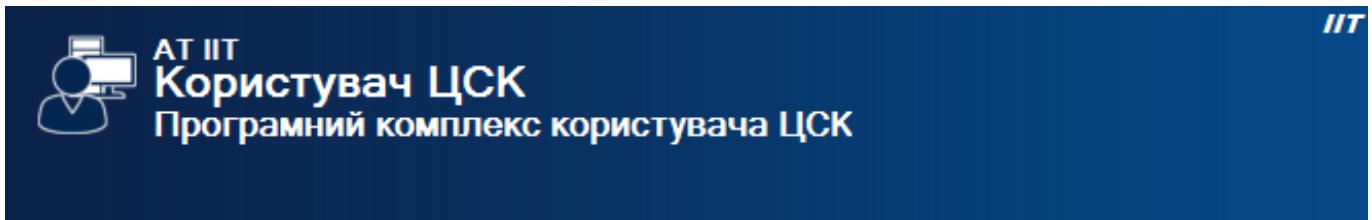




ЗАТВЕРДЖЕНИЙ
ЄААД.00021-13-ЛЗ



Інв. № ориг.	Підп. та дата	Взам. інв. №	Інв. № дубл.	Підп. та дата

Програмний комплекс користувача ЦСК Web-бібліотеки підпису користувача ЦСК

Версія 1.3.1

Настанова оператора

ЄААД.21118-13 34 02-1

Харків 2018 р.

АНОТАЦІЯ

Даний документ містить опис та настанову користувача для роботи з програмними компонентами (web-бібліотеками) підпису користувача ЦСК “ІІТ Користувач ЦСК-1. Бібліотеки підпису користувача ЦСК (web)”, які об’єднані у програмний комплекс (далі - програма). Настанова містить відомості щодо послідовності та особливостей інсталяції програми, а також встановлення параметрів роботи.

Пор. № зміни	Підпис відпов. особи	Дата внесення

3 МІСТ

1 ПРИЗНАЧЕННЯ ПРОГРАМИ	5
2 УМОВИ ВИКОНАННЯ ПРОГРАМИ	6
3 ІНСТАЛЯЦІЯ ПРОГРАМИ	8
3.1 Інсталяція програми в ОС Microsoft Windows	8
3.2 Інсталяція програми в ОС Apple MAC OS X	10
3.3 Інсталяція програми в ОС Linux Debian/Ubuntu	11
3.4 Інсталяція web-розширеннь	13
3.4.1 Інсталяція web-розширення для браузера Google Chrome	13
3.4.2 Інсталяція web-розширення для браузера Opera	14
3.4.3 Інсталяція web-розширення для браузера Mozilla Firefox	15
4 ПОЧАТОК РОБОТИ З ПРОГРАМОЮ	16
4.1 Агент підпису для ОС Microsoft Windows	16
4.1.1 Завантаження програми	16
4.1.2 Встановлення параметрів роботи програми	16
4.1.2.1 Агент підпису	17
4.1.2.2 Криптографічна бібліотека	18
4.2 Агент підпису для ОС Apple MAC OS X	19
4.2.1 Завантаження програми	19
4.2.2 Встановлення параметрів роботи програми	20
4.2.2.1 Агент підпису	20
4.2.2.2 Криптографічна бібліотека	21
4.3 Web-розширення для web-браузера (Google Chrome, Opera, Mozilla Firefox)	23
4.3.1 Завантаження програми	23
4.3.2 Встановлення параметрів роботи програми	23
4.4 NPAPI-плагін для web-браузера Mozilla Firefox	25
4.4.1 Завантаження програми	25
4.4.2 Встановлення параметрів роботи програми	25
4.5 ActiveX-компонент для web-браузера Internet Explorer	26
4.5.1 Завантаження програми	26
4.5.2 Встановлення параметрів роботи програми	28
ПЕРЕЛІК СКОРОЧЕНЬ	29
ДОДАТОК А. ВСТАНОВЛЕННЯ ПАРАМЕТРІВ РОБОТИ (ОС MICROSOFT WINDOWS)	30
A.1 Файлова сховище	30
A.2 Proxy-сервер	31
A.3 TSP-сервер	31
A.4 OCSP-сервер	32
A.5 LDAP-сервер	33
A.6 CMP-сервер	34
A.7 Особистий ключ	34
A.7.1 Експортувати	34
A.7.2 Перевірити	36
A.7.3 Згенерувати	37
A.7.4 Знищити	40
A.7.5 Резервне копіювання	40
A.7.6 Зміна паролю захисту особистого ключа	42
A.7.7 Реєстрація носіїв особистого ключа	42
A.8 Сертифікати та СВС	44
A.8.1 Переглянути сертифікати	45
A.8.2 Переглянути СВС	46
A.9 Реєстрація подій	47
ДОДАТОК Б. ВСТАНОВЛЕННЯ ПАРАМЕТРІВ РОБОТИ (ОС APPLE MAC OS X)	49

Пор. № зміни	Підпис відпов. особи	Дата внесення

Б.1 Файлове сховище	49
Б.2 Proxy-сервер	50
Б.3 TSP-сервер	50
Б.4 OCSP-сервер	52
Б.5 LDAP-сервер	52
Б.6 CMP-сервер	53
Б.7 Особистий ключ	54
Б.7.1 Перевірити	54
Б.7.2 Згенерувати	55
Б.7.3 Знищити	58
Б.7.4 Резервне копіювання	58
Б.8 Сертифікати та СВС	60
Б.8.1 Переглянути сертифікати	60
Б.8.2 Переглянути СВС	62
Б.9 Реєстрація подій	63

<i>Пор. № зміни</i>	<i>Підпис відпов. особи</i>	<i>Дата внесення</i>

1 ПРИЗНАЧЕННЯ ПРОГРАМИ

Програма призначена для застосування користувачами центру сертифікації ключів для роботи в web-браузерах і виконує наступні функції:

- управління ключами користувача:
 - генерацію ключів користувача ЦСК, запис особистого ключа на НКІ та формування запита на формування сертифіката;
 - перевірку сформованого сертифіката користувача на відповідність запиту;
 - резервне копіювання особистого ключа з одного НКІ на інший;
 - зміну паролю захисту особистого ключа;
 - знищенння особистого ключа на НКІ;
 - формування та передачу у ЦСК запита на блокування сертифіката користувача;
 - формування та передачу запита на формування нового сертифіката;
- доступ до сертифікатів ЦСК, серверів ЦСК, сертифікатів інших користувачів та СВС:
 - перегляд сертифікатів та СВС з файлового сховища;
 - пошук сертифікатів у файловому сховищі, LDAP-каталозі та за допомогою протоколу OCSP;
 - визначення статусу сертифікатів за допомогою СВС та за протоколом OCSP;
 - перевірку чинності та цілісності сертифікатів та ін.;
- захист файлів користувача:
 - підпис файлів;
 - перевірку файлів;
 - зашифрування файлів;
 - розшифрування файлів.

<i>Пор. № зміни</i>	<i>Підпись відпов. особи</i>	<i>Дата внесення</i>

2 УМОВИ ВИКОНАННЯ ПРОГРАМИ

Для роботи з веб-бібліотеками необхідно встановити бібліотеки веб-підпису за посиланнями:

- ОС Microsoft Windows - <http://iit.com.ua/download/productfiles/EUSignWebInstall.exe>
- ОС Linux (Debian\Ubuntu) x32 - <http://iit.com.ua/download/productfiles/euswi.deb>
- ОС Linux (Debian\Ubuntu) x64 - <http://iit.com.ua/download/productfiles/euswi.64.deb>
- ОС Apple Mac OS X - <http://iit.com.ua/download/productfiles/EUSignWebInstall.pkg>

Додатково, у випадку, якщо ОС або браузер не підтримує роботу з агентом підпису необхідно встановити веб-розширення для браузерів:

- Google Chrome - https://chrome.google.com/webstore/detail/%D1%96%D1%96%D1%82-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87-%D1%86%D1%81%D0%BA-1-%D0%B1%D1%96%D0%B1%D0%BB/jffafkigfgmjafhpkoibhfefeaebmccg?utm_source=chrome-app-launcher-info-dialog
- Opera - <https://addons.opera.com/uk/extensions/details/iit-end-user-ca-1-sign-web-extension/?display=uk>
- Mozilla Firefox - <https://eu.iit.com.ua/download/productfiles/eusw@iit.com.ua.xpi>

Програма може бути завантажена та виконана на ЕОМ під керуванням наступних ОС:

- Microsoft Windows XP SP 2/2003 Server/Vista/2008 Server/7/8/8.1/2012 Server/10 та вище на PC чи ноутбуках з 32-бітовою або 64-бітовою архітектурою;
- Linux на PC чи ноутбуках з 32-бітовою або 64-бітовою архітектурою;
- Apple MAC OS X 10.7 та вище на PC чи ноутбуках з 64-бітовою архітектурою.

Примітка. Агент підпису не підтримує роботу в багато користувальницькому режимі, тому в ОС Microsoft Windows Server для роботи необхідно використовувати web-розширення та NMН-модуль, ActiveX-компонент або NPAPI-плагін для застарілих браузерів.

До складу програми входять web-бібліотеки підпису користувача ЦСК, які виконані у вигляді:

- локального процесу підпису користувача ЦСК (Native messaging host - NMН-модуля) - окремого модуля, що виконується, доступ до якого з web-браузера здійснюється з використанням механізмів стандартного вводу/виводу (stdio) через java-скрипт-обортку та розширення браузера (WebExtension - web-розширення, що встановлюються окремо та необхідні для підтримки зокрема браузерів Google Chrome, Opera, Firefox та ін.);
- агента підпису користувача ЦСК - окремого модуля, що виконується, доступ до якого з web-браузера здійснюється з використанням технології JSON-RPC-запитів на основі протоколу HTTP(S) на локальному вузлі (IP-адреса - localhost) безпосередньо із загальної java-скрипт-обортки;
- NPAPI-бібліотеки підпису користувача ЦСК (Netscape Plugin Application Programming Interface - NPAPI-плагіну), доступ до функцій якої(го) з web-браузера здійснюється безпосередньо через загальну java-скрипт-обортку (необхідна для підтримки попередніх і окремих поточних версій браузерів Mozilla Firefox та ін.);
- ActiveX-компонента підпису користувача ЦСК, доступ до функцій якої(го) з web-браузера здійснюється безпосередньо через загальну java-скрипт-обортку (необхідна для підтримки браузера Internet Explorer 9 та вище).

Робота з програмою підтримується в наступних web-браузерах:

- Microsoft Internet Explorer (9 та вище (тільки 32-х розрядна версія) з використанням ActiveX-компоненту або 10 та вище з використанням агента підпису);
- Mozilla Firefox (в ОС Microsoft Windows XP та 2003 Server з використанням агента підпису з версії 22 до 40 або NPAPI-плагіну з 40 до 52, в ОС Microsoft Windows Vista та вище з використанням агента підпису з версії 22 до 58 або з використанням web-розширень та NMН-модуля з версії 50, в ОС Linux з версії 40 до 52 з використанням NPAPI-плагіну або з використанням web-розширень та NMН-модуля з версії 50, в ОС Apple MAC OS X з версії 40 до 58 з використанням агента підпису, або NPAPI-плагіну з версії 40 до 52, або з використанням web-розширень та NMН-модуля з версії 50);

Пор. № зміни	Підпис відпов. особи	Дата внесення

- Google Chrome 29 та вище (в ОС Microsoft Windows з використанням агента підпису або web-розширень та NMН-модуля, в ОС Linux з використанням web-розширень та NMН-модуля, в ОС Apple MAC OS X з використанням агента підпису або web-розширень та NMН-модуля);
- Opera 22 та вище (в ОС Microsoft Windows та Apple MAC OS X з використанням агента підпису або web-розширень та NMН-модуля з версії 35 та вище, в ОС Linux з використанням web-розширень та NMН-модуля з версії 35 та вище);
- Microsoft Edge (в ОС Microsoft Windows з використанням агента підпису);
- Safari 7 та вище (в ОС Apple MAC OS X з використанням агента підпису).

Пор. № зміни	Підпись відпов. особи	Дата внесення

3 ІНСТАЛЯЦІЯ ПРОГРАМИ

3.1 Інсталяція програми в ОС Microsoft Windows

Для інсталяції програми необхідно запустити програму інсталяції (майстер інсталяції) EUSignWebInstall.exe з інсталяційного носія (оптичного диску чи ін.) чи завантажити її з web-сторінки ЦСК.

Після запуску програми інсталяції на першій сторінці (рис. 3.1) виводиться інформація про початок інсталяції. Для продовження інсталяції необхідно натиснути кнопку “Далі”, а для завершення – “Відміна”.

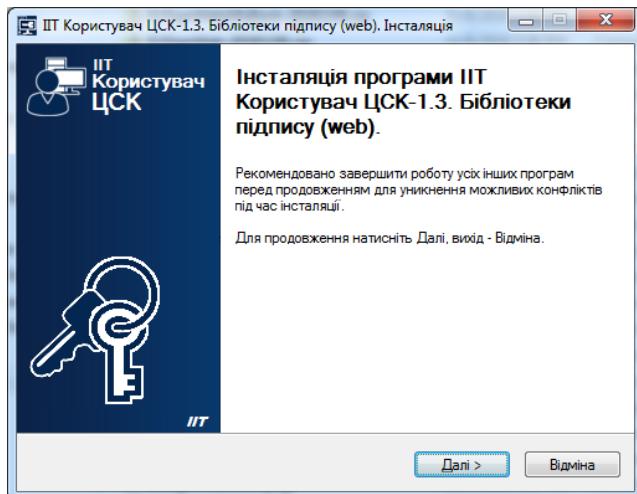


Рисунок 3.1

На наступній сторінці майстра (рис. 3.2) необхідно ознайомитись з ліцензійною угодою щодо використання програми та погодитись. Для продовження інсталяції необхідно встановити позначку “Я приймаю цю угоду” та натиснути кнопку “Далі”.

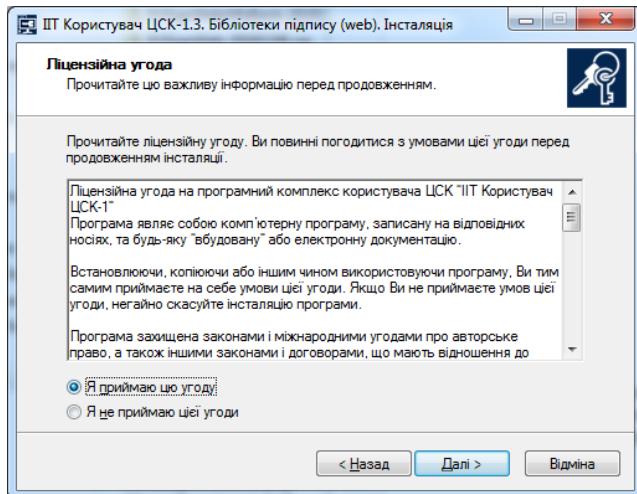


Рисунок 3.2

На наступній сторінці майстра (рис. 3.3) за необхідністю можна вказати каталог на диск до якого буде встановлено програму. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

Пор. № зміни	Підпис відпов. особи	Дата внесення

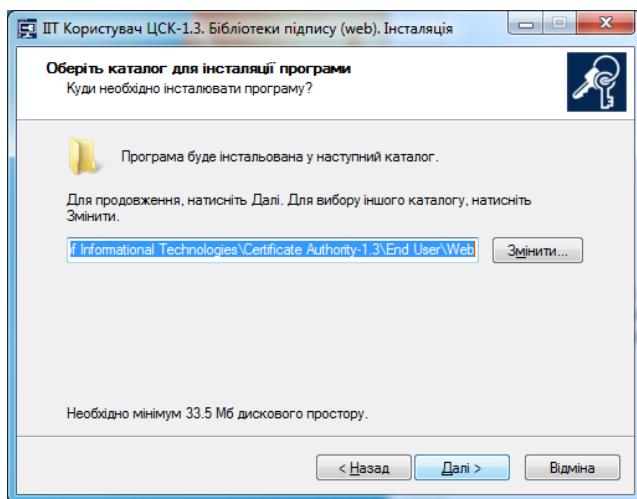


Рисунок 3.3

На наступній сторінці майстра (рис. 3.4) за необхідністю можна вказати розділ меню “Пуск” до якого буде встановлено значки запуску та дейнсталяції програми. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

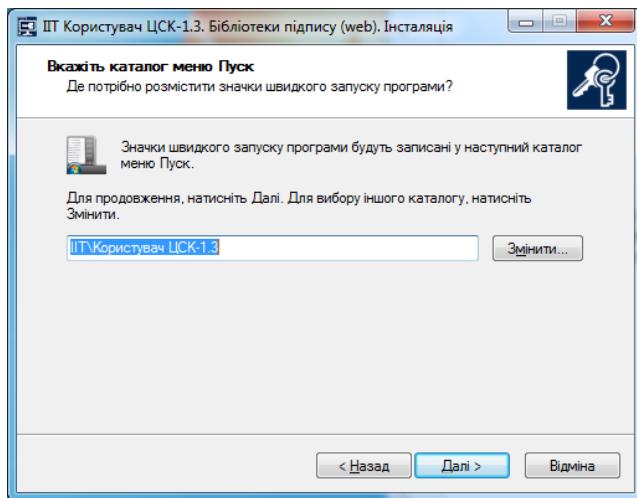


Рисунок 3.4

На наступній сторінці майстра (рис. 3.5) потрібно встановити признаки необхідності виконання майстром додаткових завдань – створення значку запуску програми на робочому столі. Для продовження інсталяції необхідно натиснути кнопку “Далі”.

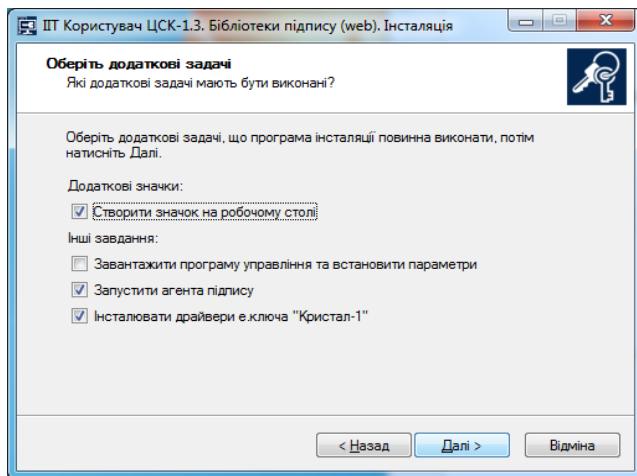


Рисунок 3.5

Після інсталяції програми, майстер завершує свою роботу.

<i>Пор. № зміни</i>	<i>Підпис відпов. особи</i>	<i>Дата внесення</i>

3.2 Інсталяція програми в ОС Apple MAC OS X

Для інсталяції програми необхідно запустити програму інсталяції (майстер інсталяції) EUSignWebInstall.pkg з інсталяційного носія (оптичного диску чи ін.) чи завантажити її з web-сторінки ЦСК.

Після запуску програми інсталяції на першій сторінці (рис. 3.6) виводиться інформація про початок інсталяції. Для продовження інсталяції необхідно натиснути кнопку “Продовжити”, а для завершення - “Відміна”.

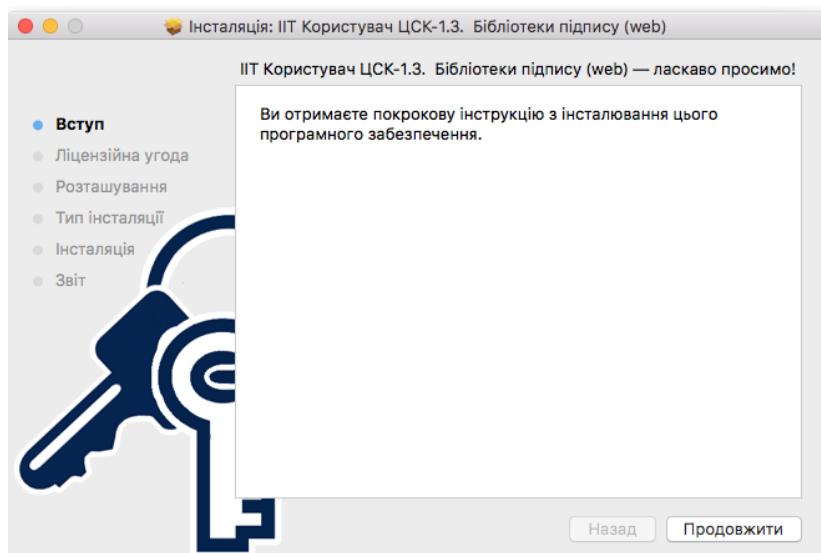


Рисунок 3.6

На наступній сторінці майстра (рис. 3.7) необхідно ознайомитись з ліцензійною угодою щодо використання програми та погодитись. Для продовження інсталяції необхідно натиснути кнопку “Погоджуєсь” та “Продовжити”.

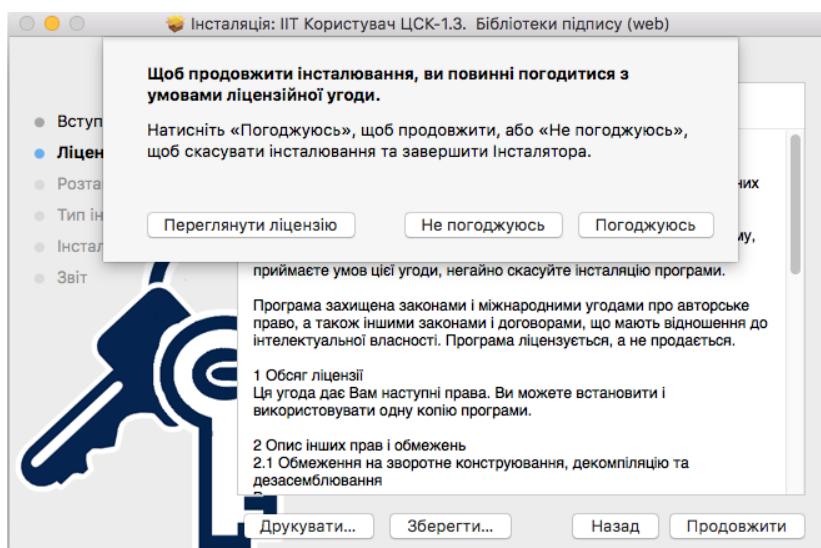


Рисунок 3.7

На наступній сторінці майстра (рис. 3.8) за необхідністю можна вказати каталог на диск, до якого буде встановлено програму. Для продовження інсталяції необхідно натиснути кнопку “Інсталювати”.

Пор. № зміни	Підпис відпов. особи	Дата внесення

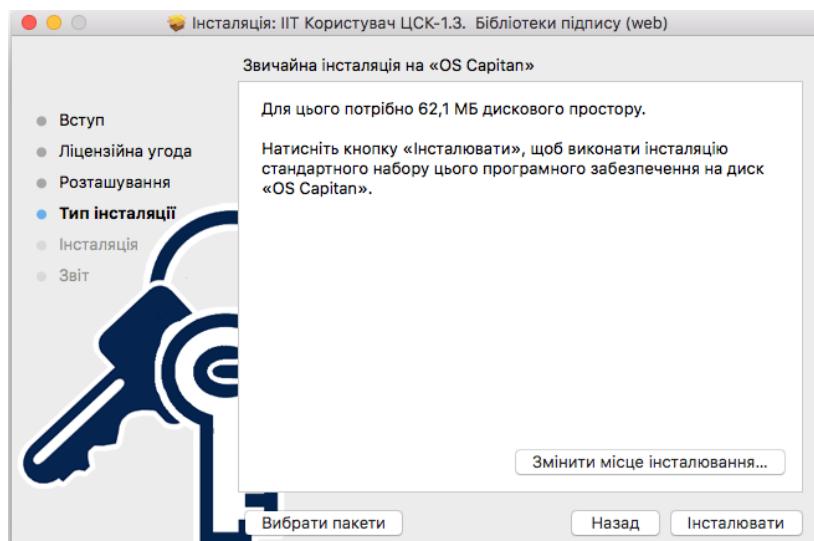


Рисунок 3.8

Після інсталяції програми, майстер завершує свою роботу (Рис. 3.9).

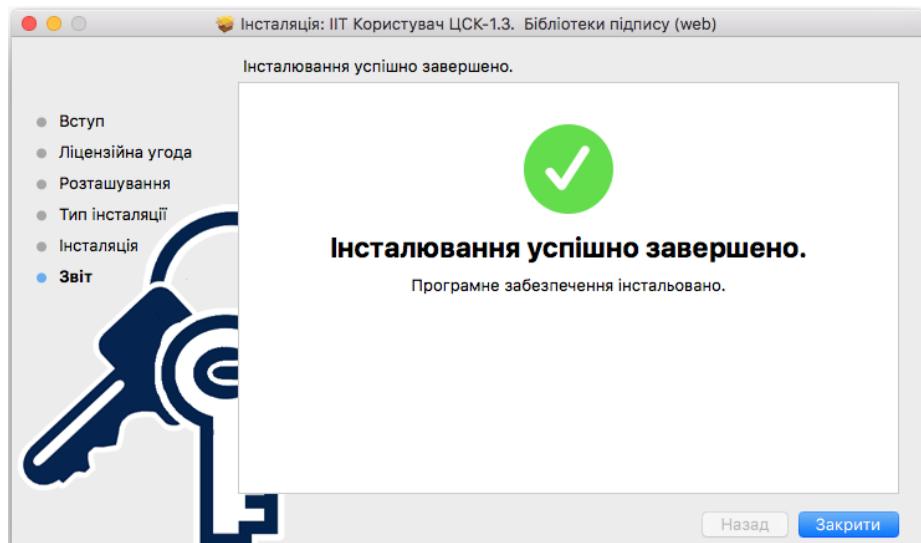


Рисунок 3.9

3.3 Інсталяція програми в ОС Linux Debian/Ubuntu

Для інсталяції програми необхідно запустити програму інсталяції (майстер інсталяції) euswi.deb (euswi.64.deb) з інсталяційного носія (оптичного диску чи ін.) чи завантажити її з web-сторінки ЦСК.

