Прим. №__

**ЗАТВЕРДЖЕНО**

UA. 35363887.00002-01 34 03-ЛЗ

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

# НАСТАНОВА ОПЕРАТОРА

“ПРОГРАМНИЙ КОМПЛЕКС КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. МОДУЛЬ ШИФРУВАННЯ”

UA. 35363887.00002-01 34 03

на 24 аркушах

Київ – 2010

**ЗМІСТ**

# 1. ВСТУП

В даному документі наведена настанова оператора програмного модуля «Модуль шифрування», який є складовою частиною програмного комплексу криптографічного захисту інформації «Криптосервер» (далі – Комплекс) та призначений для побудови захищеної мережі (шлюз захищеної мережі), який встановлюється на границі захищеної мережі (далі – ЗМ) або границі сегмента ЗМ, що функціонує в інтересах одного, декількох або всіх суб'єктів (об'єктів) даної ЗМ (сегмента ЗМ), що забезпечує створення захищених з'єднань із іншими довіреними модулями 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 шифрування» має наступні атрибути:

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

2.2 Програмне забезпечення, необхідне для функціонування МШ

Функціонування Модуля шифрування здійснюється під керуванням 785

2.3 Мова програмування

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

## 3. ФУНКЦІОНАЛЬНЕ ПРИЗНАЧЕННЯ

Модуль шифрування є програмним засобом, призначеним для побудови ЗМ (шлюз ЗМ), який встановлюється на границі ЗМ або границі сегмента ЗМ, що функціонує в інтересах одного, декількох або всіх суб'єктів (об'єктів) даної ЗМ (сегмента ЗМ), що забезпечує створення захищених з'єднань із іншими довіреними модулями шифрування.

# 4. ОПИС МОДУЛЯ ШИФРУВАННЯ

## 4.1 Перелік програмних модулів (файлів)

МШ складається з наступних частин:

- робочий модуль (файл CryptoServer.exe): виконує операції шифрування/дешифрування інформації, встановлює канал захищеного зв'язку з іншим МШ;
- бібліотека функцій криптографічних перетворень "UaCrypto": забезпечує реалізацію механізмів криптографічних перетворень під час генерації та зберігання ключових даних.

## 4.2 Робота з МШ

### 4.2.1 Інсталяція

Для забезпечення роботи МШ необхідно:

- виконати інсталяцію програмного забезпечення МШ (файл SetupCryptoServer_v1.exe);
- після генерації Центром генерації ключів ключових документів для МШ необхідно:
  - скопіювати до підкаталогу Keys робочого каталогу модуля (створюється автоматично під час інсталяції) захищений ключовий контейнер (файл з розширенням .cnt) та довгостроковий ключовий елемент (файл з розширенням .dke);
  - скопіювати до підкаталогу cert_db робочого каталогу модуля (створюється автоматично під час інсталяції) сертифікати Центру генерації ключів (ЦГК), Центру розподілу ключів (ЦРК) та власний сертифікат МШ (файли з розширенням .crt);
- виконати налаштування параметрів МШ (файл CryptoServer.ini, робочого каталогу програми).

### 4.2.2 Налаштування параметрів робочого модуля

Налаштування параметрів виконуються у ручному режимі (безпосередньо на АРМ з встановленим МШ) або централізовано, з використанням можливостей Модуля керування (далі – МК).

Опис процедури налаштування параметрів МШ за допомогою МК наведено в документі «Настанова оператора. «Програмний комплекс криптографічного захисту інформації «Криптосервер». Модуль керування».

Примітка:

*Рекомендовано виконувати налаштування параметрів МШ лише за допомогою засобів модуля керування, після чого виконувати розсилку ini-файлів для відповідних МШ.*

Параметри задаються у файлі CryptoServer.ini.

Існують наступні блоки параметрів:

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

- sid - ідентифікаційний номер МШ в структурі Комплексу;
- certdir - найменування каталогу, якій містить сертифікати \ локальна база сертифікатів, за умовчанням – Certs;
- keysdir - найменування каталогу, якій містить ключові дані, за умовчанням – Keys;
- logdir - найменування каталогу, якій містить журнали повідомлень, за умовчанням – Logs;
- contfile - назва файлу, якій містить захищений ключовий контейнер \ назва файлу-контейнера МШ;
- dkefile - назва файлу, якій містить довгостроковий ключовий елемент МШ \ назва файлу ДКЕ;
- certfile - назва файлу, якій містить сертифікат МШ (файл міститься у локальної базі сертифікатів) \ назва файлу сертифіката МШ;
- cacertfile - назва файлу, якій містить сертифікат ЦГК (файл міститься у локальної базі сертифікатів) \ назва файлу сертифіката ЦГК;
- maxthreads - Максимальна кількість клієнтських підключень, за умовчанням – 100;

Блок представлений у файлі CryptoServer.ini в єдиному екземплярі.

