Програмний комплекс IIT Користувача ЦСК Версія 1.3.1



АНОТАЦІЯ

2

Даний документ містить настанову оператора для роботи з програмним комплексом користувача центра сертифікації ключів (далі – програма). Настанова містить відомості щодо послідовності та особливостям інсталяції, встановлення параметрів роботи та використання програми.







ЗМІСТ

1 ПРИЗНАЧЕННЯ ПРОГРАМИ	4
2 УМОВИ ВИКОНАННЯ ПРОГРАМИ	5
З ІНСТАЛЯЦІЯ ПРОГРАМИ	6
4 ПОЧАТОК РОБОТИ З ПРОГРАМОЮ	9
4.1 Завантаження програми	9
4.2 Встановлення параметрів роботи програми	9
4.2.1 Файлове сховище	10
4.2.2 Ргоху-сервер	
4.2.3 ТБР-сервер 4.2.4 ОСSP-сервер	
4.2.5 LDAP-сервер	
4.2.6 СМР-сервер	13
4.3 Режими роботи програми	14
5 УПРАВЛІННЯ СЕРТИФІКАТАМИ ТА СВС	15
5.1 Отримання сертифікатів з ЦСК	15
5.2 Зчитування сертифікатів та CBC	16
5.3 Перегляд сертифікатів	16
5.4 Перегляд СВС	18
5.5 Завантаження СВС	19
5.6 Блокування власного сертифіката	19
5.7 Формування нового сертифіката	20
5.7.1 Передача запита за допомогою сервера обробки запитів ЦСК	
5.7.2 Передача запита засобами електронної пошти 5.7.3 Передача запита за допомогою файлу запита	24 24
5.8 Помилки, що можуть виникати під час роботи програми	
6 УПРАВЛІННЯ КЛЮЧАМИ	
6.1 Генерація ключів	27
6.2.3читування особистого ключа	
6.3 Резервне коліювання особистого ключа	
6.4 Зміна паролю захисту особистого ключа	
6.5 Знишення особистого ключа на носієві	
6.6 Знищення особистого ключа в пам'яті ПЕОМ	
6.7 Перегляд власного сертифіката	
6.8 Помилки, що можуть виникати під час роботи програми	
7 ЗАХИСТ ФАЙЛІВ	35
7.1 Підпис файлів	
7.2 Перевірка файлів	
7.3 Зашифрування файлів	
7.4 Розшифрування файлів	40
7.5 Помилки, що можуть виникати під час роботи програми	42
8 ПОВІДОМЛЕННЯ ОПЕРАТОРУ ТА ДОВІДКОВА СИСТЕМА	44
8.1 Перехід до web-сайту центра сертифікації ключів	44
8.2 Перегляд настанови оператору	44
ПЕРЕЛІК СКОРОЧЕНЬ	45







1 ПРИЗНАЧЕННЯ ПРОГРАМИ

Програма призначена для застосування на засобах ЕОТ користувача центра сертифікації ключів 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 HKI на інший;
 - зміну паролю захисту особистого ключа;
 - знищення особистого ключа на HKI;
 - 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 ОСЅР;
 - перевірку чинності та цілісності сертифікатів та ін.;
- захист файлів користувача:
 - підпис файлів;
 - перевірку файлів;
 - зашифрування файлів;
 - розшифрування файлів.





2 УМОВИ ВИКОНАННЯ ПРОГРАМИ

Програма може бути завантажена та виконана на ЕОМ під керуванням ОС Microsoft Windows XP/Vista/ Windows 7/8/8.1/ Windows 10/2003 Server/2008 Server/







3 ІНСТАЛЯЦІЯ ПРОГРАМИ

Щоб почати використовувати програмне забезпечення, спочатку потрібно її завантажити з web-сторінки АЦСК «Masterkey» та запустити програму інсталяції (майстер інсталяції) **EUArtMInstall.exe**.

Програмний комплекс користувача (комп'ютерна програма) «IIT Користувач ЦСК-1.3» <u>https://masterkey.ua/download/EUArtMInstall.exe</u>

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".

🔄 IIT Користувач ЦСК-1.3 (для ЦСК MASTERKEY). Інстал – 🗖 💌
Ліцензійна угода Прочитайте цю важливу інформацію перед продовженням.
Прочитайте ліцензійну угоду. Ви повинні погодитися з умовами цієї угоди перед продовженням інсталяції.
Піцензійна угода на програмний комплекс користувача ЦСК "IIT Користувач ЦСК-1" Програма являє собою комп'ютерну програму, записану на відповідних носіях, та будь-яку "вбудовану" або електронну документацію. Встановлюючи, копіюючи або іншим чином використовуючи програму, Ви тим самим приймаєте на себе умови цієї угоди. Якщо Ви не приймаєте умов цієї угоди, негайно скасуйте інсталяцію програми. Програма захищена законами і міжнародними угодами про авторське право, а також іншими законами і договорами, що мають відношення до
< <u>Н</u> азад Далі > Відміна

Рисунок 3.2

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







🌆 IIT Користувач ЦСК-1.3 (для ЦСК MASTERKEY). Інстал 😑 🗖 💌
Оберіть каталог для інсталяції програми Куди необхідно інсталювати програму?
Програма буде інстальована у наступний каталог.
Для продовження, натисніть Далі. Для вибору іншого каталогу, натисніть Змінити.
tute of Informational Technologies\Cettificate Authority-1.3\End User Змінити
< <u>Н</u> азад Далі > Відміна



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

🔄 IIT Користувач ЦСК-1.3 (для ЦСК MASTERKEY). Інстал 😑 🗖 💌
Вкажіть каталог меню Пуск Де потрібно розмістити значки швидкого запуску програми?
Значки швидкого запуску програми будуть записані у наступний каталог меню Пуск.
Для продовження, натисніть Далі. Для вибору іншого каталогу, натисніть Змінити.
IIT-Користувач ЦСК-1.3 Змінити
< <u>Н</u> азад Далі > Відміна

Рисунок 3.4

На наступній сторінці майстра (рис. 3.5) необхідно вказати каталог до якого будуть завантажуватись та зберігатися сертифікати і СВС. У параметрах роботи самої програми даний каталог визначається як "Каталог з сертифікатами та СВС" у параметрах файлового сховища (див. п. 4.2.2). Для зміни каталогу необхідно натиснути кнопку "Змінити" та обрати існуючий каталог чи створити новий. Для продовження інсталяції необхідно натиснути кнопку "Далі".

🔄 IIT Користувач ЦСК-1.3 (для ЦС	CK MASTERKEY). Інстал	• ×
Встановіть налаштування криптогр Налаштування криптографічної бібліот Використовувати іх?	рафічної бібліотеки теки знайдені в реєстрі.	A
Залишити налаштування без змін Вкажіть каталог для сертифікатів та С каталогу, натисніть Змінити.	СВС, натисніть Далі. Для вибој	ру іншого
C:\My Certificates and CRLs 13		З <u>м</u> інити
	< <u>Н</u> азад Далі >	Відміна
-	0.5	

Рисунок 3.5



Центральний офіс ТОВ «Арт-мастер» ул. Сурикова, 3 (літ А), Київ, 03035, Україна ел.: + 380 44 248-97-91, 248-89-27, факс: + 380 44 248-98-14 ⊩mail: post@am-soft.ua; http://www.am-soft.ua





На наступній сторінці майстра (рис. 3.6) потрібно встановити признаки необхідності виконання майстром додаткових завдань - створення значку запуску програми на робочому столі та запуску програми після завершення інсталяції. Для продовження інсталяції необхідно натиснути кнопку "Далі".

🔄 IIT Користувач ЦСК-1.3 (для ЦСК MASTERKEY). Інстал – 🗖 💌
Оберіть додаткові задачі Які додаткові задачі мають бути виконані?
Оберіть додаткові задачі, що програма інсталяції повинна виконати, потім натисніть Далі.
Додаткові значки:
Створити значок на робочому стол
Інші завдання:
Завантажити програму після інсталяції
(Hana Dari) Dimina
Рисунок 3.6

На наступній сторінці майстра (рис. 3.7) буде виведено інформацію про операції, що будуть виконані майстром. Для виконання інсталяції необхідно натиснути кнопку "Встановити".

🌄 IIT Користувач ЦСК-1.3 (для ЦСК MASTERKEY). Інстал 🗧	□ ×
Готовність до інсталяції Все готово до інсталяції IIT Користувач ЦСК-1.3 (для ЦСК MASTERKEY).	A
Натисніть Встановити для продовження інсталяції або натисніть Назад, як хочете переглянути або змінити деякі параметри.	що ви
Програмна група: IIT-Користувач ЦСК-1.3 Додаткові задачі: Додаткові значки: Створити значок на робочому столі	^
<	> Відміна
Duewey 2.7	

Рисунок 3.7

Після інсталяції програми, майстер завершує свою роботу.

Якщо було встановлено признак необхідності завантаження програми після інсталяції, то після завершення роботи майстра буде автоматично завантажено інстальовану програму.

Під час інсталяції також встановлюються драйвери електронного ключа "IIT. Кристал-1". Під час інсталяції драйверів може бути видане наступне вікно (рис. 3.8) із попередженням про можливу несумісність драйверів електронного ключа із ОС. Необхідно натиснути "Все равно продолжить".

Устано	вка оборудования
⚠	Программное обеспечение, устанавливаение дия
	Контроллеры универсальной последовательной шины USB
	не тестировалось на совместимость с Windows XP. (Подробнее о таком тестировании.)
	Установка этого программного обеспечения может нарушить рабиту системы. Міскохоїї рекоменяцет прекратить установку и обратиться к постаошику программного обеспечения за версней, прошедшей проворку на совмостимость.
	Все равно дродолжить Прекратить установку
	Рисунок 3.8



Центральний офіс ТОВ «Арт-мастер» вул. Сурикова, 3 (літ А), Київ, 03035, Україна тел. +380 44 248-97-1, 248-89-87, фак: -380 44 248-98-14 е-mail: post@am-soft.ua; http://www.am-soft.ua





4 ПОЧАТОК РОБОТИ З ПРОГРАМОЮ

4.1 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 CBC (за необхідністю).