Після запуску інсталяції за допомогою Ubuntu Software Center (рис. 3.10) виводиться інформація про початок інсталяції. Для продовження інсталяції необхідно натиснути кнопку "Install", а для завершення - закрити майстра.

Пор. № зміни	Підпис відпов. особи	Дата внесення

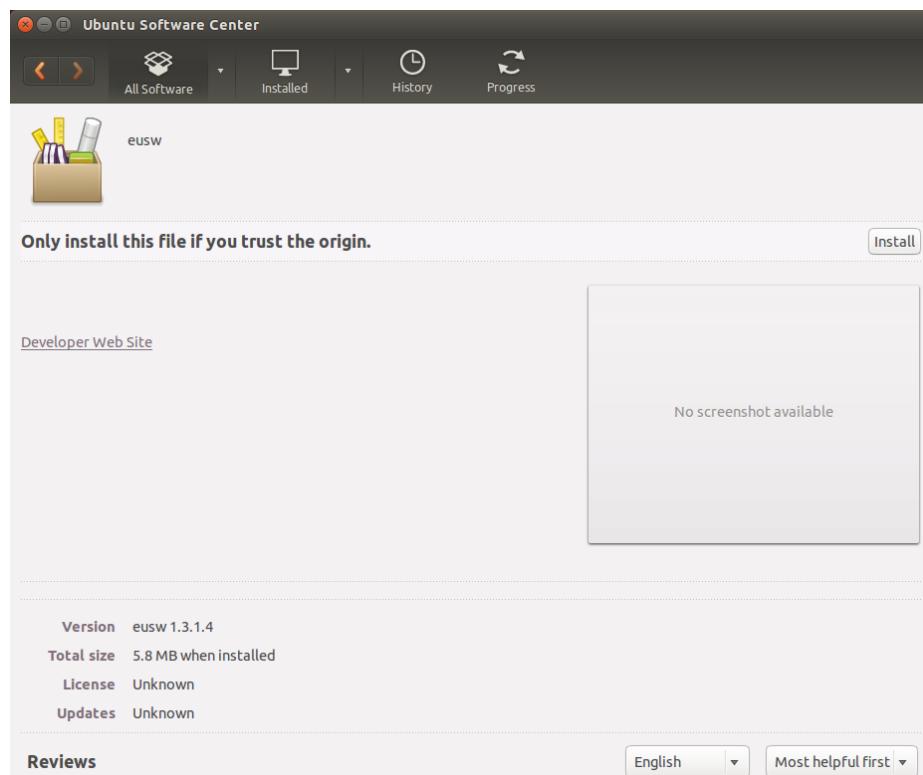


Рисунок 3.10

Після інсталяції програми, майстер завершує свою роботу (Рис.11):

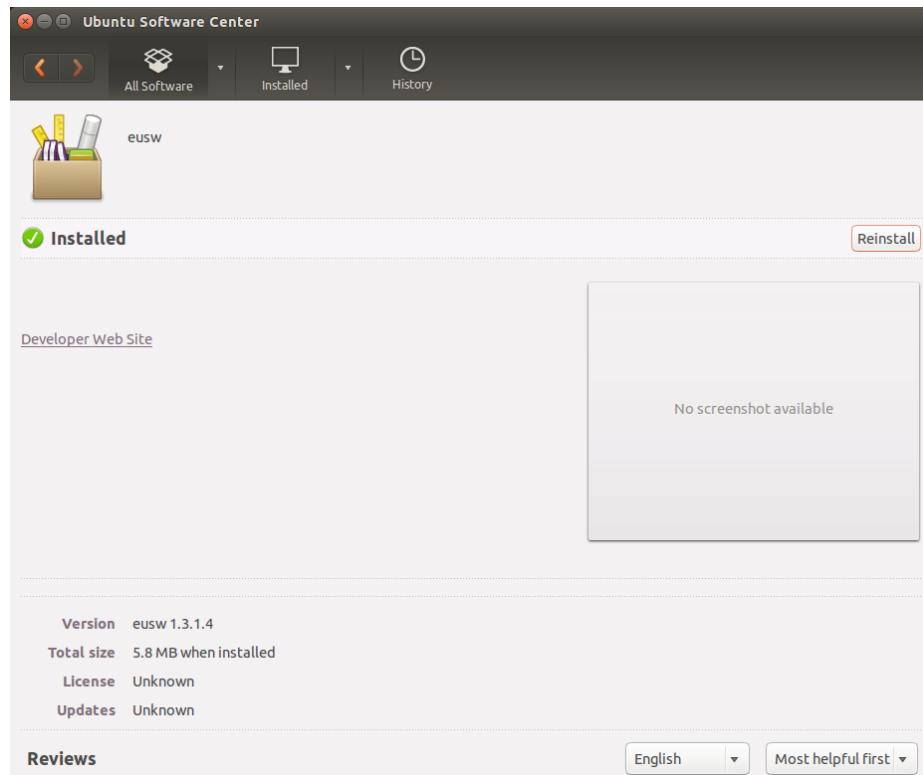


Рисунок 3.11

Також встановлення програми можливо з використанням менеджера пакетів dpkg. Для встановлення програми необхідно відкрити консоль та виконати:

```
dpkg -i eusw.deb
```

Примітка. Для підтримки апаратних НКІ необхідно встановити пакети libpcsc-lite1 та pcscd.

Пор. № зміни	Підпис відпов. особи	Дата внесення

3.4 Інсталяція web-розширеннь

Для роботи криптографічних бібліотек в ОС де не підтримується Агент підпису додатково необхідно встановити web-розширення з магазину web-розширень розробника браузерів.

3.4.1 Інсталяція web-розширення для браузера Google Chrome

Для інсталяції web-розширення необхідно перейти за посиланням https://chrome.google.com/webstore/detail/%D1%96%D1%96%D1%82-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87-%D1%86%D1%81%D0%BA-1-%D0%B1%D1%96%D0%B1%D0%BB/jffafkigfgmjafhpkoibhfefeaebmccg?hl=uk_UA та натиснути Додати в Chrome (рис. 3.12).

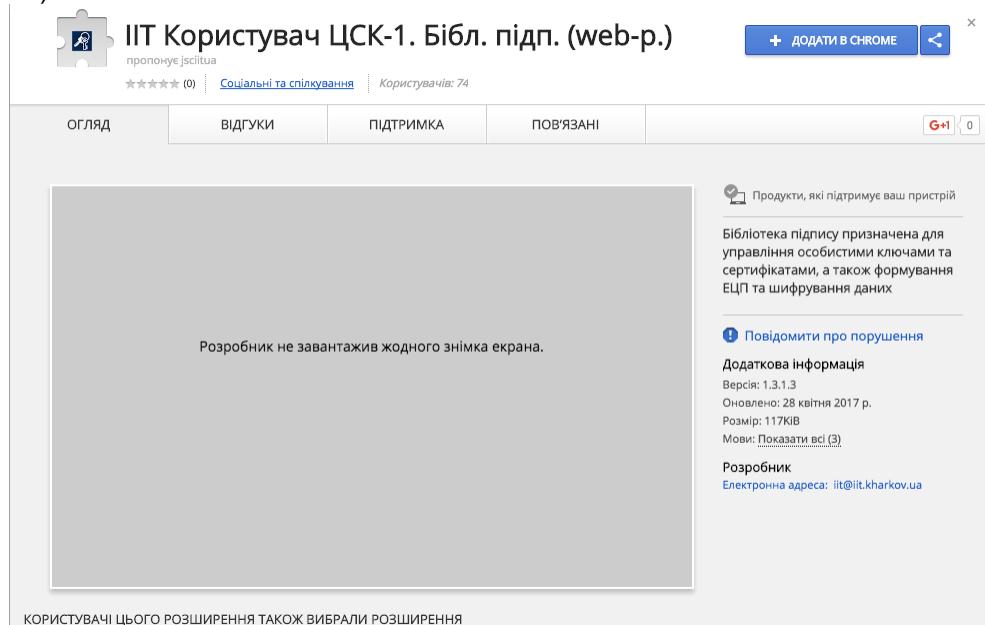


Рисунок 3.12

Після успішної інсталяції напис Додати в Chrome зміниться на Додано в Chrome (рис. 3.13).

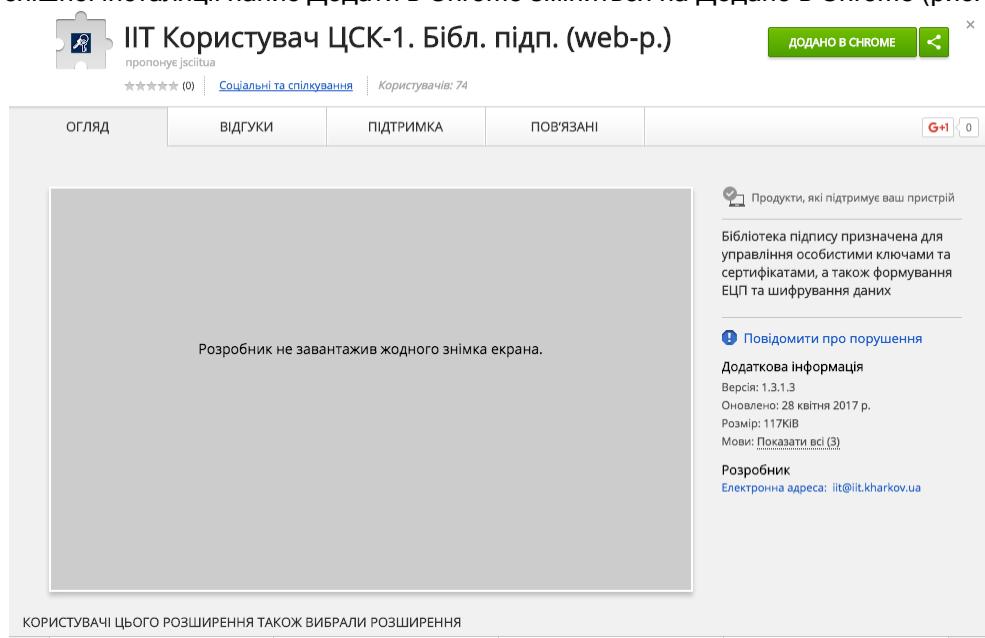


Рисунок 3.13

Примітка. У разі виникнення помилок при встановленні веб-розширення «Download interrupted», «Помилка мережі», необхідно з файлу C:\\Windows\\system32\\drivers\\etc\\hosts видалити:
127.0.0.1 clients2.google.com

Пор. № зміни	Підпись відпов. особи	Дата внесення

14
СААД.21118-13 34 02-1

Інсталяване web-розширення буде відображатися в списку розширень (рис. 3.14)

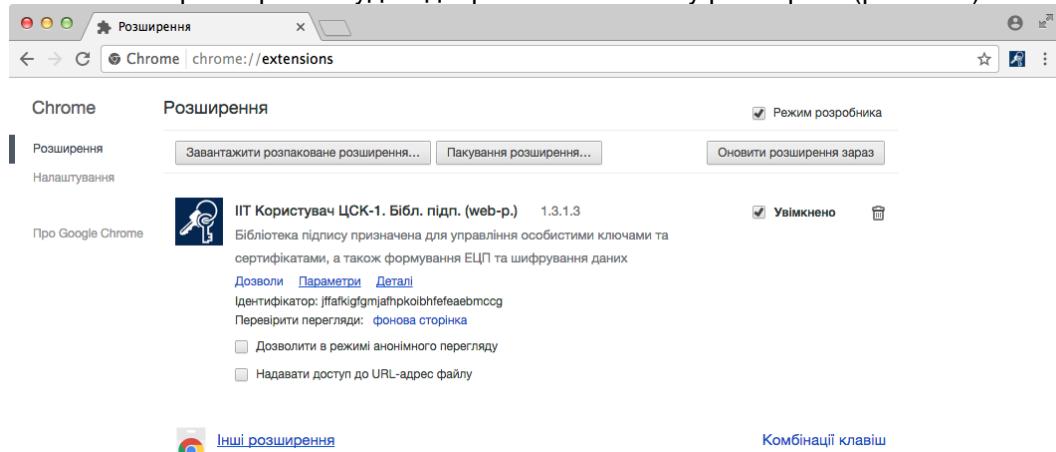


Рисунок 3.14

3.4.2 Інсталяція web-розширення для браузера Opera

Для інсталяції web-розширення необхідно перейти за посиланням <https://addons.opera.com/uk/extensions/details/iit-end-user-ca-1-sign-web-extension/?display=uk> та натиснути Додати до Opera (рис. 3.15).

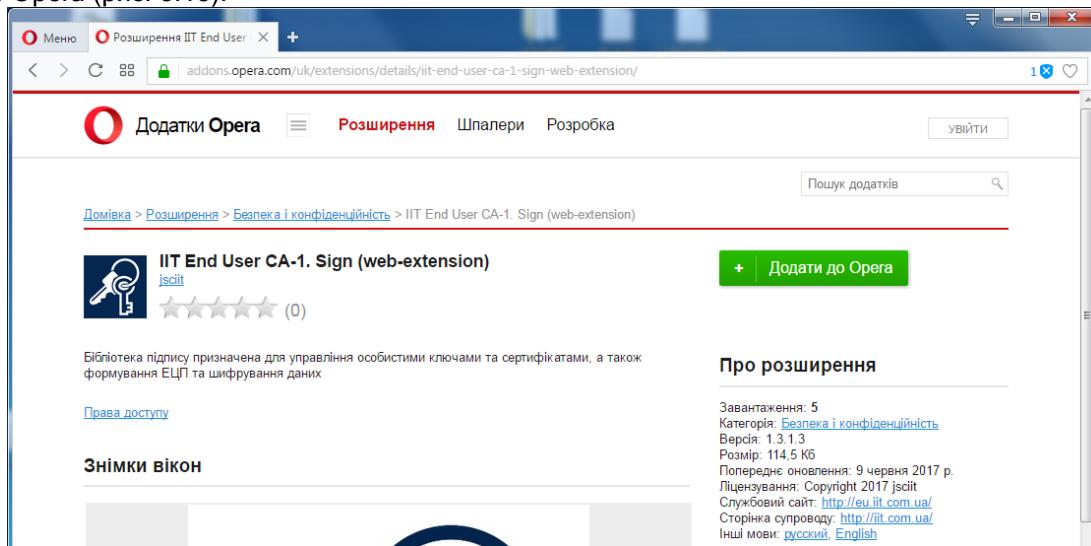


Рисунок 3.15

Після успішної інсталяції напис Додати до Opera зміниться на Встановлено (рис. 3.16).

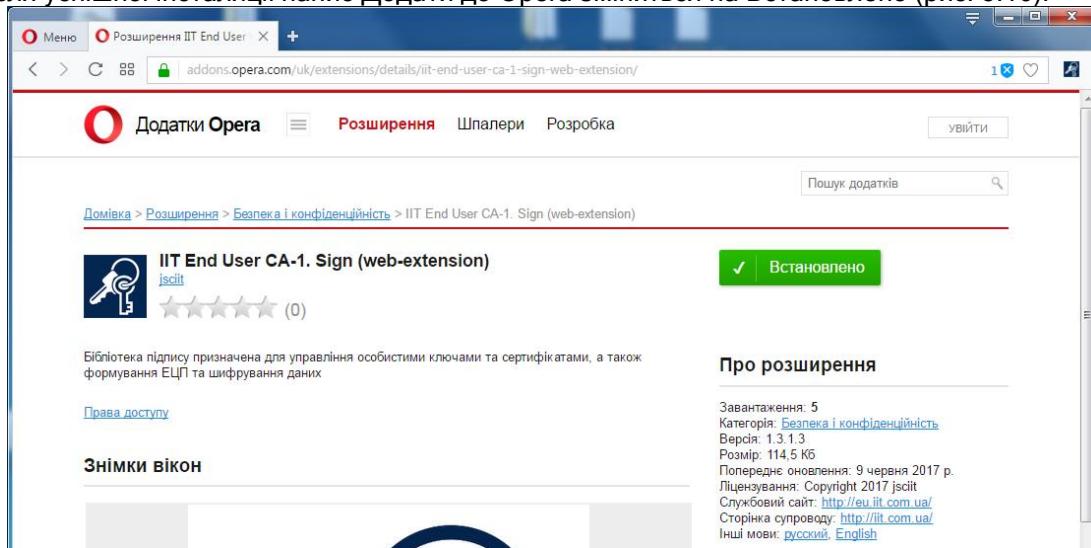


Рисунок 3.16

Пор. № зміни	Підпись відпов. особи	Дата внесення

Інстальоване web-розширення буде відображатися в списку розширень (рис. 3.17)

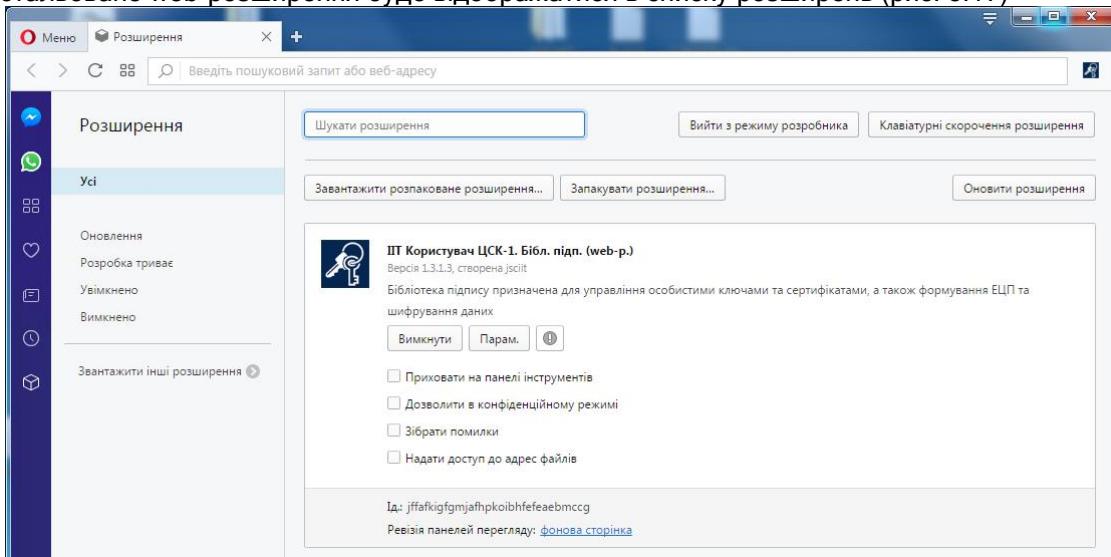


Рисунок 3.17

3.4.3 Інсталяція web-розширення для браузера Mozilla Firefox

Для інсталяції web-розширення необхідно перейти за посиланням <https://eu.iit.com.ua/download/productfiles/eusw@iit.com.ua.xpi> та натиснути Встановити (рис. 3.18).

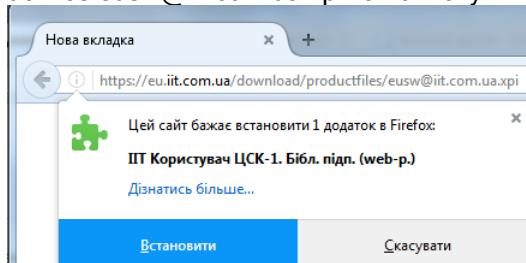


Рисунок 3.18

Після успішної інсталяції необхідно натиснути "OK" (рис. 3.19).

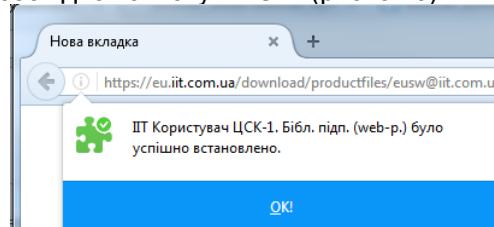


Рисунок 3.19

Інстальоване web-розширення буде відображатися в списку розширень (рис. 3.20)

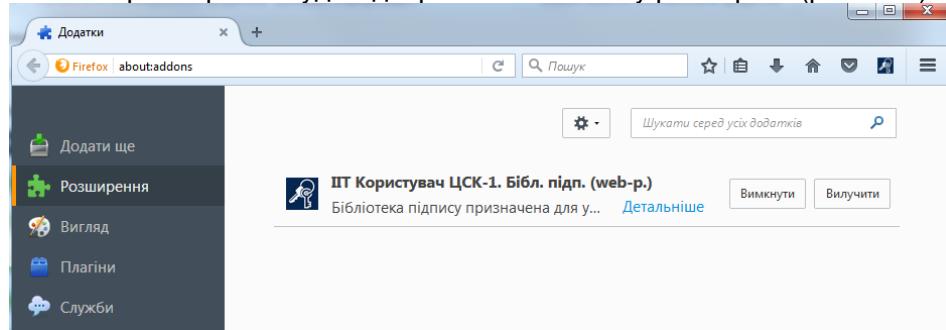


Рисунок 3.20

Пор. № зміни	Підпис відпов. особи	Дата внесення

4 ПОЧАТОК РОБОТИ З ПРОГРАМОЮ

4.1 Агент підпису для ОС Microsoft Windows

4.1.1 Завантаження програми

Для початку роботи програми у каталозі із сертифікатами та СВС обов'язково повинні бути записані:

- сертифікат ЦСК;
- сертифікати серверів ЦСК (за необхідністю);
- діючі СВС (за необхідністю).

Якщо сертифікати ЦСК, серверів ЦСК та СВС відсутні у інсталяційному пакеті, то необхідно завантажити їх з web-сторінки ЦСК чи записати їх у відповідний каталог, отримавши іншими засобами з ЦСК.

Для управління агентом підпису необхідно запустити модуль, що виконується EUSAManager.exe через файловий менеджер ОС або через меню “Пуск”, обравши у розділі “ІІТ\Користувач ЦСК-1” підпункт “ІІТ Користувач ЦСК-1.3. Агент підпису” чи за допомогою значку на робочому столі. Після запуску на екрані буде відображене головне вікно програми, що наведене на рис. 4.1.

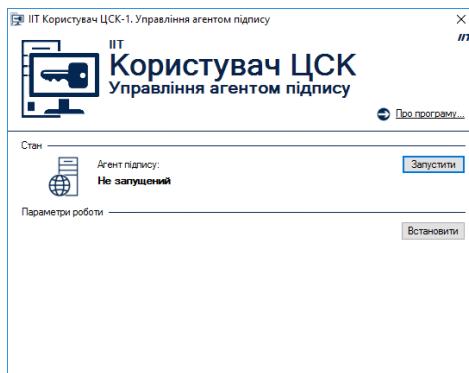


Рисунок 4.1

Запуск/зупинка агенту підпису (окремого процесу) відбувається за допомогою кнопки “Запустити”/“Зупинити”.

4.1.2 Встановлення параметрів роботи програми

При відсутності в реєстрі параметрів роботи програми, вони встановлюються за замовчанням. При цьому встановлюються лише параметри запуску та генерується SSL-сертифікат для роботи з web-сайтами, що використовують HTTP(S) з'єднання. При першому запуску агент підпису автоматично імпортує сертифікати до сховища браузера Mozilla Firefox та сховища сертифікатів ОС Windows.

Для встановлення чи зміни параметрів роботи програми необхідно перед запуском агенту натиснути “Встановити” в пункті меню “Параметри” (рис. 4.1). Вікно встановлення параметрів наведене на рис. 4.2.

Пор. № зміни	Підпис відпов. особи	Дата внесення

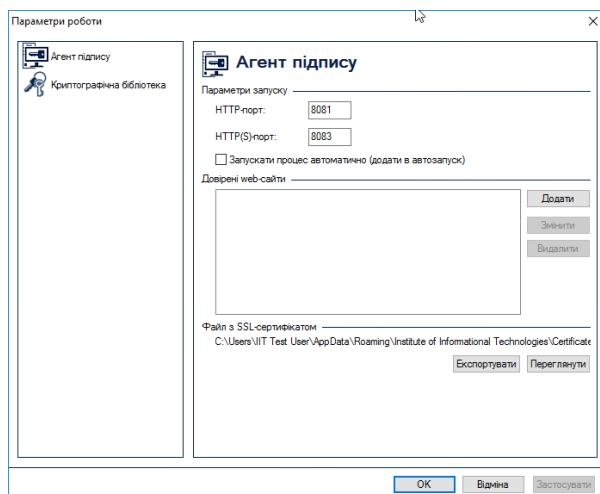


Рисунок 4.2

4.1.2.1 Агент підпису

Для налаштування параметрів агента підпису необхідно перейти до закладки “Агент підпису”. Вікно “Параметри роботи” із сторінкою “Агент підпису” наведене на рис. 4.2. На цій сторінці встановлюються наступні параметри роботи програми:

- “HTTP-порт”. Даний параметр встановлює HTTP-порт агенту підпису, який використовується для доступу до функцій програми з web-браузера.
В брандмауері операційної системи повинно бути дозволено підключення до цього порту.
- “HTTP(S)-порт”. Даний параметр встановлює HTTP(S)-порт агенту підпису, який використовується для доступу до функцій програми з web-браузера.
В брандмауері операційної системи повинно бути дозволено підключення до цього порту.
- “Запускати процес автоматично (додати в автозапуск)”. Даний параметр визначає необхідність автоматичного запуску програми при старті системи.
- “Довірені web-сайти”. Даний параметр визначає перелік web-сайтів, яким дозволено доступ до функцій програми.