Приклад заповнення параметрів блоку:

*[common]*
*sid=1001*
*certdir=cert_db*
*keysdir=Keys*
*contfile=7a541ff5d5749d694dba19d314ba864109dd33b95aee41877afe8b30b09e3e1b.cnt*
*dkefile=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, за допомогою якого буде реалізована взаємодія МШ та ЦРК. За замовченням дорівнює 10001;
- 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=127.0.0.1*
*port=10002*
*certfile=2c39a602189debe4c8f07d0b52948737fe8cd4fe680ad43486a938ad29e65be5.crt*

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

- addr - адреса комп'ютера, на який встановлено МК;
- port - номер порту, за допомогою якого буде реалізована взаємодія МШ та МК.
- sid - ідентифікатор МК. Дорівнює 3.
- restart - Періодичність спроб підключення до МК у мілісекундах; за умовчанням – 20000 (20 секунд).

Блок представлений у файлі CryptoServer.ini в єдиному екземплярі.

Приклад заповнення параметрів блоку:

*[mk]*
*addr=127.0.0.1*
*port=10002*
*sid=3*

Блоки [link*x*] (*x* – ціле число) – задають значення параметрів з'єднань, які необхідно захищати. Файл CryptoServer.ini може містити декілька таких блоків, тому при їх необхідно нумерувати під час опису (наприклад: [link1], [link2],…[link100]). У блоці задаються значення наступних параметрів:

id - ідентифікаційний номер з'єднання (параметр використовується під час з'єднання з МК);

sid - ідентифікаційний номер МШ, яким здійснюється з'єднання (параметр використовується лише для опису з'єднання client з типом server);

type - тип з'єднання. Параметр може мати наступні значення:
- client: МШ виконує роль клієнта під час з'єднання. МШ встановлюється на клієнтському АРМ;
- server: МШ виконує роль серверу під час з'єднання. МШ встановлюється безпосередньо на сервері (або на АРМ, який має повноваження доступу до ресурсів серверу);

inp_port - номер порту, який «слухає» МШ: дані одержані з цього порту вважаються вхідними та будуть перенаправлені відповідно до значень двох наступних параметрів;

out_addr - IP-адреса АРМ, на який буде перенаправлено одержані дані. У випадку, якщо це адреса АРМ з встановленим МШ дані будуть шифруватись, якщо це адреса сервера, то навпаки дешифровуватись;

out_port - номер порту, по якому буде перенаправлено одержані МШ дані.

Приклад з’єднання:

| **Клієнтська сторона** | **Серверна сторона** |
|---|---|

Налаштування взаємодії клієнтського програмного забезпечення (Клієнт) та СКБД (Сервер) без використання Комплексу.

| | | | | |
|---|---|---|---|---|
| **Клієнт:**<br>IP-адреса АРМ:<br>Налаштування ODBC:<br>Адреса серверу:<br>Порт: | <br>192.168.1.1<br><br>192.168.1.2<br>5432 | Незахищене з’єднання | **Сервер:**<br>IP-адреса АРМ:<br>СКБД:<br>Порт: | <br>192.168.1.2<br><br>5432 |

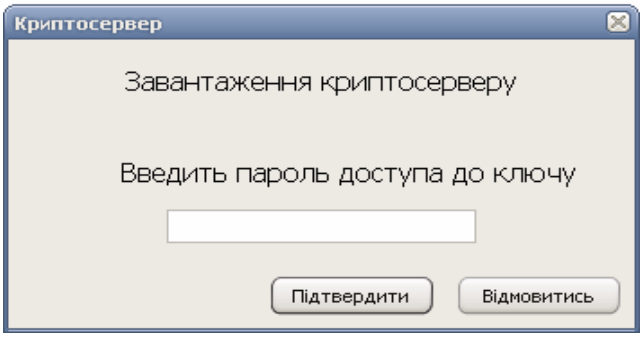
Налаштування взаємодії клієнтського програмного забезпечення (Клієнт) та СКБД (Сервер) з використанням Комплексу.