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

Для завантаження діючих сертифікатів АЦСК переходимо на web-сторінки АЦСК «Masterkey» за наступним посиланням та загружаємо усі діючи сертифікати у відповідну директорію програмного забезпечення «**IIT Користувач ЦСК-1.3**» <u>https://masterkey.ua/ca/ca-certificates?lang=ru</u>

Для завантаження програми необхідно запустити модуль, що виконується **EUArtMInstall.exe** через файловий менеджер ОС або через меню "Пуск", обравши у розділі "IIT\Користувач ЦСК-1" підпункт "Користувач ЦСК" чи за допомогою значку на робочому столі. Після запуску на екрані буде відображене головне вікно програми, що наведене на рис. 4.1.

2		Користувач І	ЦСК			-		×
Файли Текст	Особистий ключ	Сертифікати та СВС	Парам	етри	Допомога			
MASTE	RKEY							
Оберіт	ь завданн	เя						
Під Клю	писати файли пис файлів на особ очеві	истому		Перев Перев файла	вірити фай л ірка ЕЦП на і х	ни підписа	IHVX	
Заи одн	шифрувати файл шифрування файлів юго чи декількох ко	и на орис		Розш Розши зашиф	ифрувати ф фрування фрованих фай	райли лів		
	реглянути серти регляд сертифікатів Аловому сховищі	фікати з у	×=	Перег Перег схови	глянути СВ ляд СВС у фа щі	С йловом	ny	
Додаткое С Перей	30 іти до web-сайту Ц(СК						
•								

Рисунок 4.1

4.2 Встановлення параметрів роботи програми

Програма інсталяції під час свого виконання встановлює параметри роботи програми за замовчанням. При цьому встановлюються лише параметри файлового сховища з сертифікатами та CBC.

Для встановлення чи зміни параметрів роботи програми необхідно обрати підпункт "Встановити" в пункті меню "Параметри" (рис. 4.1). Вікно встановлення параметрів наведене на рис. 4.2.







	Параметри роботи
Файлове сховище Ргоху-сервер	СВС Параметри Файлового сховища
ТSР-сервер	Каталог s сертифікатами та CBC: C:\My Certificates and CRLs 13 Змінити
ОСЅР-сервер	☑ Автоматично перечитувати при виявленні змін
СМР-сервер	✓ Зберігати сертифікати, що отримані з ОСЅР-, LDAP-чи СМР-серверів Час зберігання стану перевіреного сертифіката, с: 3600
📌 Особистий ключ	Перевіряти Свс
сертифікати та СВС	
Гесстрація подій	
	ОК Відміна Застосувать
	Рисунок 4 2

4.2.1 Файлове сховище

Для настроювання параметрів файлового сховища сертифікатів та СВС необхідно перейти до закладки "Файлове сховище". Вікно "Параметри роботи" із сторінкою "Файлове сховище" наведене на рис. 4.2. На цій сторінці встановлюються наступні параметри роботи програми:

- "Каталог з сертифікатами та СВС". Даний параметр встановлює каталог файлового сховища для зберігання сертифікатів та СВС.
 - Всі сертифікати та СВС, 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 СВС у каталог чи видалення файлу з сертифікатом або СВС).
 - Якщо параметр не встановлено необхідно виконувати повторне зчитування файлового сховища після внесення змін. Для цього необхідно обрати підпункт "Зчитати сертифікати та CBC" в пункті меню "Сертифікати та CBC" або натиснути клавішу "F9" у головному вікні програми.
- "Зберігати сертифікати, що отримані з OCSP- чи LDAP-серверів". Даний параметр визначає необхідність автоматичного збереження сертифікатів, що не знайдені у файловому сховищі, а отримані з OCSP- чи LDAP-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 СВС". Параметр вказує на необхідність використання СВС в якості засобу перевірки статусу сертифікатів відкритих ключів що використовуються.
- "Тільки свого ЦСК". Даний параметр визначає необхідність використовувати при перевірці сертифікатів СВС 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 СВС (повного та часткового) при здійсненні перевірки сертифікатів.
 - Якщо параметр не встановлено достатньо лише одного повного діючого СВС. Даний параметр дозволяє не виконувати постійне завантаження останнього діючого часткового CBC.
- "Завантажувати автоматично". Даний параметр визначає можливість автоматичного завантаження СВС під час перевірки статусу сертифікатів, якщо у файловому сховищі не знайдено діючих СВС.
 - Параметр має сенс якщо у сертифікатах ЦСК, або серверів ЦСК встановлено шлях отримання СВС.

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".







4.2.2 Proxy-сервер

«**Proxy- сервер»** прописуємо якщо він у Вас використовується. Для настроювання параметрів proxyсервера необхідно перейти до закладки "Proxy-сервер" у вікні що наведене на рисунку 4.2. Вікно "Параметри роботи" із сторінкою "Proxy-сервер" наведене на рис. 4.3. 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.
- "Ім'я чи IP-адреса сервера". Даний параметр встановлює IP-адресу або DNS-ім'я proxy-сервера.
- "TCP-порт". Даний параметр встановлює TCP-порт ргоху-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 ргоху-сервера.
 - Якщо proxy-сервер працює в режимі без автентифікації даний параметр може не вводитися.
- "Зберегти пароль". Даний параметр встановлює необхідність зберігати пароль доступу до proxyсервера у реєстрі ОС.

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

Ранлосе сховище Рлжу-сервер ТSР-сервер LDAP-сервер СМР-сервер Особистий ключ Сертифікати та СВС Реестрація подій	
---	---------------------

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

4.2.3 TSP-сервер

Для настроювання параметрів TSP-сервера необхідно перейти до закладки "TSP-сервер" у вікні що наведене на рисунку 4.2. Вікно "Параметри роботи" із сторінкою "TSP-сервер" наведене на рис. 4.4. На сторінці "TSP-сервер" встановлюються наступні параметри роботи програми:

- "Ім'я чи ІР-адреса сервера". Даний параметр встановлює ІР-адресу або DNS-ім'я TSP-сервера.
 Як правило це є ІР-адреса або DNS-ім'я сервера взаємодії ЦСК.
- "TCP-порт". Даний параметр встановлює TCP-порт TSP-сервера.
 Як правило це порт протоколу HTTP (80).







Файлове сховище Ргоху-сервер	ТSP-сервер Ц Отримувати позначки часу Отримувати позначки часу	ļСК	
TSP-сервер	DNS-ім'я чи IP-адреса сервера:	: masterkey.ua	
OCSP-сервер	ТСР-порт:	80	3 сертифіката
LDAP-сервер			
СМР-сервер			
Особистий ключ			
Сертифікати та СВС			
Реєстрація подій			

Для встановлення параметрів доступу до TSP-серверу з сертифіката сервера необхідно натиснути кнопку "З сертифіката сервера...".

Для встановлення параметрів доступу до TSP-серверу з сертифіката користувача необхідно натиснути кнопку "З сертифіката користувача...".

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

4.2.4 OCSP-сервер

Для настроювання параметрів OCSP-сервера необхідно перейти до закладки "OCSP-сервер" у вікні що наведене на рисунку 4.2. Вікно "Параметри роботи" із сторінкою "OCSP-сервер" наведене на рис. 4.5. На сторінці "OCSP-сервер" встановлюються наступні параметри роботи програми:

- "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 статус сертифікатів через OCSP 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 необхідністю) за допомогою OCSP-протоколу.

Фаилове сховище Ртоху-сервер	 ОСЅР-сервер Ц(Використовувати ОСЅР-сервер — 	СК
TSP-сервер	DNS-ім'я чи IP-адреса сервера: ma:	sterkey.ua
OCSP-сервер	ТСР-порт; 80	3 сертифікат
СМР-сервер	Використовувати точки доступу	до OCSP-серверів
Особистий ключ Сертифікати та СВС Реестрація подій		

Рисунок 4.5



(ентральний офіс ТОВ «Арт-мастер» уп. Сурикова, 3 (піт А), Київ, 03035, Україна еп. ÷ 380 44 248-97-91, 248-89-27, факс: +380 44 248-98-14 -mail: post@am-soft.ua; http://www.am-soft.ua





Для встановлення параметрів доступу до OCSP-серверу з сертифіката сервера необхідно натиснути кнопку "З сертифіката сервера...".

Для встановлення параметрів доступу до OCSP-серверу з сертифіката користувача необхідно натиснути кнопку "З сертифіката користувача...".

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

4.2.5 LDAP-сервер

Для настроювання параметрів LDAP-сервера перейти до закладки "LDAP-сервер" у вікні що наведене на рисунку 4.2. Вікно "Параметри роботи" із сторінкою "LDAP-сервер" наведене на рис. 4.6. На сторінці "LDAP-сервер" встановлюються наступні параметри роботи програми:

- "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.
- "Шукати сертифікати у LDAP-каталозі". Даний параметр встановлює необхідність пошуку сертифікатів у LDAP-каталозі, у випадку якщо сертифікат не знайдено у файловому сховищі та за допомогою OCSP-протоколу.

Файлове сховище Рюху-сервер	 LDAP-сервер Використовувати LDAP-сервер DNS ім'я чи IP-здреса сервера 			
ОСЅР-сервер	ТСР-порт:	389		З сертифіката
LDAP-сервер CMP-сервер CMP-сервер Cособистий ключ Cертифікати та CBC Peecтрація подій	✓ Анонімний доступ			
		ОК	Відміна	а Застосува

Рисунок 4.6

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".

4.2.6 СМР-сервер

Для настроювання параметрів СМР-сервера необхідно перейти до закладки "СМР-сервер" у вікні що наведене на рисунку 4.2. Вікно "Параметри роботи" із сторінкою "СМР-сервер" наведене на рис. 4.7. На сторінці "СМР-сервер" встановлюються наступні параметри роботи програми:

- "Ім'я чи ІР-адреса сервера". Даний параметр встановлює ІР-адресу або DNS-ім'я СМР-сервера.
 Як правило це є ІР-адреса або DNS-ім'я сервера взаємодії ЦСК.
- "TCP-порт". Даний параметр встановлює TCP-порт СМР-сервера. Як правило це порт протоколу HTTP (80).



нтральний офіс ТОВ «Арт-мастер» . Сурикова, 3 (літ А), Київ. 03035, Україна .: +380 44 248-97-91, 248-98-27, факс: +380 44 248-98-14 ail: post@am-soft.ua; http://www.am-soft.ua



Файлове сховище Ргоху-сервер	СМР-сервер L	цск		
ТЅР-сервер	DNS-ім'я чи IP-адреса сервера:	masterkey ua		
OCSP-сервер	TCF-nopt:	80	3	сертифіката
LDAP-сервер				
СМР-сервер				
Особистий ключ				
6				
Сертифікати та СВС				
Сертифікати та СВС				
Сертифікати та СВС				

Параметри СМР-сервера можна також встановити з сертифіката за допомогою кнопки "З сертифіката...".

