистанційного керування компонентами Комплексу, такими як Центр розподілу ключів та модуль шифрування.

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

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

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

2. ЗАГАЛЬНІ ВІДОМОСТІ

2.1 Позначення та назва програми

Програмний модуль «Модуль керування» має наступні атрибути:

- Версія продукту - v. 1.0
- Назва продукту - Програмний модуль «Модуль керування»
- Розробник - ТОВ НВП «Безпека інформаційно-телекомунікаційних систем»
- Найменування файлу, що виконується - МК.exe

2.2 Програмне забезпечення, необхідне для функціонування МК

Функціонування МК здійснюється під керуванням операційних систем Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Vista.

2.3 Мова програмування

Модуль керування написано мовою програмування C++. У якості компілятору використовується CodeGear C++Builder 2007 компанії Borland.

3. ФУНКЦІОНАЛЬНЕ ПРИЗНАЧЕННЯ

Модуль керування є програмним засобом дистанційного керування компонентами Комплексу, такими як Центр розподілу ключів та модуль шифрування.

4. ОПИС ЛОГІЧНОЇ СТРУКТУРИ

4.1 Перелік програмних модулів (файлів)

МК складається з наступних частин:

- робочий модуль (файл CryptoServer.exe), якій відповідає за реалізацію сеансів захищеного зв’язку модуля керування з модулями шифрування Комплексу;
- модуль керування (файл МК.exe), що забезпечує реалізацію механізмів керування модулями шифрування Комплексу та виконувати перегляд журналу реєстрації подій;
- система керування базою даних MySQL: засіб зберігання інформації та реалізації механізмів розмежування доступу до інформації і функцій МК;
- бібліотека функцій криптографічних перетворень “UaCrypto”: забезпечує реалізацію механізмів криптографічних перетворень встановлення каналу захищено зв’язку під час роботи з компонентами Комплексу.

4.2 Робота з компонентами МК

4.2.1 Інсталяція компонентів

<u>Система керування базами даних</u>

Інсталяція бази даних MySQL, необхідної для забезпечення роботи МК, виконується під час розгортання ЦРК.

<u>Інсталяція робочого модуля та модуля керування</u>

- виконати інсталяцію програмного забезпечення МК (файл Setup_МК _v1.exe);
- виконати налаштування параметрів МК (в файлах МК.ini та CryptoServer.ini).

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

4.2.2 Алгоритм запуску МК під час впровадження Комплексу в експлуатацію

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

- за допомогою засобів ЦГК Адміністратором Комплексу повинна бути виконана генерація ключових даних всіх компонентів Комплексу;
- за допомогою засобів ЦРК Адміністратором Комплексу повинний бути виконаний імпорт сертифікатів компонентів Комплексу;
- виконати налаштування параметрів роботи МК (конфігурація файлів CryptoServer.ini та МК.ini);
- за допомогою засобів МК виконати опис захищених з'єднань;
- виконати запуск МК у режимі роботи «онлайн».

4.2.3 Порядок використання робочого модуля

Примітка:

надана нижче інформація поверхово описує можливості роботи з робочим модулем. Більш детальний опис використання зазначеного модуля можливо знайти в документі «Настанова оператора. Програмний комплекс криптографічного захисту інформації. Модуль шифрування».

Призначенням робочого модуля МК є:

- забезпечення захищеного зв'язку з модулями шифрування, які функціонують у складі Комплексу;
- забезпечення відкритого зв'язку з модулем керування МК.

Реалізація МК у такому вигляді дозволяє адміністратору Комплексу встановити один із компонентів МК (робочий модуль) на границі мережі, не дозволяючи віддаленим клієнтам безпосередньо взаємодіяти з компонентом, який має доступ до технологічної інформації, що описує параметри функціонування Комплексу в цілому.

4.2.3.1 Налаштування параметрів робочого модуля CryptoServer.exe

Налаштування параметрів робочого модуля виконується так же само, як і налаштування модуля шифрування: параметри задаються у файлі CryptoServer.ini.

Налаштування нижченаведених параметрів виконується у ручному режимі (режимі правки текстового документу).

Існують наступні блоки параметрів:

Блок [common] – задає значення загальних параметрів, таких як:

sid - ідентифікаційний номер робочого модуля МК в структурі Комплексу. Дорівнює 3;

certdir - найменування каталогу, якій містить сертифікати \ локальна база сертифікатів;

contfile - назва файлу-контейнера МК;

dkefile - назва файлу ДКЕ;

certfile - назва файлу сертифіката МК;

cacertfile - назва файлу, якій містить сертифікат ЦГК (файл міститься у локальної базі сертифікатів);

Приклад заповнення параметрів блоку:

[common]
sid=3
certdir=cert_db
contfile=Keys\7a541ff5d5749d694dba19d314ba864109dd33b95aee41877afe8b30b09e3e1b.cnt
dkefile=Keys\7a541ff5d5749d694dba19d314ba864109dd33b95aee41877afe8b30b09e3e1b.dke
certfile=7a541ff5d5749d694dba19d314ba864109dd33b95aee41877afe8b30b09e3e1b.crt
cacertfile=118aa33acc0125132648db8795e9100e47cf0c9be5b9367be0cf6dd8d76cc596.crt

Блок [ocsp] – задає значення параметрів, необхідних для підтримки взаємодії з ЦРК, а саме:

addr - адреса комп'ютера, на який встановлено ЦРК;

port - номер порту серверу ЦРК. За замовченням дорівнює 10002. Змінювати його значення не рекомендовано;

certfile - назва файлу, який містить сертифікат ЦРК (файл міститься у локальної базі сертифікатів).

Блок представлений у файлі CryptoServer.ini в єдиному екземплярі.

Приклад заповнення параметрів блоку:

[ocsp]
addr=192.168.1.110
port=10001
certfile=2c39a602189debe4c8f07d0b52948737fe8cd4fe680ad43486a938ad29e65be5.crt

Блок [link1] – задає параметри:

- захищеного з'єднання між робочим модулем та іншими МШ Комплексу. По відношенню до них робочий модуль виступає «сервером»;

– відкритого з’єднання між робочим модулем та модулем керування. По відношенню до модуля керування робочий модуль виступає «клієнтом».

У блоці задаються значення наступних параметрів:

id - ідентифікаційний номер з’єднання. Дорівнює 1. Змінювати не рекомендується;

sid - ідентифікаційний номер робочого модуля. Дорівнює 3;

type - тип з’єднання. Повинно бути вказано значення «server»;

inp_port - номер порту, який «слухає» робочий модуль. По цьому порту буде виконуватись взаємодія з МШ, які здійснюють підключення до МК. За замовченням дорівнює 10002. Змінювати його значення не рекомендовано;

out_addr - IP-адреса АРМ, на якому встановлено модуль керування;

out_port - номер порту, по якому буде реалізована взаємодія робочого модуля та модуля керування МК. За замовченням дорівнює 10003.

Приклад заповнення параметрів блоку:

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

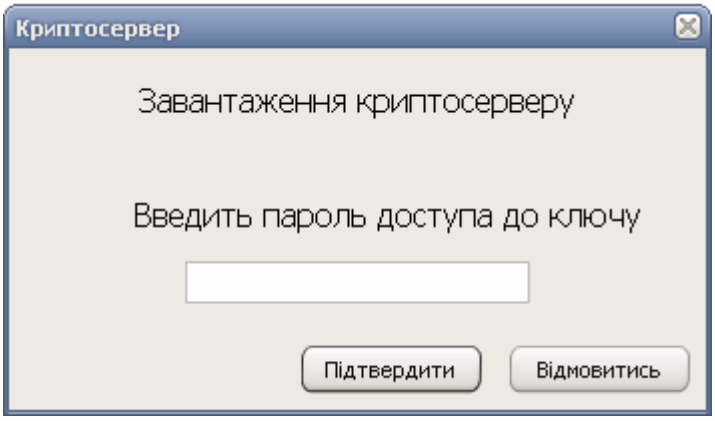
Жодних інших блоків файл налаштування CryptoServer.ini містить не повинний.

4.2.3.2 Запуск робочого модуля на виконання

Для того, щоб МК почав виконувати свої функції необхідно в першу чергу запустити робочий модуль (CryptoServer.exe) .

Для запуску робочого модуля на виконання, за умов здійснення налаштувань вищенаведених параметрів, необхідно обрати файл CryptoServer.exe, який поставляється у складі МК, та виконати його запуск, після чого ввести пароль закритого ключа МК.

Рис. 1 Вікно запиту паролю закритого ключа МК



4.2.4 Порядок використання модуля керування

4.2.4.1 Налаштування параметрів модуля керування МК.exe

Налаштування нижченаведених параметрів виконується у ручному режимі (режимі правки текстового документу).

Параметри задаються у файлі МК.ini.

Існують наступні блоки параметрів:

Блок [DB] – задає значення загальних параметрів, таких як:

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

Name - ім'я бази даних.

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

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

Приклад заповнення параметрів блоку:

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

Блок [Server] – описує налаштування, необхідні для роботи МК у режимі «онлайн» У блоці задаються значення параметрів, таких як:

Port - номер порту, по якому реалізується встановлення зв'язку. За замовченням дорівнює 10003.

Приклад заповнення параметрів блоку:

[Server]
Port=10003

Блок [Info] – задає параметри, необхідні для взаємодії модуля керування з ЦРК та робочим модулем. У блоці задаються значення параметрів, таких як:

MKPort - номер порту, по якому забезпечується взаємодія робочого модуля (CryptoServer.exe) та модуля керування МК (МК.exe). За замовченням дорівнює 10002.

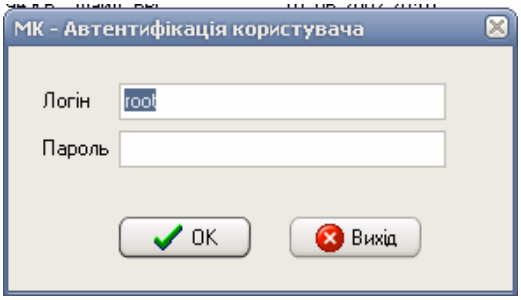
OCSPPort - номер порту, по якому забезпечується взаємодія МК та ЦРК. За замовченням дорівнює 10001.