Для додавання довіреного web-сайту необхідно натиснути “Додати”. У вікні встановлення налаштувань довіреного web-сайту (рис. 4.3) необхідно вказати URL-адресу web-сайту. Для збереження введених налаштувань необхідно натиснути “ОК”.

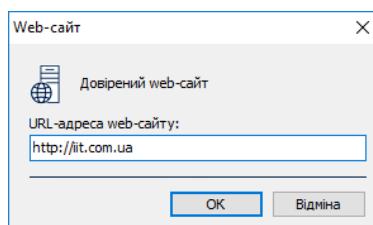


Рисунок 4.3

При зверненні web-сайту, адреса якого не внесена до списку довірених web-сайтів, буде запропоновано його додати (рис. 4.4)

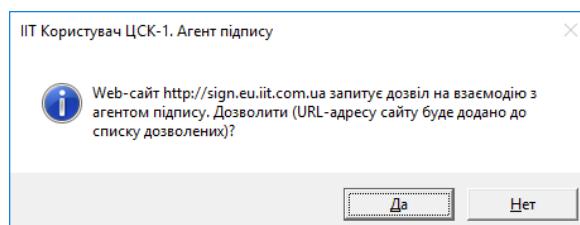


Рисунок 4.4

Пор. № зміни	Підпис відпов. особи	Дата внесення

Для перегляду та експорту SSL-сертифікату агенту підпису необхідно натиснути “Переглянути” та “Експортувати”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

Примітка. Якщо в браузері встановлено використання proxy-серверу необхідно в налаштування proxy-серверу для браузера додати адресу localhost до списку адрес, що не використовують proxy-сервер. Також при використанні веб-розширень або програм, що блокують рекламу (наприклад AdBlock) необхідно внести в виключення сайт, який використовує агент підпису.

Для браузерів Microsoft IE та Edge, якщо веб-сайт знаходиться у внутрішній мережі або додано до списку довірених веб-сайтів необхідно в налаштуваннях безпеки для зон “Місцева інtramежера” (Local intranet) та/або “Надійні веб-сайти” (Trusted sites) в налаштуваннях рівня безпеки для зон встановити параметр “Доступ до джерел даних за межами домену в значення” (Access data sources across domains) в значення “Пропонувати” (Promt).

4.1.2.2 Криптографічна бібліотека

Для встановлення параметрів криптографічної бібліотеки необхідно перейти до розділу “Криптографічна бібліотека” у вікні параметрів (рис. 4.5).

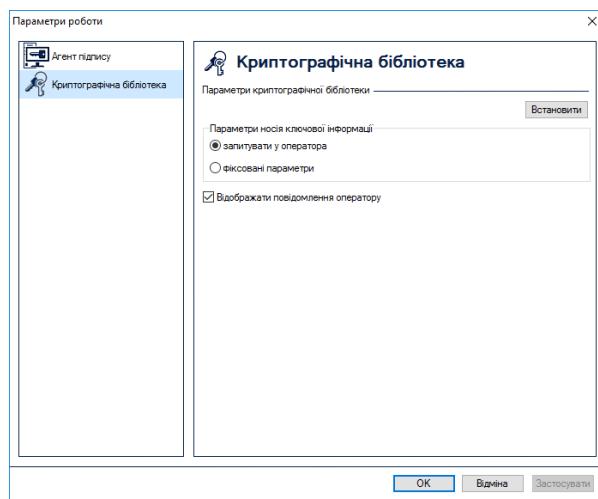


Рисунок 4.5

Вікно встановлення параметрів криптографічної бібліотеки має вигляд (рис. 4.6):

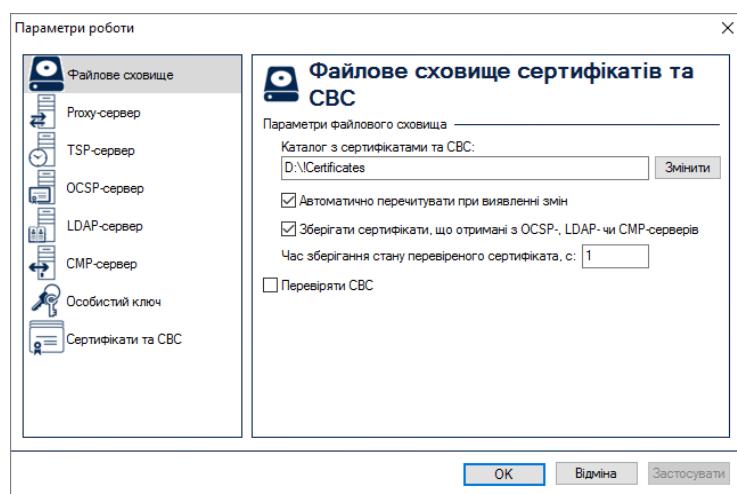


Рисунок 4.6

Детально встановлення параметрів криптографічної бібліотеки наведено в додатку А.

Для використання функцій підпису та шифрування необхідно зчитати особистий ключ користувача. Ключ може зчитуватись у автоматичному режимі або у діалоговому (ручному).

У вікні параметрів вказується спосіб зчитування особистого ключа:

Пор. № зміни	Підпис відпов. особи	Дата внесення

- запитувати у оператора (рис 4.5) (під час кожної необхідності використання особистого ключа, наприклад під час підпису відображається діалогове вікно зчитування особистого ключа (рис. А.23), у якому необхідно вказати тип носія ключової інформації та пароль);
- фіксовані параметри (якщо параметр встановлено, вікно (рис 4.5) прийме вигляд як наведено на рис. 4.7. У такому режимі параметри зчитування ключа встановлюються один раз та зберігаються у програмі, всі наступні зчитування особистого ключа відбуваються без запиту до оператора. Для встановлення параметрів доступу до НКІ необхідно у вікні (рис. 4.7) натиснути “Встановити”, та вказати тип ключового носія та пароль у діалоговому вікні що буде виведене (рис. А.23)).

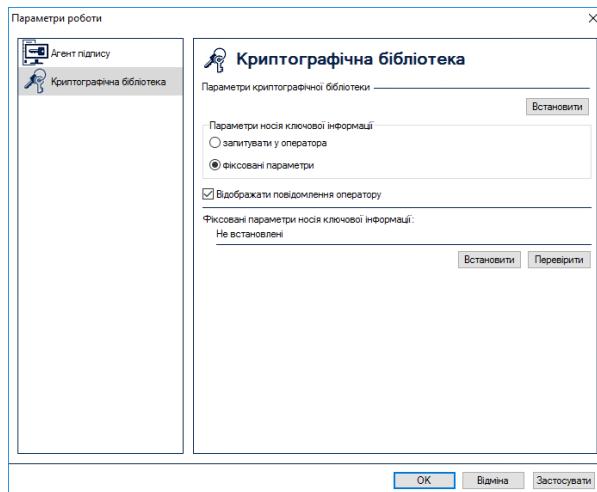


Рисунок 4.7

Для відображення графічних повідомлень криптографічної бібліотеки користувачу необхідно встановити параметр “Відображати повідомлення оператору”.

4.2 Агент підпису для ОС Apple MAC OS X

4.2.1 Завантаження програми

Для початку роботи програми у каталозі із сертифікатами та СВС обов’язково повинні бути записані:

- сертифікат ЦСК;
- сертифікати серверів ЦСК (за необхідністю);
- діючі СВС (за необхідністю).

Якщо сертифікати ЦСК, серверів ЦСК та СВС відсутні у інсталяційному пакеті, то необхідно завантажити їх з web-сторінки ЦСК чи записати їх у відповідний каталог, отримавши іншими засобами з ЦСК.

Для управління агентом підпису необхідно запустити модуль, що виконується EUSAManager через файловий менеджер ОС або через меню додатків, обравши ІІТ Користувач ЦСК-1.3. Управління агентом підпису. Після запуску на екрані буде відображене головне вікно програми, що наведене на рис. 4.8.

Пор. № зміни	Підпис відпов. особи	Дата внесення

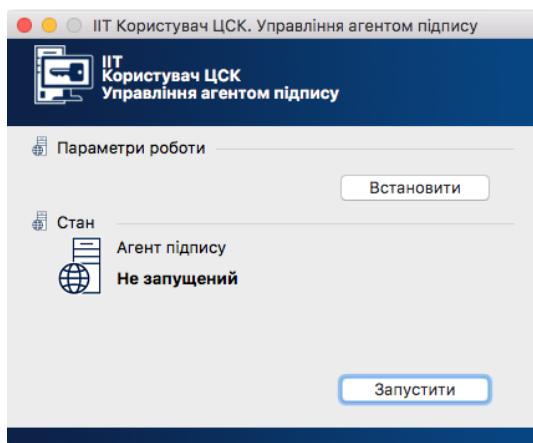


Рисунок 4.8

Запуск/зупинка агента підпису відбувається за допомогою кнопки “Запустити”/“Зупинити”.

4.2.2 Встановлення параметрів роботи програми

При відсутності параметрів роботи програми, вони встановлюються за замовчанням. При цьому встановлюються лише параметри запуску та генерується SSL-сертифікат для роботи з web-сайтами, що використовують HTTP(S) з’єднання. При першому запуску агент підпису автоматично імпортує сертифікати до сховища браузера Mozilla Firefox та сховища сертифікатів ОС Apple MAC OS X.

Для встановлення чи зміни параметрів роботи програми необхідно перед запуском агента натиснути “Встановити” в пункті меню “Параметри” (рис. 4.8). Вікно встановлення параметрів наведене на рис. 4.9.

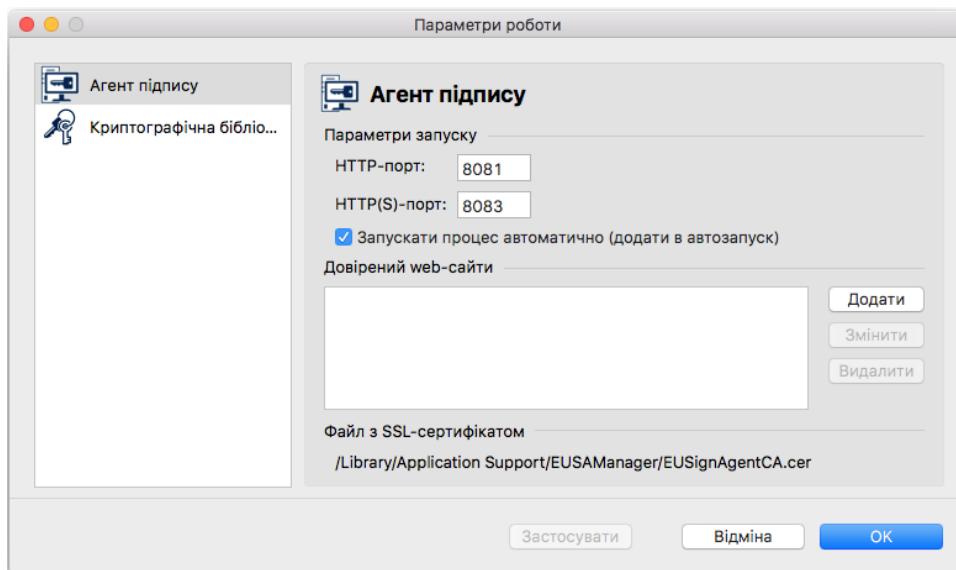


Рисунок 4.9

4.2.2.1 Агент підпису

Для налаштування параметрів агента підпису необхідно перейти до закладки “Агент підпису”. Вікно “Параметри роботи” із сторінкою “Агент підпису” наведене на рис. 4.9. На цій сторінці встановлюються наступні параметри роботи програми:

- “HTTP-порт”. Даний параметр встановлює HTTP-порт агента підпису, який використовується для доступу до функцій програми з web-браузера.
В брандмауері операційної системи повинно бути дозволено підключення до цього порту.
- “HTTP(S)-порт”. Даний параметр встановлює HTTP(S)-порт агенту підпису, який використовується для доступу до функцій програми з web-браузера.

Пор. № зміни	Підпис відпов. особи	Дата внесення

В брандмауері операційної системи повинно бути дозволено підключення до цього порту.

- “Запускати процес автоматично (додати в автозапуск)”. Даний параметр визначає необхідність автоматичного запуску програми при старті системи.
- “Довірені web-сайти”. Даний параметр визначає перелік web-сайтів, яким дозволено доступ до функцій програми.

Для додавання довіреного web-сайту необхідно натиснути “Додати”. У вікні встановлення налаштувань довіреного web-сайту (рис. 4.10) необхідно вказати URL-адресу web-сайту. Для збереження введених налаштувань необхідно натиснути “ОК”.

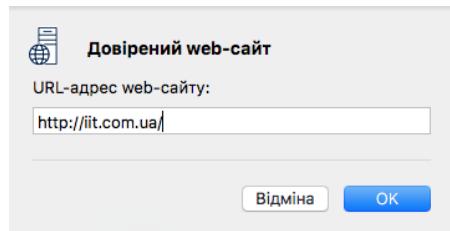


Рисунок 4.10

При зверненні web-сайту, адреса якого не внесена до списку довірених web-сайтів, буде запропоновано його додати (рис. 4.11)

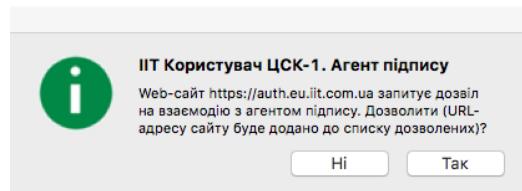


Рисунок 4.11

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

Примітка. Якщо в браузері встановлено використання proxy-серверу необхідно в налаштування proxy-серверу для браузера додати адресу localhost до списку адрес, що не використовують proxy-сервер. Також при використанні веб-розширень або програм, що блокують рекламу (наприклад AdBlock) необхідно внести в виключення сайт, який використовує агент підпису.

4.2.2.2 Криптографічна бібліотека

Для встановлення параметрів криптографічної бібліотеки необхідно перейти до розділу “Криптографічна бібліотека” у вікні параметрів (рис. 4.12).

Пор. № зміни	Підпись відпов. особи	Дата внесення

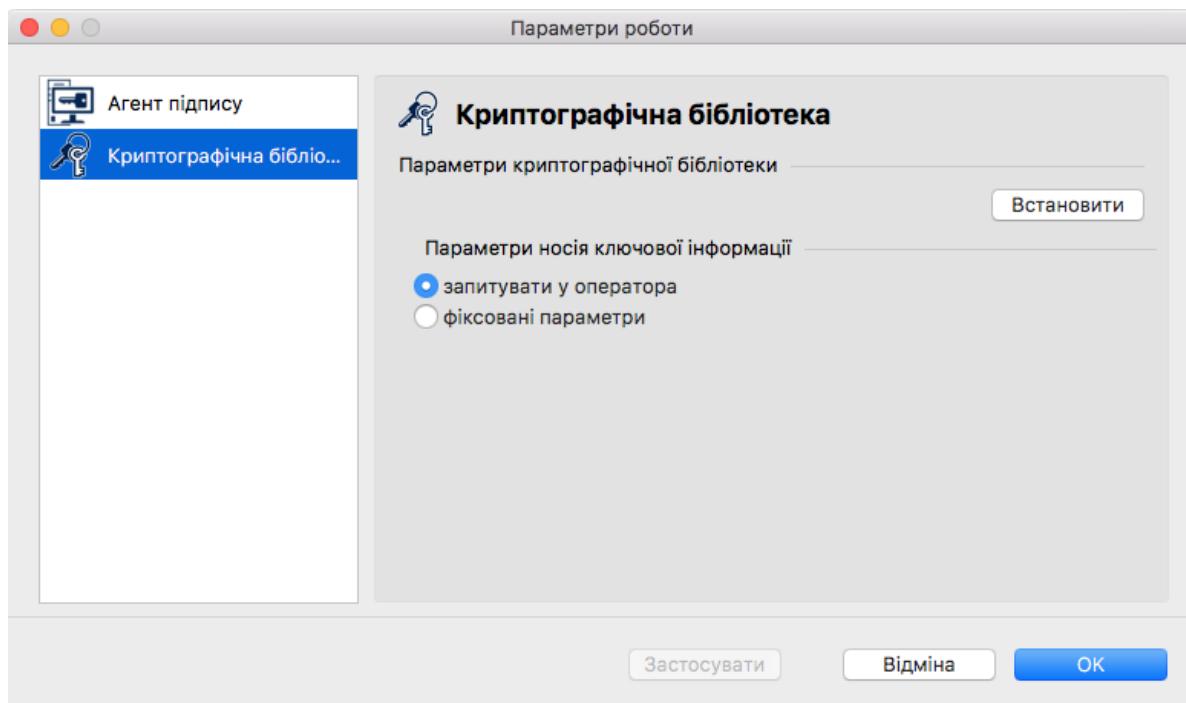


Рисунок 4.12

Вікно встановлення параметрів криптографічної бібліотеки має вигляд (рис. 4.13):

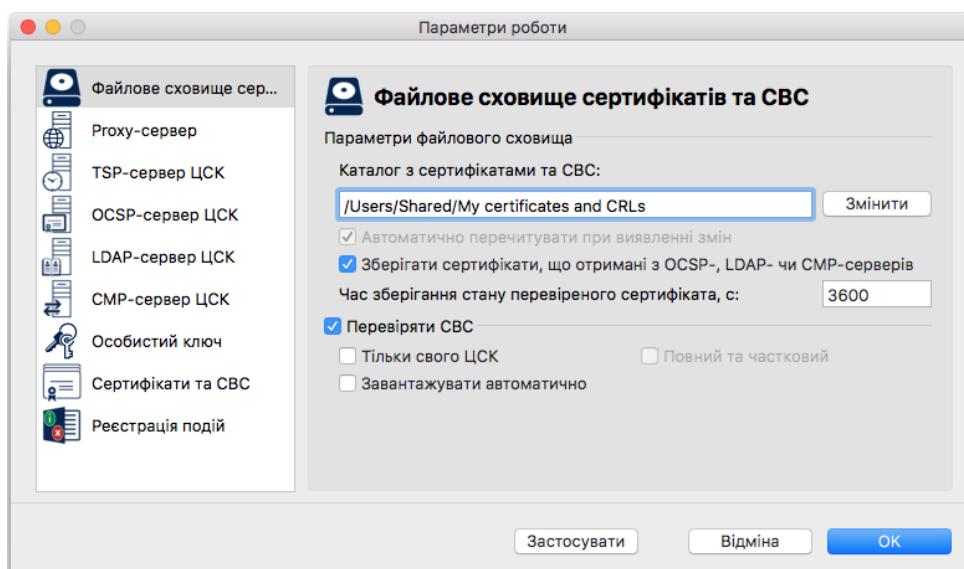


Рисунок 4.13

Детально встановлення параметрів криптографічної бібліотеки наведено в додатку Б.

Для використання функцій підпису та шифрування необхідно зчитати особистий ключ користувача. Ключ може зчитуватись у автоматичному режимі або у діалоговому (ручному).

У вікні параметрів вказується спосіб зчитування особистого ключа:

- запитувати у оператора (рис 4.12) (під час кожної необхідності використання особистого ключа, наприклад під час підпису відображається діалогове вікно зчитування особистого ключа (рис. А.23), у якому необхідно вказати тип носія ключової інформації та пароль);
- фіксовані параметри (якщо параметр встановлено, вікно (рис 4.12) прийме вигляд як наведено на рис. 4.14. У такому режимі параметри зчитування ключа встановлюються один раз та зберігаються у програмі, всі наступні зчитування особистого ключа відбуваються без запиту до оператора. Для встановлення параметрів доступу до НКІ необхідно у вікні (рис. 4.14) натиснути

Пор. № зміни	Підпис відпов. особи	Дата внесення

“Встановити”, та вказати тип ключового носія та пароль у діалоговому вікні що буде виведене (рис. Б.23)).

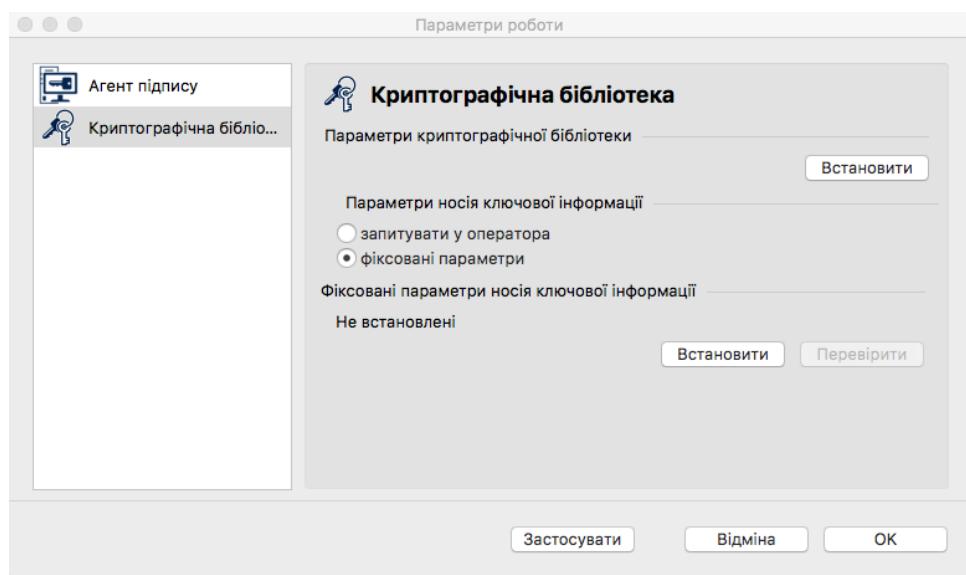


Рисунок 4.14

4.3 Web-розширення для web-браузера (Google Chrome, Opera, Mozilla Firefox)

4.3.1 Завантаження програми

Завантаження web-розширення виконується браузером автоматично при запуску, при цьому в меню браузера відображається значок в верхньому правому кутку рис. 3.14 (Google Chrome), рис. 3.17 (Opera), рис 3.20 (Mozilla Firefox).

4.3.2 Встановлення параметрів роботи програми

При відсутності параметрів роботи програми, вони встановлюються за замовчанням.

Для налаштування параметрів web-розширення необхідно перейти до закладки “Розширення” браузера та натиснути “Параметри” (рис. 3.14). Вікно “Параметри роботи” наведене на рис. 4.15. На цій сторінці встановлюються наступні параметри роботи web-розширення:

- “Довірені web-сайти”. Даний параметр визначає перелік web-сайтів, яким дозволено доступ до функцій web-розширення.

Для додавання довіреного web-сайту необхідно натиснути “Додати”. У вікні встановлення налаштувань довіреного web-сайту (рис. 4.15) необхідно вказати URL-адресу web-сайту. Для збереження введених налаштувань необхідно натиснути “Зберегти”.

Пор. № зміни	Підпись відпов. особи	Дата внесення

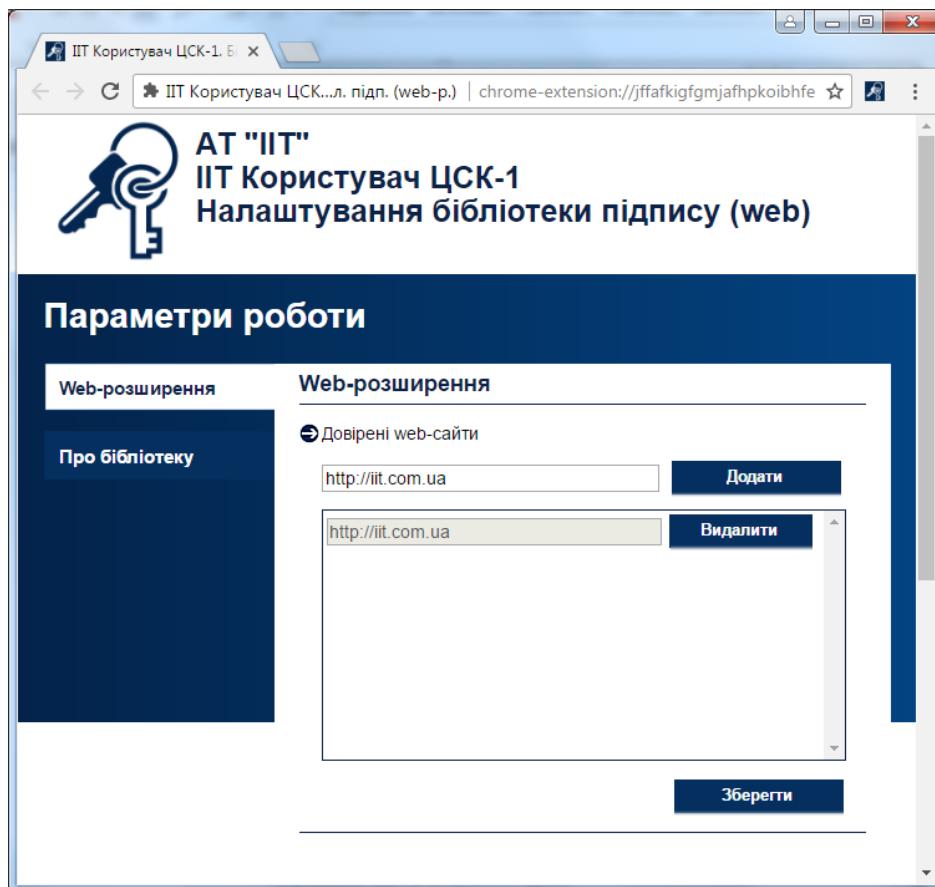


Рисунок 4.15

При зверненні web-сайту, адреса якого не внесена до списку довірених web-сайтів, буде запропоновано його додати (рис. 4.16)

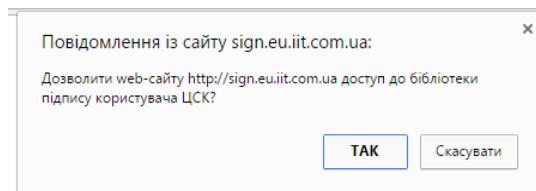


Рисунок 4.16

Для перегляду інформації про встановлене web-розширення необхідно натиснути "Про бібліотеку" у вікні "Параметри роботи" (рис. 4.15). Інформація про встановлене web-розширення має наступний вигляд (рис. 4.17):

Пор. № зміни	Підпис відпов. особи	Дата внесення

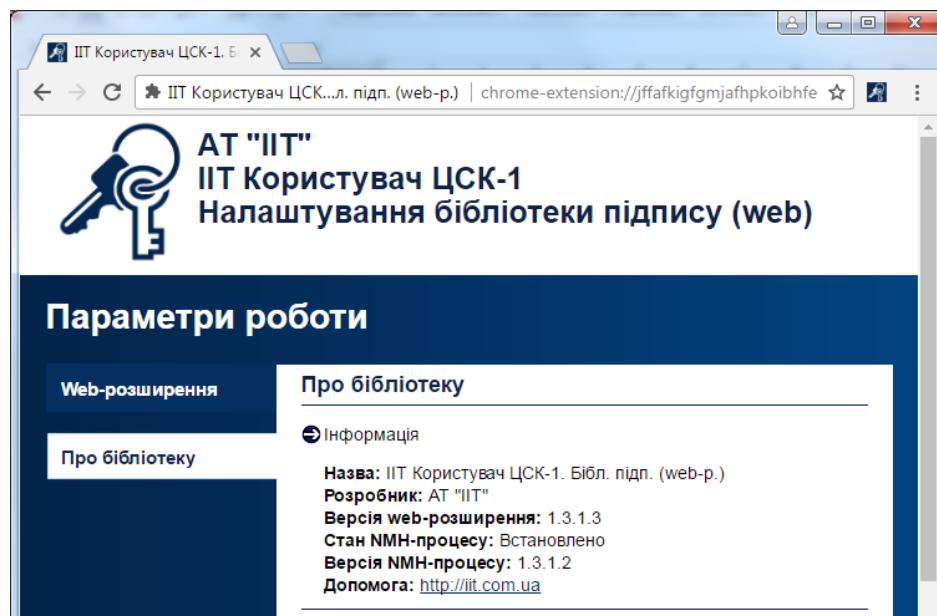


Рисунок 4.17

4.4 NPAPI-плагін для web-браузера Mozilla Firefox

4.4.1 Завантаження програми

Завантаження web-плагіну виконується браузером автоматично при запиті web-сторінки за дозволом користувача (рис. 4.18-4.19).