Для збереження внесених змін необхідно натиснути кнопку "Застосувати".

4.3 Режими роботи програми

Програма може працювати у двох режимах:

- режим on-line (із взаємодією з ЦСК);
- режим off-line (без взаємодії з ЦСК).

В першому режимі програма може взаємодіяти з ЦСК (отримувати позначки часу, використовувати ОСЅР-протокол, завантажувати СВС з web-сервера тощо).

У другому режимі програма не взаємодіє з ЦСК, навіть якщо встановлені параметри серверів ЦСК. Даний режим використовується для роботи без підключення до мережі Internet без зміни встановлених параметрів.

Для встановлення режиму роботи з ЦСК необхідно обрати підпункт меню "Перейти в режим off-line (не взаємодіяти з ЦСК)/Перейти в режим on-line (взаємодіяти з ЦСК)" в пункті меню "Параметри".

Якщо програма працює у режимі off-line інформацію про це буде виведено до нижньої частини головного вікна програми (рис.4.8).

2	Користувач	ЦСК		- 🗆	×
Файли Текст Особистий кл	оч Сертифікати та СВС	Параметри	Допомога		
MASTERKEY					
Оберіть завда	ння				
Підписати файл Підпис файлів на ключеві	и собистому	Карайл Пере Файл	звірити файл вірка ЕЦП на п ах	и ідписаних	
Зашифрувати ф Зашифрування фа одного чи декільк	айли йлів на эх корис	Розш Розш заши	инфрувати ф а ифрування фрованих файл	айли іів	
Переглянути с Перегляд сертиф файловому схови	ртифікати катів у ці	Карана Карана Схови	эглянути СВС гляд СВС у фай ищі	іловому	
Додатково Сперейти до web-сай	у ЦСК				

Рисунок 4.8



Центральний офіс ТОВ «Арт-мастер» аул. Сурикова, 3 (літ А), Київ. 03035, Україна тел.: +380 44 248-97-91, 248-89-27, факс: +380 44 248-98-14 а-mail: post⊚am-soft.ua; http://www.am-soft.ua





5 УПРАВЛІННЯ СЕРТИФІКАТАМИ ТА СВС

5.1 Отримання сертифікатів з ЦСК

Програма має засоби для отримання набору сертифікатів з ЦСК за допомогою запиту до сервера обробки запитів. До пакету сертифікатів входять сертифікат ЦЗО (якщо ЦСК акредитований), сертифікат ЦСК, сертифікати центральних серверів ЦСК (СМР, TSP, OCSP), та сертифікат користувача що робить запит. Запит формується за допомогою особистого ключа користувача.

Для отримання пакету сертифікатів необхідно обрати підпункт "Отримати з ЦСК..." в пункті меню "Сертифікати та СВС". Після чого буде виведене вікно що наведене на рис. 5.1. У вікні необхідно натиснути "Далі", після чого буде проведене зчитування особистого ключа користувача (більш детально у п.п. 6.2). Після отримання пакету сертифікатів користувачу буде виведене діалогове вікно (рис. 5.3) із переліком сертифікатів та пропозицією щодо збереження їх до файлового сховища. Для роботи із сертифікатами їх необхідно зберегти до файлового сховища.

Отримання набору сертифікатів з ЦСК	×
Отримати сертифікати з ЦСК	
Через сервер обробки запитів ЦСК (НТТР)	
Далі > Відміна	



Після зчитування особистого ключа буде виведене вікно (рис. 5.2) у якому необхідно вказати параметри доступу до сервера взаємодії ЦСК. **Ргоху- сервер** прописуємо якщо він у Вас використовується.

Отримання набор	ру сертифі	катів з ЦСК		×
Відправка запиту до	о серве	ра ЦСК		
DNS-ім'я чи IP-адреса сервера ЦСК: m TCP-порт: 8	asterkey.ua			
DNS-ім'я чи IP-адреса сервера:		ТСР-пор	т:	
	< Назад	Далi >	Відміна	9
Рису	нок 5.2			
Завантажені серт	гифікати		×	
Завантажені з СМР- Користувач_0023 СМР-сервер Тесто СМР-сервер Тесто ОСSP-сервер Тесто Тестовий ЦСК АТ Імпортувати іх у фа	сервера ЦСК с увий ЦСК АТ II увий ЦСК АТ II говий ЦСК АТ I IIT (в. 1.3) йлове сховище	ертифікати: Т (в. 1.3) Т (в. 1.3) IIT (в. 1.3) IIT (в. 1.3) е сертифікатів?		
	<u>Y</u> es	<u>N</u> o		

Рисунок 5.3



Центральний офіс ТОВ «Арт-мастер» вул. Сурикова, 3 (літ А), Київ, 03035, Україна тел. + 380 44 248-379.1 248-89-27, факс. + 380 44 248-98-14 е-mail: post@am-soft.ua; http://www.am-soft.ua





5.2 Зчитування сертифікатів та CBC

Програма автоматично виконує зчитування сертифікатів та СВС з файлового сховища при першій необхідності після свого запуску. При внесенні змін (запису чи видалення сертифікатів чи СВС) до файлового сховища під час роботи програми, якщо не встановлено параметр "Автоматично перечитувати файлове сховище при виявленні змін" (див п. 4.2.1), необхідно перечитати файлове сховище. Для цього необхідно обрати підпункт "Зчитати сертифікати та СВС" в пункті меню "Сертифікати та СВС" або натиснути клавішу F9.

5.3 Перегляд сертифікатів

Для перегляду сертифікатів що містяться у файловому сховищі необхідно обрати підпункт "Переглянути сертифікати..." в пункті меню "Сертифікати та СВС" або натиснути клавішу F10. Вікно із сертифікатами наведене на рис. 5.4.

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 СМР-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.

Для перегляду сертифіката необхідно натиснути на відповідному записі про сертифікат у списку. Сертифікат буде відображено у вікні що наведене на рисунках 5.5 та 5.6.

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. 4.2) - за допомогою СВС, ОСЅР-протоколу тощо. Результатом перевірки буде вікно що наведене на рис. 5.7. Якщо у цьому вікні натиснути "Сертифікат", сертифікат буде відображений у вікні детального перегляду (рис. 5.6).

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.





	Сертифікати	×
Сертифікати Кількість: 7, тип власників: Тервер	и ЦСК 🗸	Пошук за власником:
Власник СМР-сервер АЦСК "МАSTERKEY" ТОВ СМР-сервер АЦСК "МАSTERKEY" ТОВ СОР-сервер АЦСК "МАSTERKEY" ТО ОСSР-сервер Центральний засвідчувал СSP-сервер Центральний засвідчувал TSP-сервер ЦСК "МАSTERKEY" ТОВ TSP-сервер ЦСК "МАSTERKEY" ТОВ "	ЦСК АЦСК "MASTERKEY" ТОВ "АРТ-МАСТЕР" АЦСК "MASTERKEY" ТОВ "АРТ-МАСТЕР" АЦСК "MASTERKEY" ТОВ "АРТ-МАСТЕР" Центральний засвідчувальний орган Центральний засвідчувальний орган Центральний засвідчувальний орган	Серійний номер 4E6929B96F6EA0750200000610000050870C00 4E6929B96F6EA075020000061000004F870C00 30B7327BF00575B202000000100000820000 3004751DEF2C78AE0200000010000008000000 3004751DEF2C78AE02000000100000050000000 3004751DEF2C78AE02000000100000010000000
О Імпортувати		ОК

Рисунок 5.4

	Сертифікат	×
📻 Сертиф	ыкат	
LICK:	ALICK "MASTERKEY" TOB "APT-MACTEP"	
Користувач:	CMP-cepsep ALICK "MASTERKEY" TOB "APT-MACTEP"	
Дійсний:	з 18.12.2015 до 18.12.2020	
Реєстраційний номер:	4E6929B96F6EA0750200000610000004F870C00	
Використання ключів:	ЕЦП у державних алгоритмах і протоколах	
 Детальна інфо Наступний сер 	ормація Этифікат	
		ОК
	Рисунок 5.5	
	Сертифікат	×
👳 Сертиф	ікат	



Рисунок 5.6



Центральний oфic TOB «Арт-мастер» вул. Сурикова, 3 (літ. А), Київ, 03035, Україна теп.: +380 44 248-79-1, 248-89-27, факс.: +380 44 248-98-14 е-mail: post@am-soft.ua; http://www.am-soft.ua



18





5.4 Перегляд СВС

Для перегляду списків відкликаних сертифікатів (СВС) необхідно натиснути підпункт "Переглянути СВС..." в пункті меню "Сертифікати та СВС" або натиснути клавішу F11. Вікно із списками відкликаних сертифікатів наведене на рис. 5.8.

Вікно перегляду СВС дозволяє видаляти СВС з файлового сховища, переглядати СВС та завантажувати СВС 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 5.9 та 5.10.

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.