Приклад заповнення параметрів блоку:

[Info]
MKPort=10002
OCSPPort=10001

Для одержання доступу до ресурсів модуля керування необхідно виконати запуск на виконання файлу МК.exe після чого ввести логін та пароль адміністратора/користувача бази даних .

Рис. 2 Вікно запиту паролю



Після того, як робочий модуль та модуль керування були запущені вважається, що МК готовий до роботи.

4.2.4.2 Інтерфейс користувача

Після запуску модуля керування на виконання користувач отримує можливість працювати з графічним інтерфейсом, відображеним на рис. 3.

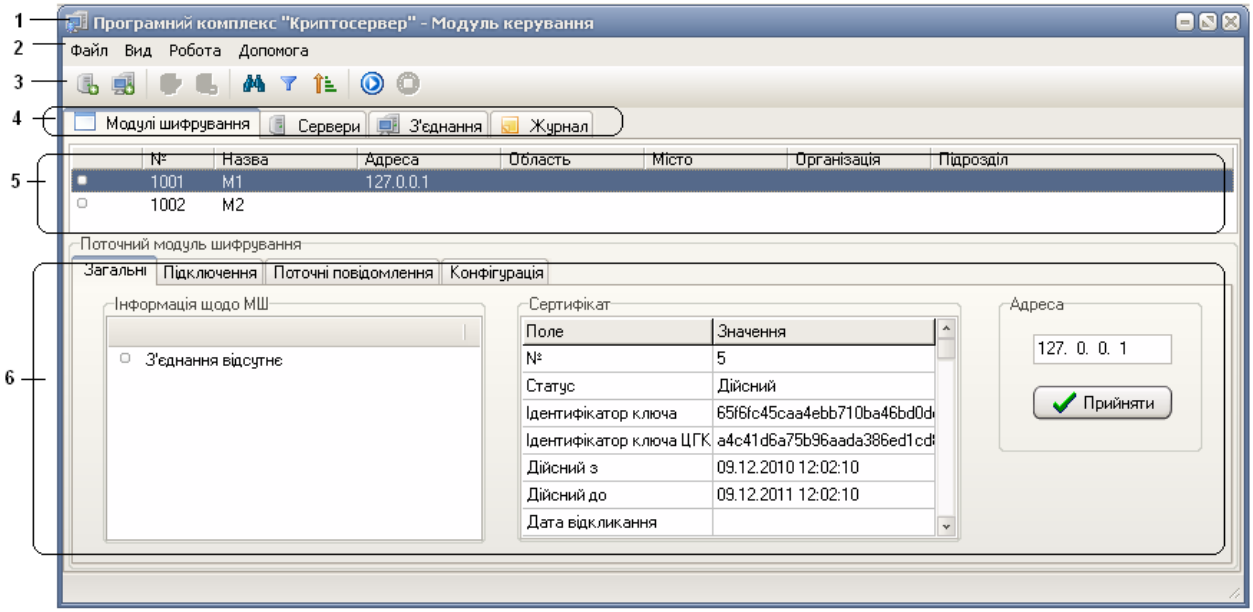


Рис. 3 Інтерфейс користувача

де,

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

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

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

2.1 Пункт меню *«Файл»* (рис. 4) містить наступні підпункти:

- *«резервне копіювання»*: дозволяє виконати налаштування для резервного копіювання бази даних;
- *«сховати в іконку»*: скрити програму в індикатор запущених програм («трей»);
- *«вихід»*: закрити програму.

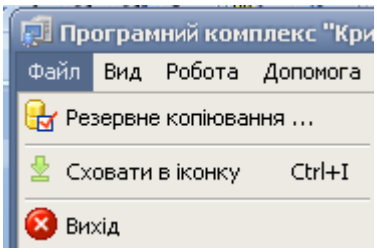


Рис. 4 Пункт меню *«Файл»*

2.2 Пункт меню «Вид» (рис. 5) містить підпункти:

- *«Модулі шифрування»*: дозволяє скрити (у випадку наявності) або відобразити (у випадку відсутності) закладку «*Модулі шифрування*»;
- *«Сервери»*: дозволяє скрити (у випадку наявності) або відобразити (у випадку відсутності) закладку «*Сервери*»;

– *«З'єднання»*: дозволяє скрити (у випадку наявності) або відобразити (у випадку відсутності) закладку «*З'єднання*»;

– *«Поточний МШ»*: дозволяє скрити (у випадку наявності) або відобразити (у випадку відсутності) закладку «*Поточний модуль шифрування*»;

– *«Фільтр»*: дозволяє виконати фільтрацію даних за вказаними параметрами;

– *«Сортування»*: дозволяє виконати сортування даних за вказаними параметрами;

– *«Пошук»*: дозволяє виконати пошук запису за вказаними критеріями.

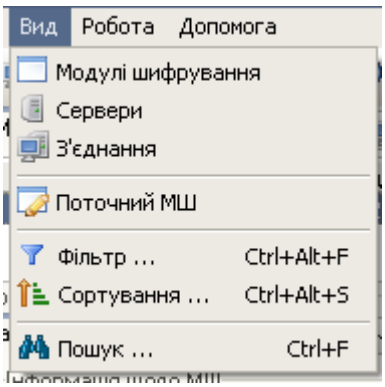


Рис. 5 Пункт меню *«Вид»*

2.3 Пункт меню *«Робота»* містить підпункти:

– *«Новий сервер»*: дозволяє виконати налаштування серверної частини захищеного з'єднання;

– *«Нове з'єднання»*: дозволяє виконати налаштування клієнтської частини захищеного з'єднання;

– *«Властивості»*: дозволяє переглянути детальну інформацію, яка описує або серверну, або клієнтську частину захищеного з'єднання;

– *«Видалити»*: дозволяє видалити інформацію, яка описує або серверну, або клієнтську частину захищеного з'єднання;

– *«Старт серверу»*: дозволяє запустити режим роботи ЦРК «онлайн»;

– *«Зупинка серверу»*: дозволяє зупинити режим роботи ЦРК «онлайн»;

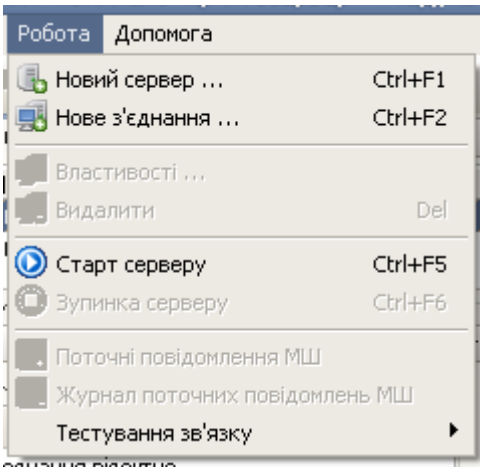


Рис. 6 Пункт меню *«Робота»*

2.4 Пункт меню «Допомога» надає довідкову інформацію.

3 - панель інструментів: призначена для забезпечення швидкого доступу до деяких функцій. Містить наступні інструменти:

- реєстрація нового серверу, кнопка ;
- реєстрація нового з'єднання, кнопка ;
- перегляд/редагування параметрів серверу/з'єднання, кнопка ;
- видалення запису, що описує сервер/з'єднання, кнопка ;
- пошук записів, кнопка ;
- фільтрація записів, кнопка ;
- сортування записів, кнопка ;
- старт серверу МК, кнопка ;
- завершити роботу серверу МК, кнопка .

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

5 - область відображення інформації про МШ, сервери, з'єднання та записи журналу реєстрації повідомлень.

6 - закладки з детальною інформацією, що описує МШ. Відображається лише у випадку активної області відображення інформації про МШ.

4.2.4.3 Перегляд інформації

Модуль керування надає можливість адміністратору переглянути інформацію, що відображається на чотирьох закладках:

- модулі шифрування;
- сервери;
- з'єднання;
- журнал.

4.2.4.3.1 Закладка *«Модулі шифрування»*

Загальний опис

МК не надає адміністратору можливості роботи безпосередньо з даними, що характеризують МШ. Для виконання цих функцій призначений ЦРК. МК

дає можливість лише виконати перегляд інформації. Для її відображення призначена закладка *«Модулі шифрування»*.

Верхня частина закладки (5 на рис. 3) відображає інформацію, яка надає перелік зареєстрованих засобами ЦРК в базі даних записів про МШ. В якості інформаційних полів, що описують МШ виступають:

- поле активності МШ (наявності зв'язку з МШ) на поточний момент: представлено у вигляді графічного позначення та має 2 значення:
  - МШ неактивний: ;
  - МШ активний: ;
- поле *«№»*: номер МШ в структурі Комплексу;
- поле *«назва»:* назва МШ;
- поле *«адреса»*: надає інформацію щодо IP-адреси ПЕОМ з встановленим МШ, який виконує роль «серверу» при організації захищеного зв'язку;
- поля *«область»*, *«місто»*, *«організація»*, *«підрозділ»*: надають інформацію щодо місцезнаходження МШ та підрозділів організації, що його експлуатує.

Нижня частина закладки (6 на рис. 3) містить інформаційну область *«Поточний модуль шифрування»* з більш детальними даними про поточний (обраний) запис МШ (запис позначається синім кольором). Згадана інформаційна область в свою чергу має наступні закладки:

- *«Загальні»*: надає відомості щодо:
  - наявності з'єднання між обраним (поточним) МШ та МК. Повідомлення надається в текстовому вигляді та дублює графічне позначення закладки *«Модулі шифрування»* (див. вище);
  - сертифікату обраного МШ;
  - IP-адреси ПЕОМ з встановленим МШ, який виконує роль «серверу» при організації захищеного зв'язку. Значення IP-адреси на даній закладці можливо редагувати;

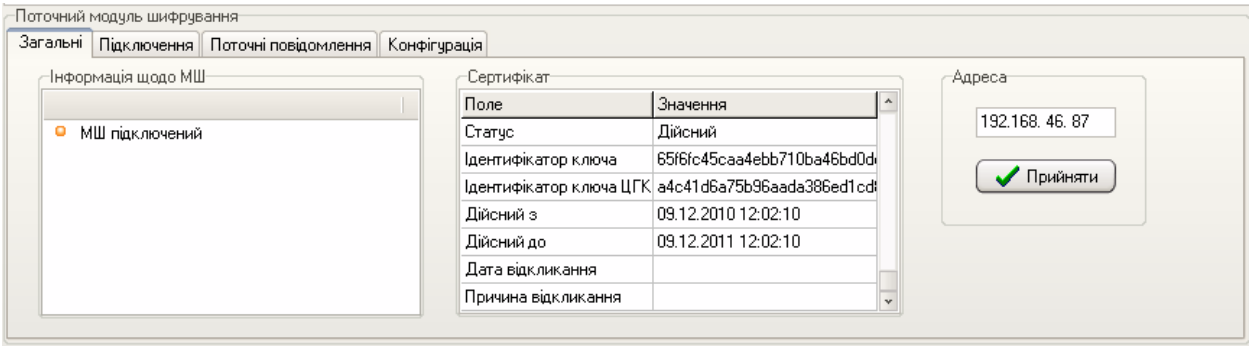


Рис. 7 Закладка *«Загальні»*

- «*підключення*»: вміст журналу МШ «Підключення». Детальний опис полів журналу наведений у документі «». Дані відображаються, якщо МШ підключений до МК.