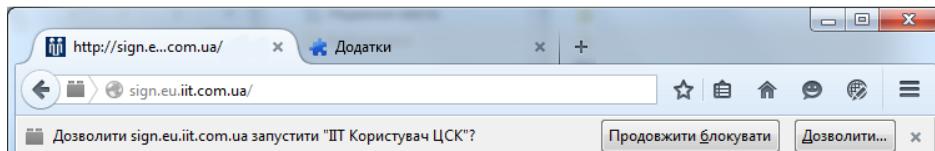


Рисунок 4.18

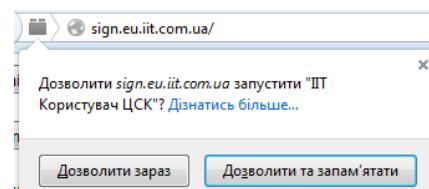


Рисунок 4.19

4.4.2 Встановлення параметрів роботи програми

При відсутності параметрів роботи програми, вони встановлюються за замовчанням.

Для налаштування параметрів web-плагіну необхідно перейти до закладки “Додатки” браузера та натиснути “Плагіни” (рис. 4.20). Вікно “Параметри роботи” наведене на рис. 4.20. На цій сторінці можна встановити параметри запуску web-плагіну.

Пор. № зміни	Підпис відпов. особи	Дата внесення

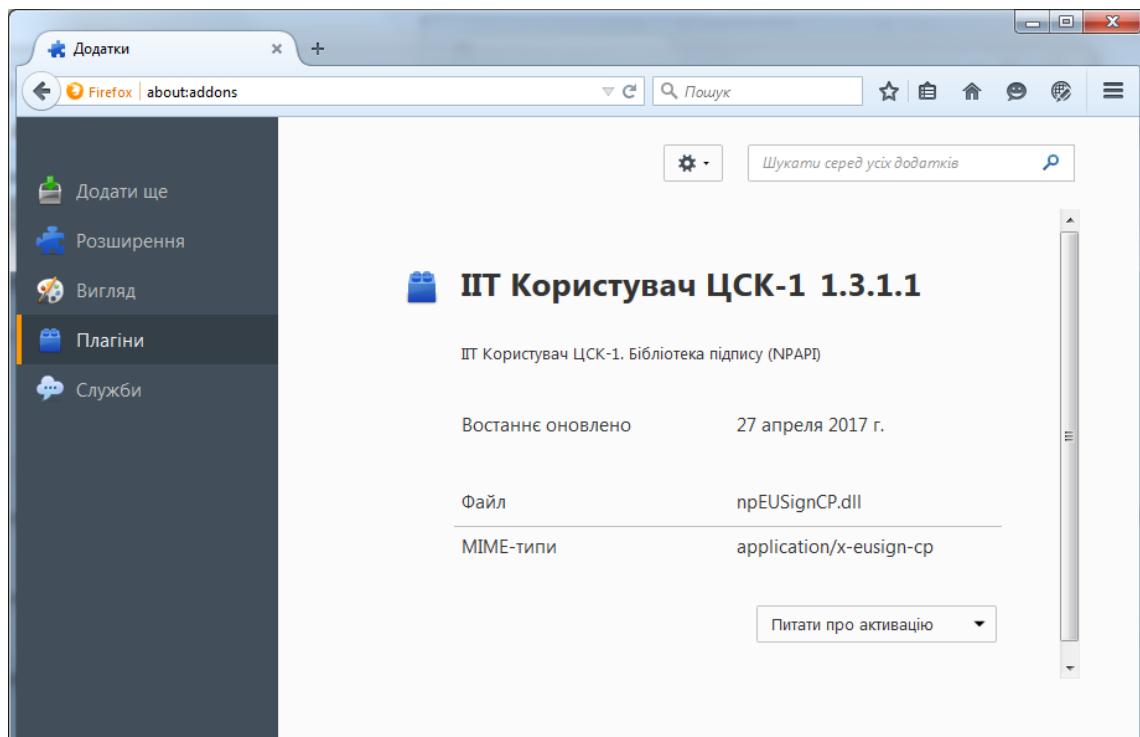


Рисунок 4.20

4.5 ActiveX-компонент для web-браузера Internet Explorer

4.5.1 Завантаження програми

Завантаження Active-X компонента виконується браузером автоматично при запиті web-сторінки за дозволом користувача (рис. 4.21).

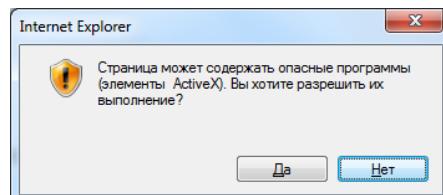


Рисунок 4.21

Для роботи веб-сайту з ActiveX-компонентом необхідно в налаштуваннях безпеки для зони “Надійні сайти” (“Властивості браузера” -> “Безпека” ->“Надійні сайти”, рис. 4.22), дозволити “Використання елементів управління ActiveX, що не помічені як безпечні для використання” (“Властивості браузера” -> “Безпека” ->“Надійні сайти” -> “Інший...”, рис. 4.23), а також додати веб-сайт до переліку надійних веб-сайтів (“Властивості браузера” -> “Безпека” ->“Надійні сайти” -> “Сайти”, рис. 4.24).

Якщо веб-сайт належить до зони "Місцева інtramережа" в налаштуваннях безпеки для цієї зони необхідно дозволити “Використання елементів управління ActiveX, що не помічені як безпечні для використання”.

Пор. № зміни	Підпис відпов. особи	Дата внесення

27
СААД.21118-13 34 02-1

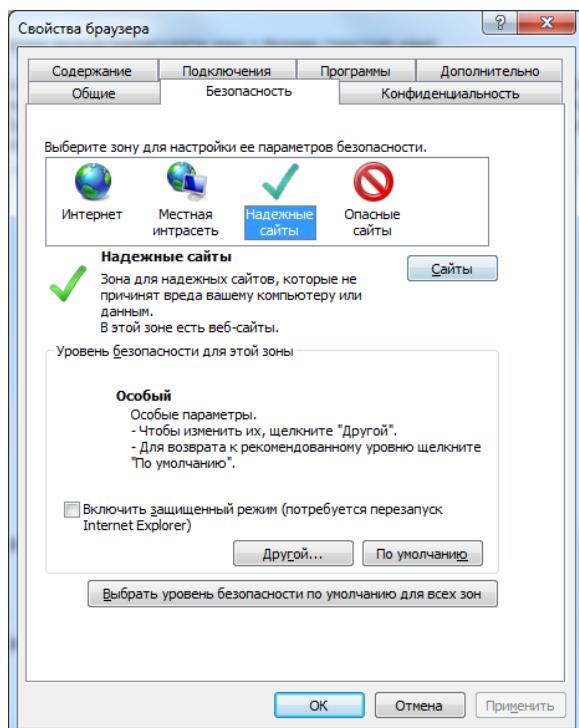


Рисунок 4.22

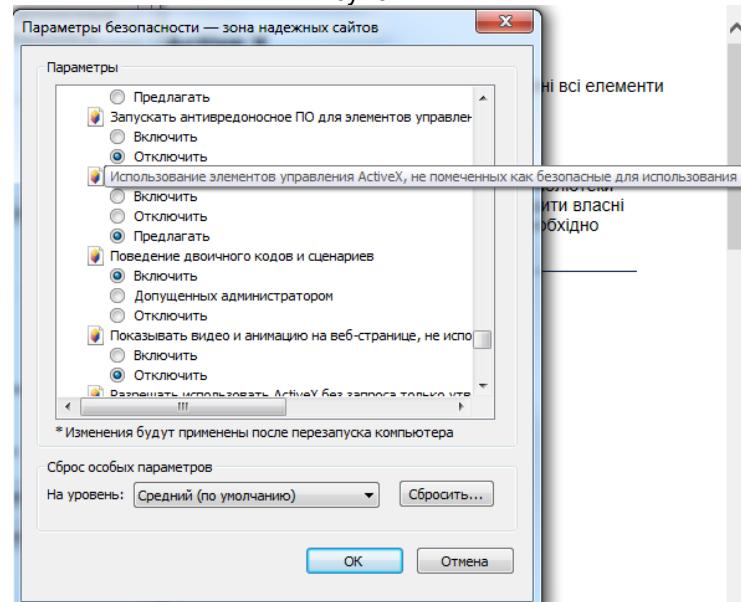


Рисунок 4.23

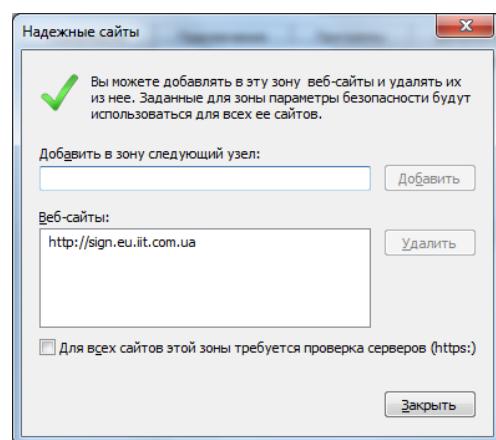


Рисунок 4.24

Пор. № зміни	Підпис відпов. особи	Дата внесення

4.5.2 Встановлення параметрів роботи програми

При відсутності параметрів роботи програми, вони встановлюються за замовчанням.

Для налаштування параметрів ActiveX-компоненту необхідно перейти до закладки “Налаштувати надстройки” браузера та натиснути “Панелі інструментів та розширень” (рис. 4.25). На цій сторінці можна встановити параметри запуску ActiveX-компоненту на веб-сайтах.

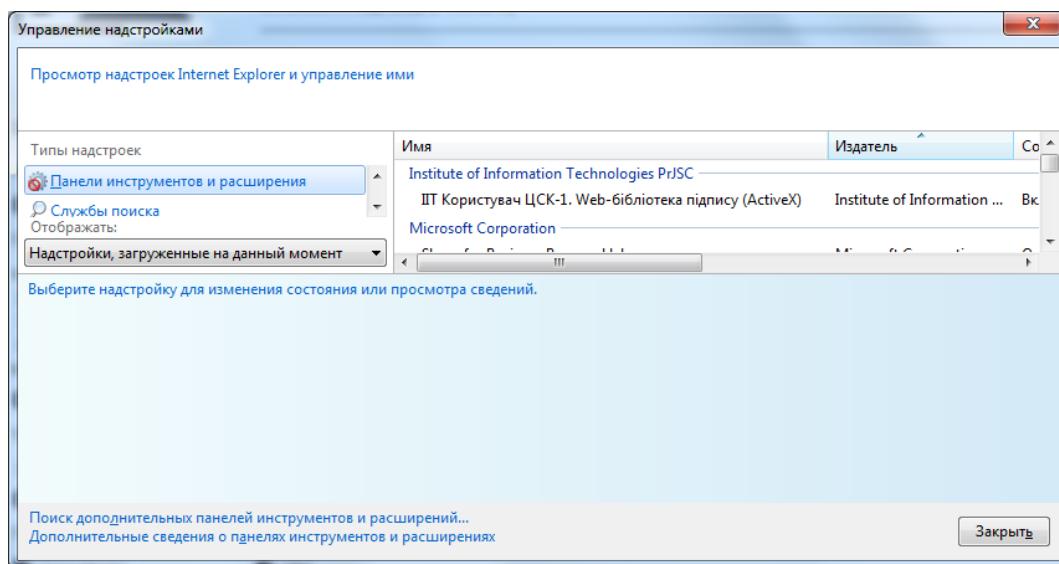


Рисунок 4.25

Пор. № зміни	Підпись відпов. особи	Дата внесення

ПЕРЕЛІК СКОРОЧЕНЬ

ОС	Операційна система
ЕЦП	Електронний цифровий підпис
КЗІ	Криптографічний захист інформації
ДКЕ	Довгостроковий ключовий елемент
СВС	Список відкликаних сертифікатів
ЦСК	Центр сертифікації ключів
НКІ	Носій ключової інформації (особистого ключа)
ПЕОМ	Персональна електронно-обчислювальна машина
CMP	Certificate Management Protocol (протокол управління обслуговуванням сертифікатів)
OCSP	Online Certificate Status Protocol (протокол визначення статусу сертифіката)
LDAP	Lightweight Directory Access Protocol (протокол доступу до каталогу)
TSP	Time-Stamp Protocol (протокол отримання позначок часу)
HTTP	Hyper Text Transfer Protocol

Пор. № зміни	Підпись відпов. особи	Дата внесення

ДОДАТОК А. ВСТАНОВЛЕННЯ ПАРАМЕТРІВ РОБОТИ (ОС MICROSOFT WINDOWS)

Встановлення чи зміна параметрів роботи криптографічної бібліотеки виконується з використанням вікна параметрів наведеного на рис. А.1.

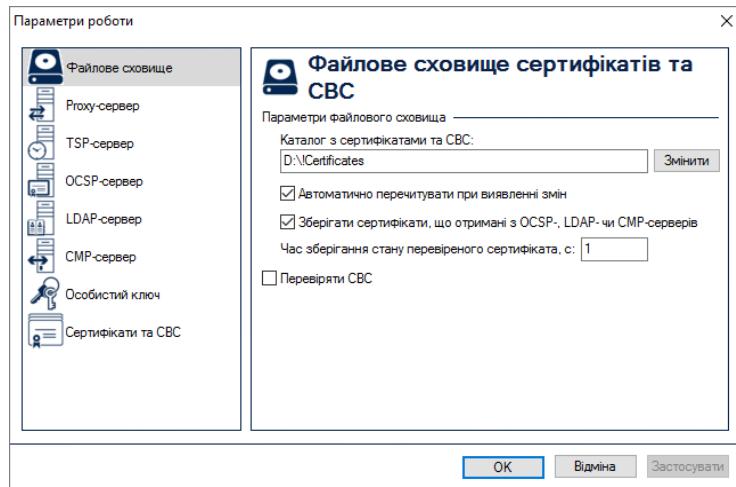


Рисунок А.1

A.1 Файлове сховище

Для настроювання параметрів файлового сховища сертифікатів та CBC необхідно перейти до закладки “Файлове сховище”. Вікно “Параметри роботи” із сторінкою “Файлове сховище” наведене на рис. А.1. На цій сторінці встановлюються наступні параметри роботи програми:

- “Каталог з сертифікатами та CBC”. Даний параметр встановлює каталог файлового сховища для зберігання сертифікатів та CBC.
Всі сертифікати та CBC, що завантажуються не засобами програми повинні записуватися у даний каталог.
- “Автоматично перечитувати при виявлені змін”. Даний параметр визначає необхідність автоматичного перечитування каталогу файлового сховища програмою при внесенні будь-яких змін до цього каталогу (запису нового сертифіката чи CBC у каталог чи видалення файлу з сертифікатом або CBC).
- “Зберігати сертифікати, що отримані з OCSP-, LDAP-серверів чи CMP-серверів”. Даний параметр визначає необхідність автоматичного збереження сертифікатів, що не знайдені у файловому сховищі, а отримані з OCSP-, LDAP-серверів чи CMP-серверів у файлове сховище.
- “Час зберігання стану перевіреного сертифікату”. Даний параметр визначає час протягом якого сертифікати що вже перевірені не будуть повторно перевірятися.
Застосування такого механізму збереження стану сертифіката протягом певного часу забезпечує зменшення ресурсів системи на перевірку сертифіката при частих звертаннях (механізм кешування статусу сертифіката).
- “Перевіряти CBC”. Параметр вказує на необхідність використання CBC в якості засобу перевірки статусу сертифікатів відкритих ключів що використовуються.
- “Тільки свого ЦСК”. Даний параметр визначає необхідність використовувати при перевірці сертифікатів CBC лише свого ЦСК у ланцюжку.
Для цього повинен бути зчитаний особистий ключ користувача, оскільки ЦСК користувача визначається за допомогою параметрів особистого ключа.
- “Повний та частковий”. Даний параметр визначає необхідність перевірки наявності двох діючих CBC (повного та часткового) при здійсненні перевірки сертифікатів.
Якщо параметр не встановлено достатньо лише одного повного діючого CBC. Даний параметр дозволяє не виконувати постійне завантаження останнього діючого часткового CBC.
- “Завантажувати автоматично”. Даний параметр визначає можливість автоматичного завантаження CBC під час перевірки статусу сертифікатів, якщо у файловому сховищі не знайдено діючих CBC.
Параметр має сенс якщо у сертифікатах ЦСК, або серверів ЦСК встановлено шлях отримання CBC.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

A.2 Proxy-сервер

Для настроювання параметрів proxy-сервера необхідно перейти до закладки “Proxy-сервер” у вікні що наведене на рисунку А.1. Вікно “Параметри роботи” із сторінкою “Proxy-сервер” наведене на рис. А.2. На сторінці “Proxy-сервер” встановлюються наступні параметри роботи програми:

- “Підключатися через proxy-сервер”. Встановлює необхідність використання proxy-сервера під час підключення до серверів обробки запитів.
- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я proxy-сервера.
- “TCP-порт”. Даний параметр встановлює TCP-порт proxy-сервера.
- “Автентифікуватися на proxy-сервері”. Встановлює необхідність автентифікації (вводу логіну та паролю) під час підключення до proxy-сервера.
- “Ім’я користувача”. Даний параметр встановлює ім’я користувача proxy-сервера.
Якщо proxy-сервер працює в режимі без автентифікації даний параметр може не вводитися.
- “Пароль”. Даний параметр встановлює пароль доступу користувача до proxy-сервера.
Якщо proxy-сервер працює в режимі без автентифікації даний параметр може не вводитися.
- “Зберегти пароль”. Даний параметр встановлює необхідність зберігати пароль доступу до proxy-сервера у реєстрі ОС.

У випадку якщо даний параметр не встановлено, введення паролю буде запрошуватися при першому підключення до proxy-сервера у програмі.

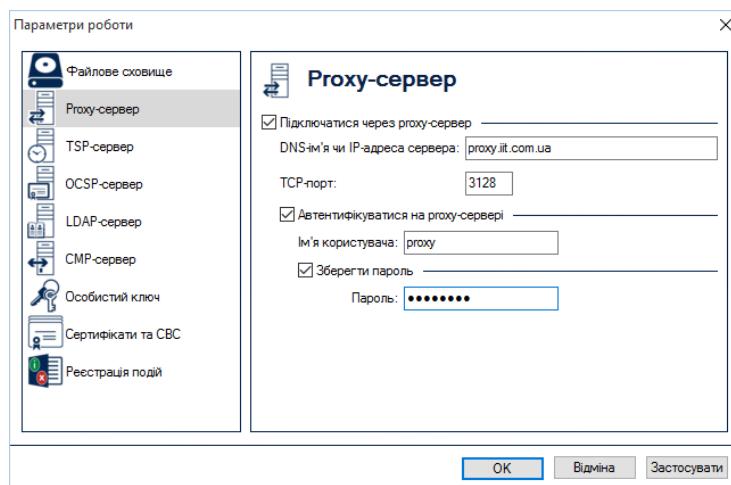


Рисунок А.2

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

A.3 TSP-сервер

Для настроювання параметрів TSP-сервера необхідно перейти до закладки “TSP-сервер” у вікні що наведене на рисунку А.1 Вікно “Параметри роботи” із сторінкою “TSP-сервер” наведене на рис. А.3. На сторінці “TSP-сервер” встановлюються наступні параметри роботи програми:

- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я TSP-сервера.
Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
- “TCP-порт”. Даний параметр встановлює TCP-порт TSP-сервера.
Як правило це порт протоколу HTTP (80).

Пор. № зміни	Підпис відпов. особи	Дата внесення

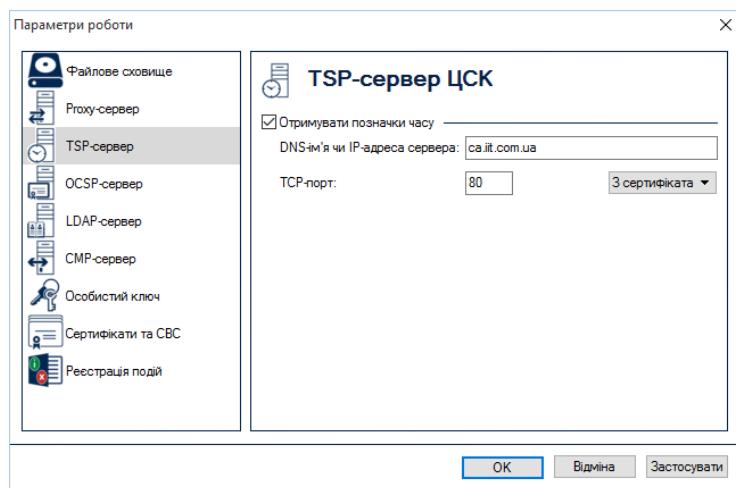


Рисунок А.3

Для встановлення параметрів доступу до TSP-серверу з сертифіката сервера необхідно натиснути кнопку “З сертифіката” та з випадаючого меню обрати “сервера”.

Для встановлення параметрів доступу до TSP-серверу з сертифіката користувача необхідно натиснути кнопку “З сертифіката” та з випадаючого меню обрати “користувача”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

A.4 OCSP-сервер

Для настроювання параметрів OCSP-сервера необхідно перейти до закладки “OCSP-сервер ЦСК” у вікні що наведене на рисунку А.1. Вікно “Параметри роботи” із сторінкою “OCSP-сервер ЦСК” наведене на рис. А.4. На сторінці “OCSP-сервер ЦСК” встановлюються наступні параметри роботи програми:

- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я OCSP-сервера.
Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
- “TCP-порт”. Даний параметр встановлює TCP-порт OCSP-сервера.
Як правило це порт протоколу HTTP (80).
- “Перевіряти до перевірки у файловому сховищі”. Даний параметр встановлює черговість перевірки статусу сертифіката.

Якщо параметр встановлено, статус сертифіката перевіряється спочатку за допомогою OCSP-протоколу, потім за допомогою файлового сховища.

Якщо параметр не встановлено, перевірка здійснюється спочатку за допомогою файлового сховища, а потім (за необхідностю) за допомогою OCSP-протоколу.

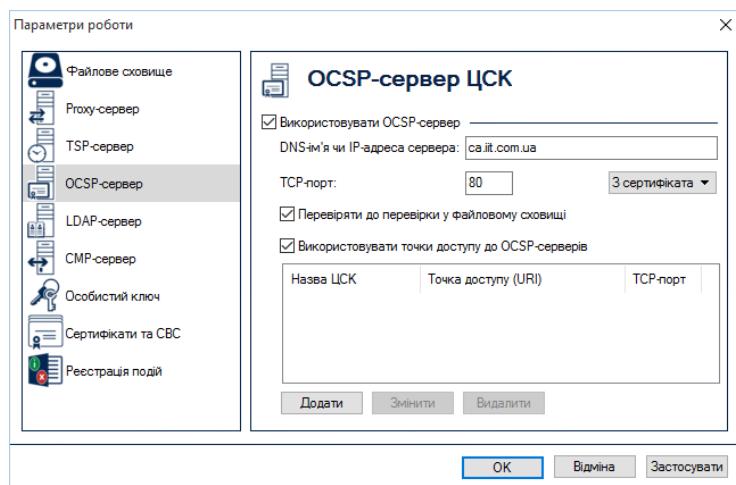


Рисунок А.4

Для встановлення параметрів доступу до OCSP-серверу з сертифіката OCSP-сервера необхідно натиснути кнопку “З сертифіката” та з випадаючого меню обрати “сервера”.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Для встановлення параметрів доступу до OCSP-серверу з сертифіката користувача необхідно натиснути кнопку “З сертифіката” та з випадаючого меню обрати “користувача”.