| | | | | |
|---|---|---|---|---|
| **Клієнт:**<br>IP-адреса АРМ:<br>Налаштування ODBC:<br>Адреса серверу:<br>Порт: | <br>192.168.1.1<br><br>127.0.0.1<br>50000 | | **Сервер:**<br>IP-адреса АРМ:<br>СКБД:<br>Порт: | <br>192.168.1.2<br><br>5432 |
| Примітка:<br>Клієнт та МШ1 встановлені на одному АРМ.<br>У випадку, якщо МШ1 та Клієнт розташовані на різних АРМ в параметрі ODBC «Адреса серверу» вказується IP-адреса АРМ, на якому розташовано МШ1. | | | Примітка:<br>Сервер та МШ2 встановлені на одному АРМ.<br>У випадку, якщо МШ2 та Сервер розташовані на різних АРМ в параметрі МШ2 «out_addr» вказується IP-адреса АРМ, на якому розташовано Сервер. | |
| Незахищене з’єднання | | | Незахищене з’єднання | |
| **Модуль шифрування 1:**<br>*[link1]*<br>*id=1*<br>*sid=1*<br>*type=client*<br>*inp_port=50000*<br>*out_addr=192.168.1.2*<br>*out_port=50001* | | Захищене з’єднання | **Модуль шифрування 2:**<br>*[link1]*<br>*id=3*<br>*type=server*<br>*inp_port=50001*<br>*out_addr=127.0.0.1*<br>*out_port=5432* | |

### 4.2.3 Запуск МШ

Для запуску МШ на виконання, за умов здійснення налаштувань вищенаведених параметрів, необхідно обрати файл CryptoServer.exe та виконати його запуск, після чого ввести пароль закритого ключа.

Рис. 1 Вікно запиту паролю доступу до ключу під час запуску МШ




Після запуску МШ виконує функції шифрування інформації у відповідності до виконаних налаштувань.

### 4.2.4 Інтерфейс користувача

Після запуску програмного модуля на виконання користувач отримує можливість працювати з графічним інтерфейсом, відображеним на рис. 2.

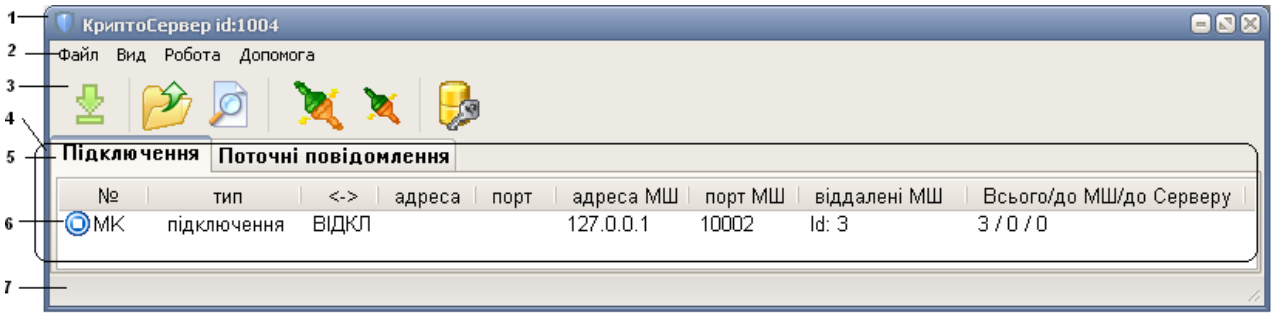



Рис. 2 Інтерфейс користувача

де,

1 - заголовок програми: відображає ідентифікаційний номер МШ у складі Комплексу

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

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

Пункт меню *«Файл»* містить наступні підпункти:

- *«завантажити ключові дані»:* дозволяє виконати зміну ключів (завантаження нового набору ключових даних);
- *«відкрити журнал із файлу»:* дозволяє відкрити журнал реєстрації подій, збережений в каталозі на жорсткому диску.

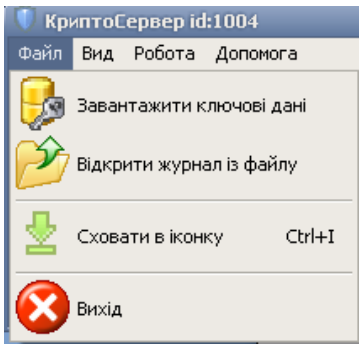


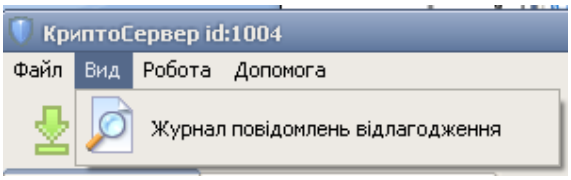

Рис. 3 Підпункти пункту меню «*Файл*»

При цьому буде відкрито вкладення *«Журнал хххх-хх-хх»*. Де *хххх-хх-хх* - дата створення файлу.

- *«сховати в іконку»*: скрити програму в індикатор запущених програм («трей»);
- *«вихід»*: закрити програму.

Пункт меню *«Вид»* містить підпункт «*Журнал повідомлень відлагодження*».