  Панель інструментів закладки містить наступні інструменти, що призначені для віддаленого керування МШ (використовуються, якщо МШ підключений до МК):

  - «*Автоматичне оновлення інформації про підключення*», кнопка ; інструмент призначений для включення або виключення автоматичного оновлення даних журналу (отримання даних від МШ);
  - «*Провести тестове підключення неактивних Клієнтів до віддалених Серверів*», кнопка ; інструмент тестування зв'язку, що призначений для перевірки можливості мережного з'єднання між МШ клієнтської частини з віддаленим відкритим сервером через МШ серверної частини. Аналіз результатів тестування здійснюється за вмістом колонки «*Всього / до МШ / до Серверу*»;
  - «*Перевірити зв'язок неактивних Клієнтів з віддаленими МШ*», кнопка ; інструмент тестування зв'язку, що призначений для перевірки можливості створення захищеного з'єднання між МШ клієнтської частини та МШ серверної частини. Аналіз результатів тестування здійснюється за вмістом колонки «*Всього / до МШ / до Серверу*»;

- «*Поточні повідомлення*»: вміст журналу МШ «Поточні повідомлення». Детальний опис полів журналу наведений у документі «». Дані відображаються, якщо МШ підключений до МК.

Панель інструментів закладки містить наступні інструменти, що призначені для віддаленого керування МШ (використовуються, якщо МШ підключений до МК):

- «*Отримати журнал поточних повідомлень МШ*», кнопка ; інструмент призначений отримання вмісту журналу поточних повідомлень МШ;

– *«Конфігурація»*: містить автоматично сформовані для обраного МШ налаштування, які можливо експортувати в файл (кнопка *«Зберегти»*) та за допомогою незначного редагування використовувати для роботи МШ.

Рис. 8 Закладка *«Конфігурація»*

<u>Аналіз інформації, що описує МШ</u>

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

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

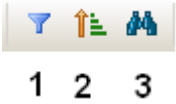


Рис. 9 Інструменти, призначені для виконання операцій з даними

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

Фільтрація:

- необхідно відкрити закладку *«Модулі шифрування»*;
- за допомогою кнопки «*Фільтрування записів*» (1 на рис. 9) одержати вікно запиту, рис. 10;
- обрати з переліку один з наступних параметрів фільтрації:

- *«номер»*: відображення переліку МШ, номери яких відповідають переліку та/або діапазону значень, що введені у полі фільтру;
- *«назва»:* відображення переліку МШ, назви яких відповідають переліку та/або діапазону значень, що введені у полі фільтру;
- *«область»:* відображення переліку МШ, що знаходяться в межах обраної області;
- *«місто»:* відображення переліку МШ, що знаходяться в межах обраного міста;
- *«організація»:* відображення переліку МШ, що експлуатуються обраною організацією;
- *«підрозділ»:* відображення переліку МШ, що експлуатуються обраним підрозділом.

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

Рис. 11 Вікно з параметрами фільтрації

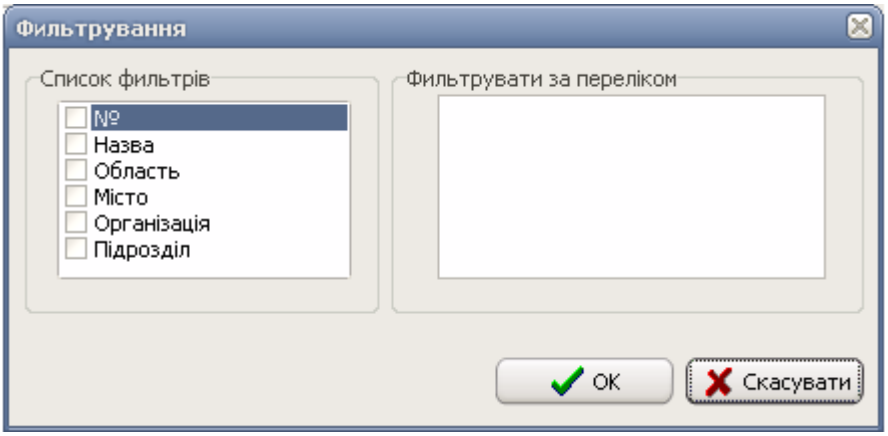


Рис. 12 Формат вводу діапазону номерів МШ під час фільтрації

Рис. 13 Формат вводу переліку номерів МШ під час фільтрації

Для того, щоб зняти фільтрацію необхідно убрати всі «галочки» у вікні з параметрами фільтрації та натиснути кнопку *«ОК»*.

Сортування:

- необхідно відкрити закладку «*Модулі шифрування*»;
- за допомогою кнопки «*Сортування записів*» (2 на рис. 9) одержати вікно запиту, рис. 14;

- обрати з переліку поле, за даними якого буде виконано сортування. Сортування виконується за наступними полями:
  - «*номер*»;
  - «*назва*»;
  - «*область*»;
  - «*місто*»;
  - «*організація*»;
  - «*підрозділ*».

Для того щоб обрати направлення сортування (за збільшення або за спаданням) необхідно натиснути лівою кнопкою маніпулятора на обраному параметрі. Як результат дії користувач отримує графічне зображення напрямку сортування(рис. 15). Після цієї операції необхідно підтвердити необхідність сортування шляхом натискання кнопки «*ОК*» у вікні (рис. 14).

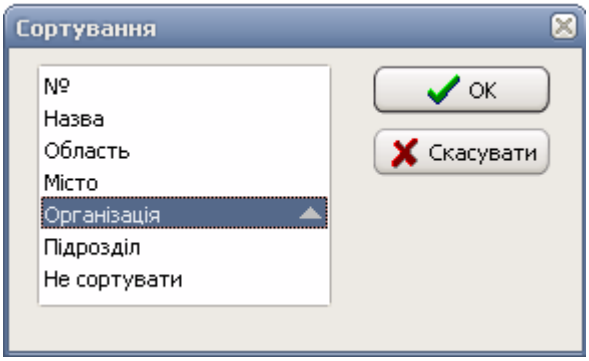


Рис. 14 Вікно параметрів сортування

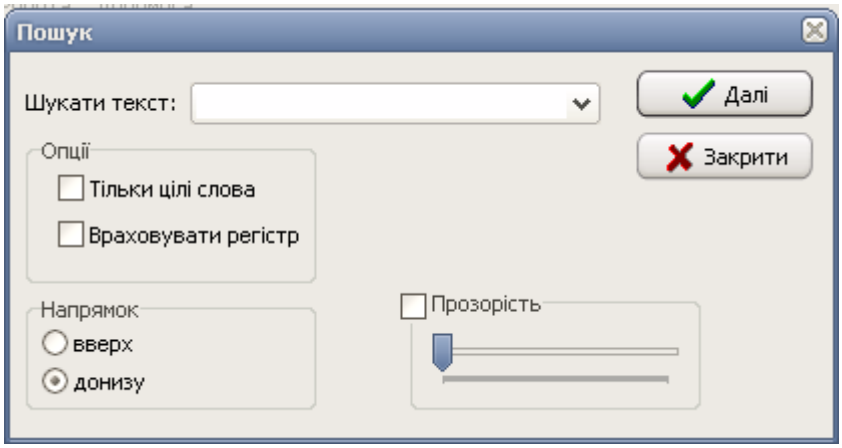
Рис. 15 Приклад напрямків сортування

Пошук

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

- відкрити закладку «*Модулі шифрування*»;
- за допомогою кнопки «*Пошук записів*» (3 на рис. 9) одержати вікно запиту, рис. 16;
- задати текст, пошук якого виконується в інформаційних полях, що описують сертифікати та натиснути кнопку «*Далі*».

Рис. 16 Вікно введення параметрів пошуку



4.2.4.3.2 Закладка «Сервери»

Надає інформацію, яка характеризує налаштування серверної частини захищеного зв'язку, а саме:

- порядковий номер запису;
- назва запису;
- номер МШ в структурі Комплексу, який буде виконувати роль серверу для інших МШ, що працюють в межах описаних з'єднань (далі – МШ-сервер);
- IP-адреса ПЕОМ з встановленою серверною частиною програмного забезпечення, до якого виконується доступ з боку клієнтського застосування (наприклад IP-адреса ПЕОМ з встановленою СКБД. Таким чином між МШ-сервером та СКБД буде встановлено відкритий канал);
- номер порту, по якому буде виконуватись з'єднання між МШ-сервером та серверною частиною ПЗ;
- номер порту МШ, по якому МШ-ссервер буде одержувати запити від інших МШ, що працюють в межах описаних з'єднань.