Для використання декількох точок доступу необхідно встановити позначку “Використовувати точки доступу до OCSP-серверів” та натиснути “Додати”. У вікні встановлення налаштувань точок доступу до OCSP-серверів (рис. А.5) необхідно вказати назву, URL-адресу та порт доступу до OCSP-сервера ЦСК. Для автоматичного встановлення всіх необхідних параметрів з сертифіката, необхідно натиснути “З сертифіката”. Для збереження введених налаштувань необхідно натиснути “Додати”.

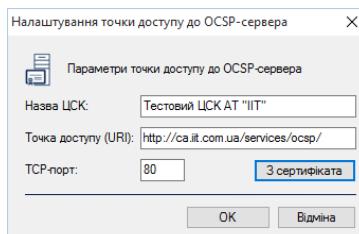


Рисунок А.5

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

A.5 LDAP-сервер

Для настроювання параметрів LDAP-сервера перейти до закладки “LDAP-сервер” у вікні що наведене на рисунку А.1 Вікно “Параметри роботи” із сторінкою “LDAP-сервер” наведене на рис. А.6. На сторінці “LDAP-сервер” встановлюються наступні параметри роботи програми:

- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я LDAP-сервера.
Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
- “TCP-порт”. Даний параметр встановлює TCP-порт LDAP-сервера.
Як правило це порт протоколу LDAP (389).
- “Анонімний доступ”. Даний параметр встановлює застосування анонімного доступу до LDAP-сервера (без використання імені користувача та паролю).
- “Ім’я користувача”. Даний параметр використовується якщо не встановлено параметр “Анонімний доступ” та встановлює ім’я користувача LDAP-сервера.
- “Пароль доступу”. Даний параметр використовується якщо не встановлено параметр “Анонімний доступ” та встановлює пароль доступу користувача до LDAP-сервера.

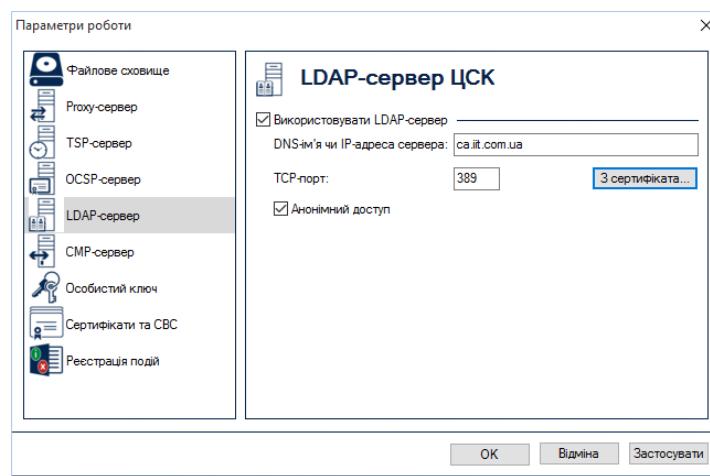


Рисунок А.6

За замовчанням встановлюються параметри LDAP-сервера що вказані у відповідному сертифікаті ЦСК. Параметри LDAP-сервера можна також встановити з сертифіката за допомогою кнопки “З сертифіката...”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

Пор. № зміни	Підпис відпов. особи	Дата внесення

A.6 CMP-сервер

Для настроювання параметрів CMP-сервера необхідно перейти до закладки “CMP-сервер” у вікні що наведене на рисунку А.1. Вікно “Параметри роботи” із сторінкою “CMP-сервер” наведене на рис. А.7. На сторінці “CMP-сервер” встановлюються наступні параметри роботи програми:

- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я CMP-сервера.

Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.

- “TCP-порт”. Даний параметр встановлює TCP-порт CMP-сервера.

Як правило це порт протоколу HTTP (80).

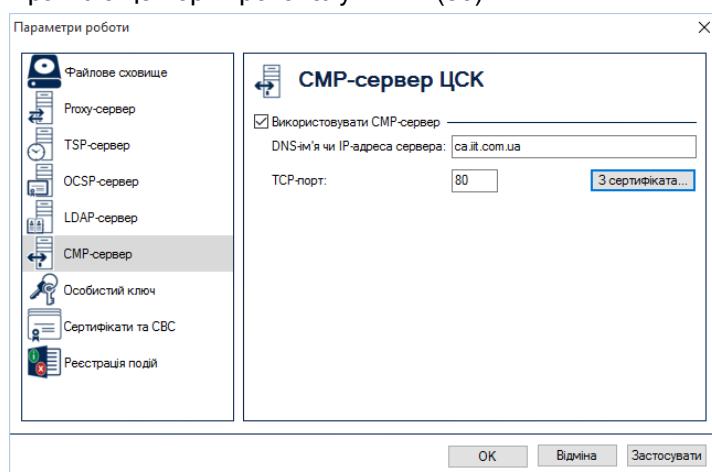


Рисунок А.7

Параметри CMP-сервера можна також встановити з сертифіката за допомогою кнопки “З сертифіката...”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

A.7 Особистий ключ

Для проведення основних операцій з особистим ключем необхідно перейти до розділу "Особистий ключ" у вікні параметрів (рис. А.8).

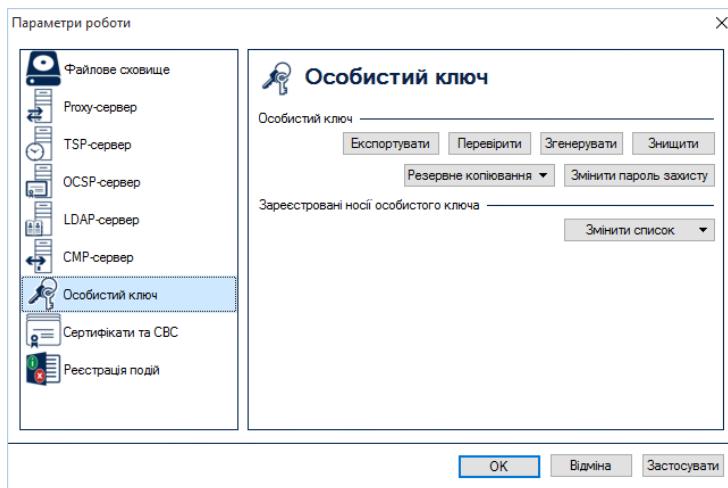


Рисунок А.8

У розділі “Особистий ключ” є можливість експортувати, перевірити, згенерувати, знищити, зробити резервне копіювання та змінити пароль захисту особистого ключа.

A.7.1 Експортувати

Функція експорту особистого ключа дозволяє експортувати у контейнер особистих ключів і сертифікатів та експорт у контейнер особистих ключів

Пор. № зміни	Підпис відпов. особи	Дата внесення

Для експорту особистого ключа необхідно натиснути “Експортувати” у розділі “Особистий ключ” (рис. А.9). Під час експорту здійснюється зчитування особистого ключа (рис.А.10).

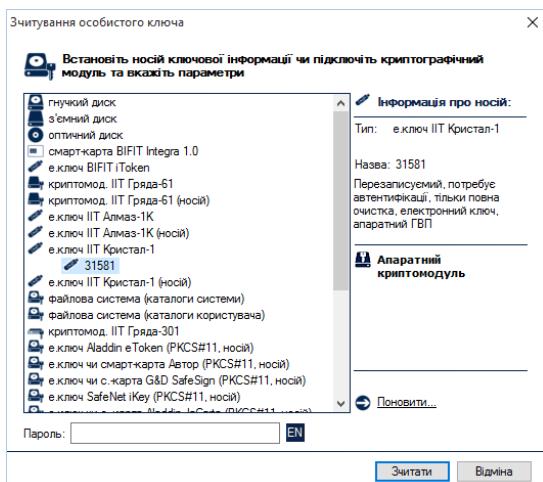


Рисунок А.9

Після зчитування особистого ключа необхідно обрати типи особистих ключі для експорту, а також вказати параметри експорту (рис. А.10). Надається можливість експорту у контейнер особистих ключів і сертифікатів (*.pfx) та у контейнер особистих ключів (*.pk8).

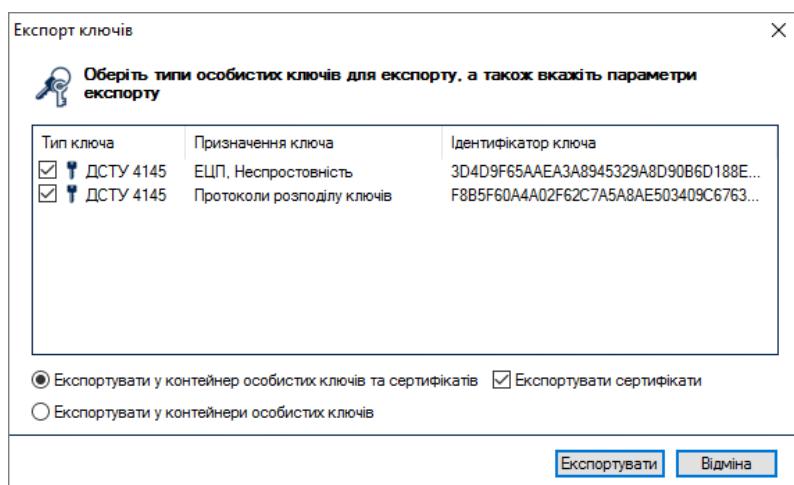


Рисунок А.10

Після вибору параметрів експорту необхідно вказати пароль доступу до контейнеру особистих ключів (рис. А.11) та вказати назву та розміщення файлу-контейнеру особистих ключів (рис. А.12).

Примітка. Пароль доступу до контейнеру особистих ключів може як відрізнятись, так і співпадати з паролем захисту особистого ключа, що знаходиться на носіїві ключової інформації, з якого проводиться експорт.

Примітка. Надається можливість вказати будь-яке розміщення та назву файлу-контейнеру особистого ключа.

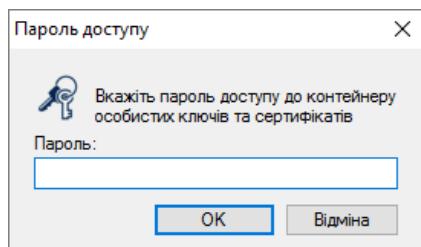


Рисунок А.11

Пор. № зміни	Підпис відпов. особи	Дата внесення

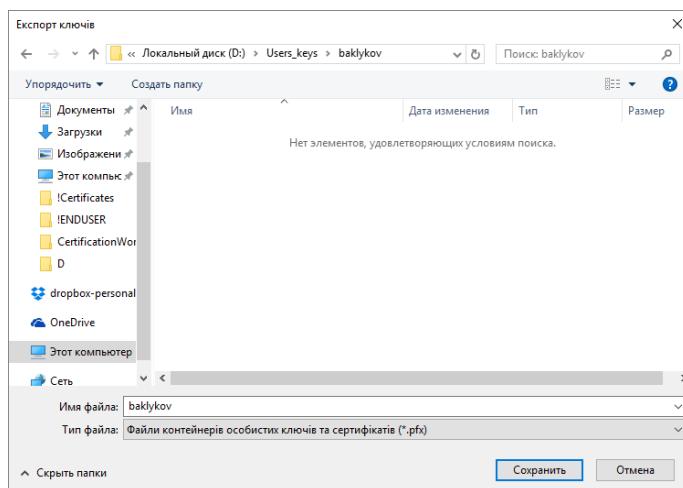


Рисунок А.12

A.7.2 Перевірити

Виконується перевірка особистого ключа. Для перевірки особистого ключа необхідно натиснути “Перевірити” у розділі “Осбистий ключ” (рис.А.8). Під час перевірки здійснюється зчитування особистого ключа (рис. А.13 та виконується пошук відповідного сертифіката (рис. А.13 - А.15).

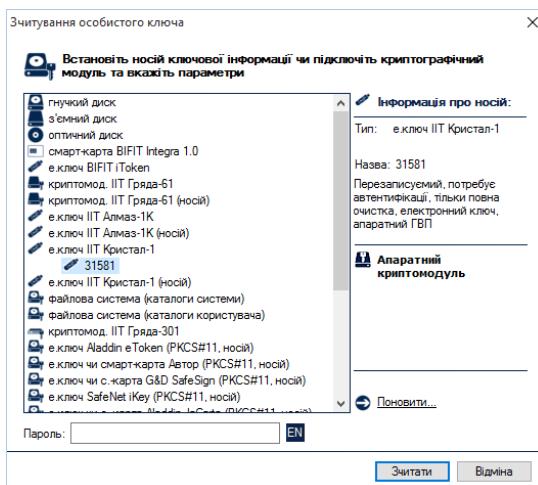


Рисунок А.13

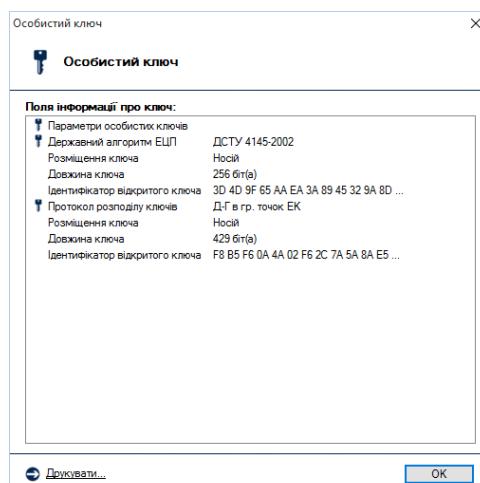


Рисунок А.14

Пор. № зміни	Підпис відпов. особи	Дата внесення

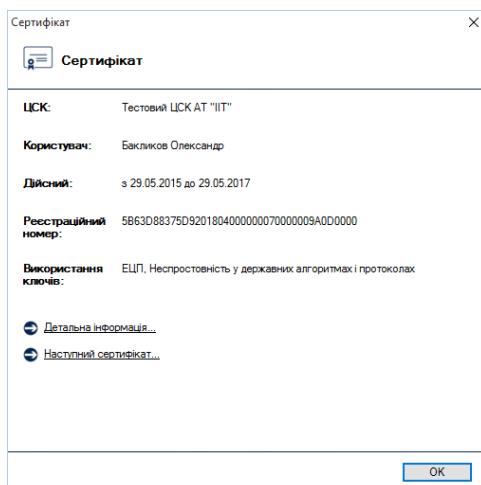


Рисунок А.15

A.7.3 Згенерувати

Для генерації ключів необхідно обрати підпункт “Згенерувати” в пункті меню “Особистий ключ” (рис А.8).

На сторінці (рис. А.16) необхідно обрати алгоритми та протоколи, в яких планується використовувати згенеровані ключі. Для більшості випадків, обирається параметр за замовчанням “Для державних алгоритмів та протоколів”.

Примітка. У разі необхідності можлива генерація особистого ключа для “міжнародних алгоритмів і протоколів” та “державних та міжнародних алгоритмів і протоколів”.

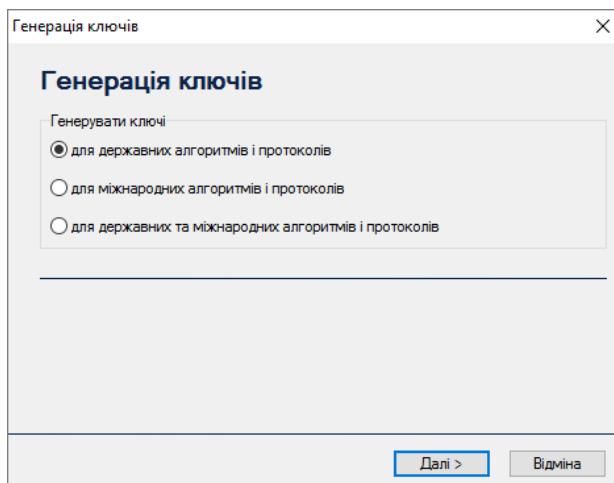


Рисунок А.16

На наступній сторінці (рис. А.17) необхідно вказати параметри криптографічних алгоритмів та протоколів (для більшості випадків ці параметри можна залишити за замовчанням).

Якщо параметр “Використовувати окремий ключ для протоколу розподілу” встановлено, то буде згенеровано 2 ключа: один для ЕЦП, другий для протоколу розподілу. Якщо параметр не встановлено, то буде згенеровано один ключ, що буде використовуватись як для ЕЦП, так і для зашифрування.

Пор. № зміни	Підпис відпов. особи	Дата внесення

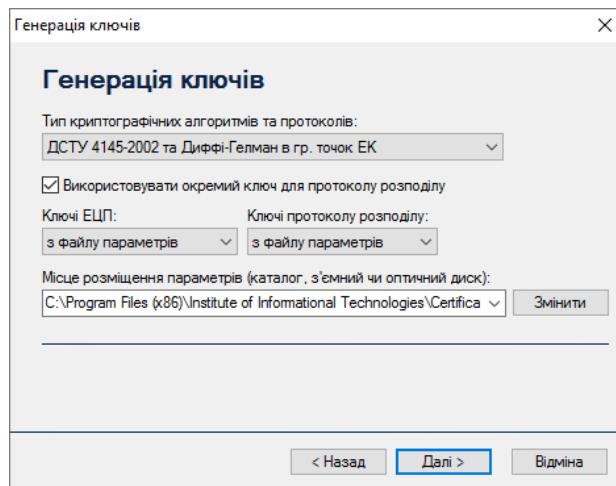


Рисунок А.17

Далі необхідно встановити НКІ для запису особистого ключа у пристрій запису та на наступній сторінці майстра (рис. А.18) вказати:

- тип носія ключової інформації (НКІ);
- назву носія;
- пароль доступу до ключового носія (якщо в якості носія використовується криптомодуль) або пароль захисту особистого ключа (з підтвердженням).

Ключові носії можуть бути наступних типів:

- гнучкі диски;
- оптичні диски;
- з'ємні диски (flash-диски);
- файлова система;
- криптомодулі ("ІІТ.Гряда-61", "ІІТ.Гряда-301");
- електронні ключі ("ІІТ.Кристал-1", "ІІТ.Алмаз-1К", Aladdin eToken R2, PRO, та інші).

Пароль захисту особистого ключа повинен відповідати наступним вимогам:

- довжина - не менше 8 символів;
- не повинен містити однакові символи;
- не повинен містити підряд більше ніж 2 символи з розкладинки клавіатури;
- дозволені символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка. Такі вимоги носять рекомендаційний характер.

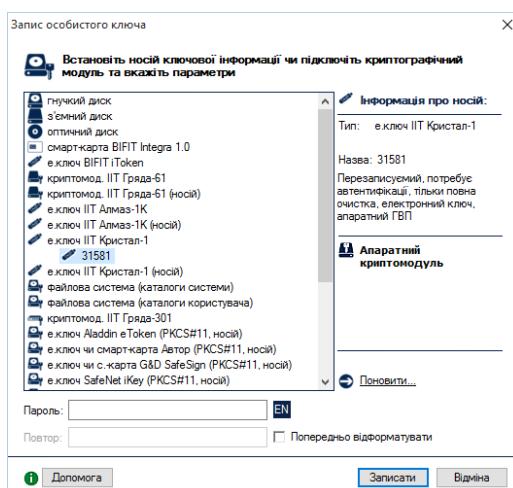


Рисунок А.18

Пор. № зміни	Підпис відпов. особи	Дата внесення

Після запису особистого ключа на НКІ або до файлу, буде виведено вміст простих запитів на формування сертифікату з відкритим ключем ЕЦП та протоколу розподілу для державних алгоритмів та протоколів (рис. А.19-А.20), після перевірки вмісту простих запитів необхідно натиснути "OK".

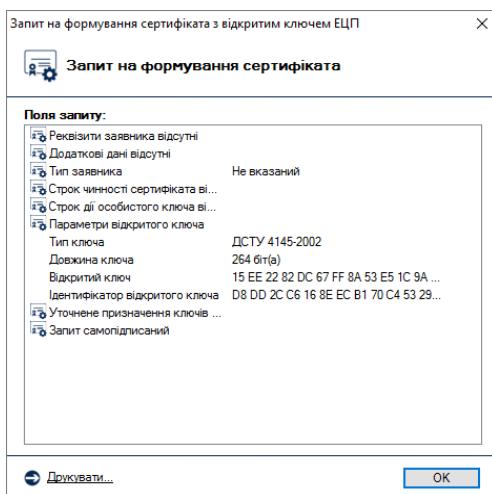


Рисунок А.19

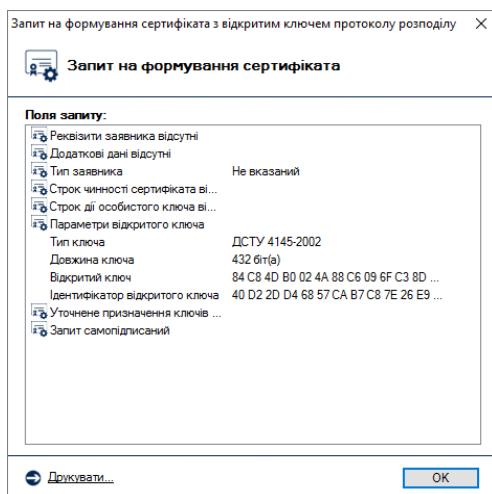


Рисунок А.20

У наступному вікні (рис. А.21) необхідно буде вказати ім'я файлів для запису простих запитів на формування сертифікатів з відкритим ключем ЕЦП та протоколу розподілу у файли. Запити повинен бути записаний на носій інформації чи на жорсткий диск. Після цього запити повинні бути передані у пункт реєстрації ЦСК для формування сертифікатів.

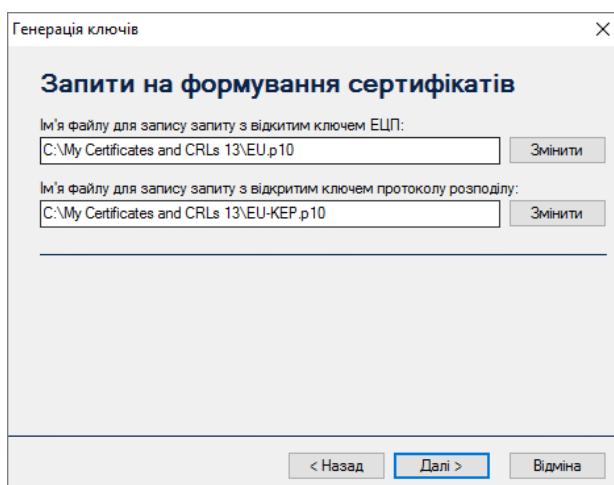


Рисунок А.21

Пор. № зміни	Підпис відпов. особи	Дата внесення

Після виконання всіх дій майстер завершує свою роботу (рис. А.22).

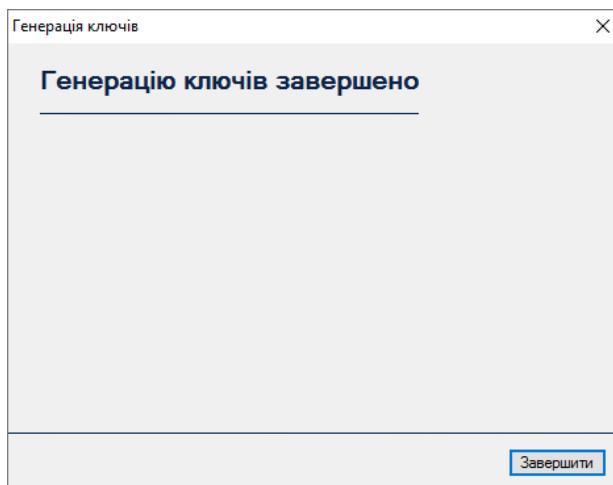


Рисунок А.22

A.7.4 Знищити

Особистий ключ на НКІ повинен знищуватись спеціальними засобами, які вбудовані у програму, що забезпечують його гарантоване знищення.

Для знищенння особистого ключа необхідно натиснути підпункт “Знищити” пункту меню ”Особистий ключ”, за допомогою вікна що наведене на рис. А.23. У вікні вказується носій ключової інформації та пароль. Для знищенння необхідно натиснути ”Знищити”.

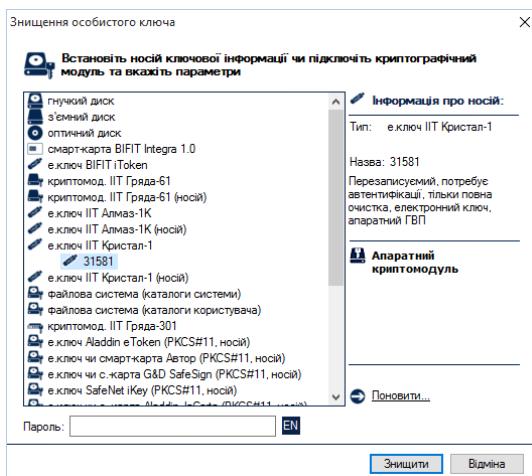


Рисунок А.23

A.7.5 Резервне копіювання

Функція дозволяє здійснити резервне копіювання особистого ключа з одного НКІ на інший, з НКІ до файлу та з файлу до НКІ. Для резервного копіювання необхідно натиснути підпункт “Резервне копіювання” пункту меню ”Особистий ключ” та обрати режим резервного копіювання (рис.А.24).