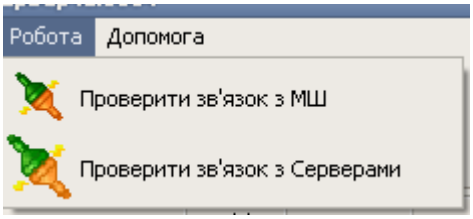
Рис. 4 Підпункт пункту меню «*Вид*»




Пункт меню *«Робота»* містить наступні підпункти:

- *«перевірити зв'язок з МШ»*: виконати перевірку можливості створення захищених з'єднань з МШ типу «сервер» для неактивних з'єднань типу «клієнт» згідно таблиці налаштувань;
- *«перевірити зв'язок з Серверами»*: виконати перевірку можливості створення з'єднань з віддаленими відкритими серверами через МШ типу «сервер» для неактивних з'єднань типу «клієнт» згідно таблиці налаштувань;

Рис. 5 Підпункти пункту меню «*Робота*»




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

- скрити програму в «трей», кнопка ;
- відобразити/сховати локальний журнал повідомлень, кнопка ;
- перегляд журналів, що збережені на диску, кнопка ;

- виконати тестове підключення неактивних до віддалених серверів, кнопка  ;
- виконати тестове підключення неактивних клієнтів з віддаленим МШ, кнопка  ;
- завантажити ключові дані, кнопка  .

4 - область роботи з повідомленнями (блокнот): надає можливість користувачу виконувати переключення між сторінками журналів та виконувати аналіз повідомлень.

5 - закладка сторінок блокноту: дозволяє виконати переключення між журналами повідомлень.


Рис. 4 Закладки блокноту

6 - область відображення повідомлень: відображає зміст відкритого журналу та надає можливість виконати аналіз та фільтрацію повідомлень за параметрами.

7 - полоса статусу: надає текстову інформацію щодо події, яку планується виконати.

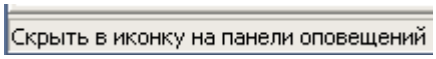



Рис. 5 Приклад повідомлення в полосі статусу.

### 4.2.5 Робота з журналами

#### 4.2.5.1 Журнал «Підключення»

Стаціонарний журнал, що не потребує додаткових дій для його перегляду. Він відображає стан поточних підключень та надає інформацію щодо налаштування МШ. Журнал містить наступні поля:

№ - наведено ідентифікаційний номер з'єднання (поле id при описі розділу [link] файлу налаштувань CryptoServer.ini);

Тип - вказано тип з’єднання (клієнт або сервер);

Порт - зазначено порт, до якого буде звертатись МШ при наявності підключення до нього відповідно клієнтського застосування (для типу «клієнт») або іншого МШ (для типу «сервер»);

адреса МШ - зазначена адреса комп’ютеру, з яким при наявності підключення буде виконувати спробу з’єднатись МШ;

віддалені МШ - ідентифікаційний номер МШ у складі Комплексу, з яким буде встановлено (для типу з’єднання «клієнт» при відсутності запиту з боку клієнтського застосування) або вже встановлено зв'язок (для всіх типів з’єднань при наявності запитів).

Всього / до МШ / до Серверу - статистика мережних та захищених з’єднань; відображається відповідно:

- загальна кількість спроб підключень /
- кількість успішних підключень до МШ /
- кількість успішних підключень до відкритого серверу

Для прикладу розглянемо наступні варіанти підключень.

4.2.5.1.1 Опис журналу МШ *«Підключення»* одразу після його (МШ) запуску на виконання та без активних з’єднань

В першій строчці журналу відображаються дані щодо підключення МШ до модуля керування, а саме:

- адреса МШ (127.0.0.1): адреса комп’ютера, на якому функціонує модуль керування;
- порт МШ (10002): порт, який модуль керування прослуховує;
- віддалені МШ (Id 3): ідентифікаційний номер модуля керування в складі Комплексу.

В другій строчці наведено дані безпосередньо самого МШ. У нашому випадку:

- номер з’єднання 1;
- роль, яку виконує МШ – сервер;

- порт та IP-адреса серверної частини програмного забезпечення, з якою МШ встановлює відкрите з'єднання: 5432 та 192.168.46.87;
- порт, який «прослуховує» МШ та по якому буде виконуватись підключення МШ-клієнтів і встановлюватись захищене з'єднання: 10010;
- у полі «віддалені МШ» зазначено, що підключень до МШ з боку МШ-клієнтів немає;
- загальна кількість спроб підключень – 8, з них успішних підключень до МШ – 8, кількість успішних підключень до відкритого серверу – 8.