Списе	ки відкликаних	сертифікатів			x
Списки відкликаних серти Кількість: 2	ифікатів				
ЦСК	Серійний номер	Час формування	Наступний	P.	Т
Центральний засвідчувальний орган Центральний засвідчувальний орган	7313 73C1	06.04.2018 22:28:46 10.04.2018 12:28:46	13.04.2018 22:28:46 10.04.2018 14:28:46	c J	
<				>	
🕤 імпортувати			C	Ж	

Рисунок 5.8







Список	відкликаних	сертифікатів		
LICK:	Центральний за	свідчувальний орган		
^р еєстраційний юмер:	7313			
Час формування:	06.04.2018 19:28 Наступний - 13.0	4.2018 19:28		
Призначення:	Для використан	ня у державних алгорит	мах і протоколах	
• • • • • • •				
🕑 детальна інфо	рмація			
			OK	
	Рис	сунок 5.9		
	Список відкл	иканих сертифіка	TIB	
🗧 Список	відкликаних	сертифікатів		
Загальна інфор	відкликаних	сертифікатів		
Список Загальна інфор	відкликаних мація:	сертифікатів	Vkoaïiuu:OII=	^
Список Загальна інфор Реквізити ЦСІ Час формува	відкликаних мація: К	сертифікатів О=Міністерство юстиції 06.04.2018.22-28:46	України;0U=	^
Список Загальна інфор Реквізити ЦСІ Час формуван Час наступно	відкликаних мація: К ння го формування	сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46	України;0U=	^
Список Загальна інфор Реквізити ЦС Час формуван Час наступно Р РН	відкликаних мація: К ння го формування	сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313	України;ОU=	^
Список Загальна інфор Реквізити ЦС Час формуван Час наступно РН Ішрентифікатор	відкликаних мація: К К го формування відкритого клю	Сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313 вD B7 3E 7B F0 D5 75 f	України;ОU= 32 48 02 78 3D	^
Список Загальна інфор Реквізити ЦС Час формуван Час наступно РН Ідентифікатор Список відклика	відкликаних мація: К к о формування о відкритого клю аних сертифікаті	Сертифікатів 0=Мністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313 BD B7 3E 7B F0 D5 75 f в:	України;ОU= 32 48 02 78 3D	^
Список Загальна інфор Реквізити ЦСІ Час формуван Час наступно РН Ідентифікатор Слисок відклика Е САРОТР614E66	відкликаних мація: К к о формування о відкритого клю аних сертифікатії 39058040000002	Сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313 BD B7 3E 7B F0 D5 75 f в: 30.10.2012 14:08:53	України;ОU= 32 48 02 78 3D 	^ ~
Список Загальна інфор Реквізити ЦС Час формува Час наступно РН Ідентифікатор Список відклика Е САРОІТ614665 САРОІТ614665	відкликаних мація: К к ння го формування відкритого клю аних сертифікаті 39058040000002.	Сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313 BD B7 3E 7B F0 D5 75 f в: 30.10.2012 14:08:53 30.10.2012 14:08:53	України;ОU= 32 48 02 78 3D ==4/st= 620 2 Блокування Поновлення	^ ~
Загальна інфор Реквізити ЦС Час формузан Час наступно РН Ідентифікатор Список відклика С САРОІГ614666 Е САРОІГ614666 С АРОІГ614666	відкликаних мація: к к ня відкритого кле відкритого кле заних сертифікаті 39058040000002 39058040000002	Сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313 BD B7 3E 7B F0 D5 75 F 45.00.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53	України, ОU= 32 48 02 78 3D 	^ •
Загальна інфор Реквізити ЦС Час формуван Час наступно Р РН Пантикрікатор Список відклика Е САF01F614E66 Е САF01F614E66 Е САF01F614E66 Е САF01F614E66	відкликаних мація: К К відкрито клю відкрито клю заробра (2000) заробра (2000) заробра (2000) заробра (2000) сертифікаті	Сертифікатів 0=Міністерство юстиції 06.04.2018 22:28.46 13.04.2018 22:28.46 7313 BD B7 3E 7B F0 D5 75 f в: 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53	України;0U= 32 48 02 78 3D 	×
Список Загальна інфор Реквізити ЦС Час формува Час наступно Р РН Ідентифікатор Тинсок відклика С АРО1F614E66 Е САРО1F614E66 Е САРО1F614E66 Е САРО1F614E66	відкликаних мація: К к відкритого кло знох сертифікаті зво5в040000002 зво5в040000002 зво5в040000002	Сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 13.04.2018 22:28:46 7313 BD B7 3E 7B F0 D5 75 f 00.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:03:53 31.10.2012 10:47:30	України;ОU= 32 48 02 78 3D 	~
Список Загальна інфор Реквізити ЦС Час фориува Час наступна Р РН Ідентифікатор Список відклика Е САРОІГ614E66 Е САРОІГ614E66 Е САРОІГ614E66 Е САРОІГ614E66 Е САРОІГ614E66	відкликаних мація: к к няя відфитого кло вико сертифікаті зро58040000002 зро58040000002 зро58040000002 зро58040000001	Сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313 BD B7 3E 7B F0 D5 75 f 50.01.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 16:35:39 31.10.2012 10:47:30 13.11.2012 18:30:55	України, ОU= 32 48 02 78 3D Блокування Поновлення Не визначена Зміна даних Не визначена Формуванн	•
Список Загальна інфор Реквізити ЦС Час фориува Час наступно Р РН Цантифікатор Список відклика С АгОГБ14665 Е САРОГБ14665 Е САРОГБ14665 Е САРОГБ14665 Е САРОГБ14665 Е САРОГБ14665 В САРОГБ14665	відкликаних мація: к к няя о формування відкритого клю занок сертифікаті зароБв040000002 зароБв040000002 зароБв040000003 зароБв040000001	Сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313 BD B7 3E 7B F0 D5 75 f 50.010.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 16:35:39 31.10.2012 10:47:30 13.11.2012 18:30:55	України, ОU= 32 48 02 78 3D 	×
Список Загальна інфор Реквізити ЦС Час фориза час наступна Р Н Цантифікатор Список відклика С ААРОІГ614666 Е САРОІГ614666 Е САРОІГ614666 Е САРОІГ614666 Е САРОІГ614666 Значення:	ВІДКЛИКАНИХ мація: К к няя с формування в відфитого клю анос сертифікаті зво58040000002 зво58040000003 зво58040000001	Сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313 BD B7 3E 7B F0 D5 75 f 50.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 16:35:39 31.10.2012 10:47:30 13.11.2012 18:30:55	України, ОU= 32 48 02 78 3D 	 ▲ ↓
Список Загальна інфор Реквізити ЦС Часкоринзан Час наступно Р РН Цантичкатор РИС Слиготе іздклика Слиготе ізделика Слиготе і 4666 Слиготе і 4666 Значення:	відкликаних мація: К к відкритого кло відкритого кло ворання	Сертифікатів О=Міністерство юстиції 06.04.2018 22:28:46 13.04.2018 22:28:46 7313 BD B7 3E 7B F0 D5 75 F 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 14:08:53 30.10.2012 16:35:39 31.10.2012 10:47:30 13.11.2012 18:30:55	України, ОU= 32 48 02 78 3D алісь в 270 0 Блокування Поновлення Не визначена Формуванн	•

5.5 Завантаження СВС

Для автоматичного завантаження списку відкликаних сертифікатів з web-сервера ЦСК необхідно відповідну позначку ("Завантажувати автоматично") у вікні параметрів що наведене на рис. 4.2.

5.6 Блокування власного сертифіката

Для блокування власного сертифіката необхідно обрати підпункт "Заблокувати власний сертифікат" в пункті меню "Сертифікати та СВС". Підтвердити повідомлення блокування сертифіката.

Повідомлення оператору	×
🛕 Заблокувати власний сертифікат?	
<u>Y</u> es <u>N</u> o	

Наступним кроком є зчитування особистого ключа та сертифіката користувача (див. п. 6.2).

Після зчитування особистого ключа почне роботу майстер блокування сертифіката. Запит буде переданий через сервер взаємодії ЦСК за протоколом НТТР де у наступному вікні (рис. 5.11) необхідно ввести параметри підключення до сервера взаємодії ЦСК:

- DNS-ім'я чи IP-адресу сервера (як правило це DNS-ім'я чи IP-адреса сервера взаємодії ЦСК);
- TCP-порт (як правило порт протоколу HTTP (80));
- параметри доступу до proxy-сервера (за необхідністю та якщо вони не встановлювались в параметрах роботи).







Після встановлення параметрів необхідно натиснути кнопку "Далі".;

Програмний комплекс користувача ЦСК

DNS-ім'я чи IP-а,	дреса сервера ЦСł	K: masterkey.ua		
ГСР-порт:		80		
Підключати	ся через ргоху-сере	зер		
DNS-ім'я чи ІГ	о-адреса сервера:		ТСР-пор	т:

Рисунок 5.11

Якщо під час відправки запита не виникало помилок буде виведено вікно що наведене на рис. 5.12.

Блокування сертифіката	×
Сертифікат заблоковано	
	-
L	Завершити

Рисунок 5.12

5.7 Формування нового сертифіката

Користувач може самостійно формувати нові сертифікати якщо має діючий ключ та такі операції дозволяються регламентом роботи ЦСК.

Примітка. Після формування нового сертифіката сервер обробки запитів здійснює автоматичне скасування попереднього сертифіката.

Для формування нового сертифіката необхідно обрати підпункт "Сформувати новий сертифікат" в пункті меню "Сертифікати та СВС". Перше вікно майстра формування нового сертифіката наведене на рис. 5.13. За допомогою цього вікна здійснюється генерація нових ключів користувача. Якщо обирається генерація на новий носій, спочатку виконується генерація ключа (рис. 5.14), а потім зчитування діючого особистого ключа (рис. 5.15). Якщо генерація здійснюється на текучий носій, спочатку виконується зчитування діючого ключа, а потім генерація нового.