Пор. № зміни	Підпис відпов. особи	Дата внесення

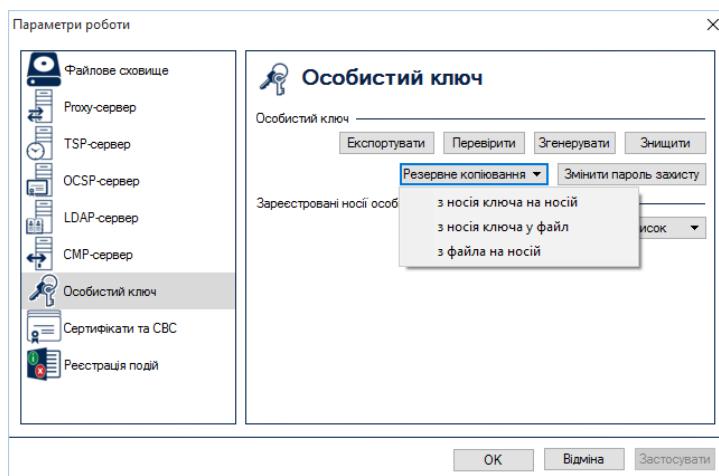


Рисунок А.24

У випадку резервного копіювання особистого ключа в режимі “з носія на носій”, зчитування особистого ключа здійснюється за допомогою вікна що наведене на рис. А.8. Запис особистого ключа здійснюється за допомогою вікна що наведене на рис. А.25.

Увага! Під час резервного копіювання пароль захисту особистого ключа не змінюється.

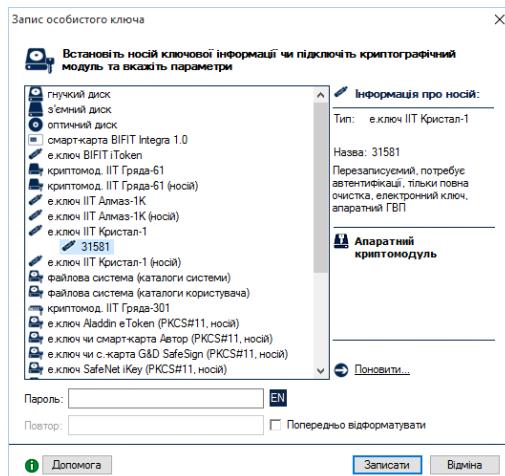


Рисунок А.25

У випадку резервного копіювання особистого ключа в режимі “з носія у файл”, зчитування особистого ключа здійснюється за допомогою вікна що наведене на рис. А.8. Запис особистого ключа здійснюється за допомогою вікна що наведене на рис. А.26

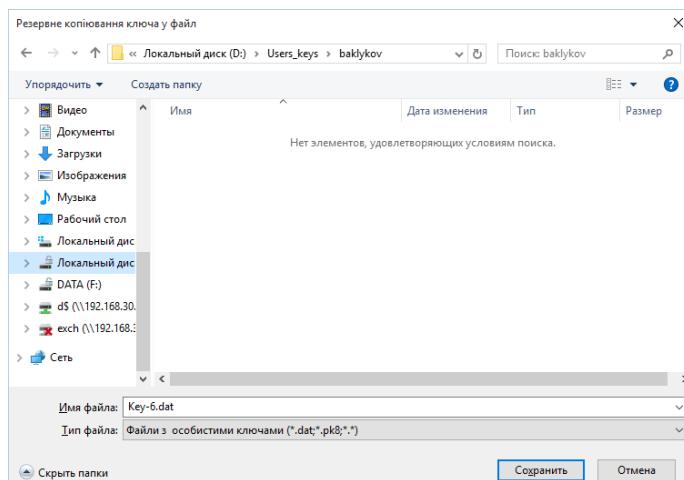


Рисунок А.26

Пор. № зміни	Підпис відпов. особи	Дата внесення

У випадку резервного копіювання особистого ключа в режимі “з файлу на носій”, зчитування особистого ключа здійснюється за допомогою вікна що наведене на рис. А.27. Запис особистого ключа здійснюється за допомогою вікна що наведене на рис. А.18.

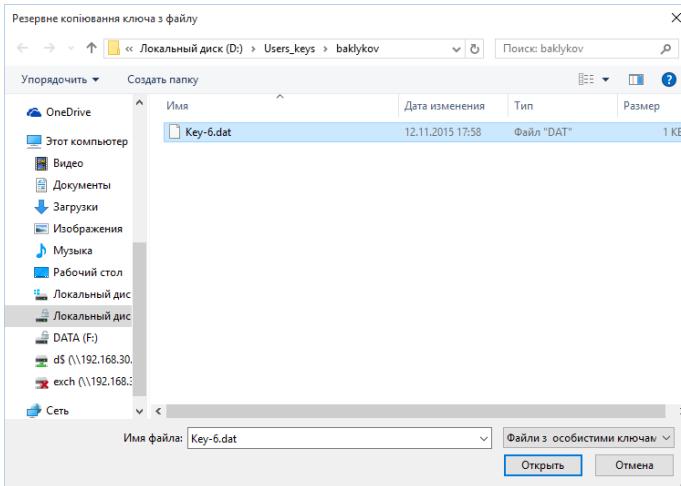


Рисунок А.27

Примітка. Якщо в якості засобу зберігання особистого ключа використовується електронний ключ “Кристал-1” в апаратному режимі роботи, резервна копія ключа не створюється, оскільки такі засоби не передбачають функції резервного копіювання ключів. Резервну копію особистого ключа можливо створити, якщо особистого ключа зберігається у електронному ключу “Кристал-1” в режимі роботи носій. При цьому під час запису особистого ключа вказується пароль, що був використаний під час зчитування особистого ключа.

A.7.6 Зміна паролю захисту особистого ключа

Для зміни паролю захисту особистого ключа необхідно обрати підпункт “Змінити пароль” в пункті меню “Особистий ключ”. Вікно зміни паролю захисту особистого ключа наведене на рис. А.28. У вікні необхідно вказати:

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

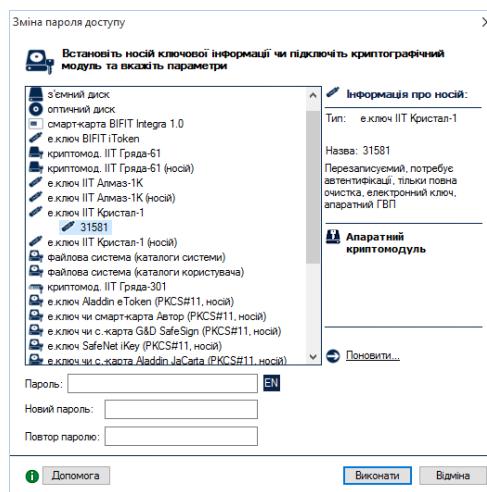


Рисунок А.28

A.7.7 Реєстрація носіїв особистого ключа

На сторінці "Особистий ключ" (рис. А.29) можливо змінити список зареєстрованих носіїв особистих ключів. Параметр дозволяє встановлювати параметри особистого ключа, що зберігається на файловій системі або в мережному криптомулі "Гряда-301".

Пор. № зміни	Підпис відпов. особи	Дата внесення

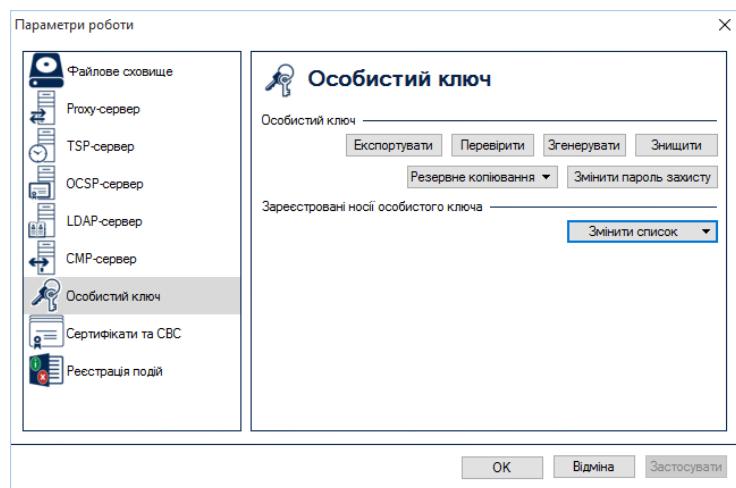


Рисунок А.29

Параметр дозволяє додавати, змінювати та видаляти носії особистих ключів.

Для зміни списку носіїв на файловій системі необхідно обрати "Змінити список" та у випадаючому меню обрати "Каталогів файлової системи".

Для додавання каталогу з ключовими даними необхідно натиснути "Додати" (рис. А.30). При додаванні каталогу з ключовими даними необхідно вказати назву каталогу та його розміщення на файловій системі (рис. А.31).

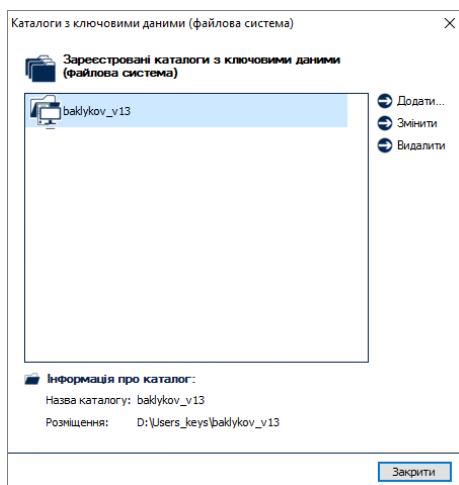


Рисунок А.30

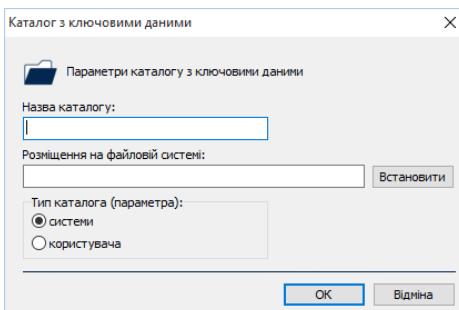


Рисунок А.31

Для зміни параметру каталогу з ключовими даними необхідно обрати каталог на натиснути "Змінити" (рис. А.30).

Примітка. Можливо змінити тільки шлях на файловій системі.

Для видалення каталогу з ключовими даними необхідно обрати відповідну назву зареєстрованого каталогу (рис. А.30), та натиснути "Видалити".

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

Пор. № зміни	Підпис відпов. особи	Дата внесення

Для зміни списку носіїв в мережному криптомодулі "Гряда-301" необхідно обрати "Змінити список" та у випадаючому меню обрати "Мережні криптомодулі Гряда-301".

Для реєстрації мережного криптомодуля необхідно натиснути "Додати" (рис. А.32). При додаванні мережного криптомодуля необхідно вказати назву модуля, його серійний номер, IP-адресу та маску IP-адреси криптомодуля (рис. А.33).

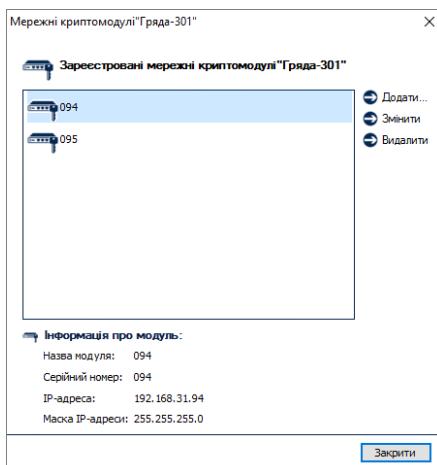


Рисунок А.32

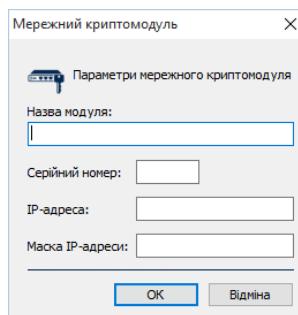


Рисунок А.33

Для зміни параметру мережного криптомодуля необхідно обрати "Змінити" (рис. А.32).

Примітка. Можливо змінити тільки серійний номер, IP-адресу та маску IP-адреси криптомодуля.

Для видалення каталогу з ключовими даними необхідно обрати відповідну назву зареєстрованого криптомодуля (рис. А.32), та натиснути "Видалити".

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

A.8 Сертифікати та СВС

Для перегляду сертифікатів та списків відкліканіх сертифікатів необхідно перейти до закладки "Сертифікати та СВС" у вікні, що наведено на рисунку А.33

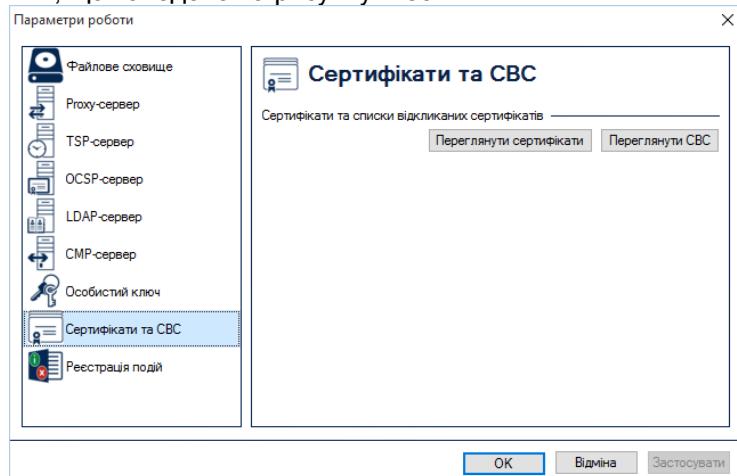


Рисунок А.33

Пор. № зміни	Підпис відпов. особи	Дата внесення

A.8.1 Переглянути сертифікати

Для перегляду сертифікатів що містяться у файловому сховищі необхідно натиснути “Переглянути сертифікати” у вікні що наведене на рис. А.33. Вікно із сертифікатами наведене на рис. А.34

За допомогою даного вікна можна видаляти сертифікати з файлового сховища, перевіряти та переглядати сертифікати.

Сертифікати у вікні відсортовані за типами власників (тип власника обирається у верхній частині вікна у випадаючому списку):

- всі сертифікати;
- сертифікати центрів сертифікації ключів;
- сертифікати серверів ЦСК;
- сертифікати CMP-серверів;
- сертифікати TSP-серверів;
- сертифікати OCSP-серверів;
- сертифікати користувачів ЦСК;
- адміністратори реєстрації.

Для перегляду списку сертифікатів власника певного типу необхідно обрати відповідний тип власника у верхній частині вікна у списку що випадає.

Для перегляду сертифіката необхідно натиснути на відповідному записі про сертифікат у списку. Сертифікат буде відображене у вікні, що наведене на рисунку А.35. Для перегляду детальної інформації, що міститься в сертифікаті необхідно натиснути “Детальна інформація” (рис. А.36).

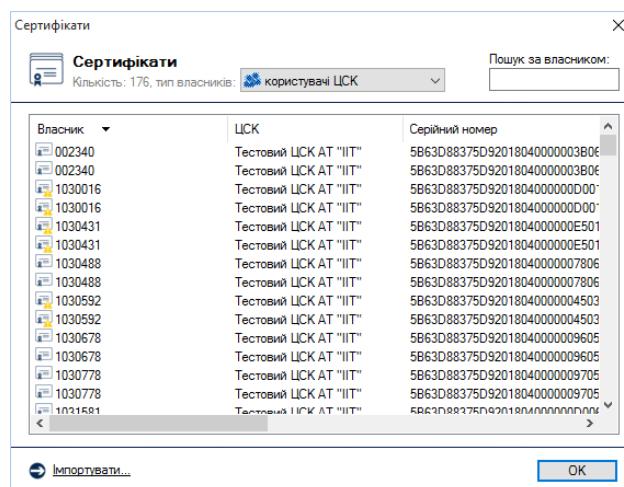


Рисунок А.34

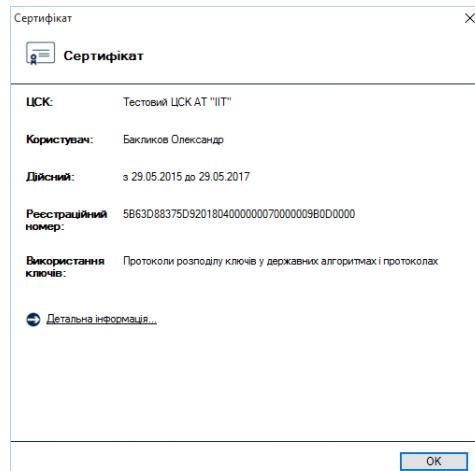


Рисунок А.35

Пор. № зміни	Підпис відпов. особи	Дата внесення

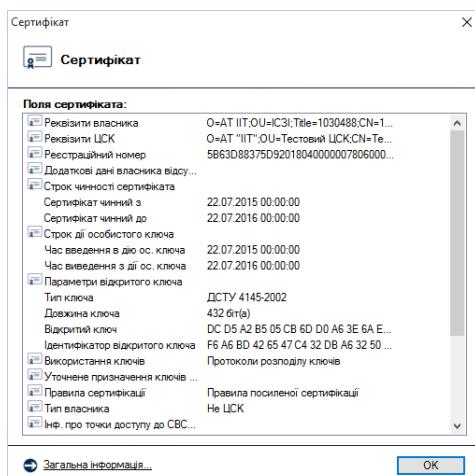


Рисунок А.36

Для видалення сертифікатів з файлового сховища необхідно виділити у списку відповідні записи про сертифікати та натиснути кнопку “Видалити”.

Для перевірки сертифіката необхідно виділити відповідний запис про сертифікат у списку та натиснути кнопку “Перевірити”. Перевірка сертифіката здійснюється відповідно до встановлених параметрів роботи (див. п. А.1-А.6) - за допомогою CBC, OCSP-протоколу тощо. Результатом перевірки буде вікно що наведене на рис. А.37. Якщо у цьому вікні натиснути “Сертифікат”, сертифікат буде відображені у вікні детального перегляду (рис. А.35).

Для імпорту сертифіката до файлового сховища необхідно натиснути “Імпортувати”, та обрати потрібний сертифікат на будь-якому носії інформації.

Для експорту сертифіката з файлового сховища в інше місце (носій інформації тощо), необхідно натиснути “Експортувати”, та обрати інше місце розташування.

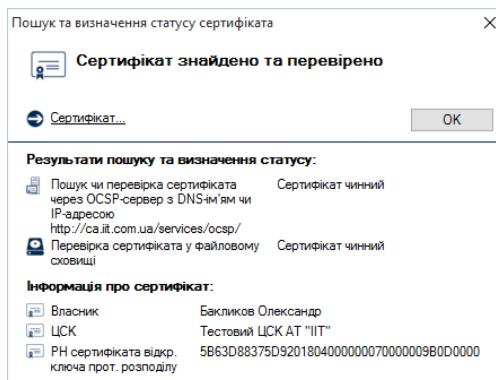


Рисунок А.37

A.8.2 Переглянути CBC

Для перегляду списків відкликаних сертифікатів (CBC) що містяться у файловому сховищі необхідно натиснути “Переглянути CBC” у вікні що наведене на рис. А.33 Вікно із CBC наведене на рис. А.38.

Вікно перегляду CBC дозволяє видаляти CBC з файлового сховища, переглядати CBC та завантажувати CBC з web-сервера ЦСК.

Для перегляду CBC необхідно натиснути на відповідному записі про CBC у списку. CBC буде відображене у вікні що наведене на рисунках А.39 та А.40.

Для видалення файлу CBC з файлового сховища необхідно виділити відповідний запис про CBC у списку та натиснути кнопку “Видалити”.

Для імпорту CBC до файлового сховища необхідно натиснути “Імпортувати”, та обрати потрібний CBC на будь-якому носії інформації.

Пор. № зміни	Підпис відпов. особи	Дата внесення

ЦСК	Серійний номер	Час формування	Наступний	Реквізити
Тестовий ЦСК АТ "ІІТ"	5D19	02.09.2015 12:29:47	02.09.2015 14:29:47	O=AT
Тестовий ЦСК АТ "ІІТ"	5D01	01.09.2015 14:29:47	02.09.2015 14:29:47	O=AT

[Імпортувати...](#) [OK](#)

Рисунок А.38

ЦСК: Тестовий ЦСК АТ "ІІТ"

Реєстраційний номер: 5D19

Час формування: 02.09.2015 09:29, Наступний: 02.09.2015 11:29

Призначення: Для використання у державних алгоритмах і протоколах

[Детальніша інформація...](#)

[OK](#)

Рисунок А.39

Загальна інформація:

- Реквізити ЦСК: O=AT "ІІТ";OU=Тестовий ЦСК;CN=Te...
- Час формування: 02.09.2015 12:29:47
- Час наступного формування: 02.09.2015 14:29:47
- 5D19
- РН: 5B63D8375D9201804000000A5...
- Ідентифікатор відкритого ключа: 5B63 D8 83 75 D9 20 18 CD B4 B1 0E ...
- Експерт: ССС

Список відкликаних сертифікатів:

5B63D8375D9201804000000A5...	01.09.2015 17:50:19	Не визначена
5B63D8375D9201804000000A5...	01.09.2015 17:50:13	Не визначена

Значення:

[Загальна інформація...](#) [OK](#)

Рисунок А.40

A.9 Реєстрація подій

Для встановлення параметрів, які відповідають за реєстрацію подій, що пов'язані з роботою криптобібліотеки, необхідно натиснути “Реєстрація подій” у вікні параметрів роботи (рис. А.1). Вікно із доступними параметрами наведене на рис. А.41

Пор. № зміни	Підпис відпов. особи	Дата внесення

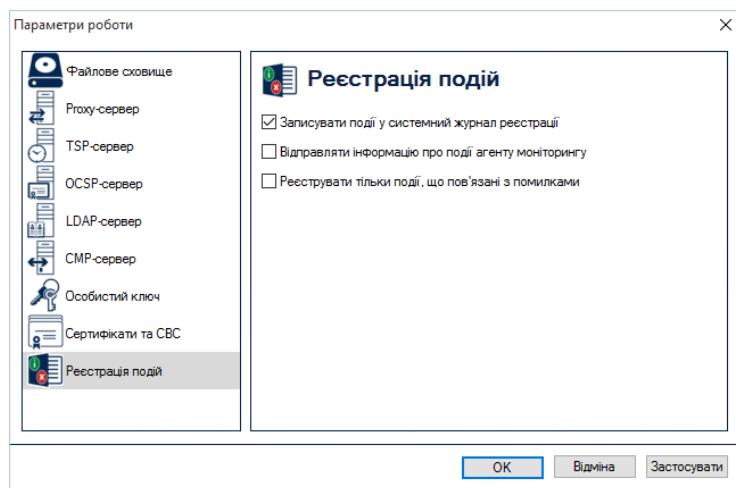


Рисунок А.41

Доступні наступні параметри реєстрації подій:

- Записувати події у системний журнал реєстрації;
- Відправляти інформацію агенту моніторингу;
- Реєструвати тільки події, що пов'язані з помилками.

У випадку встановлення параметру “Відправляти інформацію агенту моніторингу” необхідно вказати DNS-ім’я чи IP-адресу та порт агента моніторингу (рис. А.42), що повинен бути заздалегідь встановлений та налаштований.

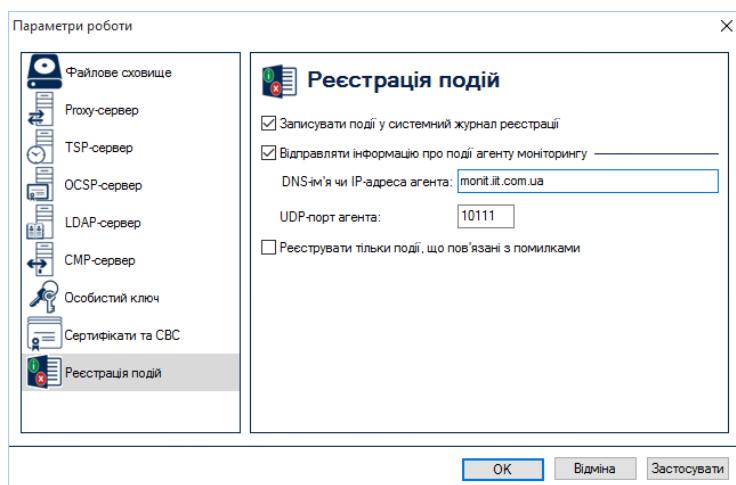


Рисунок А.42

У випадку встановлення параметру “Реєструвати події, що пов’язані з помилками” до системного журналу ОС будуть заноситись тільки повідомлення, що пов’язані з помилками в роботі криптобібліотеки.

Пор. № зміни	Підпис відпов. особи	Дата внесення

ДОДАТОК Б. ВСТАНОВЛЕННЯ ПАРАМЕТРІВ РОБОТИ (ОС APPLE MAC OS X)

Встановлення чи зміна параметрів роботи криптографічної бібліотеки виконується з використанням вікна параметрів наведеного на рис. Б.1.

