САЙФЕР
Системы защиты информации
Интернет-банкинг

Сайфер ПРО, ТОВ
04107, Київ, вул. Нагірна 25/27, 3-ій поверх

Тел.: +38 (044) 484-4612
Факс: +38 (044) 483-0322
E-mail: info@cipher.com.ua
Web: www.cipher.com.ua

Дата модифікації: 13.07.2021

42125815.001.IE.37

Система криптографічного захисту інформації "Шифр-X.509"

Модуль гарантованого видалення ключових контейнерів. Керівництво з експлуатації

Зміст

Список скорочень та умовних позначень

LDAP	Lightweight Directory Access Protocol
PIN	Personal Identification Number
PKCS#11	Cryptographic Token Interface (Cryptoki)
TCP	Transmission Control Protocol
USB	Universal Serial Bus
АРМ	Автоматизоване робоче місце
БД	База даних
ЕП	Електронний підпис
ОС	Операційна система
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс
СВС	Список відкликаних сертифікатів
СКЗІ	Система криптографічного захисту інформації
СУБД	Система управлінням базами даних
ЦР	Центр реєстрації
ЦСК	Центр сертифікації ключів

Введення

Огляд

Даний документ є керівництвом користувача по роботі з Модулем гарантованого видалення ключових контейнерів, призначеного для роботи під керівництвом ОС Windows 7 і вище, у складі СКЗІ «Шифр-X.509».

Модуль призначений для гарантованого видалення інформації про ключовий контейнер з різних типів носіїв, як файлових, так і захищених.

Системні вимоги

Апаратне забезпечення

Мінімальна апаратна конфігурація:

- Відповідає вимогам ОС Microsoft Windows 7.
- Вільного дискового простору: 20Мб.
- USB-порт: v1.1+.

Рекомендована апаратна конфігурація:

- Відповідає вимогам ОС Microsoft Windows 10.
- Вільного дискового простору: 1Гб.
- USB-порт: v1.1+.

Програмне забезпечення

Мінімальна конфігурація:

- Microsoft Windows 7.

Рекомендована конфігурація:

- Microsoft Windows 10.

Захищені ключові носії

Програма підтримує роботу із захищеними ключовими носіями, завдяки інтерфейсу PKCS#11, Таблиця 1.

Таблиця 1. Список підтримуваних захищених ключових носіїв

№	Виробник	Модель	Тип
1	ТОВ Автор, Україна	Author Secure Token-337	Token
2	ТОВ Автор, Україна	Author Secure SmartCard-336	SmartCard
3	ТОВ Мікрокрипт, Україна	Armorino	Token + Flash
4	Giesecke & Devrient, Німеччина	StarSign Crypto SmartCard	SmartCard
5	Giesecke & Devrient, Німеччина	StarSign Crypto USB Token	Token, Token + Flash
6	ТОВ Авест Україна, Україна	Avest Key	Token
7	SafeNet, США	SafeNet Crypto eToken	Token
8	Gemalto, США	IDPrime Series	Token+SmartCard
9	ТОВ Ефіт технолоджіс, Україна	Efit Key	Token

Встановлення та налаштування

Попередні налаштування

У цьому розділі наведені обов'язкові та не обов'язкові дії для налаштування ОС перед встановленням основного ПЗ.

Встановлення ПЗ для роботи із захищеним носієм

Для роботи сервера із захищеними носіями, обов'язковим є встановлення драйвера захищеного ключового носія чи спеціального ПЗ користувача.

Після встановлення ПЗ для роботи із захищеними носіями, слід переконатися, що захищені носії знайдені ОС та відображаються у «Диспетчере устройств». Для цього необхідно перейти «Пуск» -> «Control Panel» -> «Device Manager» -> «SmartCard Reader».

Якщо захищений носій не знайдений, слід звернутися до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника СКЗІ «Шифр-X.509».

Подальше встановлення ПЗ можливе лише після повного усунення питань пов'язаних з коректною роботою захищених носіїв.