Эгенерувати на новий носій Эгенерувати на поточний носій Эгенерувати на поточний носій Эгенерувати на поточний носій Далі > Відміна Pucynox 5.13 Формування нових сертифікатів Эгенерувати сертифікатів Тип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелиман в гр. точок ЕК Використовувати окремий ключ для протоколу розподілу: з файлу параметрів (латалог. з'ємний чи оптичний диск): С. Ргодгая Files (х86) Unstitute of Informational Technologies Certifica (Javinutu 		вання нових сертифікатів	×
 Эгенерувати на новий носій Эгенерувати на поточний носій Эгенерувати на поточний носій Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Рисунок 5.13 Формування нових сертифікатів Папі > Відміна Відміна Відміна Відміна Відміна Відміна Відміна Відміна Відміна Відміна Відміна Відміна Відміна Відміна Відміна В	Генерація нов	их ключів	
О в опереонны повилноси: О Згенерувати на поточний носій Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Генерація нових ключів Потокрація нових ключів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК ✓ Використовувати окремий ключ для протоколу розподілу: з файлу параметрів ✓ Видміна Місце розміщення параметрів (каталог., з'ємний чи оптичний диск): С.\Program Files (к86)\Institute of Informational Technologies\Certifica ✓ Змінити	Эгенерувати на новий н	ncià	
ОЗгенерувати на поточний носій Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Гип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК ✓ Використовувати окремий ключ для протоколу розподілу: З файлу параметрів ✓ Місце розміщення параметрів (каталог, з'ємний чи оптичний диск): С:\Program Files (x86)\Institute of Informational Technologies\Cettfica ✓ Змінити			
Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Гип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК Використовувати окремий ключ для протоколу розподілу: Використовувати окремий ключ для протоколу розподілу: з файлу параметрів Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів Місце розміщення параметрів (каталог, з'ємний чи оптичний диск): С:\Program Files (x86)\Institute of Informational Technologies\Certifica Змінити	 Згенерувати на поточни 	ий носій	
Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Генерація нових ключів ПСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК Ф Використовувати окремий ключ для протоколу розподілу: Використовувати окремий ключ для протоколу розподілу: в файлу параметрів V із файлу параметрів V Місце розміщення параметрів (каталог., з'ємний чи оптичний диск): С.\Program Files (x86)\Institute of Informational Technologies\Cettfica V Змінити			
Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Генерація нових ключів Тип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК ✓ Використовувати окремий ключ для протоколу розподілу: з файлу параметрів ✓ Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів ✓ Місце розміщення параметрів (каталог., з'ємний чи оптичний диск): С.\Program Files (x86)\Institute of Informational Technologies\Certifica ✓ Змінити			
Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Гип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК Використовувати окремий ключ для протоколу розподілу Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів Ключі протоколу розподілу: з файлу параметрів (каталог., з'ємний чи оптичний диск): С.\Program Files (x86)\Institute of Informational Technologies\Certifica v Змінити			
Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Сенерація нових ключів Відміна Тип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК ∨ Використовувати окремий ключ для протоколу розподілу Ключі протоколу розподілу: з файлу параметрів ∨ з файлу параметрів ∨ Місце розміщення параметрів (каталог, з'ємний чи оптичний диск): Змінити			
Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Генерація нових ключів Тип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК Використовувати окремий ключ для протоколу розподілу: мочі ЕЦП: ключі протоколу розподілу: з файлу параметрів Місце розміщення параметрів (каталог., з'ємний чи оптичний диск): С:\Program Files (x86)\Institute of Informational Technologies\Certifica Змінити			
Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Гип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК Використовувати окремий ключ для протоколу розподілу: в файлу параметрів Ключі протоколу розподілу: з файлу параметрів Саталог., з'ємний чи оптичний диск): С.\Program Files (x86)\Institute of Informational Technologies\Certifica V Змінити			
Далі > Відміна Рисунок 5.13 Формування нових сертифікатів Гип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК v Використовувати окремий ключ для протоколу розподілу Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів v Місце розміщення параметрів (каталог., з'ємний чи оптичний диск): С.\Program Files (x86)\Institute of Informational Technologies\Certifica v Змінити			
Рисунок 5.13 Формування нових сертифікатів Генерація нових ключів Тип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК v Використовувати окремий ключ для протоколу розподілу Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів v Місце розміщення параметрів (каталог., з'ємний чи оптичний диск): С:\Program Files (x86)\Institute of Informational Technologies\Cettifica v Змінити		Далі > Віді	міна
Формування нових сертифікатів Генерація нових ключів Тип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК ✓ Використовувати окремий ключ для протоколу розподілу Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів ✓ з файлу параметрів ✓ Місце розміщення параметрів (каталог, з'ємний чи оптичний диск): С:\Program Files (x86)\Institute of Informational Technologies\Cettfica ✓ Змінити		Рисунок 5.13	
Генерація нових ключів Тип криптографічних алгоритмів та протоколів: ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК Використовувати окремий ключ для протоколу розподілу Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів \$ з файлу параметрів Місце розміщення параметрів (каталог, з'ємний чи оптичний диск): С.\Program Files (x86)\Institute of Informational Technologies\Cettifica	Форму	вання нових сертифікатів	×
Тип криптографічних алгоритмів та протоколів: [ДСТУ 4145-2002 та Диффі-Гелман в гр. точок ЕК v Використовувати окремий ключ для протоколу розподілу Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів v Місце розміщення параметрів (каталог, з'ємний чи оптичний диск): С:VProgram Files (x86)\Institute of Informational Technologies\Cettfica v Змінити	Гонорація нов		
Тип криптографічних алгоритмів та протоколів: 	теперація нові		
Дст в чти зе сода та двуффинелиман в гр. точок стк ▼ Використовувати окремий ключ для протоколу розподілу Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів ▼ Місце розміщення параметрів (каталог, з'ємний чи оптичний диск): С:\Program Files (x86)\Institute of Informational Technologies\Certifica ▼	Тип криптографічних алгори	тмів та протоколів:	
У Використовувати окремий ключ для протоколу розподілу Ключі ЕЦП: Ключі протоколу розподілу: з файлу параметрів У Файлу параметрів Місце розміщення параметрів (каталог, з'ємний чи оптичний диск): С:\Program Files (x86)\Institute of Informational Technologies\Certifica	DCTV /1/5-2002> Duthetial		
Ключі протоколу розподлу: Ключі протоколу розподлу: з файлу параметрів Місце розміщення параметрів (каталог, з'ємний чи оптичний диск): С:\Program Files (x86)\Institute of Informational Technologies\Certifica	ДСТУ 4145-2002 та Диффі-І		
Micце розміщення параметрів (каталог, з'ємний чи оптичний диск): [C:\Program Files (x86)\Institute of Informational Technologies\Certifica v Змінити	ДСТУ 4145-2002 та Диффі- Використовувати окреми	й ключ для протоколу розподілу	
плоце розмицення нараметрів (каталог, з смінии чи оптичния диск); [C:\Program Files (x86)\Institute of Informational Technologies\Certifica v] Змінити	ДСТУ 4145-2002 та Диффі-	й ключ для протоколу розподілу Ключі протоколу розподілу:	
	ДСТУ 4145-2002 та Диффі- Використовувати окреми Ключі ЕЦП: з файлу параметрів ✓	й ключ для протоколу розподілу Ключі протоколу розподілу: з файлу параметрів V	
	ДСТУ 4145-2002 та Диффі-І	й ключ для протоколу розподілу Ключі протоколу розподілу: s файлу параметрів v is (каталог, s'ємний чи оптичний диск); a of Informational Technologies (Certifica v	нти
	ДСТУ 4145-2002 та Диффі- Використовувати окреми Ключі ЕЦП: s файлу параметрів Місце розміщення параметр C:\Program Files (x86)\Institute	й ключ для протоколу розподілу Ключі протоколу розподілу: з файлу параметрів v ів (каталог, з'ємний чи оптичний диск): e of Informational Technologies\Certifica v Змін	нити
	ДСТУ 4145-2002 та Диффі- Використовувати окреми Ключі ЕЦП: з файлу параметрів Місце розміщення параметр C:\Program Files (x86)\Institute	й ключ для протоколу розподілу Ключі протоколу розподілу: з файлу параметрів v ів (каталог, з'ємний чи оптичний диск); a of Informational Technologies\Certifica v Змін	нити
	ДСТУ 4145-2002 та Диффі- Макористовувати окремии Ключі ЕЦП: з файлу параметрів Місце розміщення параметр С:\Program Files (x86)\Institute	й ключ для протоколу розподілу Ключі протоколу розподілу: s файлу параметрів v is (каталог, з'ємний чи оптичний диск): e of Informational Technologies\Certifica v Змін	нити
< Назад Далі > Відміна	ДСТУ 4145-2002 та Диффі- Використовувати окреми Ключі ЕЦП: з файлу параметрів ✓ Місце розміщення параметр C:\Program Files (x86)\Institut	й ключ для протоколу розподілу Ключі протоколу розподілу: э файлу параметрів	чіна



Рисунок 5.14







EN

Зчитати Відміна

Рисунок 5.15

Після зчитування діючого особистого ключа, та генерації нового ключа, у наступному вікні майстра формування нового сертифіката (рис. 5.16) необхідно вказати спосіб за який буде передано запит до сервера обробки запитів ЦСК.

Формування нових сертифікатів
Запит на формування сертифікатів
Відправити через сервер обробки запитів ЦСК (НТТР)
О Відправити засобами електронної пошти
🔿 Зберегти у файл
< Назад Далі > Відміна

Рисунок 5.16

5.7.1 Передача запита за допомогою сервера обробки запитів ЦСК

У разі якщо запит повинен бути переданий через сервер взаємодії ЦСК за протоколом НТТР у наступному вікні (рис. 5.17) необхідно ввести параметри підключення до сервера взаємодії ЦСК:

- DNS-ім'я чи IP-адресу сервера (як правило це DNS-ім'я чи IP-адреса сервера взаємодії ЦСК);
- ТСР-порт (як правило порт протоколу НТТР (80));

Пароль:

 параметри доступу до ргоху-сервера (за необхідністю та якщо вони не встановлювались в параметрах роботи).

Після встановлення параметрів необхідно натиснути кнопку "Далі".







DNS-im's un IP-anneca censena LICK	· masterkev ua
ТСР-порт:	80
Підключатися через ргоху-серв	lep
DNS-ім'я чи IP-адреса сервера:	ТСР-порт:



Якщо під час відправки запита не виникало помилок, буде виведено новий сертифікат користувача у вікні що наведене на рис. 5.18, та вікно що наведене на рис. 5.19.

ифікати	×
ікат	
Тестовий ЦСК АТ IIT (в. 1.3)	
Користувач_0023	
з 30.11.2012 до 30.11.2013	
0AF8E59333B0CC1D04000002007010080D80100	
ЕЦП, Неспростовність, Протоколи розподілу ключів у державних алгоритмах і протоколах	
pMalia	
тифікат	
ОК	
Рисунок 5.18	
	ифікати ікат Тестовий ЦСК АТ IIT (в. 1.3) Користувач_0023 в 30.11.2012 до 30.11.2013 0АРВЕ59333B0CC1D04000002007010080D80100 ЕЦП, Неспростовність, Протоколи розподілу ключів у державних апгоритиках і протоколах ривція пифікат ОК РИСУНОК 5.18

Формування нових сертифікатів	×
Сертифікати сформовано	
[Завершити

Рисунок 5.19







5.7.2 Передача запита засобами електронної пошти

У разі якщо запит повинен бути переданий засобами електронної пошти у наступному вікні (рис. 5.20) необхідно ввести параметри підключення до поштового сервера:

24

- DNS-ім'я чи IP-адресу поштового сервера;
- TCP-порт (як правило це порт протоколу SMTP (25));
- ім'я користувача поштового сервера;
- поштову адресу сервера взаємодії ЦСК;
- поштову адресу відправника.

Після встановлення параметрів необхідно натиснути кнопку "Далі".