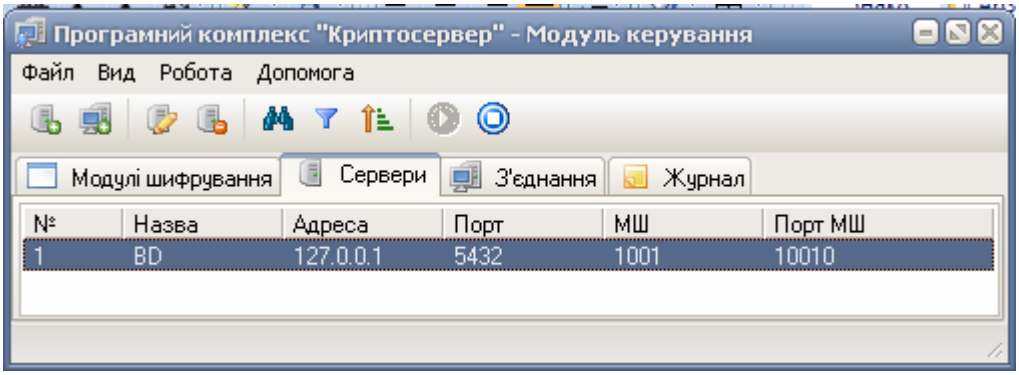


Рис. 9 Закладка *«Сервери»*

4.2.4.3.3 Закладка «З’єднання»

Надає інформацію, яка характеризує налаштування клієнтської частини захищеного зв’язку, а саме:

- порядковий номер запису;
- назва запису;
- номер МШ в структурі Комплексу, який буде виконувати роль клієнта в межах описаного з’єднання (далі – МШ-клієнт);
- номер порту МШ, який буде використовуватись («прослуховуватись») для зв’язку з клієнтською частиною ПЗ;
- порядковий номер серверу, для зв’язку з яким виконаний опис поточного з’єднання;
- назва серверу, для зв’язку з яким виконаний опис поточного з’єднання;
- порядковий номер МШ-серверу в структурі Комплексу;
- номер порту МШ-серверу, який буде використовуватись для створення захищеного каналу між МШ-клієнтом та МШ-сервером.

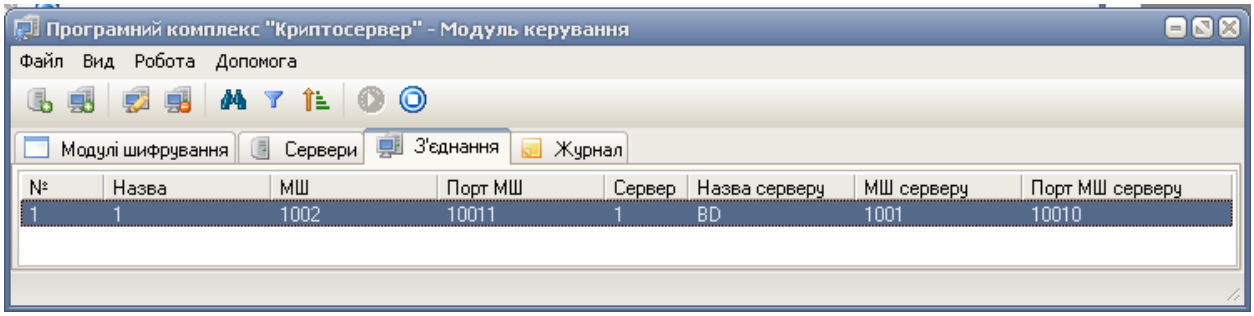


Рис. 10 Закладка «З’єднання»

4.2.4.3.4 Закладка «Журнал»

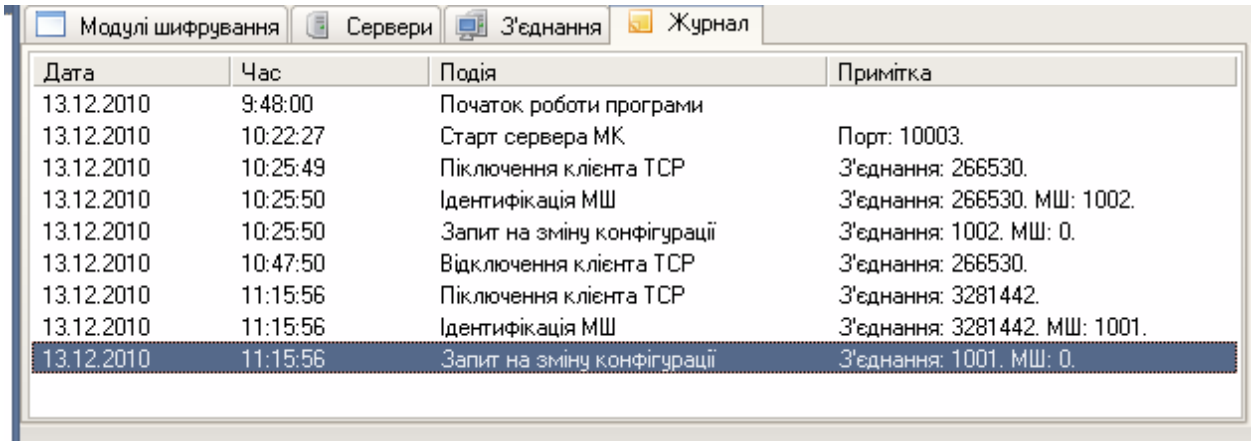
Надає інформацію, яка описує зареєстровані події. Реєструються наступні типи подій:

- початок роботи програми;
- завершення роботи програми;
- збереження резервної копії бази даних;
- відновлення бази даних з резервної копії;
- реєстрація нового з’єднання;
- зміна параметрів з’єднання;
- видалення з’єднання;
- створення нового серверу;
- зміна параметрів серверу;

- видалення серверу;
- старт серверу МК;
- зупинка серверу МК;
- надсилання команди на створення налаштувань МШ;
- надсилання команди на видалення налаштувань МШ;
- підключення клієнта TCP;
- відключення клієнта TCP;
- ідентифікація МШ;
- запит на зміну конфігурації;
- видалення МШ;
- зміна IP-адреси МШ;
- обробка команди.

Журнал надає відомості щодо:

- дати та часу виникнення події;
- типу події;
- додаткового опису події, який надає адміністратору більш детальну для аналізу інформацію.



Дата	Час	Подія	Примітка
13.12.2010	9:48:00	Початок роботи програми	
13.12.2010	10:22:27	Старт сервера МК	Порт: 10003.
13.12.2010	10:25:49	Піключення клієнта TCP	З'єднання: 266530.
13.12.2010	10:25:50	Ідентифікація МШ	З'єднання: 266530. МШ: 1002.
13.12.2010	10:25:50	Запит на зміну конфігурації	З'єднання: 1002. МШ: 0.
13.12.2010	10:47:50	Відключення клієнта TCP	З'єднання: 266530.
13.12.2010	11:15:56	Піключення клієнта TCP	З'єднання: 3281442.
13.12.2010	11:15:56	Ідентифікація МШ	З'єднання: 3281442. МШ: 1001.
13.12.2010	11:15:56	Запит на зміну конфігурації	З'єднання: 1001. МШ: 0.

Рис. 11 Закладка *«Журнал»*

4.2.4.4 Робота з даними

4.2.4.4.1 Сервери

Сервер – це умовне позначення запису, який описує серверну частину захищеного з’єднання, визначає параметри функціонування МШ-серверу.

<u>Створення запису</u>

Створити опис параметрів МШ-серверу можливо за допомогою:

- підпункту меню *«Вид» > «Сервери»*;
- інструменту *«Реєстрація нового серверу»*;

- комбінації гарячих клавіш Ctrl+F1;
- підпункту *«Новий сервер»* меню, що «вспливає», рис. 12: «клік» правою кнопкою маніпуляторі типу «миша» на області відображення інформації про сервери (рис. 9).

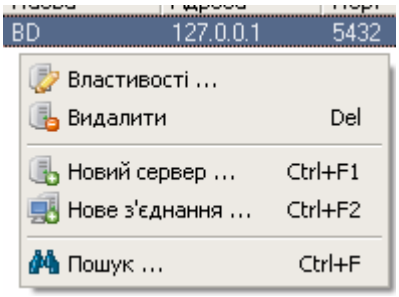


Рис. 12 Підпункти меню, що «вспливає»

Як результат дії користувач отримує вікно введення даних про сервер, рис. 13.

Вікно містить наступні області:

- інформаційна область «*Параметри відкритого сервера*»: в її межах виконується опис реальних параметрів серверної частини ПЗ (наприклад СКБД), а саме:
  - «*назва*»: назва запису, що описує сервер;
  - «*IP-адреса*»: IP-адреса ПЕОМ з встановленою серверною частиною ПЗ;
  - «*порт*»: порт, який використовується серверною частиною ПЗ для взаємодії з клієнтськими частинами.
- інформаційна область «*Модуль шифрування*»: в її межах виконується опис параметрів МШ, який буде виконувати роль МШ-серверу, а саме:
  - «*номер МШ*»: надає можливість вибору необхідного МШ із переліку (рис. 15). Для одержання переліку доступних МШ необхідно натиснути кнопку *«…»*;
  - поля «*назва*», «*адреса*», «*область*», «*місто*», «*організація*», «*підрозділ*» являються інформативними та редагуванню не підлягають;
  - «*номер порту*»: надає можливість обрати номер порту, по якому буде виконуватись взаємодія з МШ-клієнтами.

УВАГА! Обрати номер порту можливо лише із використанням переліку портів, які будуть надані (рис. 16).