Встановлення допоміжного ПЗ

Для виконання різних додаткових функцій, необхідна наявність додаткового ПЗ, яке дозволить системному адміністратору успішно виконати функції налаштування та перевірки налаштувань серверів ЦСК, а також самого робочого місця оператора центру прийому дзвінків.

Для цих цілей слід встановити інструментарії, який наведено у Таблиця 2.

Таблиця 2. Перелік рекомендованого додаткового ПЗ та його призначення

№	Назва	Версія	Призначення	Розповсюдження	Примітки
1	7-ZIP	18.05	Архівація журналів аудиту	Free	Необов'язково
2	Foxit PDF Reader	8.1	Перегляд супровідної документації	Free	Необов'язково
3	Free PDF Converter doPDF	9.0	Створення PDF документів	Free	Необов'язково
4	Avira Free Antivirus / ESET Smart Security/ Dr. Web Antivirus		Захист від вірусів	Комерційне	Обов'язково
Допоміжне ПЗ зі складу СКЗІ «Шифр-X.509»					
5	Модуль роботи з ключовим контейнером	2.0.0+	Перегляд вмісту ключового контейнера	Комерційне	Рекомендовано
6	Модуль перегляду об'єктів PKI	2.0.0+	Перегляд сертифікатів, запитів на сертифікати, CRC	Комерційне	Рекомендовано

Встановлення

Для встановлення необхідно завершити всі невиконувані задачі, після чого запустити файл **setup_CiX509_KCC.exe** з інсталяційного носія, після чого з'явиться стандартний діалог системи захисту ОС про дії, які можуть привезти для порушення функціонування ОС.

Слід обрати **Далее** для переходу до діалогу **Приветствия**, Рис. 1.