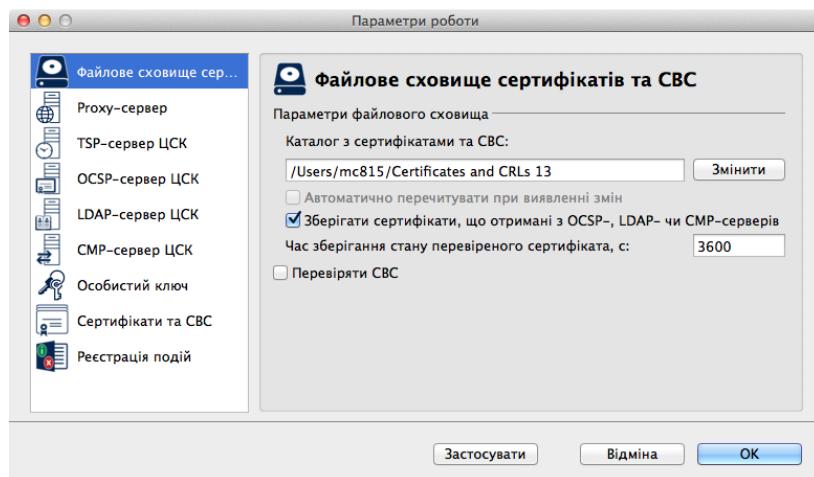


Рисунок Б.1

Б.1 Файлове ховище

Для настроювання параметрів файлового ховища сертифікатів та CBC необхідно перейти до закладки “Файлове ховище”. Вікно “Параметри роботи” із сторінкою “Файлове ховище” наведене на рис. Б.1. На цій сторінці встановлюються наступні параметри роботи програми:

- “Каталог з сертифікатами та CBC”. Даний параметр встановлює каталог файлового ховища для зберігання сертифікатів та CBC.
Всі сертифікати та CBC, що завантажуються не засобами програми повинні записуватися у даний каталог.
- “Автоматично перечитувати при виявлені змін”. Даний параметр визначає необхідність автоматичного перечитування каталогу файлового ховища програмою при внесенні будь-яких змін до цього каталогу (запису нового сертифіката чи CBC у каталог чи видалення файлу з сертифікатом або CBC).
- “Зберігати сертифікати, що отримані з OCSP-, LDAP- чи CMP-серверів”. Даний параметр визначає необхідність автоматичного збереження сертифікатів у файлове ховище, що не знайдені у файловому ховищі, а отримані з OCSP-, LDAP- чи CMP-серверів.
- “Час зберігання стану перевіреного сертифікату”. Даний параметр визначає час протягом якого сертифікати що вже перевірені не будуть повторно перевірятися.
Застосування такого механізму збереження стану сертифіката протягом певного часу забезпечує зменшення ресурсів системи на перевірку сертифіката при частих звертаннях (механізм кешування статусу сертифіката).
- “Перевіряти CBC”. Параметр вказує на необхідність використання CBC в якості засобу перевірки статусу сертифікатів відкритих ключів що використовуються.
- “Тільки свого ЦСК”. Даний параметр визначає необхідність використовувати при перевірці сертифікатів CBC лише свого ЦСК у ланцюжку.
Для цього повинен бути зчитаний особистий ключ користувача, оскільки ЦСК користувача визначається за допомогою параметрів особистого ключа.
- “Повний та частковий”. Даний параметр визначає необхідність перевірки наявності двох діючих CBC (повного та часткового) при здійсненні перевірки сертифікатів.
Якщо параметр не встановлено достатньо лише одного повного діючого CBC. Даний параметр дозволяє не виконувати постійне завантаження останнього діючого часткового CBC.
- “Завантажувати автоматично”. Даний параметр визначає можливість автоматичного завантаження CBC під час перевірки статусу сертифікатів, якщо у файловому ховищі не знайдено діючих CBC.
Параметр має сенс якщо у сертифікатах ЦСК, або серверів ЦСК встановлено шлях отримання CBC.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

Б.2 Proxy-сервер

Для настроювання параметрів proxy-сервера необхідно перейти до закладки “Proxy-сервер” у вікні що наведене на рисунку Б.1. Вікно “Параметри роботи” із сторінкою “Proxy-сервер” наведене на рис. Б.2. На сторінці “Proxy-сервер” встановлюються наступні параметри роботи програми:

- “Підключатися через proxy-сервер”. Встановлює необхідність використання proxy-сервера під час підключення до серверів обробки запитів.
- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я proxy-сервера.
- “TCP-порт”. Даний параметр встановлює TCP-порт proxy-сервера.
- “Автентифікуватися на proxy-сервері”. Встановлює необхідність автентифікації (вводу логіну та паролю) під час підключення до proxy-сервера.
- “Ім’я користувача”. Даний параметр встановлює ім’я користувача proxy-сервера.
Якщо proxy-сервер працює в режимі без автентифікації даний параметр може не вводитися.
- “Зберегти пароль”. Даний параметр встановлює необхідність зберігати пароль доступу до proxy-сервера у реєстрі ОС.
- “Пароль”. Даний параметр встановлює пароль доступу користувача до proxy-сервера.
Якщо proxy-сервер працює в режимі без автентифікації даний параметр може не вводитися.
У випадку якщо даний параметр не встановлено, введення паролю буде запрошууватися при першому підключення до proxy-сервера у програмі.

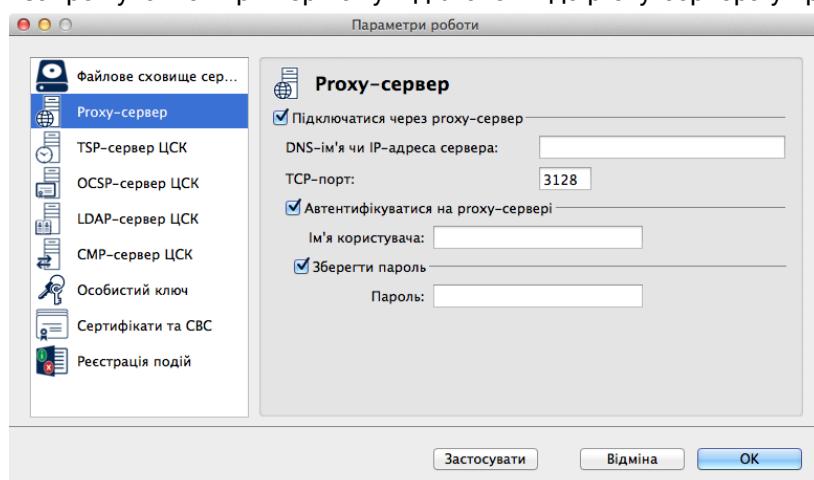


Рисунок Б.2

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

Б.3 TSP-сервер

Для настроювання параметрів TSP-сервера необхідно перейти до закладки “TSP-сервер ЦСК” у вікні що наведене на рисунку Б.1. Вікно “Параметри роботи” із сторінкою “TSP-сервер ЦСК” наведене на рис. Б.3. На сторінці “TSP-сервер ЦСК” встановлюються наступні параметри роботи програми:

- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я TSP-сервера.
Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
- “TCP-порт”. Даний параметр встановлює TCP-порт TSP-сервера.
Як правило це порт протоколу HTTP (80).

Пор. № зміни	Підпис відпов. особи	Дата внесення

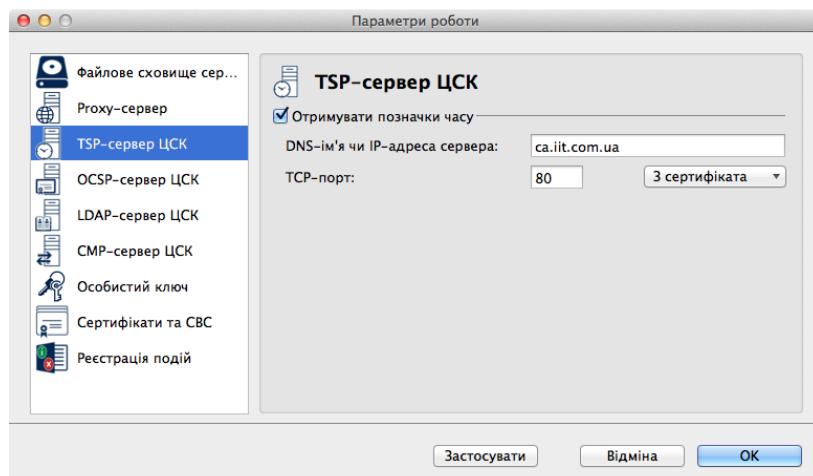


Рисунок Б.3

Для встановлення параметрів доступу до TSP-серверу з сертифіката TSP-сервера необхідно натиснути кнопку “З сертифіката” та з випадаючого меню обрати “сервера”.

Для встановлення параметрів доступу до TSP-серверу з сертифіката користувача необхідно натиснути кнопку “З сертифіката” та з випадаючого меню обрати “користувача”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Б.4 OCSP-сервер

Для настроювання параметрів OCSP-сервера необхідно перейти до закладки “OCSP-сервер ЦСК” у вікні що наведене на рисунку Б.1. Вікно “Параметри роботи” із сторінкою “OCSP-сервер ЦСК” наведене на рис. Б.4. На сторінці “OCSP-сервер ЦСК” встановлюються наступні параметри роботи програми:

- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я OCSP-сервера.

Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.

- “TCP-порт”. Даний параметр встановлює TCP-порт OCSP-сервера.

Як правило це порт протоколу HTTP (80).

- “Перевіряти до перевірки у файловому сховищі”. Даний параметр встановлює черговість перевірки статусу сертифікату.

Якщо параметр встановлено, статус сертифікату перевіряється спочатку за допомогою OCSP-протоколу, потім за допомогою файлового сховища.

Якщо параметр не встановлено, перевірка здійснюється спочатку за допомогою файлового сховища, а потім (за необхідностю) за допомогою OCSP-протоколу.

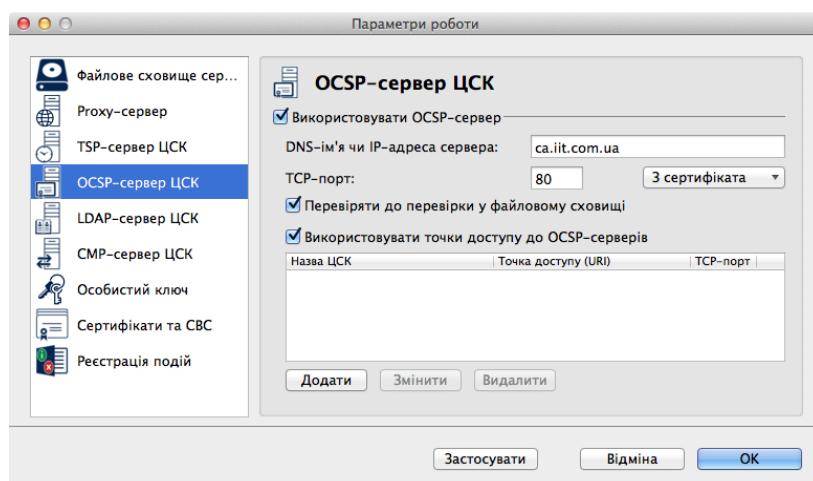


Рисунок Б.4

Для встановлення параметрів доступу до OCSP-серверу з сертифіката OCSP-сервера необхідно натиснути кнопку “З сертифіката” та з випадаючого меню обрати “сервера”.

Для встановлення параметрів доступу до OCSP-серверу з сертифіката користувача необхідно натиснути кнопку “З сертифіката” та з випадаючого меню обрати “користувача”.

Для використання декількох точок доступу необхідно встановити позначку “Використовувати точки доступу до OCSP-серверів” та натиснути “Додати”. У вікні встановлення налаштувань точок доступу до OCSP-серверів (рис. Б.5) необхідно вказати назву, URL-адресу та порт доступу до OCSP-сервера ЦСК. Для автоматичного встановлення всіх необхідних параметрів з сертифіката, необхідно натиснути “З сертифіката”. Для збереження введених налаштувань необхідно натиснути “Додати”.

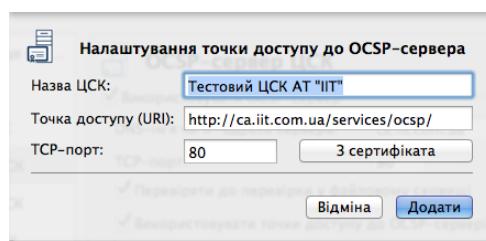


Рисунок Б.5

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

Б.5 LDAP-сервер

Для настроювання параметрів LDAP-сервера перейти до закладки “LDAP-сервер ЦСК” у вікні що наведене на рисунку Б.1. Вікно “Параметри роботи” із сторінкою “LDAP-сервер ЦСК” наведене на рис. Б.6. На сторінці “LDAP-сервер ЦСК” встановлюються наступні параметри роботи програми:

Пор. № зміни	Підпис відпов. особи	Дата внесення

- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я LDAP-сервера.
Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
- “TCP-порт”. Даний параметр встановлює TCP-порт LDAP-сервера.
Як правило це порт протоколу LDAP (389).
- “Анонімний доступ”. Даний параметр встановлює застосування анонімного доступу до LDAP-сервера (без використання імені користувача та паролю).
- “Ім’я користувача”. Даний параметр використовується, якщо не встановлено параметр “Анонімний доступ” та встановлює ім’я користувача LDAP-сервера.
- “Пароль доступу”. Даний параметр використовується, якщо не встановлено параметр “Анонімний доступ” та встановлює пароль доступу користувача до LDAP-сервера.

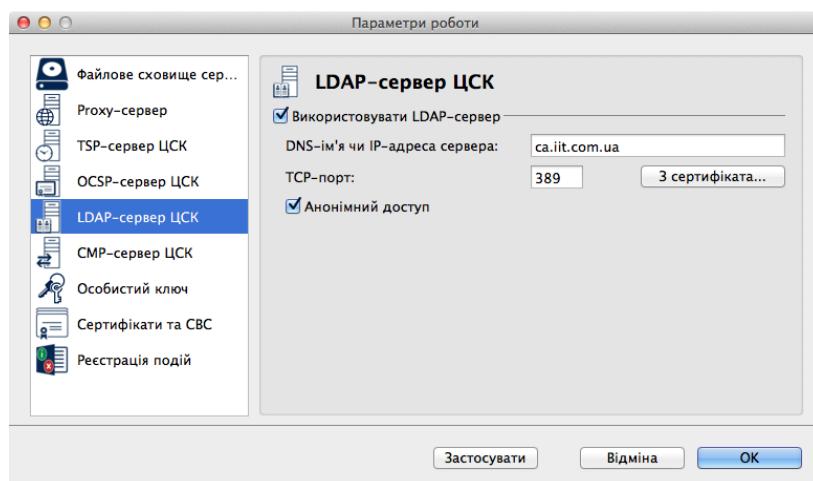


Рисунок Б.6

За замовчанням встановлюються параметри LDAP-сервера що вказані у відповідному сертифікаті сервера або ЦСК. Параметри LDAP-сервера можна також встановити з сертифіката за допомогою кнопки “З сертифіката...”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

Б.6 CMP-сервер

Для настроювання параметрів CMP-сервера необхідно перейти до закладки “CMP-сервер ЦСК” у вікні що наведене на рисунку Б.2. Вікно “Параметри роботи” із сторінкою “CMP-сервер ЦСК” наведене на рис. Б.7. На сторінці “CMP-сервер ЦСК” встановлюються наступні параметри роботи програми:

- “DNS-ім’я чи IP-адреса сервера”. Даний параметр встановлює IP-адресу або DNS-ім’я CMP-сервера.
Як правило це є IP-адреса або DNS-ім’я сервера взаємодії ЦСК.
- “TCP-порт”. Даний параметр встановлює TCP-порт CMP-сервера.
Як правило це порт протоколу HTTP (80).

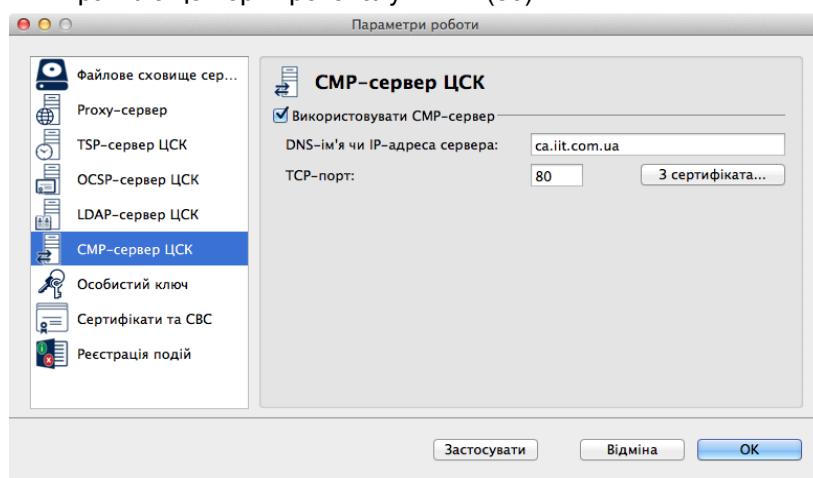


Рисунок Б.7

Пор. № зміни	Підпис відпов. особи	Дата внесення

Параметри CMP-сервера можна також встановити з сертифіката за допомогою кнопки “З сертифіката...”.

Для збереження внесених змін необхідно натиснути кнопку “Застосувати”.

Б.7 Особистий ключ

Для проведення основних операцій з особистим ключем необхідно перейти до розділу "Особистий ключ" у вікні параметрів (рис. Б.8).

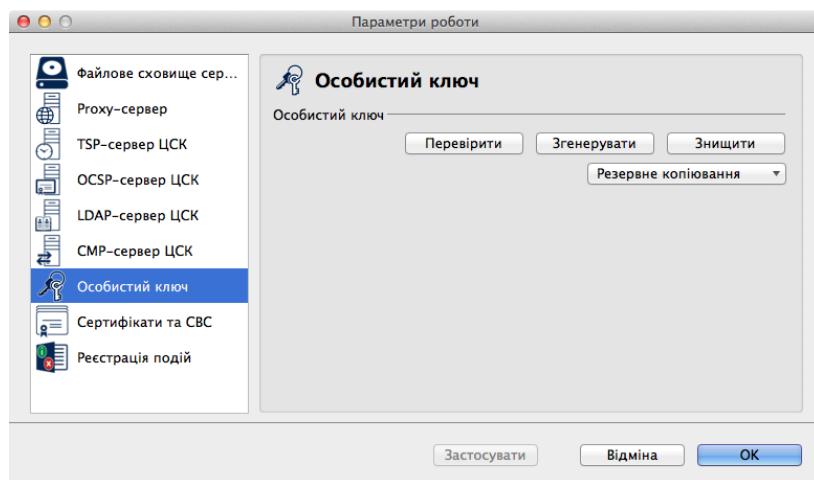


Рисунок Б.8

У розділі “Особистий ключ” є можливість перевірити, згенерувати, знищити та зробити резервне копіювання особистого ключа.

Б.7.1 Перевірити

Виконується перевірка особистого ключа. Для перевірки особистого ключа необхідно натиснути “Перевірити” у розділі “Особистий ключ” (рис. Б.8). Під час перевірки здійснюється зчитування особистого ключа та виконується пошук відповідного сертифіката (рис Б.10).

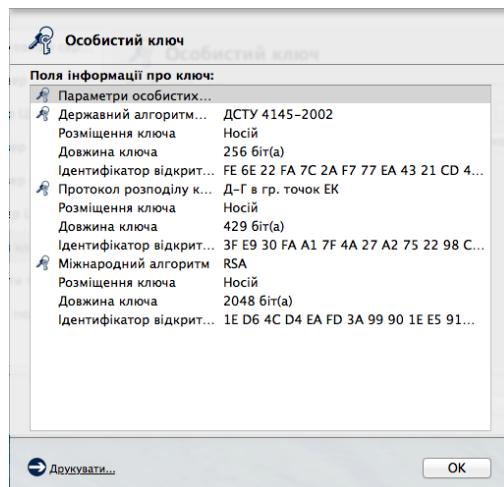


Рисунок 4.9

Пор. № зміни	Підпис відпов. особи	Дата внесення

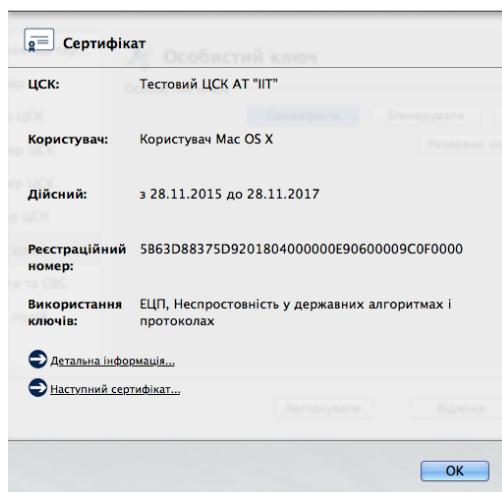


Рисунок Б.10

Б.7.2 Згенерувати

Для генерації ключів необхідно обрати підпункт “Згенерувати” в пункті меню “Особистий ключ” (рис Б.8). На сторінці (рис. Б.11) необхідно обрати алгоритми та протоколи, в яких планується використовувати згенеровані ключі. Для більшості випадків, обирається параметр за замовчанням “Для державних алгоритмів та протоколів.

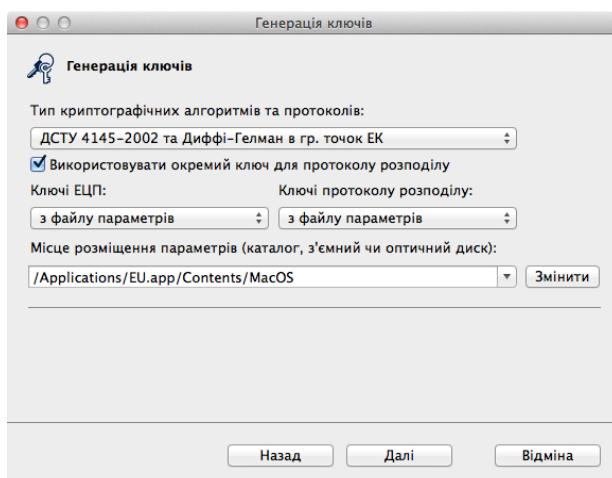


Рисунок Б.11

У випадку необхідності збереження особистого ключа до файлу, потрібно встановити позначку “Зберегти особистий ключ до файлу” (рис. Б.12). У відповідних полях необхідно вказати ім’я та пароль захисту особистого ключа.

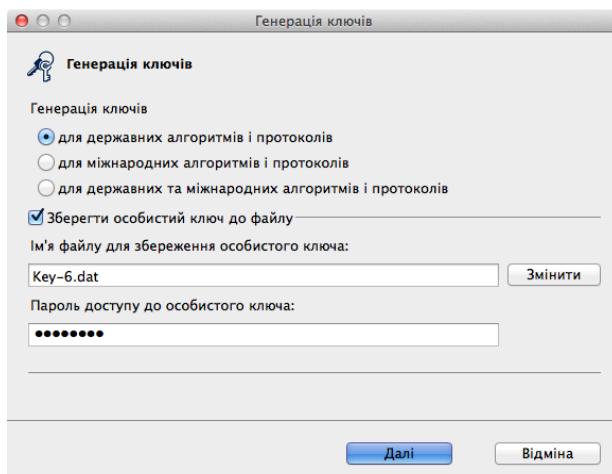


Рисунок Б.12

Пор. № зміни	Підпис відпов. особи	Дата внесення

На наступній сторінці (рис. Б.13) вказати параметри криптографічних алгоритмів та протоколів (для більшості випадків ці параметри можна залишити за замовчанням).

Якщо параметр "Використовувати окремий ключ для протоколу розподілу" встановлено, то буде згенеровано 2 ключа: один для ЕЦП, другий для протоколу розподілу. Якщо параметр не встановлено, то буде згенеровано один ключ, що буде використовуватись як для ЕЦП, так і для зашифрування.

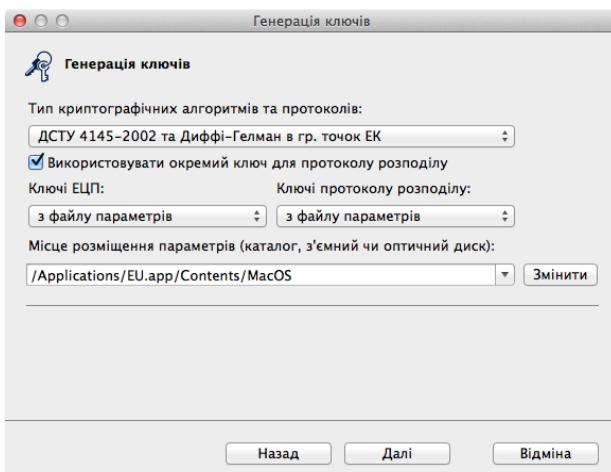


Рисунок Б.13

Далі необхідно встановити НКІ для запису особистого ключа у пристрій запису та на наступній сторінці майстра (рис. Б.14) вказати:

- тип носія ключової інформації (НКІ);
- назву носія;
- пароль доступу до ключового носія (якщо в якості носія використовується криптомодуль) або пароль захисту особистого ключа (з підтвердженням).

Примітка. У випадку встановленої позначки “Зберегти особистий ключ до файлу” (рис. Б.12) вікно, що зображене на рис. Б.14 виведене не буде, а особистий ключ відразу буде записано до файлу.

Ключові носії можуть бути наступних типів:

- з’ємні диски (flash-диски);
- файлова система;
- електронні ключі (“IIT.Кристал-1”, “IIT.Алмаз-1К”, Aladdin eToken R2, PRO, та інші).

Пароль захисту особистого ключа повинен відповідати наступним вимогам:

- довжина - не менше 8 символів;
- не повинен містити однакові символи;
- не повинен містити підряд більше ніж 2 символи з розкладинки клавіатури;
- дозволені символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Примітка. Такі вимоги носять рекомендаційний характер.