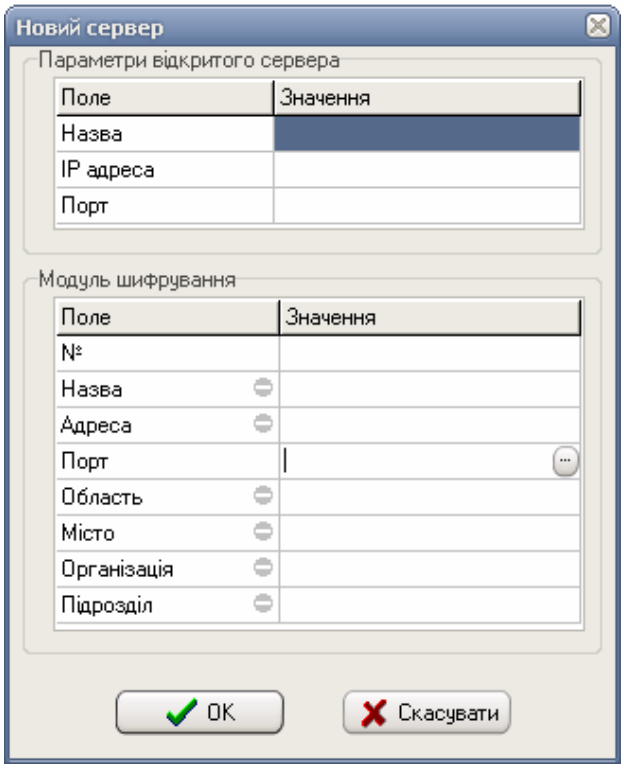


Рис. 13 Вікно введення даних, що характеризують МШ-сервер

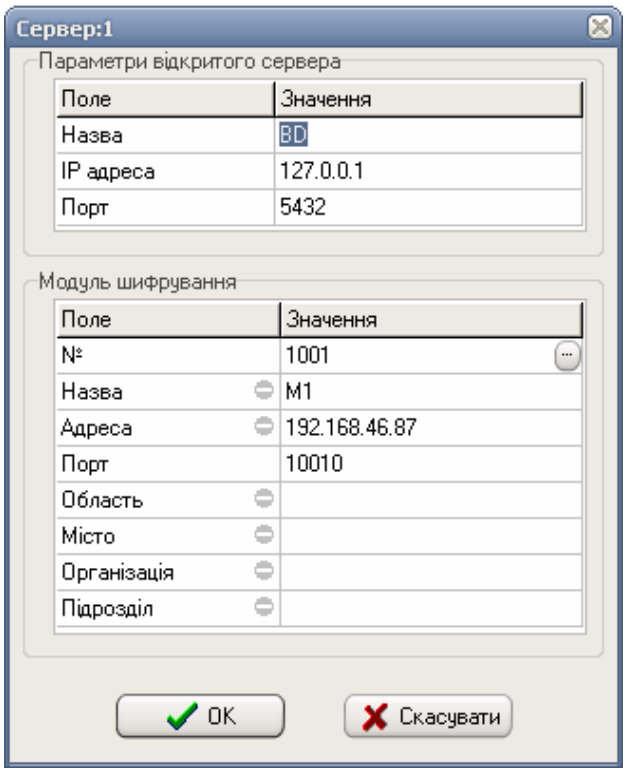


Рис. 14 Зразок опису параметрів, що характеризують МШ-сервер

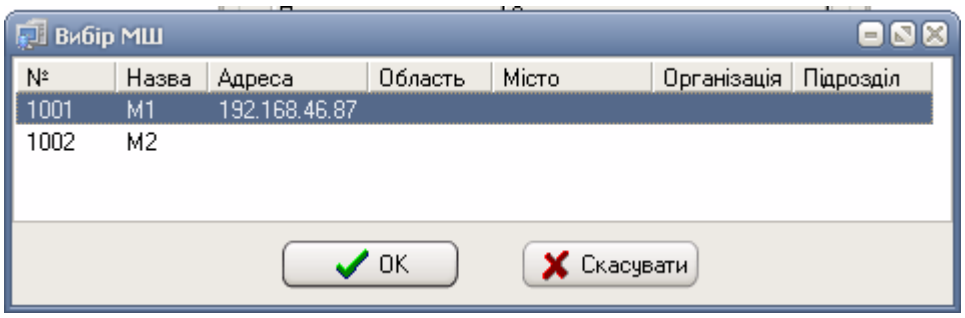


Рис. 15 Перелік МШ, наданий під час опису параметрів МШ-серверу

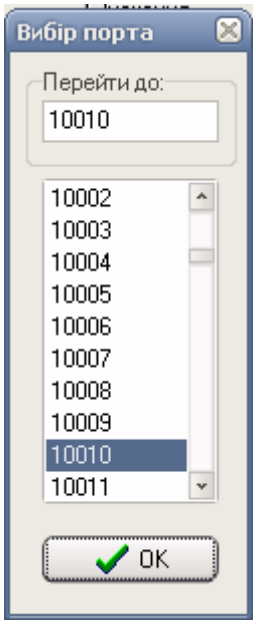


Рис. 16 Перелік номерів портів, наданий під час опису параметрів МШ-серверу

Як було зазначено вище, під час опису параметрів МШ-серверу у вікні введення даних (рис. 13) поле «*адреса*» недоступне для редагування. В той же час, даний параметр надає відомості для МШ-клієнтів про місцезнаходження МШ-серверу та є важливим для роботи Комплексу.

Для того, щоб виконати налаштування параметру «адреса» необхідно після створення нового «серверу»:

- перейти до закладки «*Модулі шифрування*». При цьому адміністратор буде мати можливість одержати графічне (1 на рис. 17) та текстове (2 на рис. 17) повідомлення про те, що МШ, обраний для виконання ролі МШ-сервер, потрібує визначення даних про його IP-адресу;
- задати IP-адресу у відповідному полі (3 на рис. 17) та натиснути кнопку «*Прийняти*».

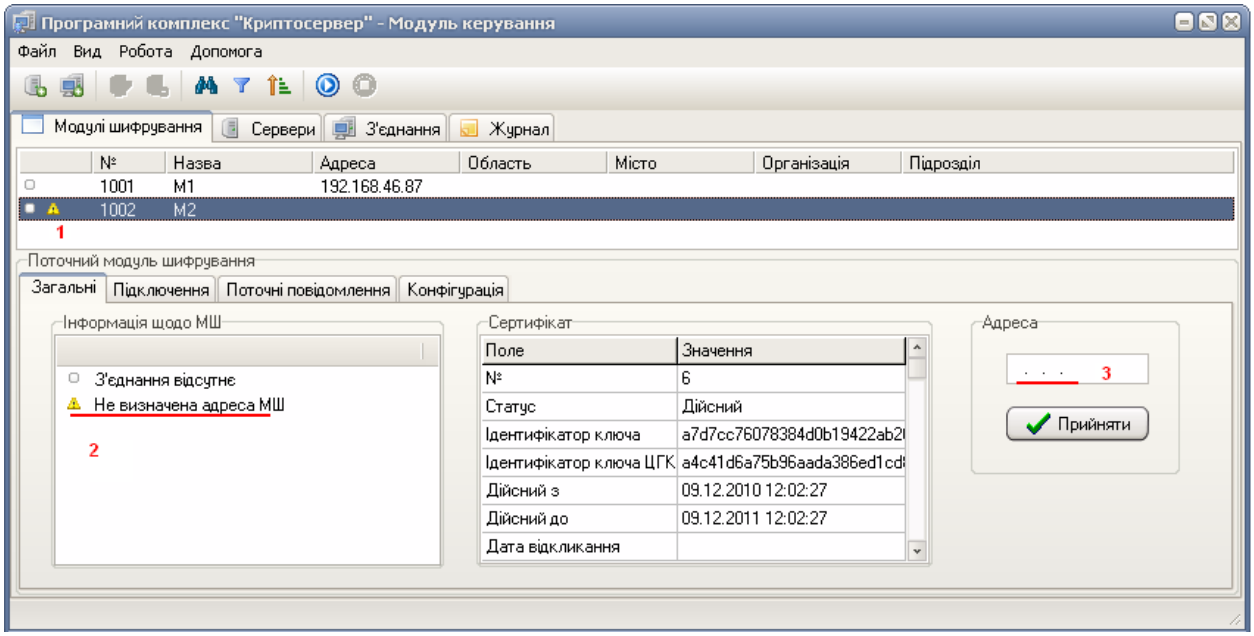


Рис. 17 Приклад повідомлень про необхідність введення IP-адреси МШ-серверу

Після того, як всі вищевказані дії було виконано опис параметрів МШ-серверу можливо вважати завершеним.

Як результат виконання налаштувань, наведених на рис. 14, буде виконано зміни в конфігураційному файлі CryptoServer.ini МШ з ідентифікаційним номером 1001, а саме додано блок параметрів:

[link1]

type=server – роль МШ при реалізації з'єднання: сервер

id=1 – ідентифікаційний номер описаного з'єднання: 1

sid=1001 – ідентифікаційний номер МШ у структурі Комплексу 1001

inp_port=10010 – порт, який «прослуховує» МШ та по якому встановлюється захищене з'єднання: 10010

out_addr=127.0.0.1 – IP-адреса серверу ПЗ, з якими встановлюється

відкрите з’єднання: 127.0.0.1

out_port=5432 – порт серверу ПЗ, по якому встановлюється відкрите з’єднання: 5432

Видалення запису

Для того, щоби видалити запис, який описує налаштування МШ-серверу необхідно із переліку на закладці *«Сервери»* обрати потрібний запис та видалити його за допомогою:

- інструменту *«Видалення серверу»*;
- підпункту меню *«Робота»* > *«Видалення серверу»*;
- підпункту *«Видалити»* меню, що «вспливає», рис. 12;
- «гарячої» клавіші *Del*.

Після підтвердження необхідності видалення запису буде знищено як сам запис з налаштуваннями МШ-серверу, так і пов’язані з ним записи з налаштуваннями МШ-клієнтів.

Перегляд та редагування запису

Для того, щоби виконати детальний перегляд запису (який описує налаштування МШ-серверу), або виконати редагування його даних необхідно із переліку на закладці *«Сервери»* обрати потрібний запис та виконати перегляд/редагування його за допомогою:

- інструменту *«перегляд та редагування параметрів серверу»*;
- підпункту меню *«Робота»* > *«Властивості»*;
- підпункту *«Властивості»* меню, що «вспливає», рис. 12.

Аналіз інформації, що описує сервер

МК надає можливість користувачу виконати наступні операції з даними, що зберігаються в базі даних та описують параметри МШ-серверу:

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

Фільтрація:

- необхідно відкрити закладку *«Сервери»*;
- за допомогою кнопки «*Фільтрування записів*» (1 на рис. 9) одержати вікно запиту, рис. 18;
- обрати з переліку один з наступних параметрів фільтрації:

- *«номер»*: відображення записів, що описують МШ-сервери, номери яких відповідають переліку та/або діапазону значень, що введені у полі фільтру
- *«номер МШ»*: відображення записів, ролі МШ-серверу в яких виступають МШ, номери яких відповідають переліку та/або діапазону значень, що введені у полі фільтру;
- *«поточний МШ»:* відображення записів, в ролі МШ-серверу в яких виступає поточний в закладці «Модулі шифрування» МШ. Слід зауважити, що фільтрація може бути складною: із використанням одночасно декількох параметрів.