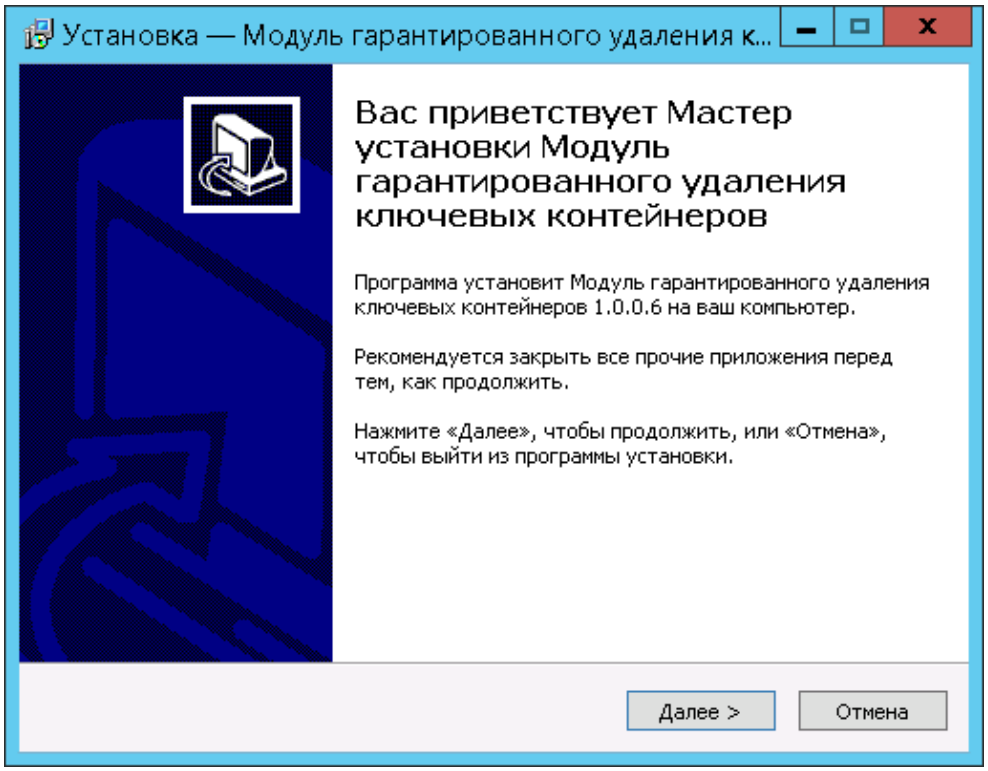

Рис. 1. Діалог Приветствие

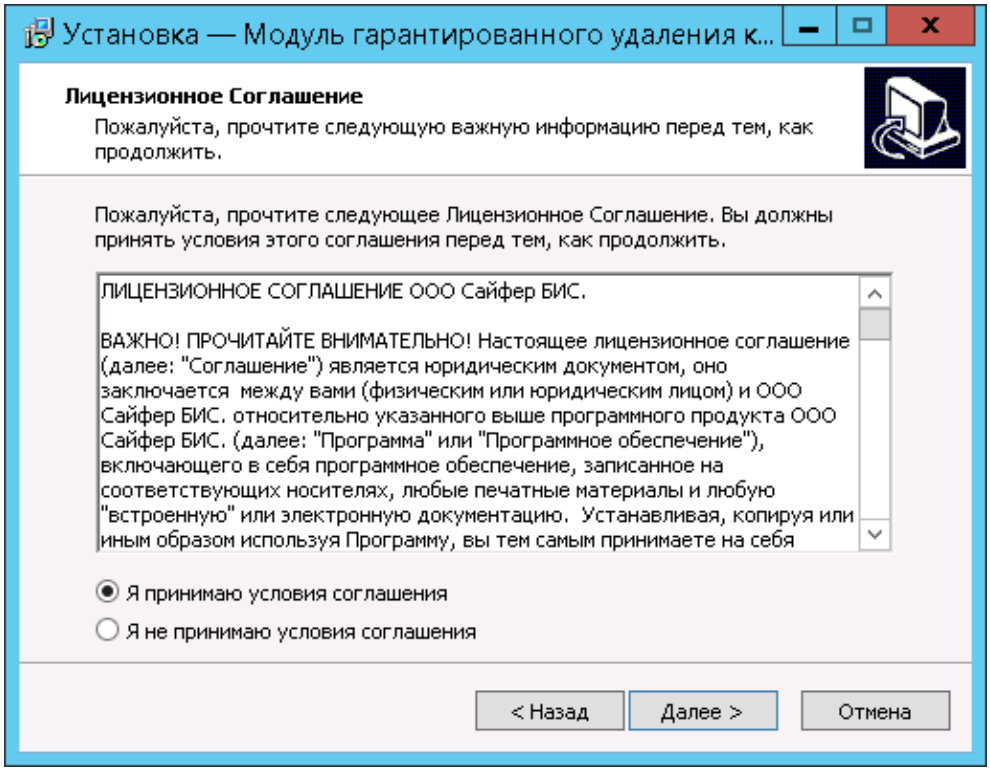

Рис. 2. Діалог з інформацією про ліцензію на використання ПЗ

На діалозі **Приветствия** слід натиснути для переходу на наступний діалог, Рис. 2, для ознайомлення з **Лицензионным соглашением**, тобто з ліцензією про використання ПЗ. Для продовження встановлення слід прийняти дане погодження, явно указавши **Я принимаю условия соглашения**. Для переходу до наступного діалогу, необхідно натиснути кнопку **Далее**.

Далі відображається діалог з пропозицією обрати **Выбор папки для установки**, Рис. 3, куди буде встановлено Модуль гарантованого видалення ключових контейнерів. На даний момент під ОС Windows доступна лише 32-х розрядна версія програми.