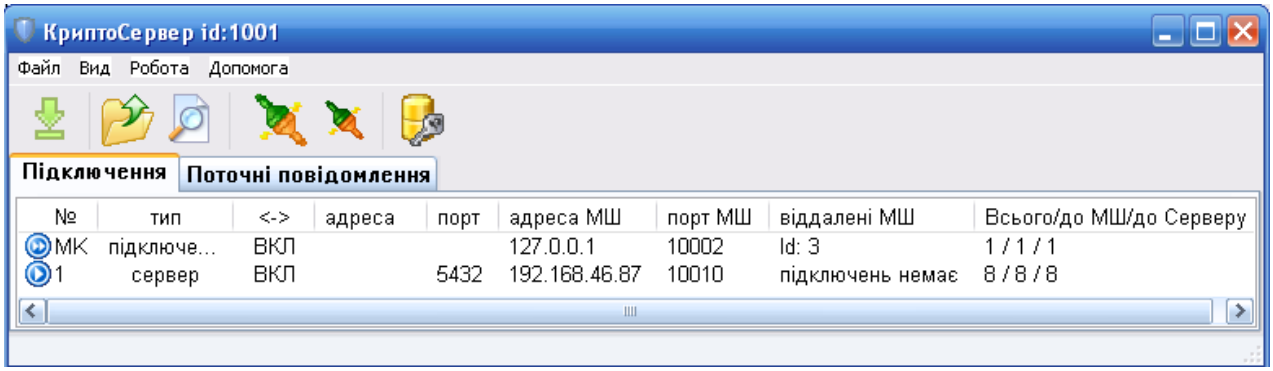



Рис. 6 Журнал «Підключення» (без підключень з боку клієнтського застосування)

4.2.5.1.2 Опис журналу МШ-серверу після встановлення з'єднання

Після того, як клієнтське застосування виконає запит на з'єднання в закладці буде відображена відповідна інформація. Для з'єднання типу «сервер», в полі

№ - наведено порядковий номер з'єднання, який є складним номером, що складається з ідентифікаційного номеру з'єднання (поле id при описі розділу [link] файлу налаштувань CryptoServer.ini) та порядкового номеру з'єднання (наприклад 1.1 – id =1, з'єднання являється першим в переліку з'єднань);

Тип - підключення. Вказує на те, що було виконано підключення до серверу. При цьому в строчці, що описує відповідний сервер, буде зазначена кількість поточних підключень.

Порт - зазначено реальний порт серверу (наприклад, сервер баз даних), до якого виконує спробу підключитись клієнтське застосування;

Адреса - зазначена адреса комп'ютеру (наприклад, комп'ютер на якому встановлена СКБД), з яким виконує з'єднання клієнтське застосування;

адреса МШ - зазначено IP-адресу комп'ютера на якому встановлено МШ-клієнт, який підключено до МШ-серверу;

порт МШ - наведена технологічна інформація щодо портів, які використовуються МШ-сервером для обробки вхідних з'єднань;

віддалені МШ - ідентифікаційний номер МШ-клієнту у складі Комплексу, який виконав підключення до МШ-серверу.

Всього/ до МШ/ до серверу - статистика мережних та захищених з'єднань; відображається відповідно:

– загальна кількість спроб підключень /
– кількість успішних підключень до МШ /
– кількість успішних підключень до відкритого серверу.

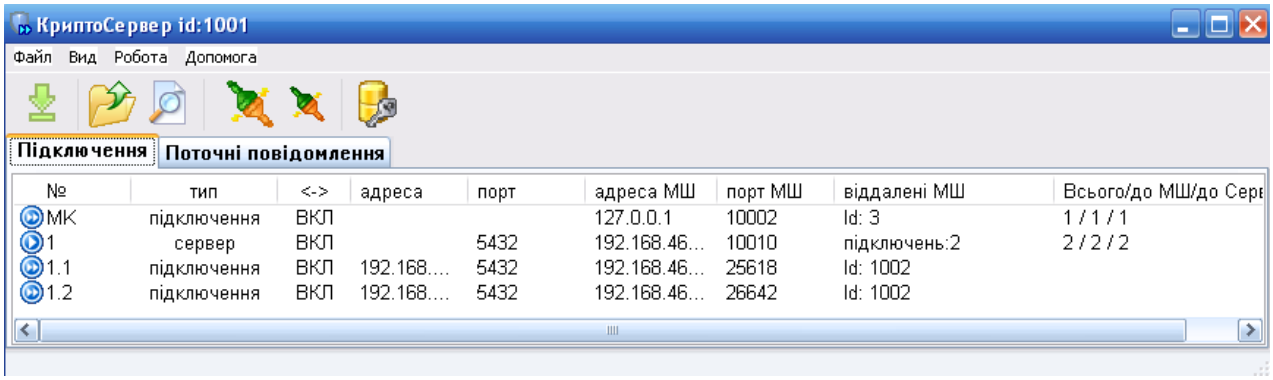



Рис. 7 Приклад журналу «Підключення» для МШ, який відповідає за з'єднання типу «сервер»(з підключеннями з боку клієнтського застосування)

4.2.5.1.3 Опис журналу МШ-клієнта після встановлення з’єднання

Після того, як клієнтське застосування виконає запит на з’єднання в закладці буде відображена відповідна інформація. Для з’єднання типу «клієнт» при описі підключення, в полі

№ - наведено порядковий номер з’єднання, який є складним номером, що складається з ідентифікаційного номеру з’єднання (поле id при описі розділу [link] файлу налаштувань CryptoServer.ini) та порядкового номеру з’єднання (наприклад 1.1 – id =1, з’єднання являється першим в переліку з’єднань);

Тип - підключення. Вказує на те, що було виконано підключення до серверу.