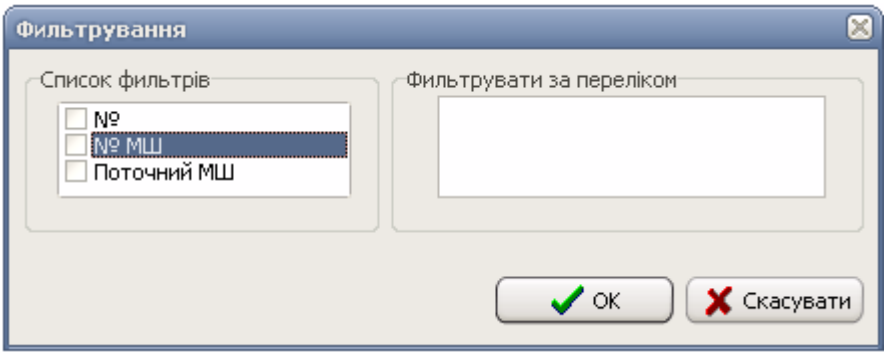


Рис. 18 Вікно з параметрами фільтрації

Для того, щоб зняти фільтрацію необхідно убрати всі «галочки» у вікні з параметрами фільтрації та натиснути кнопку *«ОК»*.

Сортування:

- необхідно відкрити закладку «*Сервери*»;
- за допомогою кнопки «*Сортування записів*» (2 на рис. 9) одержати вікно запиту, рис. 19;
- обрати з переліку поле, за даними якого буде виконано сортування. Сортування виконується за наступними полями:
  - «*номер*»;
  - «*назва*»;
  - «*адреса*»;
  - «*порт*»;
  - «*порт МШ*».

Для того щоб обрати направлення сортування (за збільшення або за спаданням) необхідно натиснути лівою кнопкою маніпулятора на обраному параметрі. Як результат дії користувач отримує графічне зображення

напрямку сортування. Після цієї операції необхідно підтвердити необхідність сортування шляхом натискання кнопки «*ОК*» у вікні (рис. 19).

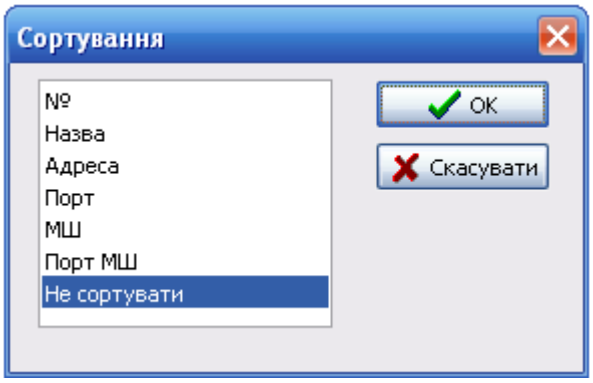


Рис. 19 Вікно параметрів сортування

Пошук

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

- відкрити закладку «*Сервери*»;
- за допомогою кнопки «*Пошук записів*» (3 на рис. 9) одержати вікно запиту, рис. 20;
- задати текст, пошук якого виконується в інформаційних полях, що описують сервери та натиснути кнопку «*Далі*».

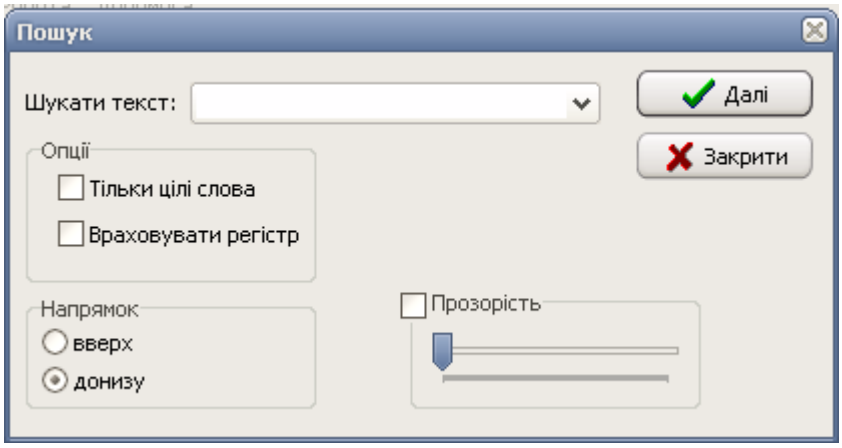


Рис. 20 Вікно введення параметрів пошуку

4.2.4.4.2 З'єднання

З'єднання – це умовне позначення запису, який описує клієнтську частину захищеного з'єднання, визначає параметри функціонування МШ-клієнту.

<u>Створення запису</u>

Створити опис параметрів МШ-клієнту можливо за допомогою:

- підпункту меню *«Вид» > «З'єднання»*;

- інструменту *«Реєстрація нового з'єднання»*;
- комбінації гарячих клавіш Ctrl+F2;
- підпункту *«Нове з'єднання»* меню, що «вспливає», рис. 12: «клік» правою кнопкою маніпуляторі типу «миша» на області відображення інформації про з'єднання (рис. 10).

Як результат дії користувач отримує вікно введення даних про з'єднання, рис. 21.

Вікно містить наступні області:

- інформаційна область «*Загальні*»: адміністратор вказує назву з'єднання (текстове повідомлення, що дозволяє відрізнити один запис з параметрами МШ-клієнту від іншого);
- інформаційна область «*Сервер*»: адміністратор обирає з переліку вже виконаних налаштувань МШ-серверу необхідний, після чого виконується автоматичне заповнення всіх інформаційних полів (за умови коректного опису налаштувань МШ-серверу);
- інформаційна область «*Модуль шифрування*»:
  - адміністратор обирає з переліку МШ, який буде виконувати роль МШ-клієнту, після чого виконується автоматичне заповнення всіх інформаційних полів;
  - адміністратор вказує номер порту, по якому буде виконуватись взаємодія між МШ-клієнтом та клієнтською частиною програмного забезпечення (відкритий зв'язок).

Як результат виконання налаштувань, наведених на рис. 22, буде виконано зміни в конфігураційному файлі CryptoServer.ini МШ з ідентифікаційним номером 10002, а саме додано блок параметрів:

[link1]

type=client	– роль МШ при реалізації з'єднання: клієнт;
id=2	– ідентифікаційний номер з'єднання: 2;
sid=1001	– ідентифікаційний номер МШ, з яким встановлюється захищений зв'язок: 1001;
inp_port=10011	– порт, який «прослуховує» МШ та по якому встановлюється відкрите з'єднання: 10011;
out_addr=192.168.46.87	– IP-адреса МШ-серверу, з якими встановлюється захищене з'єднання: 192.168.46.223;
out_port=10010	– порт МШ-серверу, по якому встановлюється закрите з'єднання: 10010.

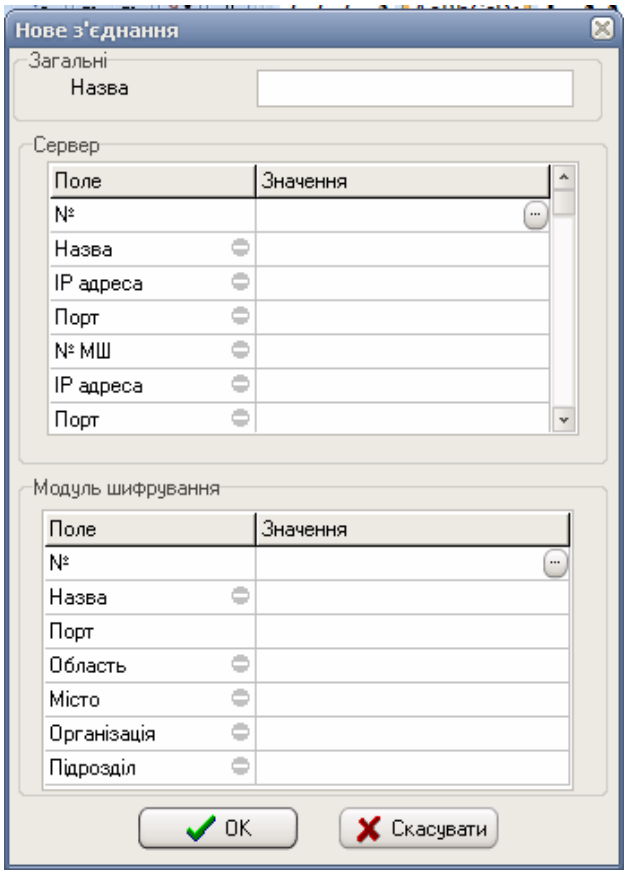


Рис. 21 Вікно введення параметрів МШ-клієнту

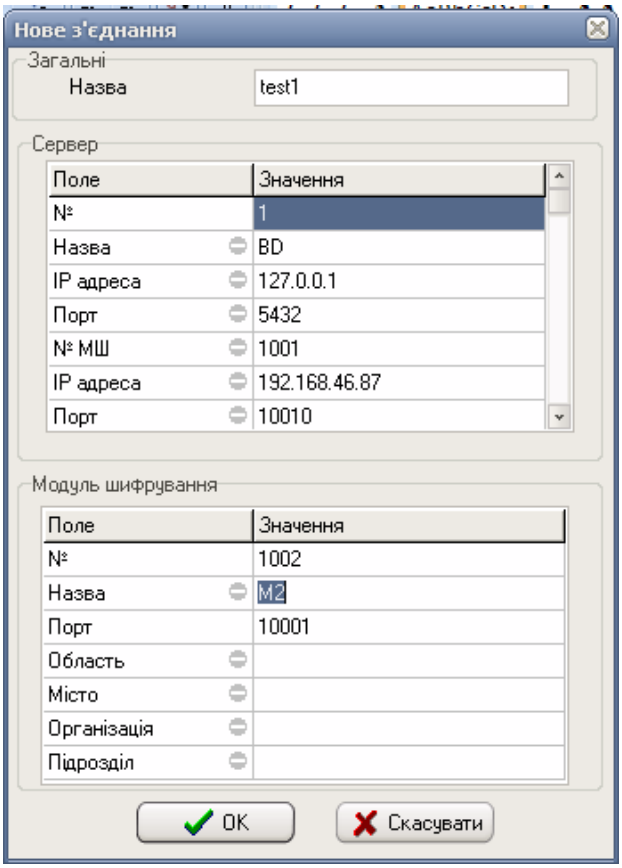


Рис. 22 Приклад вже виконаних налаштувань

Видалення запису

Для того, щоби видалити запис, який описує налаштування МШ-клієнту необхідно із переліку на закладці *«З'єднання»* обрати потрібний запис та видалити його за допомогою:

- інструменту *«Видалення з'єднання»*;
- підпункту меню *«Робота»* > *«Видалення з'єднання»*;
- підпункту *«Видалити»* меню, що «вспливає», рис. 12;
- «гарячої» клавіші *Del*.