Формування нових сертифікатів
Відправка запиту до сервера ЦСК
Поштова адреса сервера ЦСК: info@masterkey.ua
Поштова адреса відправника: baklykov@gmail.com
Поштовий сервер (SMTP)
DNS-ім'я чи IP-адреса сервера: 64.233.162.109
ТСР-порт: 25
Iм'я користувача сервера: baklykov
Пароль доступу до сервера:
< Назад Далі > Відміна

Рисунок 5.20

Після відправлення поштового повідомлення майстер завершує свою роботу (рис.5.21).



Рисунок 5.21

5.7.3 Передача запита за допомогою файлу запита

Для відправки запита іншими засобами (нештатними засобами електронної пошти програми чи ін.) запит може бути збережений у файл (рис. 5.22).





, Україна 44 206-13-79



Рисунок 5.22

Після збереження запиту до файлу майстер завершує свою роботу (рис. 5.23).

Формування нових сертифікатів	×
Запит сформовано	
	Завершити

Рисунок 5.23

5.8 Помилки, що можуть виникати під час роботи програми

5.7.1 Помилка під час завантаження СВС

Вікно з повідомленням про помилку наведене на рисунку 5.24.



Рисунок 5.24

Така помилка може виникати:



Центральний офіс ТОВ «Арт-мастер» вул. Сурикова, 3 (ліг. А), Київ, 03035, Україна теп.: +380 44 248-97-91, 248-98-27, факс: +380 44 248-98-14 е-mail: post@am-soft.ua, http://www.am-soft.ua



B ∉Mast

- не вказано адресу proxy-сервера (або не встановлено признак необхідності його використання) у параметрах роботи програми;
- якщо не вірно вказані параметри аутентифікації proxy-сервера;
- у сертифікаті, що вказувався як джерело шляху отримання СВС не вказано, або вказано невірний шлях отримання СВС;
- не має доступу до web-сторінки завантаження CBC.
- 5.7.2 Помилки під час перевірки сертифікатів

Під час перевірки сертифікатів можуть виникати помилки аналогічні до помилок що описані у п.п. 5.7.1 та пов'язані із доступом серверів обробки запитів ЦСК по каналам зв'язку. При виникненні помилок насамперед необхідно перевірити параметри роботи програми у відповідності до розділу 4.







6 УПРАВЛІННЯ КЛЮЧАМИ

6.1 Генерація ключів

Для генерації ключів необхідно обрати підпункт "Згенерувати ключі" в пункті меню "Особистий ключ". На першій сторінці майстра (рис. 6.1) за необхідністю можна 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.

	Генерація ключів	>
Генерація клк	учів	
Тип криптографічних алгор	итмів та протоколів:	
ДСТУ 4145-2002 та Дифф	і-Гелман в гр. точок ЕК 🛛 🗸	
 Використовувати окрем 	ий ключ для протоколу розподілу	
Ключі ЕЦП:	Ключі протоколу розподілу:	
з файлу параметрів	 з файлу параметрів 	
Місце розміщення параме	прів (каталог, з'ємний чи оптичний диск):	
C:\Program Files (x86)\Institu	te of Informational Technologies\Certifica 🗸 Зміни	ити
	Далі > Відмі	на
	Рисунок 6 1	

Далі необхідно встановити НКІ для запису особистого ключа у пристрій запису та на наступній сторінці майстра (рис. 6.2) 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 3,5" (дискети);
- з'ємні диски (flash-диски);
- оптичні диски (CD-R, CD-RW, DVD-R або DVD-RW);
- електронні ключі ("IIT.Кристал-1", , Aladdin eToken R2, PRO, Технотрейд uaToken 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 6.2

Після запису особистого ключа на НКІ, буде виведено вміст простого запиту на формування сертифікату з відкритим ключем ЕЦП для державних алгоритмів та протоколів (рис. 6.3), після перевірки вмісту простого запиту необхідно натиснути "ОК".

Запит на формування сертифіката з відкритим ключем ЕЦП	×	
⋥ Запит на формування сертифіката		
Поля запиту:		
 Реквізити заявника відсутні Додаткові дані відсутні Додаткові дані відсутні Тип заявника Не вказаний Строк чинності сертифіката ві Строк чинності сертифіката ві Строк чинності сертифіката ві Параметри відкритого ключа ві Параметри відкритого ключа ДСТУ 4145-2002 Довжина ключа ДСТУ 4145-2002 Довжина ключа 264 біт(а) Відкритий ключ F2 F8 8D 4A A0 3C 95 1A 28 CF 8D CD Ідентифікатор відкритого ключа 29 EB F0 62 10 82 65 2A E7 A2 A2 CD Уточнене призначення ключів Запит самопідлисаний 		
• Друкувати ОК		

Рисунок 6.3

На наступній сторінці майстра (рис. 6.4) необхідно вказати спосіб передачі запиту до центру сертифікації ключів: за допомогою файлу, або відправити електронною поштою.

У першому випадку у наступному вікні (рис. 6.5) необхідно буде вказати ім'я файлу для запису простого запиту на формування сертифіката 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.







	ерація ключів
Запити на форму	вання сертифіката
	• •
Эберегти у файл	
🔘 Відправити засобами електр	онної пошти до ЦСК
	< Назад Далі > Відміна
F	^э исунок 6.4
Ген	ерація ключів
Запити на форму	вання сертифікатів
Санити на форму	
Ім'я файлу для запису запиту з від	акитим ключем ЕЦП:
Ім'я файлу для запису запиту з від С:\Certificates\EU-D718F388.p10	акитим ключем ЕЦП: Змінити
In/s файлу для запису запиту з від С:\Certificates\EU-D718F388.p10	акитим ключем ЕЦП: Змінити
Iм'я файлу для запису запиту з від [C:\Certificates\EU-D718F388.p10 Ім'я файлу для запису запиту з від [C:\Certificates\EII-КЕР-Е949D942	акитим ключем ЕЦП: Змінити акритим ключем протоколу розподілу: о 10

Рисунок 6.5

< Назад Далі >

Відміна

У випадку якщо запит передається за допомогою електронної пошти, у вікні (рис. 6.6) необхідно буде вказати параметри доступу до поштового сервера, та електронну поштову адресу центра сертифікації ключів.

Генерація ключів	×
Відправка запиту до сервера ЦСК	
Поштова адреса сервера ЦСК: info@masterkey.ua	
Поштова адреса відправника: baklykov@gmail.com	
Поштовий сервер (SMTP)	
DNS-ім'я чи IP-адреса сервера: 64.233.162.109	
TCP-nopt: 25	
Iм'я користувача сервера: baklykov	
Пароль доступу до сервера:	
< Назад Далі >	Відміна
Рисунок 6.6	

Після виконання всіх дій майстер завершує свою роботу (рис. 6.7).









6.2 Зчитування особистого ключа

Для роботи з більшістю функцій програми (захисту файлів та ін.) необхідне попереднє зчитування особистого ключа користувача. Ініціювання зчитування особистого ключа може бути виконане автоматично при виборі певної функції програми чи виконане шляхом вибору підпункту "Зчитати ..." в пункті меню "Особистий ключ" або шляхом натискання комбінації клавіш Ctrl+K.

У вікні, що з'явиться (рис. 6.8) необхідно вказати:

- тип HKI з особистим ключем;
- назву носія;
- пароль доступу до носія та захисту особистого ключа.

Зчитування діючого особис	сто	го ключа
Встановіть носій ключової інформації чи піди модуль та вкажіть параметри	клю	очіть криптографічний
Priyчкий диск sieмний диск isieмний диск im EN ormuruний диск im cmaprixapta Astop (318) im cmaprixapta Astop (318) im cmaprixapta BIFIT Integra 1.0 exnov BIFIT Integra 1.0 exnov BIFIT Integra 1.0 exnov IIT Annas-1K exnov IIT Annas-1K exnov IIT Annas-1K exnov IIT Kpuctan-1 exnov IIT Couple IIT HotiX exnov IIT Couple III exnov IIIT Couple IIII exnov IIIT Couple IIII ex	< >	 Інформація про носій: Тип: з'ємний диск Назва: F:\ Перезаписуемий, не потребує автентифікації Поновити Ключ у файлі (на диску)
		Зчитати Відміна

Рисунок 6.8

Після введення параметрів необхідно натиснути кнопку "Зчитати".

Інформація про те, що особистий ключ зчитаний та знаходиться в пам'яті ПЕОМ відображається до панелі стану вікна, як наведено на рисунку 6.9.









6.3 Резервне копіювання особистого ключа

Для резервного копіювання особистого ключа з одного НКІ на інший необхідно обрати підпункт "Резервне копіювання особистого ключа" в пункті меню "Особистий ключ".

Під час резервного копіювання особистий ключ зчитується за допомогою вікна що наведене на рисунку 6.10. Під час резервного копіювання пароль захисту особистого ключа не вказується, та змінити його не можливо.

Зчитування діючого особи	сто	ого ключа	×
Встановіть носій ключової інформації чи піди модуль та вкажіть параметри	клк	очіть криптографічний	
🖴 гнучкий диск	^	📕 Інформація про носій:	
📕 з'ємний диск			_
F:\		Тип: з'ємний диск	
оптичний диск			
📼 смарт-карта Автор (318)		Назва: F:\	
🚥 смарт-карта BIFIT Integra 1.0		Перезаписуємий, не потребує	
🥙 е.ключ BIFIT iToken		автентифікації	
🛷 е.ключ IIT Алмаз-1К			
💞 е.ключ IIT Алмаз-1К (носій)			
🖋 е.ключ IIT Кристал-1			
🖋 е.ключ IIT Кристал-1 (носій)			
🖴 файлова система (каталоги системи)			
🖴 файлова система (каталоги користувача)			
🖴 е.ключ Aladdin eToken (PKCS#11, носій)			
🖴 е.ключ чи смарт-карта Автор (PKCS#11, носій)			
🖴 е.ключ чи с. карта G&D SafeSign (PKCS#11, носій)			
🖴 е.ключ SafeNet iKey (PKCS#11, носій)		-	_
🖴 е.ключ чи с. карта Aladdin JaCarta (PKCS#11, носій)		Поновити	
🖴 е.ключ чи смарт-карта Автор (PKCS#11)	5	🔿 Ключ у файлі (на диску)	
On (DV/CC#11	*	•	
Пароль: ЕМ			
		Зчитати Відміна	

Рисунок 6.10

Після зчитування особистий ключ записується до резервного носія за допомогою вікна що наведене на рисунку 6.11.