Порт - зазначена технологічна інформація щодо портів, які використовуються МШ для внутрішньої обробки підключення;

Адреса - зазначена IP-адреса комп’ютера, з якого ініціюється з’єднання клієнтським застосуванням;

адреса МШ - зазначено IP-адресу комп’ютера на якому встановлено МШ-сервер, до якого підключено МШ-клієнт;

порт МШ - наведено порт МШ-сервера, що використовується для обробки вхідних з’єднань;

віддалені МШ - ідентифікаційний номер МШ-сервера у складі Комплексу, до якого виконано підключення з боку МШ-клієнту;

Всього/
до МШ/
до Серверу - статистика мережних та захищених з’єднань; відображається відповідно:

- загальна кількість спроб підключень /
- кількість успішних підключень до МШ /
- кількість успішних підключень до відкритого серверу.

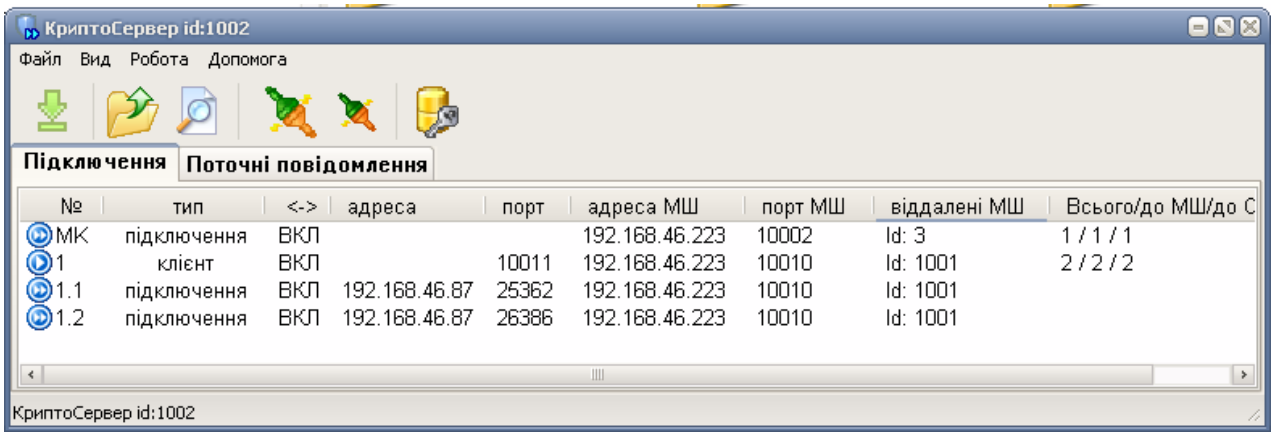



Рис. 8 Приклад журналу «*Підключення*» для МШ, який відповідає за з'єднання типу «клієнт» (з підключеннями з боку клієнтського застосування)

#### 4.2.5.2 Журнал «*Поточні повідомлення*»

Стаціонарний журнал, що не потребує додаткових дій для його перегляду.

Відображає інформацію щодо виконання МШ своїх основних функцій в період з моменту останнього запуску МШ на виконання до поточного моменту.

В журналі наведено інформацію щодо:

- порядкового номеру події;
- часу події;
- типу події;
- ідентифікаційного номеру з'єднання;
- IP-адреси та порту джерела (з яких ініціюється з'єднання);
- IP-адреси та порту призначення (до яких виконується з'єднання).

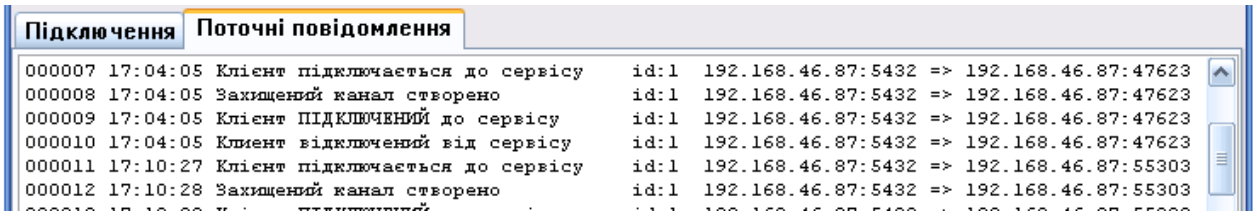



Рис. 9 Приклад журналу «Поточні повідомлення»

#### *4.2.5.3* Журнал *«Повідомлення відлагодження»*

Для перегляду журналу необхідно використати кнопку на панелі інструментів *«Відобразити журнал повідомлень відладки»*  .