Після підтвердження необхідності видалення запису він буде знищений.

Перегляд та редагування запису

Для того, щоби виконати детальний перегляд запису (який описує налаштування МШ-клієнту), або виконати редагування його даних необхідно із переліку на закладці *«З'єднання»* обрати потрібний запис та виконати перегляд/редагування його за допомогою:

- інструменту *«Перегляд та редагування параметрів з'єднання»*;
- підпункту меню *«Робота»* > *«Властивості»*;

- підпункту *«Властивості»* меню, що «вспливає», рис. 12.

Аналіз інформації, що описує з’єднання

МК надає можливість користувачу виконати наступні операції з даними, що зберігаються в базі даних та описують з’єднання:

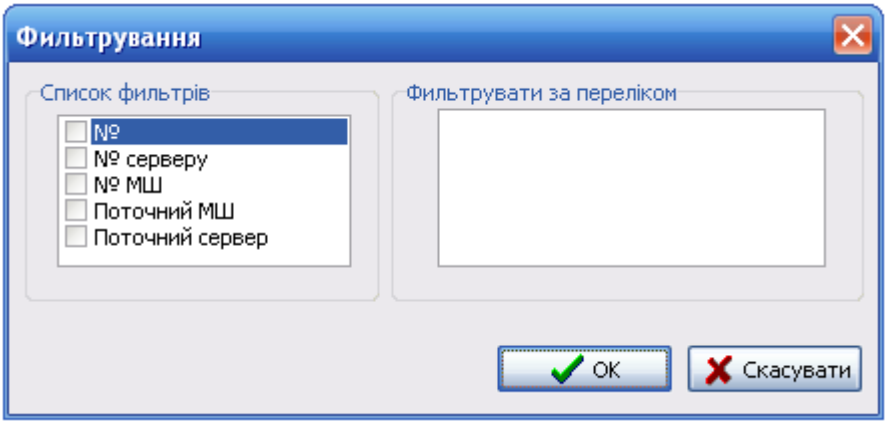
- фільтрування даних за вказаними параметрами;
- сортування даних за вказаними параметрами;
- пошук даних за заданими критеріями.

Фільтрація:

- необхідно відкрити закладку *«З’єднання»*;
- за допомогою кнопки «*Фільтрування записів*» (1 на рис. 9) одержати вікно запиту, рис. 23;
- обрати з переліку один з наступних параметрів фільтрації:
  - *«номер»*: відображення переліку описів МШ-клієнтів, номери яких відповідають переліку та/або діапазону значень, що введені у полі фільтру;
  - *«номер серверу»:* відображення переліку описів МШ-клієнтів, які пов’язані з наведеним номером запису, що опису налаштування МШ-серверу;
  - *«номер МШ»:* відображення переліку описів МШ-клієнтів, що пов’язані з вказаним номером МШ;
  - *«поточний МШ»:* відображення переліку описів МШ-клієнтів, що пов’язані з обраним в закладці *«Модулі шифрування»* МШ;
  - *«поточний сервер»:* відображення переліку описів МШ-клієнтів, які пов’язані з обраним в закладці *«Сервери»* описом МШ-серверу.

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

Рис. 23 Вікно з параметрами фільтрації



Для того, щоб зняти фільтрацію необхідно убрати всі «галочки» у вікні з параметрами фільтрації та натиснути кнопку *«ОК»*.

Сортування:

- необхідно відкрити закладку «*З'єднання*»;
- за допомогою кнопки «*Сортування записів*» (2 на рис. 9) одержати вікно запиту, рис. 24;
- обрати з переліку поле, за даними якого буде виконано сортування. Сортування виконується за наступними полями:
  - «*номер*»;
  - «*назва*»;
  - «*МШ*»;
  - «*порт МШ*»;
  - «*сервер*»;
  - «*назва серверу*»;
  - *«МШ серверу»;*
  - *«порт МШ серверу».*

Для того щоб обрати направлення сортування (за збільшення або за спаданням) необхідно натиснути лівою кнопкою маніпулятора на обраному параметрі. Як результат дії користувач отримує графічне зображення напрямку сортування. Після цієї операції необхідно підтвердити необхідність сортування шляхом натискання кнопки «*ОК*» у вікні (рис. 24).

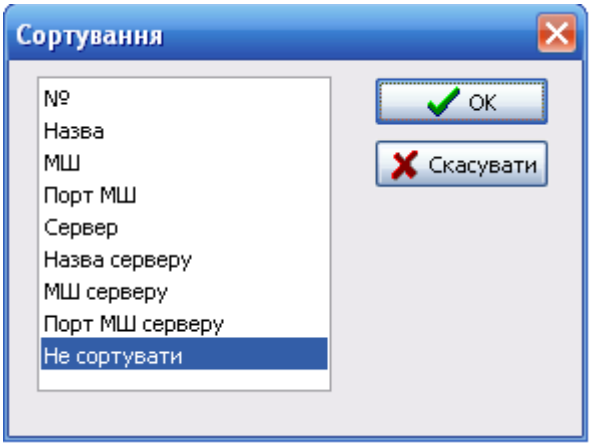


Рис. 24 Вікно параметрів сортування

Пошук

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

- відкрити закладку «*З'єднання*»;
- за допомогою кнопки «*Пошук записів*» (3 на рис. 9) одержати вікно запиту, рис. 25;
- задати текст, пошук якого виконується в інформаційних полях, що описують сертифікати та натиснути кнопку «*Далі*».

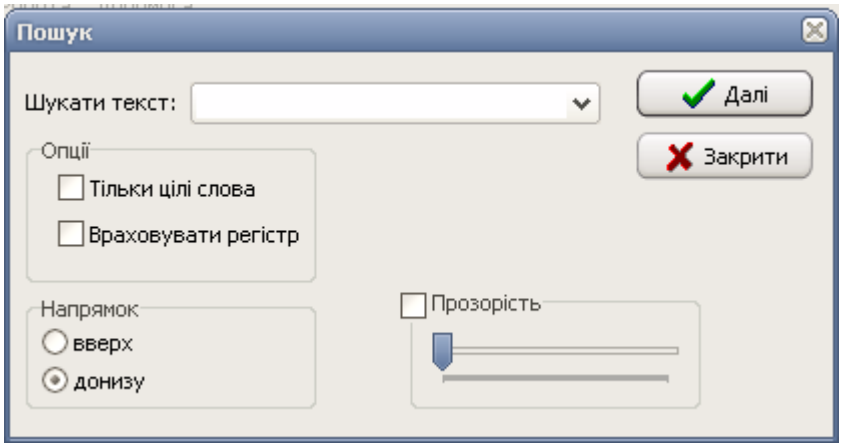


Рис. 25 Вікно введення параметрів пошуку

4.2.4.5 Журнал

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

<u>Перегляд переліку зареєстрованих подій в поточному сеансі роботи</u>

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

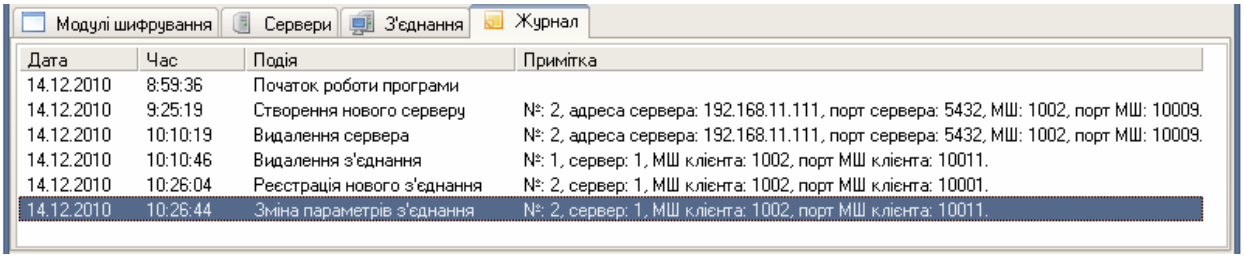


Рис. 26 Закладка «*Журнали*»

Журнал реєстрації подій надає інформацію щодо:

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

<u>Фільтрація подій</u>

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

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

Як результат користувач одержує доступ до вікна (рис. 27) з наступними параметрами фільтрації:

- «*тип повідомлення*»: дозволяє виконати перегляд подій, які мають один з наведених нижче типів повідомлення:
  - початок роботи програми;
  - завершення роботи програми;
  - збереження резервної копії бази даних;
  - відновлення бази даних з резервної копії;
  - реєстрація нового з’єднання;
  - зміна параметрів з’єднання;
  - видалення з’єднання;
  - створення нового серверу;
  - зміна параметрів серверу;
  - видалення серверу;
  - старт серверу МК;
  - зупинка серверу МК;
  - надсилання команди на створення налаштувань МШ;
  - надсилання команди на видалення налаштувань МШ;

- підключення клієнта TCP;
- відключення клієнта TCP;
- ідентифікація МШ;
- запит на зміну конфігурації;
- видалення МШ;
- зміна IP-адреси МШ;
- обробка команди.