6.4 Зміна паролю захисту особистого ключа

Для зміни паролю захисту особистого ключа необхідно обрати підпункт "Змінити пароль захисту особистого ключа" в пункті меню "Особистий ключ". Вікно зміни паролю захисту особистого ключа наведене на рис. 6.12. У вікні необхідно вказати:

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



Рисунок 6.12

6.5 Знищення особистого ключа на носієві

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



Центральний офіс ТОВ «Арт-мастер» вул. Сурикова, 3 (ліг. А), Київ, 03035, Україна теп.: +380 44 248-97-91, 248-98-27, факс: +380 44 248-98-14 е-mail: post@am-soft.ua, http://www.am-soft.ua





Для знищення особистого ключа необхідно обрати підпункт "Знищити особистий ключ на носієві ключової інформації" в пункті меню "Особистий ключ". Вікно знищення особистого ключа наведене на рис. 6.13. У вікні необхідно вказати тип та назву НКІ і натиснути кнопку "Виконати".

Знищення особистого к	люча	×
Встановіть носій ключової інформації чи підклі модуль та вкажіть параметри	ючіть криптографічний	
гнучкий диск s'ємний диск s'ємний диск G:\ ontrичний диск G:\ ontrичний диск cmapt-карта Автор (318) cmapt-карта BIFIT Integra 1.0 ekmov BIFIT IOKen ekmov BIFIT IOKen ekmov BIFIT IOKen ekmov IIT Ализа-1K (носій) ekmov IIT Кристал-1 ekmov IIT Кристал-1	 Неформація про носій: Тип: з'ємний диск Назва: F:\ Перезаписуємий, не потребує автентифікації Поновити Ключ у файлі (на диску) 	_
	Знищити Відміна	

Рисунок 6.13

6.6 Знищення особистого ключа в пам'яті ПЕОМ

Якщо при зчитуванні особистого ключа не було встановлено параметр "Зчитувати повторно при кожній операції", ключ залишається у пам'яті до завершення роботи програми (див. п. 6.2). Якщо необхідно знищити ключ з пам'яті не виходячи з програми необхідно обрати підпункт "Знищити особистий ключ у пам'яті" в пункті меню "Особистий ключ" або натиснути клавішу F12.

6.7 Перегляд власного сертифіката

Після зчитування особистого ключа користувач може переглянути власний сертифікат. Для перегляду власного сертифіката необхідно обрати підпункт "Переглянути власний сертифікат" в пункті меню "Особистий ключ". Сертифікат буде відображено до вікон що наведені на рисунках 5.2, 5.3.

6.8 Помилки, що можуть виникати під час роботи програми

6.8.1 Помилка під час зчитування особистого ключа

Вікно з повідомленням про помилку наведене на рисунку 6.14.

Повідол	ллення оператору 🛛 🛛 🔀
8	Виникла помилка при зчитуванні особистого ключа. Опис помилки: Виникла помилка при розборі даних (пошкоджені дані чи невірний формат)
	ОК
	Рисунок 6.14

Така помилка може виникати:

- якщо не вірно вказаний пароль доступу до особистого ключа;
- пошкоджений носій ключової інформації;
- пошкоджені дані на носії ключової інформації.

Найчастіше така помилка трапляється у наслідок вказування невірного паролю захисту особистих ключів.

6.8.2 Помилка під час зчитування особистого ключа

Вікно з повідомленням про помилку наведене на рисунку 6.15.









Така помилка може виникати:

- якщо не знайдено сертифікат ЦСК у файловому сховищі під час зчитування особистого ключа користувача;
- якщо не знайдено сертифікат відкритих ключів користувача у файловому сховищі.

6.8.3 Помилка під час блокування власного сертифіката

Вікно з повідомленням про помилку наведене на рисунку 6.17.

Повідом	илення оператору 🛛 🛛 🔀
8	Виникла помилка при відправці запиту на блокування сертифіката до сервера обробки запитів ЦСК. Опис помилки: Виникла помилка при передачі запиту на сервер ЦСК за протоколом НТТР
	ОК
	Рисунок 6.17

Така помилка може виникати:

- якщо не вказано параметри (адреса, порт) proxy-сервера, а підключення до сервера обробки запитів ЦСК здійснюється за допомогою нього;
- якщо не вірно вказано параметри аутентифікації proxy-сервера;
- якщо особистий ключ користувача не є дійсним;
- якщо відсутній доступ до сервера обробки запитів ЦСК.







7 ЗАХИСТ ФАЙЛІВ

7.1 Підпис файлів

Для підпису файлів (накладання ЕЦП) необхідно натиснути на панелі "Підписати файли" у головному вікні програми, або обрати підпункт "Підписати" у пункті меню "Файли", або натиснути клавішу F5. Якщо особистий ключ ще не було зчитано, відбувається його зчитування відповідно до п. 6.2.

Вікно підпису файлів наведене на рис. 7.1. Вікно містить наступні параметри:

- список файлів, які необхідно підписати;
- признак запису ЕЦП у зовнішній файл;
- признак запису підписаних файлів чи файлів з ЕЦП у окремий каталог;
- ім'я каталогу для запису підписаних даних чи файлів з ЕЦП.

Список файлів містить імена файлів що необхідно підписати. Файли додаються до списку за допомогою кнопки "Додати" та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку "Видалити".

Признак запису ЕЦП у зовнішньому файлі встановлює необхідність запису ЕЦП у окремий файл з розширенням ".p7s" без включення вмісту файлу що підписується. За замовчанням підпис записується до вихідного файлу та до розширення файлу додається суфікс ".p7s". Запис ЕЦП до зовнішнього файлу потрібен у випадку, коли файл підписується декількома користувачами, або при необхідності доступу до структури (вмісту) файлу без зняття з нього ЕЦП.

Признак запису підписаних файлів у окремий каталог встановлює необхідність запису підписаних файлів або файлів з ЕЦП до окремого каталогу що задається параметром "Каталог для запису підписаних даних чи файлів з ЕЦП". Якщо признак не встановлено підписані файли чи файли з ЕЦП будуть записуватися у каталог з вихідними файлами.

ім'я файлу		ЕЦП	Стан	A
		n. Inchy area Int		1
🚺 ЕЦП у зовншньо	ну файлі (^{ж. в.} р7с) – Алгорити Е Ц	п: ДСТУ 4145 💌	Додати	Зидалити
 ЕЦП у зовнішньо Вкажіть (за необхідні 	ну файлі (** р7s) – Алгорити ELl спо) каталог для запису підлиса	П: ДСТУ 4145 💌	<u>Додати</u> в s ЕЦП (*.*.р7s)	Зидалитн
 ЕЦП у зовншньо Вкажіть (за необхідні Використовувати 	ну файлі (** p7s) – Алгорити EL спо) каталог для запису підлиса окремий кеталог для підлисани	П: ДСТУ 4145 💌 аних файлів чи файлів хх файлів чи файлів з	<u>Додати</u> в s ЕЦП (*.*.,р7s) ЕЦП	зиделити

Рисунок 7.1

Після встановлення значень параметрів вікно може мати вигляд як наведено на рис. 7.2.







Рисунок 7.2

Для підпису файлів необхідно натиснути кнопку "Підписати".

Після здійснення підпису файлів вікно буде містити інформацію про результати підпису (рис. 7.3).

Ім'я файлу	Iм'я файлу з ЕШП
	C:\Program Files\Institute of Informational Te
۹	

Рисунок 7.3

7.2 Перевірка файлів

Для перевірки підпису (ЕЦП) файлів необхідно натиснути на панелі "Перевірити файли" у головному вікні програми, або обрати підпункт "Перевірити підпис" у пункті меню "Файли", або натиснути клавішу F6.

Вікно перевірки файлів наведене на рис. 7.4. Вікно містить наступні параметри:

- список файлів, які необхідно перевірити;
- признак запису файлів без ЕЦП у окремий каталог;
- ім'я каталогу для запису файлів без ЕЦП.

Список файлів містить імена файлів що необхідно перевірити. Файли додаються до списку за допомогою кнопки "Додати" та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку "Видалити".

Признак запису файлів без ЕЦП у окремий каталог встановлює необхідність запису файлів після зняття ЕЦП у окремий каталог що задається параметром "Каталог для запису файлів без ЕЦП". Якщо признак не встановлено файли без ЕЦП будуть записуватися у каталог з підписаними файлами.



ентральний офіс ТОВ «Арт-мастер» л. Сурикова, 3 (літ. А), Київ, 03035, Україна л.: +380 44 248-97-91, 248-98-27, факс: +380 44 248-98-14 mäl: post@am-soft.ua; http://www.am-soft.ua





And Andrew Street and a street stre			
Вкажіть файли, які необхідно перезірити			
м'я файлу	Стан	1	
1			
		Додати	Видалити
Вкажіть (за необхідністю) каталог для запису файлів б	ies EUN	Додати	Видалити
Вкажть (за необхідністо) катапог для запису файлів б П Використовувати окремий каталог	ies EUN	Додати	Видалити
Вкажть (за необхідністю) каталог для запису файлів б П Використовувати окремий каталог	ies EUN	Додати	Видалити Эмінити

Після встановлення значень параметрів вікно може мати вигляд як наведено на рис. 7.5.

2	Перевірка підписаних файлів		
	Вкажіть файли, які необхідно перевірити		
	Ім'я файлу	Стан	
	C\Program Files\Institute of Informational Technologies\C	Підлис не переврений	
		Додати	Еиделити
	Вкажіть (за необхідністю) каталог для запису файлів без ELI П Використовувати окремий каталог	Додати	Енделити
	Вкажіть (за необхідністю) каталог для запису файлів без ЕЦГ П Використовувати окремий каталог	Додати	Виделити Змінити

Для перевірки файлів необхідно натиснути кнопку "Перевірити".

Після здійснення перевірки файлів вікно буде містити інформацію про результати підпису (рис. 7.6).

В разі вдалої перевірки можна також переглянути інформацію про підписаний файл (для цього необхідно натиснути на відповідний запис про файл). Вікно наведене на рис. 7.7.







ш	Користув	ач ЦСК-1			_02
	Перев	ірка підписани	с файлів		
	Результат	и перезірки файлів			
	IM's dais	70		Im's datiny des EUD	
		gram files unstluce of in	romaionai ecrnoiogies w	C: VALorriectors all (hepesipe	ниц
0	Для эсеер	шения натионість кног	іку "Закрити" Рисунок 7.6		Закрити
	Підписа	ні дані Підписані да	ні		×
	82	Підписувач:	Користувач		
		Організація та підрозділ:	AT "IIT" AT "IIT"		
		Посада:	Користувач		
		Сертифікат ЦСК:	AT "IIT"		
		Реєстраційний номер:	16F7F644892E7F1E0400	0000010000019000000	
		Час підпису:	30.11.2012 14:30:37		
	🗿 Де	етальна інформація	<u>.</u>		
				ОК	
			D		

Рисунок 7.7

У детальній інформації наводиться сертифікат користувача що підписав файл.