Відображає інформацію щодо внутрішніх повідомлень та критичних помилок МШ (помилки конфігурування, тощо). Дані, що містяться дозволяють адміністратору МШ визначити можливі причини непрацездатності МШ.

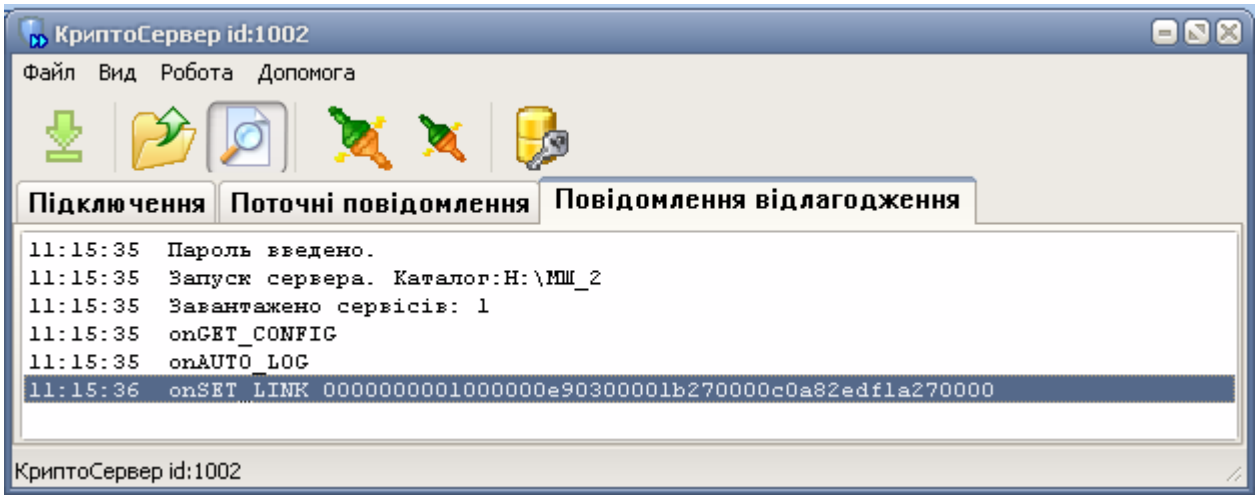



Рис. 10 Журнал «Повідомлення від лагодження»

#### 4.2.5.4 Журнал реєстрації подій, що зберігається на жорсткому диску

Для перегляду змісту журналу, що зберігається у файлах на жорсткому диску необхідно або використати підпункт меню *«Файл» > «Відкрити журнал із файлу»,* або відповідний інструмент панелі інструментів.

Програма надає можливість користувачеві обрати необхідний файл журналу реєстрації подій, який відображає інформацію щодо функціонування МШ під час попередніх запусків.