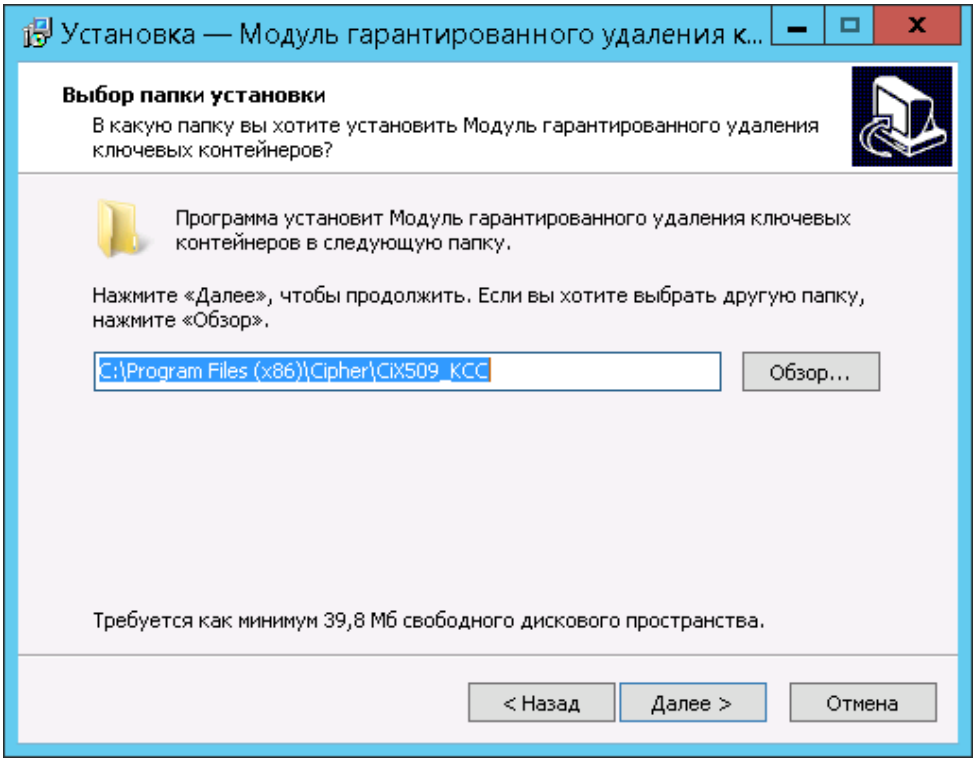

Рис. 3. Діалог вибору папки, куди буде встановлено модуль

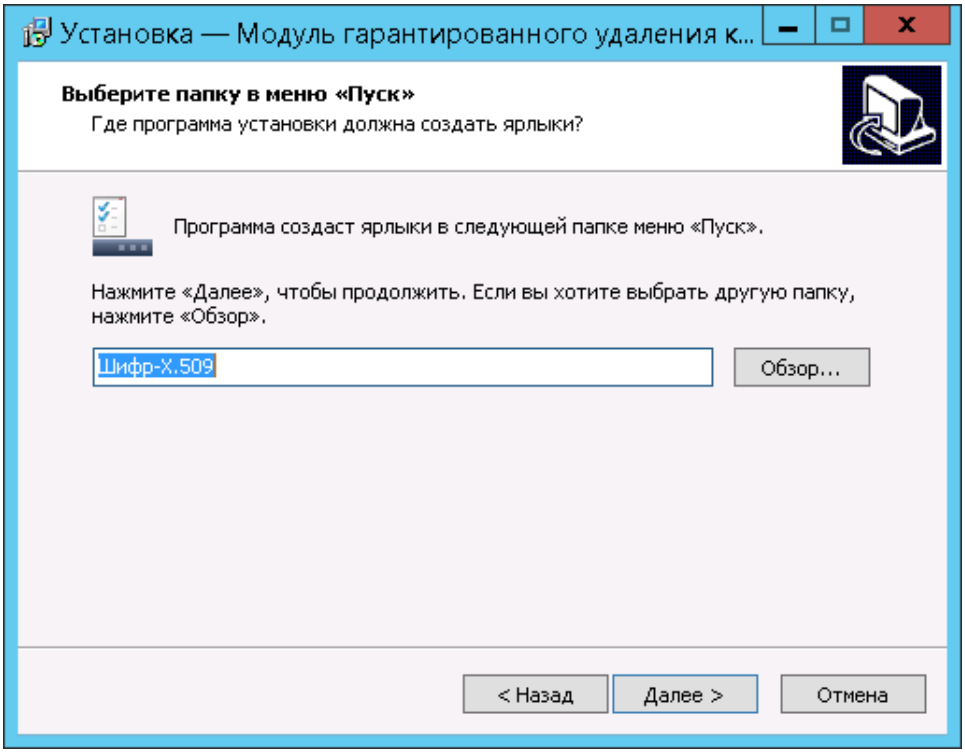

Рис. 4. Діалог вибору папки в меню «Пуск», куди буде встановлено компонент

Наступний діалог **Выбор папки в меню «Пуск»**, дозволить обрати в яку папку в меню «Пуск» будуть встановлені компоненти Модулю гарантованого видалення ключових контейнерів, Рис. 4.