Пор. № зміни	Підпис відпов. особи	Дата внесення

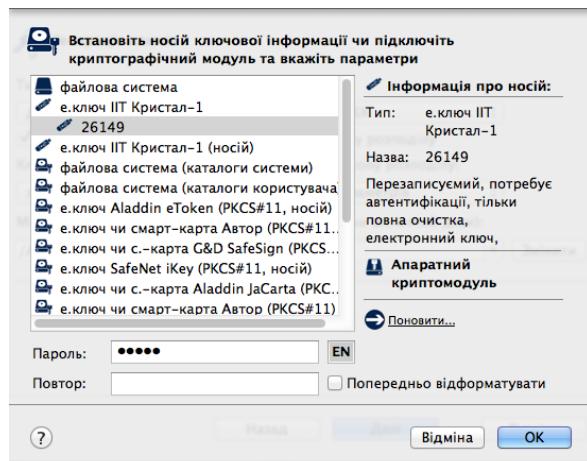


Рисунок Б.14

Після запису особистого ключа на НКІ або до файлу, буде виведено вміст простих запитів на формування сертифікату з відкритим ключем ЕЦП та протоколу розподілу для державних алгоритмів та протоколів (рис. Б.15), після перевірки вмісту простих запитів необхідно натиснути "ОК".

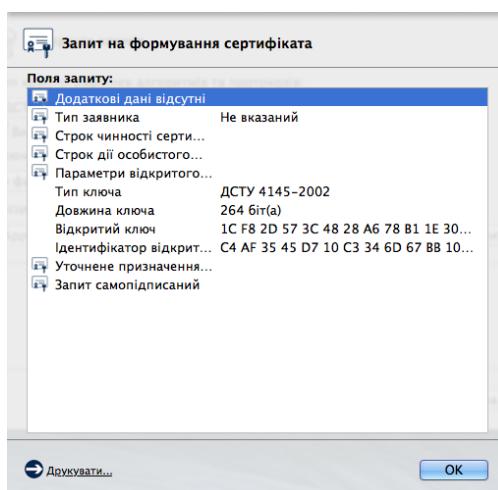


Рисунок Б.15

У наступному вікні (рис. Б.16) необхідно буде вказати ім'я файлів для запису простого запиту на формування сертифікатів з відкритим ключем ЕЦП та протоколу розподілу у файл. Запит повинен бути записаний на носій інформації чи на жорсткий диск. Після цього запит повинен бути переданий у пункт реєстрації ЦСК для формування сертифіката.

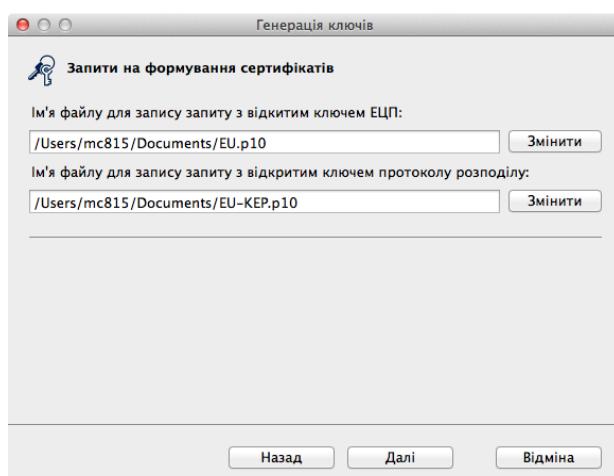


Рисунок Б.16

Пор. № зміни	Підпис відпов. особи	Дата внесення

Після виконання всіх дій майстер завершує свою роботу (рис. Б.17).

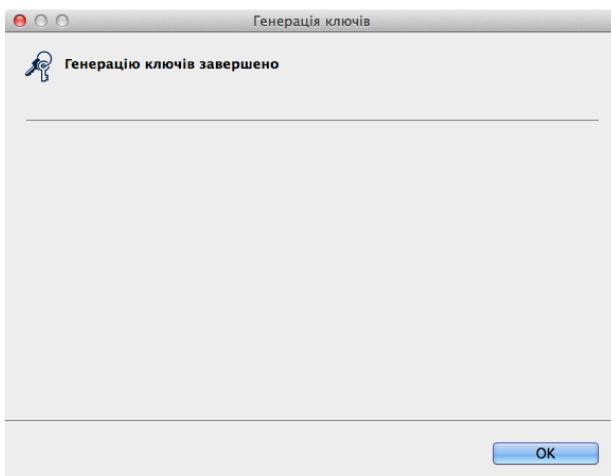


Рисунок Б.17

Б.7.3 Знищити

Особистий ключ на НКІ повинен знищуватись спеціальними засобами, які вбудовані у програму, що забезпечують його гарантоване знищення.

Для знищення особистого ключа необхідно натиснути підпункт "Знищити" пункту меню "Особистий ключ", за допомогою вікна що наведене на рис. Б.18. У вікні вказується носій ключової інформації та пароль. Для знищення необхідно натиснути "Знищити".

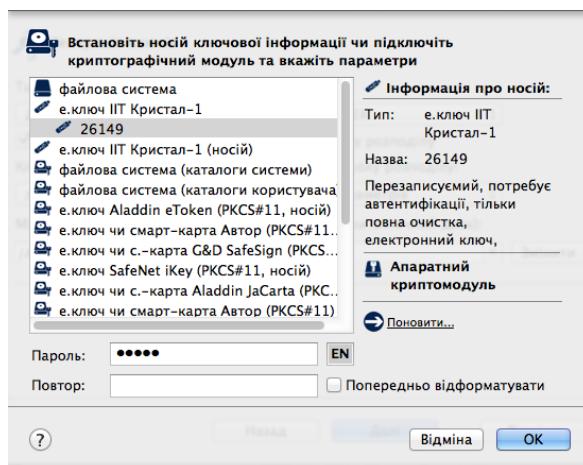


Рисунок Б.18

Б.7.4 Резервне копіювання

Функція дозволяє здійснити резервне копіювання особистого ключа з одного НКІ на інший, з НКІ до файлу та з файлу до НКІ. Для резервного копіювання необхідно натиснути підпункт "Резервне копіювання" пункту меню "Особистий ключ" та обрати режим резервного копіювання (рис. Б.19).

Пор. № зміни	Підпис відпов. особи	Дата внесення

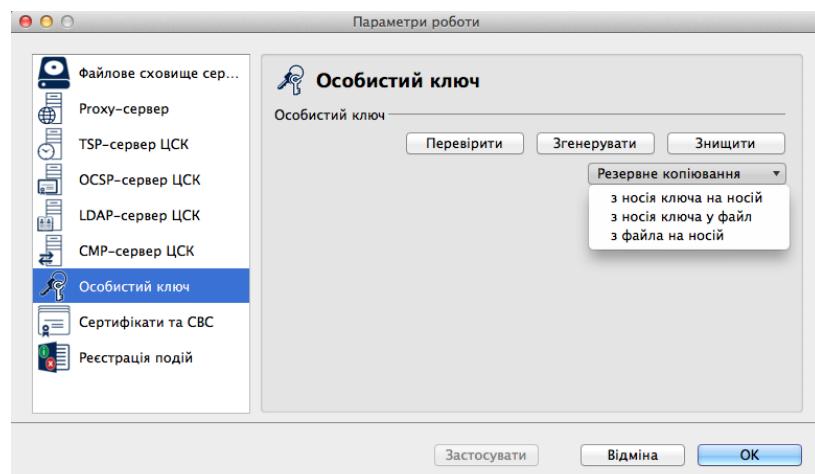


Рисунок Б.19

У випадку резервного копіювання особистого ключа в режимі “з носія на носій”, зчитування особистого ключа здійснюється за допомогою вікна що наведене на рис. Б.9. Запис особистого ключа здійснюється за допомогою вікна що наведене на рис. Б.20.

Увага! Під час резервного копіювання пароль захисту особистого ключа не змінюється.

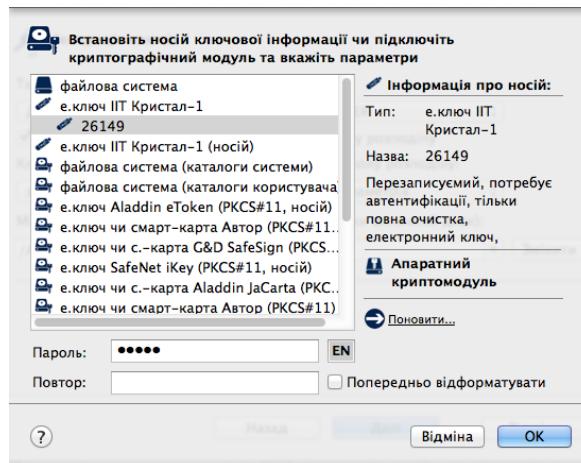


Рисунок Б.20

У випадку резервного копіювання особистого ключа в режимі “з носія у файл”, зчитування особистого ключа здійснюється за допомогою вікна що наведене на рис. Б.9. Запис особистого ключа здійснюється за допомогою вікна що наведене на рис. Б.21

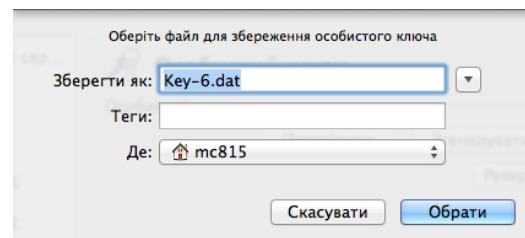


Рисунок Б.21

У випадку резервного копіювання особистого ключа в режимі “з файлу на носій”, зчитування особистого ключа здійснюється за допомогою вікна що наведене на рис. Б.22. Запис особистого ключа здійснюється за допомогою вікна що наведене на рис. Б.20.

Пор. № зміни	Підпис відпов. особи	Дата внесення

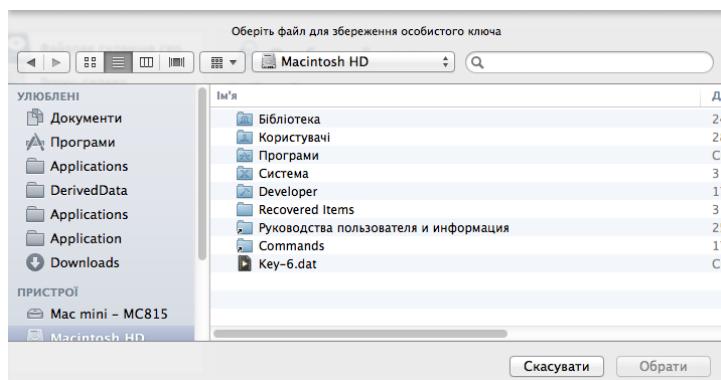


Рисунок Б.22

Примітка. Якщо в якості засобу зберігання особистого ключа використовується електронний ключ “Кристал-1” в апаратному режимі роботи, резервна копія ключа не створюється, оскільки такі засоби не передбачають функції резервного копіювання ключів. Резервну копію особистого ключа можливо створити, якщо особистого ключа зберігається у електронному ключу “Кристал-1” в режимі роботи носій. При цьому під час запису особистого ключа вказується пароль, що був використаний під час зчитування особистого ключа.

Б.8 Сертифікати та СВС

Для перегляду сертифікатів та списків відкліканих сертифікатів необхідно перейти до закладки “Сертифікати та СВС” у вікні, що наведено на рисунку Б.23.

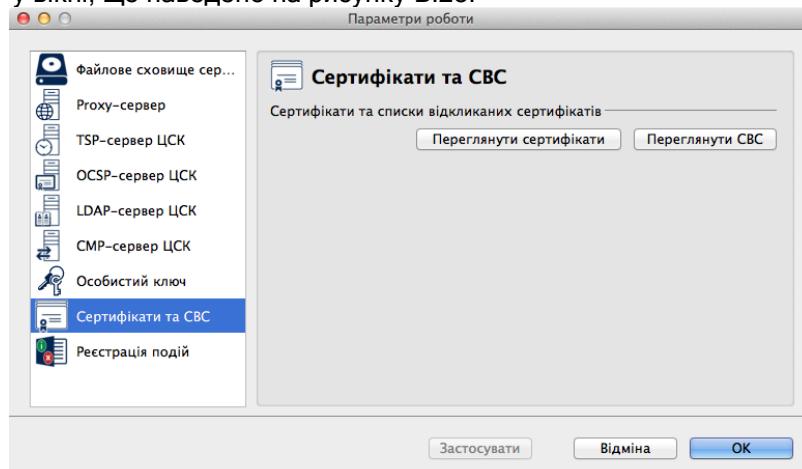


Рисунок Б.23

Б.8.1 Переглянути сертифікати

Для перегляду сертифікатів що містяться у файловому сховищі необхідно натиснути “Переглянути сертифікати” у вікні що наведене на рис. Б.23. Вікно із сертифікатами наведене на рис. Б.24

За допомогою даного вікна можна видаляти сертифікати з файлового сховища, перевіряти та переглядати сертифікати.

Сертифікати у вікні відсортовані за типами власників (тип власника обирається у верхній частині вікна у випадаючому списку):

- всі сертифікати;
- сертифікати центрів сертифікації ключів;
- сертифікати серверів ЦСК;
- сертифікати CMP-серверів;
- сертифікати TSP-серверів
- сертифікати OCSP-серверів
- сертифікати користувачів.

Для перегляду списку сертифікатів власника певного типу необхідно обрати відповідний тип власника у верхній частині вікна у списку що випадає.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Для перегляду сертифіката необхідно натиснути на відповідному записі про сертифікат у списку. Сертифікат буде відображене у вікні, що наведене на рисунку Б.25. Для перегляду детальної інформації, що міститься в сертифікаті необхідно натиснути “Детальна інформація” (рис. Б.26).

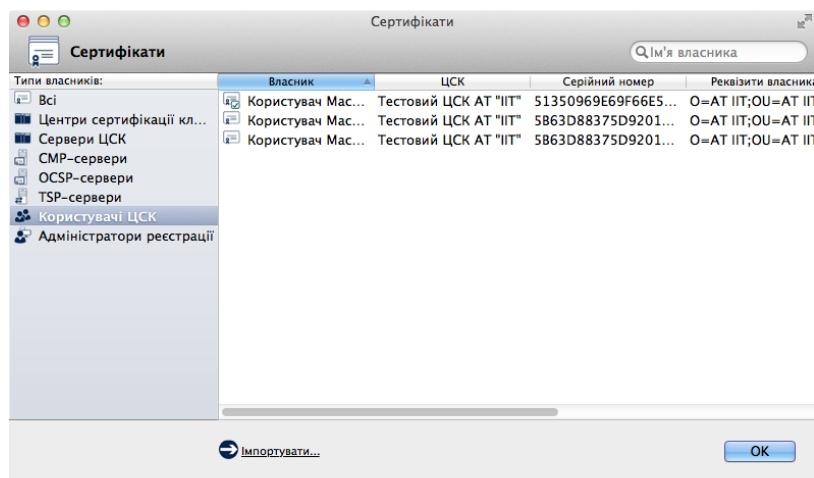


Рисунок Б.24

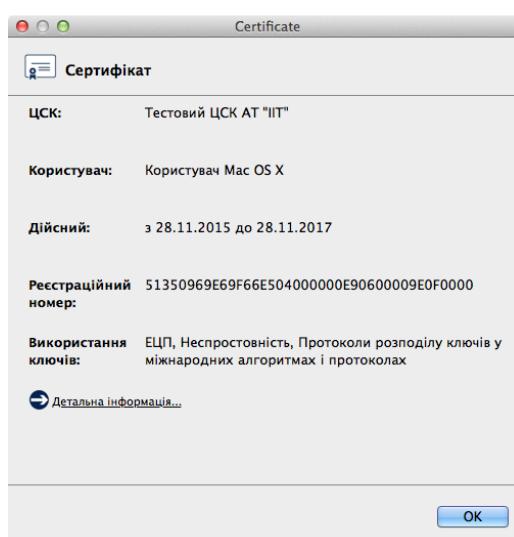


Рисунок Б.25

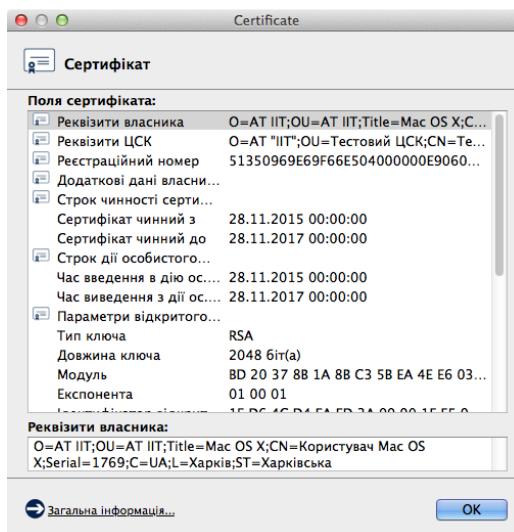


Рисунок Б.26

Для видалення сертифікатів з файлового сховища необхідно виділити у списку відповідні записи про сертифікати та натиснути кнопку “Видалити”.

Пор. № зміни	Підпис відпов. особи	Дата внесення

Для перевірки сертифіката необхідно виділити відповідний запис про сертифікат у списку та натиснути кнопку “Перевірити”. Перевірка сертифіката здійснюється відповідно до встановлених параметрів роботи (див п. Б.4.1-Б.6) - за допомогою CBC, OCSP-протоколу тощо. Результатом перевірки буде вікно що наведене на рис. Б.27. Якщо у цьому вікні натиснути “Сертифікат”, сертифікат буде відображені у вікні детального перегляду (рис. Б.25).

Для імпорту сертифіката до файлового сховища необхідно натиснути “Імпортувати”, та обрати потрібний сертифікат на будь-якому носії інформації.

Для експорту сертифіката з файлового сховища в інше місце (носій інформації тощо), необхідно натиснути “Експортувати”, та обрати інше місце розташування.

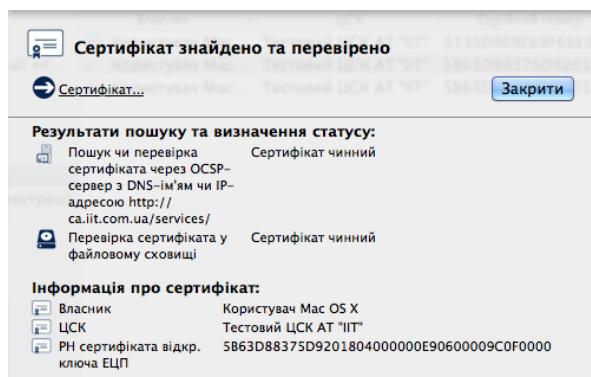


Рисунок Б.27

Б.8.2 Переглянути CBC

Для перегляду списків відкликаних сертифікатів (CBC) що містяться у файловому сховищі необхідно натиснути “Переглянути CBC” у вікні що наведене на рис. Б.25. Вікно із CBC наведене на рис Б.28.

Вікно перегляду CBC дозволяє видаляти CBC з файлового сховища, переглядати CBC та завантажувати CBC з web-сервера ЦСК.

Для перегляду CBC необхідно натиснути на відповідному записі про CBC у списку. CBC буде відображено у вікні що наведене на рисунках Б.29 та Б.30.

Для видалення файла CBC з файлового сховища необхідно виділити відповідний запис про CBC у списку та натиснути кнопку “Видалити”.

Для імпорту CBC до файлового сховища необхідно натиснути “Імпортувати”, та обрати потрібний CBC на будь-якому носії інформації.

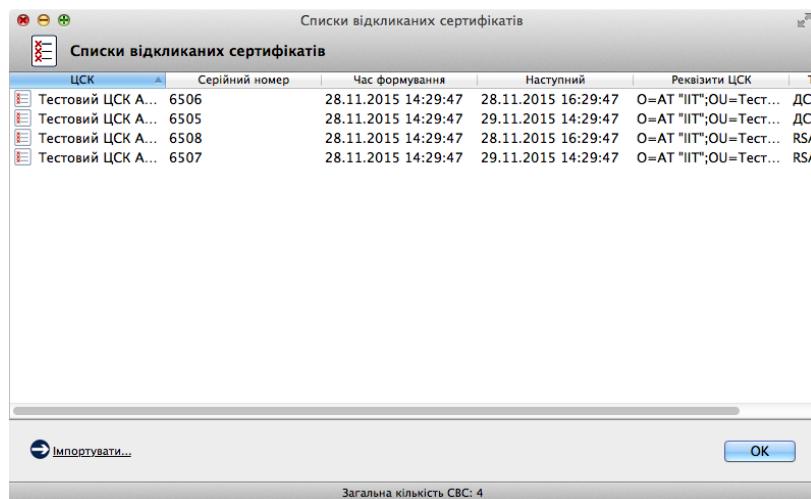


Рисунок Б.28

Пор. № зміни	Підпись відпов. особи	Дата внесення

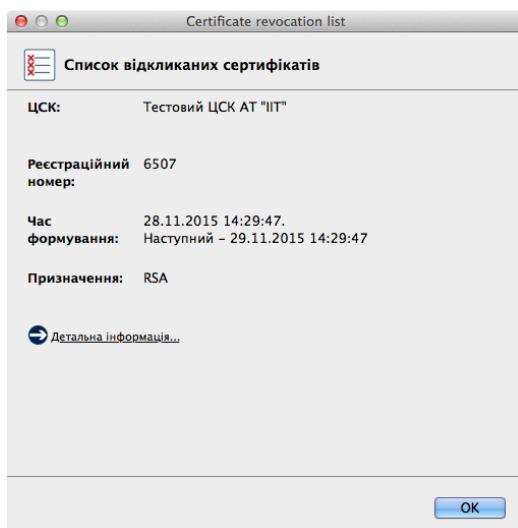


Рисунок Б.29

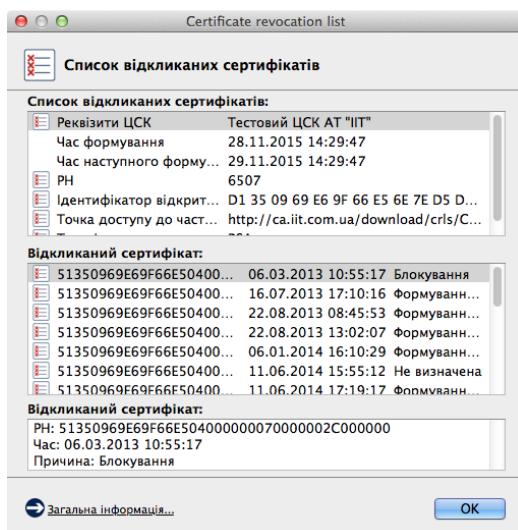


Рисунок Б.30

Б.9 Реєстрація подій

Для встановлення параметрів, які відповідають за реєстрацію подій, що пов'язані з роботою криптобібліотеки, необхідно натиснути “Реєстрація подій” у вікні параметрів роботи (рис. Б.2). Вікно із доступними параметрами наведене на рис. Б.31

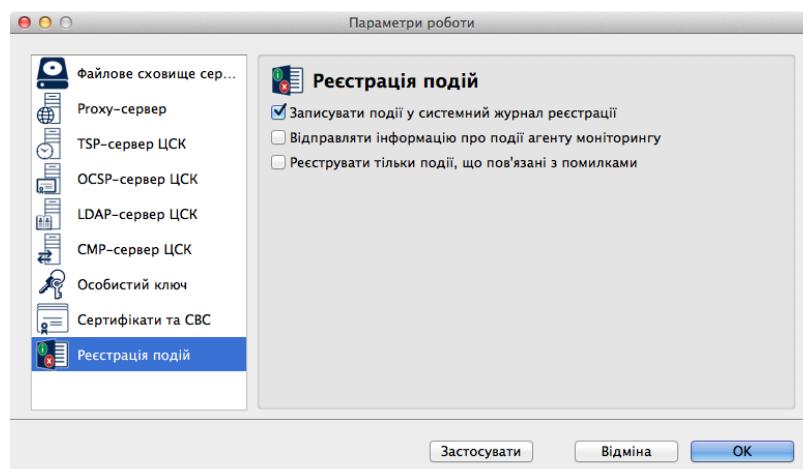


Рисунок Б.31

Пор. № зміни	Підпис відпов. особи	Дата внесення

Доступні наступні параметри реєстрації подій:

- Записувати події у системний журнал реєстрації;
- Відправляти інформацію агенту моніторингу;
- Реєстрації подій, що пов'язані з помилками.

У випадку встановлення параметру “Відправляти інформацію агенту моніторингу” необхідно вказати DNS-ім’я чи IP-адресу та порт агента моніторингу (рис. Б.32), що повинен бути заздалегідь встановлений та налаштований.

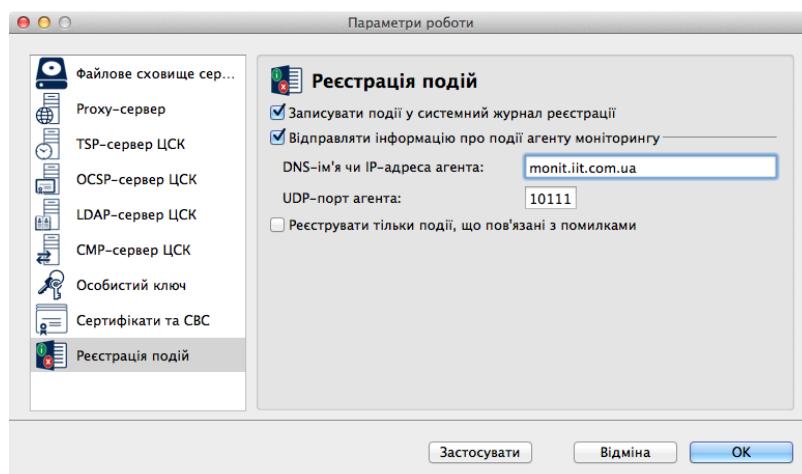


Рисунок Б.32

У випадку встановлення параметру “Реєструвати події, що пов’язані з помилками ” до системного журналу ОС будуть заноситись тільки повідомлення, що пов’язані з помилками в роботі криптобібліотеки.

Пор. № зміни	Підпис відпов. особи	Дата внесення