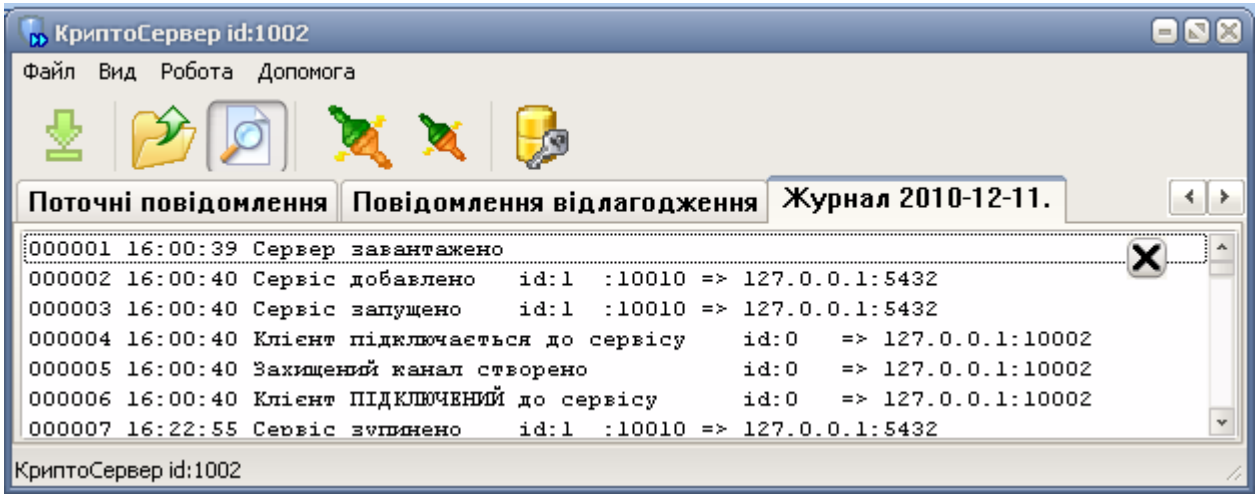



Рис. 11 Журнал реєстрації подій

### 4.2.6 Завантаження нового набору ключових даних

Для того, щоб спростити адміністратору процедуру оновлення набору ключових даних передбачена функція, що ініціюється за допомогою або інструменту *«Завантажити ключові дані»*, або підпункту меню *«Файл»* > *«Завантажити ключові дані»*.

Як результат, МШ надасть запит на введення нового набору ключових даних, після чого автоматично виконає зміну у файлі налаштувань CryptoServer.ini.

Для того, щоб зміни були прийняті необхідно виконати перезапуск МШ.

### 4.2.7 Тестування зв’язку

У МШ реалізовані наступні механізми тестування зв’язку:

- Перевірка можливості створення захищених з’єднань з МШ типу «сервер». Здійснюється з використанням пункту меню *«Робота»* > *«Перевірити зв'язок з МШ»* або інструменту *«виконати тестове підключення неактивних до віддалених серверів»* панелі інструментів. Під час процедури тестування для кожного неактивного (не підключеного) з’єднання типу «клієнт» за таблицею налаштувань здійснюється спроба встановити захищене з’єднання із МШ типу «сервер» та відключення, у випадку успішної спроби. Аналіз результатів тестування здійснюється за

вмістом поля «*Всього / до МШ / до Серверу*» журналу «Підключення».

- Перевірка можливості створення мережних з'єднань з віддаленими відкритими серверами через МШ типу «сервер». Здійснюється з використанням пункту меню *«Робота» > «Перевірити зв'язок з Серверами»* або інструменту *«виконати тестове підключення неактивних клієнтів з віддаленим МШ»* панелі інструментів. Під час процедури тестування для кожного неактивного (не підключеного) з'єднання типу «клієнт» за таблицею налаштувань здійснюється спроба встановити з'єднання із МШ типу «сервер», подальша спроба встановити відкрите з'єднання між МШ типу «сервер» та відповідним віддаленим відкритим сервером та відключення, у випадку успішної спроби. Аналіз результатів тестування здійснюється за вмістом поля «*Всього / до МШ / до Серверу*» журналу «Підключення».

### 4.2.8 Завершення роботи

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

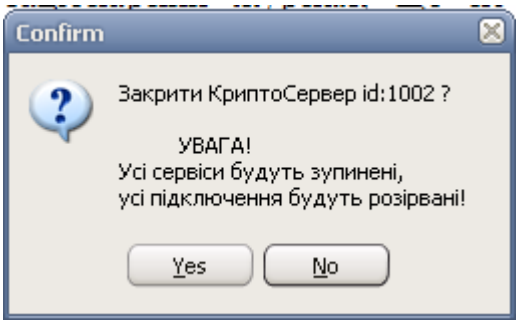



Рис. 12 Запит при завершенні роботи МШ

### 4.2.9 Повідомлення оператору

- Сервер завантажено;
- Сервер зупинено;
- Сервіс запущено;
- Сервіс зупинено;
- Клієнт підключається до сервісу;
- Захищений канал створено;

- Клієнт підключений до сервісу;
- Клієнт відключений від сервісу;
- Сервіс добавлено;
- Сервіс видалено;
- Помилка. При розшифруванні ключа;
- Помилка. OCSP запиту;
- Помилка. Немає відповіді від OCSP сервера;
- Помилка. Невірна відповідь OCSP сервера;
- Помилка. OCSP сервера;
- Помилка. Невірний підпис відповіді OCSP сервера;
- Помилка. OCSP: Сертифікат недійсний;
- Помилка. При формуванні OCSP запиту;
- Помилка. Невірний формат даних;
- Помилка. Невірний формат сертифіката;
- Помилка. Невірний сертифікат;
- Помилка. Невірний підпис сертифіката;
- Помилка. Невірний формат команди;
- Помилка. Сервер перевантажений. Частину запитів відхилено;
- Помилка. Відкриття сервера;
- Помилка. Підключення;
- Помилка. Підключення до серверу на віддаленому МШ;
- Помилка. Розшифрування даних.

## 5. УМОВИ ВИКОНАНЯ ПРОГРАМИ

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

Склад технічних засобів визначається вимогами зазначеної операційної системи.

Вимоги до персоналу не висуваються.

**Аркуш реєстрації змін**

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