Якщо ЕЦП містився в файлі з даними, при перевірці підпису буде створено копію файлу без підпису без розширення ".p7s". За замовчанням (якщо не встановлено окремого каталогу для файлів без підпису) файл буде записаний до того ж каталогу у якому знаходився підписаний файл.

7.3 Зашифрування файлів

Для зашифрування файлу необхідно натиснути на панелі "Зашифрувати файли" у головному вікні програми, або обрати підпункт "Зашифрувати" у пункті меню "Файли", або натиснути клавішу F7.

Вікно зашифрування файлів наведене на рис. 7.8. Вікно містить наступні параметри:

- список файлів, які необхідно зашифрувати;
- признак необхідності додаткового підпису файлу;
- признак запису зашифрованих файлів у окремий каталог;
- ім'я каталогу для запису зашифрованих файлів.

Список файлів містить імена файлів що необхідно зашифрувати. Файли додаються до списку за допомогою кнопки "Додати" та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку "Видалити".







Признак додаткового підпису файлів ("Додатково підписати") встановлює необхідність підпису файлу. За замовчанням здійснюється лише зашифрування кожного файлу.

Вихідні зашифровані файли мають розширення ".p7e".

Признак запису зашифрованих файлів у окремий каталог встановлює необхідність запису зашифрованих файлів до окремого каталогу що задається параметром "Каталог для запису зашифрованих файлів".

Ім'я файлу	Підписати Стан
Додатково підписати	Додати Видалит
Додатново підписати	Додати Видалит
Додатново підписати Вкажіть (за необхідністю) каталог для	Додати Виралит І запису зацифрованих файлів (*p7e)
Додатново підписати Вкажіть (за необхідністю) каталог для Використовувати окремий катало	Додати Видали I запису зашифрованих файлів (*.1.p7e) * для зашифрсеаних файлів



Ім'я файлу		Підписати	Стан	-
E:\Program Fi	es:Wicrosoft Games)Chess:Uhess.exe es:Wicrosoft Games)Chess:Uhess.MCE.png	Tak Hi	Не заши Не заши	Фрований Фрований
🔽 Додатково під	лисати		Додати	Видалит
І√ Додатково під Бкажіть (за необх	лисати ідністо) каталог для запису зашифсовачио	файлів (р7е	Додати	Видалит

Рисунок 7.9

Для зашифрування файлів використовується особистий ключ користувача що виконує зашифрування та сертифікат(и) користувача(ів) для якого(их) зашифровується файл. Тому у вікні що наведене на рис. 7.10 необхідно обрати користувачів для яких виконується зашифрування файлу. Зашифрований файл може бути відкритим лише користувачем для якого виконувалось зашифрування.









Рисунок 7.10

Під час шифрування здійснюється перевірка параметрів ключових даних користувачів що були обрані у списку (рис 7.10). Якщо параметри ключів користувачів для яких виконується шифрування будуть відрізнятись від параметрів ключів користувача що виконує шифрування, користувачу буде видане повідомлення про неможливість виконування шифрування у зв'язку з відмінністю параметрів та процес шифрування буде припинено. Для запобігання цього слід переглянути сертифікат користувача на адресу якого виконується шифрування та перевірити відповідність параметрів власних ключів параметрам ключів цього користувача.

Після здійснення зашифрування файлів буде виведене наступне вікно (рис. 7.11) з інформацією про результати зашифрування.

Ім'я файлу	IM	я зашифрованого фай.	ny
C:\Program Fles\Microsoft Games\Chv C:\Program Fles\Microsoft Games\Chv	s\Chess.exe C:\ s\ChessMCE.png C:\	Program Files Microsoft Program Files Microsoft	Games \Chess \(Games \Chess \(

Рисунок 7.11

7.4 Розшифрування файлів

Для розшифрування файлів необхідно натиснути на панелі "Розшифрувати файли" у головному вікні програми, або пункт меню "Розшифрувати" у розділі меню "Файли", або натиснути клавішу F8. Вікно розшифрування файлів наведене на рис. 7.12. Форма містить наступні параметри:

- список зашифрованих файлів, які необхідно розшифрувати;
- признак запису розшифрованих файлів у окремий каталог;
- ім'я каталогу для запису розшифрованих файлів.

Список файлів містить імена файлів що необхідно розшифрувати. Файли додаються до списку за допомогою кнопки "Додати" та стандартного діалогового вікна вибору файлів ОС. Для видалення файлів зі списку необхідно виділити відповідні файли у списку та натиснути кнопку "Видалити".







Признак запису розшифрованих файлів у окремий каталог встановлює необхідність запису розшифрованих файлів у окремий каталог що задається параметром "Каталог для запису розшифрованих файлів".

Экажіть файли, які необхідно перевірити		
Ім'я файлу	Стан	
	Подат	и
Экажть (за необхідністо) каталог для запису Файлів би	<u>Подат</u> ез ЕЦП	иВидалити
Экажть (за необлядністо) каталог для сапису файлів би Пвикористовувати окрамий каталог	Подат вз ЕЦЛ	л Видалити
Экажть (за необхідністо) каталог для запису файлів бе Використовувати окрамий каталог	Додат 25 ЕЦЛ	я Відэлті Змнитя

Рисунок 7.12

Після встановлення значень параметрів, вікно розшифрування файлів може мати вигляд як наведено на рис. 7.13.

la coatian		Стан	1
C:\Program Files\Micro	soft Games \Chess \Chess \Chess exe.p.7e soft Games \Chess \ChessMCE.png	Не розшифрований Не розшифрований	
		Додати	видали

Рисунок 7.13

Для розшифрування файлів необхідно натиснути кнопку "Розшифрувати". Після розшифрування буде виведено інформацію про результати розшифрування (рис. 7.14).

В разі вдалого розшифрування є можливість переглянути інформацію про розшифровані файли (рис. 7.15), для чого необхідно натиснути на запис про відповідний файл.

За замовчанням (якщо не встановлено окремого каталогу для розшифрованих файлів) розшифровані файли будуть записані до того ж каталогу у якому знаходилися зашифровані.







незультати розшифрування файлів	
м'я файлу	Ім'я розшифрованого файл
 [■] C:\Frogram Files\Microsoft Games\Chess\Chess\ChessMCE.png.p.7e [■] C:\Frogram Files\Microsoft Games\Chess\ChessMCE.png.p.7e 	C.\Chess.exe (розшифрован C.\ChessMCEpng (розшифр

Рисунок 7.14

Підписан	і та зашифровані	дані	×
1	Підписані та	зашифровані дані	
\$	Відправник:	Користувач	
	Організація та підрозділ:	AT "IIT" AT "IIT"	
	Посада:	Користувач	
	Сертифікат		
	LICK:	AT "IIT"	
	Реєстраційний номер:	16F7F644892E7F1E04000000100000019000000	
	Час підпису:	30.11.2012 14:46:57	
ම Д ет	тальна інформація		
		ОК]

Рисунок 7.15

7.5 Помилки, що можуть виникати під час роботи програми

7.5.1 Помилка під час підпису, перевірці або шифруванні даних

Вікно з повідомленням про помилку наведене на рисунку 7.16.

Пошук та визначення	статусу серти	фіката 🛛 🔀		
Статус сертифіката можливо визначений не вірно. Використати його?				
🗿 <u>Сертифікат</u>		Так Ні		
Результати пошуку та визначення статусу:				
 Пошук чи перевірка сертифіката через ОСЅР-сервер Перевірка сертифіката у файловому сховищі 		Виникла помилка при обміні даними з DCSP-сервером Сертифікат чинний		
Інформація про сертифікат:				
🚎 Власник 🔄 ЦСК 🙀 РН	Room_22_ci ЦСК IIT 1F263E0725	ystal_test iDDE 97A0400000200000029000000		
	Рисунов	< 7.16		



Центральний офіс ТОВ «Арт-мастер» вул. Сурикова, 3 (піт А), Київ, 03035, Україна тел.: +380 44 248-97-91, 248-98-27, факс: +380 44 248-98-14 е-паії: post@am-soft.ua; http://www.am-soft.ua

Така помилка може виникати:

- якщо не вказано параметри (адреса, порт) proxy-сервера, а підключення до сервера обробки запитів ЦСК здійснюється за допомогою нього;
- якщо не вірно вказано параметри аутентифікації proxy-сервера;
- якщо особистий ключ користувача не є дійсним;
- якщо відсутній доступ до (TSP, OCSP або LDAP) сервера ЦСК.

7.5.2 Помилка під час шифрування у зв'язку з відмінністю параметрів ключів користувачів

Якщо параметри ключів користувачів для яких виконується шифрування будуть відрізнятись від параметрів ключів користувача що виконує шифрування, користувачу буде видане повідомлення про неможливість виконування шифрування у зв'язку з відмінністю параметрів та процес шифрування буде припинено. Для запобігання цього слід переглянути сертифікат користувача на адресу якого виконується шифрування та перевірити відповідність параметрів власних ключів параметрам ключів цього користувача.

8 ПОВІДОМЛЕННЯ ОПЕРАТОРУ ТА ДОВІДКОВА СИСТЕМА

8.1 Перехід до web-сайту центра сертифікації ключів

Для переходу до web-сайту центра сертифікації ключів необхідно натиснути посилання "Перейти до web-сайту ЦСК..." у головному вікні програми.

8.2 Перегляд настанови оператору

Для виведення настанови оператора необхідно обрати підпункт "Настанова оператору" в пункті меню "Допомога", або натиснути клавішу F1, або натиснути посилання "Відкрити настанову оператору..." у головному вікні програми.

ПЕРЕЛІК СКОРОЧЕНЬ

OC	Операційна система
ЕЦΠ	Електронний цифровий підпис
K3I	Криптографічний захист інформації
ДКЕ	Довгостроковий ключовий елемент
CBC	Список відкликаних сертифікатів
ЦСК	Центр сертифікації ключів
HKI	Носій ключової інформації (особистого ключа)
ПЕОМ	Персональна електронно-обчислювальна машина
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