– «*дата / час*»: відображаються всі події, час реєстрації яких потрапляє до вказаного періоду;

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

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

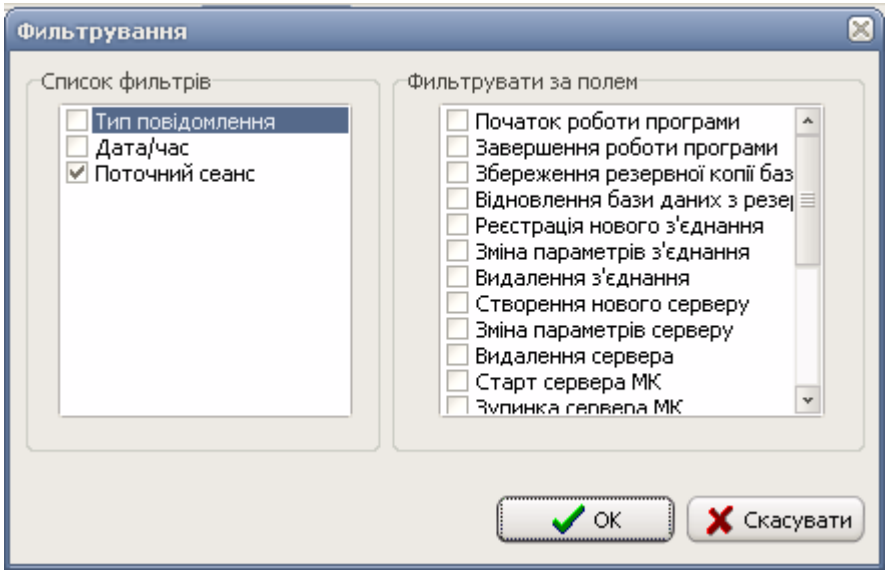


Рис. 27 Вікно з параметрами фільтрації журналу реєстрації подій

<u>Пошук зареєстрованих подій за вказаними критеріями</u>

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

– відкрити закладку «*Журнал*»;

– одержати вікно запиту (рис. 28) за допомогою:
  - або інструменту «*Пошук записів*»;
  - або «гарячих клавіш» Ctrl+F;

- або підпункту меню «*Вид*»> *«Пошук»;*

– задати текст, пошук якого виконується в інформаційних полях запису журналу реєстрації подій та натиснути кнопку «*Далі*».

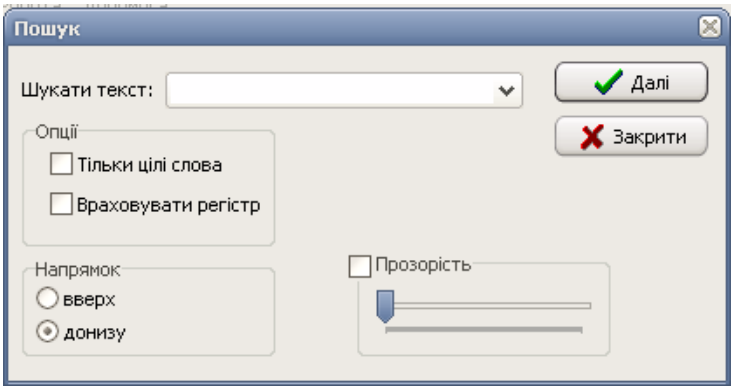


Рис. 28 Вікно введення параметрів пошуку

4.2.4.6 Резервування інформації

<u>Створення резервної копії</u>

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

Для резервного збереження інформації необхідно виконати наступну послідовність дій:

– обрати підпункт меню *«Файл» > «Резервне копіювання»;*

– обрати у вікні, що зображено на рис. 29, необхідні параметри збереження. Надається можливість зберегти інформацію:

- за командою адміністратора, натиснувши кнопку «*Виконати*», рис 29. За результатом виконання адміністратор одержує повідомлення, наведене на рис. 30;
- під час запуску ЦРК на виконання;
- одразу по завершенню роботи ЦРК;
- за вказаною періодичністю.

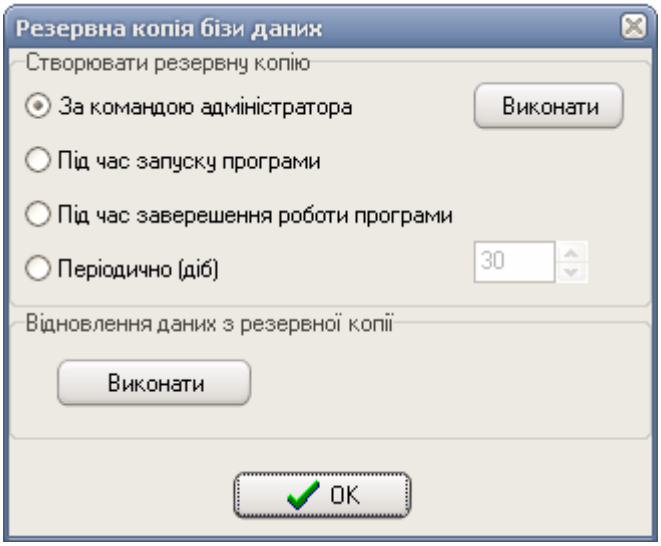


Рис. 29 Вікно вибору параметрів резервування

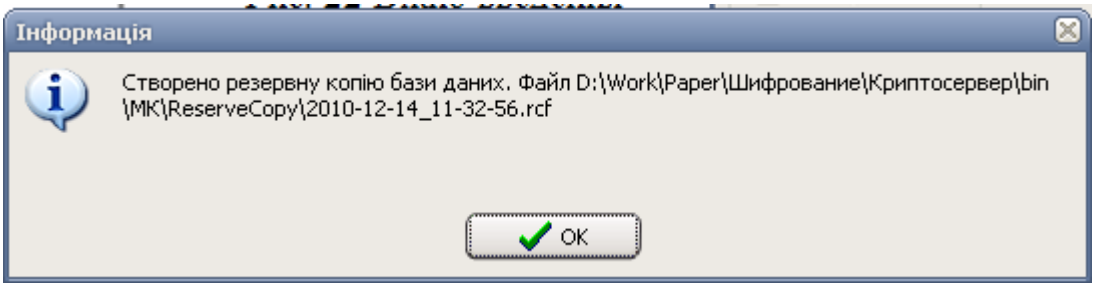


Рис. 30 Приклад повідомлення про створення резервної копії

Відновлення із резервної копії

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

Для відновлення інформації необхідно виконати наступну послідовність дій:

- обрати підпункт меню *«Файл» > «Резервне копіювання»;*
- обрати кнопку «*Виконати*» відновлення даних з резервної копії, рис. 29;
- обрати необхідний файл із наданого переліку, рис. 31;
- за результатами операції отримати повідомлення, вказане на рис. 32.

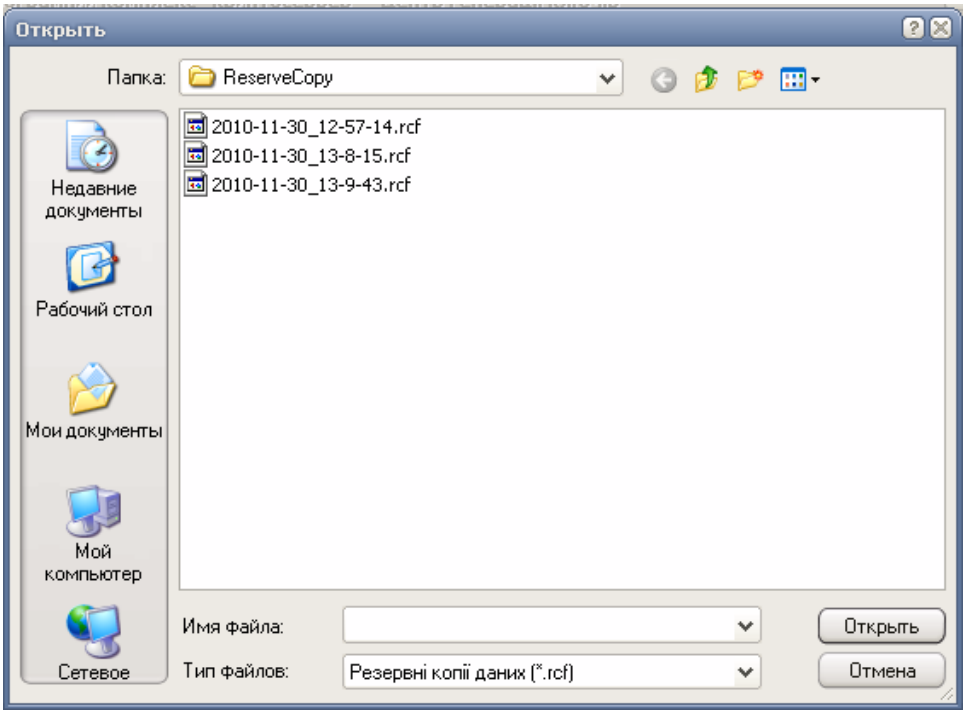


Рис. 31 Вибір файлу, що містить резервну копію даних

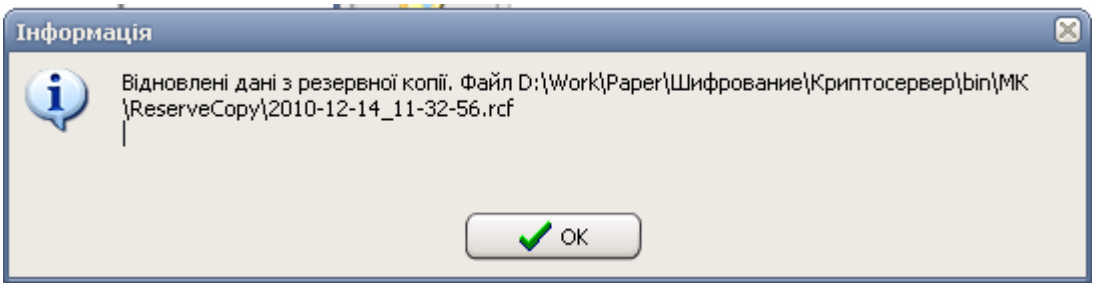


Рис. 32 Повідомлення про відновлення даних

4.2.4.7 Робота МК у режимі «онлайн»

Для того, щоб МК мав можливість виконувати функції керування компонентами Комплексу необхідно задати режим роботи «онлайн».

Для цього необхідно скористатись:

- або інструментом *«Виконати старт серверу МК»*;
- або комбінацією «гарячих» клавіш Ctrl+F5;
- або підпунктом меню *«Робота»> «Старт серверу МК»*.

5. УМОВИ ВИКОНАНЯ ПРОГРАМИ

Модуль керування функціонує на ПЕОМ під керуванням операційних систем Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Vista.

Склад технічних засобів визначається вимогами зазначеної операційної системи.

Вимоги до персоналу не висуваються.

.

Аркуш реєстрації змін

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