Наступний діалог **Выберите дополнительные задачи**, дозволяє вказати, чи слід створювати ярлики застосування на робочому столі, Рис. 5.

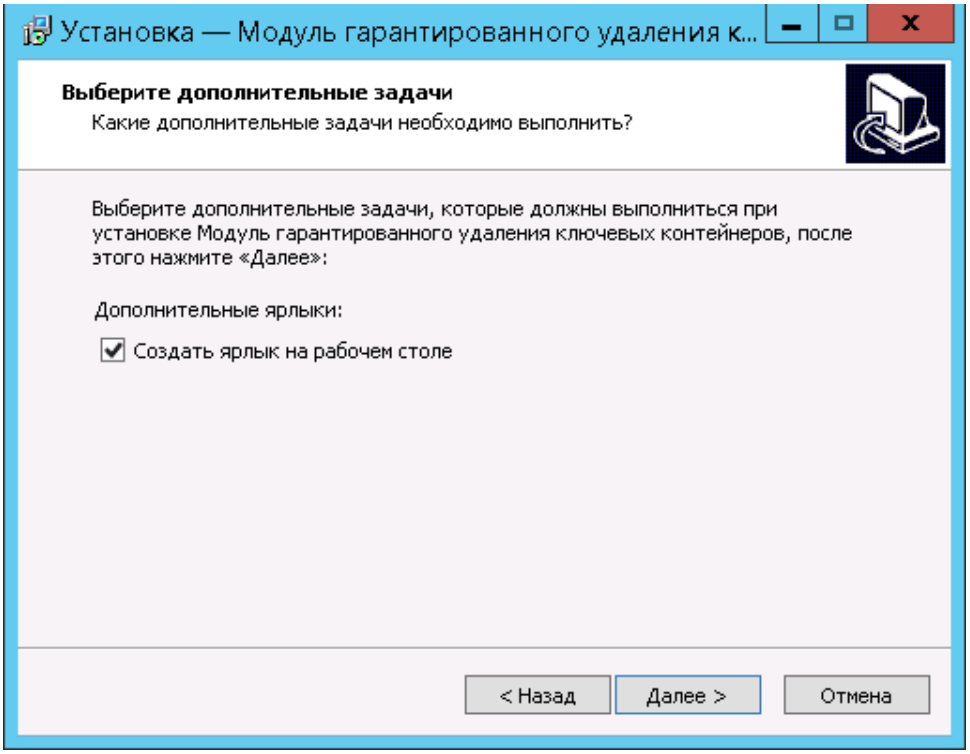

Рис. 5. Діалог вибору додаткових задач

Наступний діалог **Все готово к установке**, дозволяє в одному місці побачити всі налаштування та безпосередньо приступити до копіювання файлів, Рис. 6, для початку встановлення слід натиснути кнопку **Установить.**

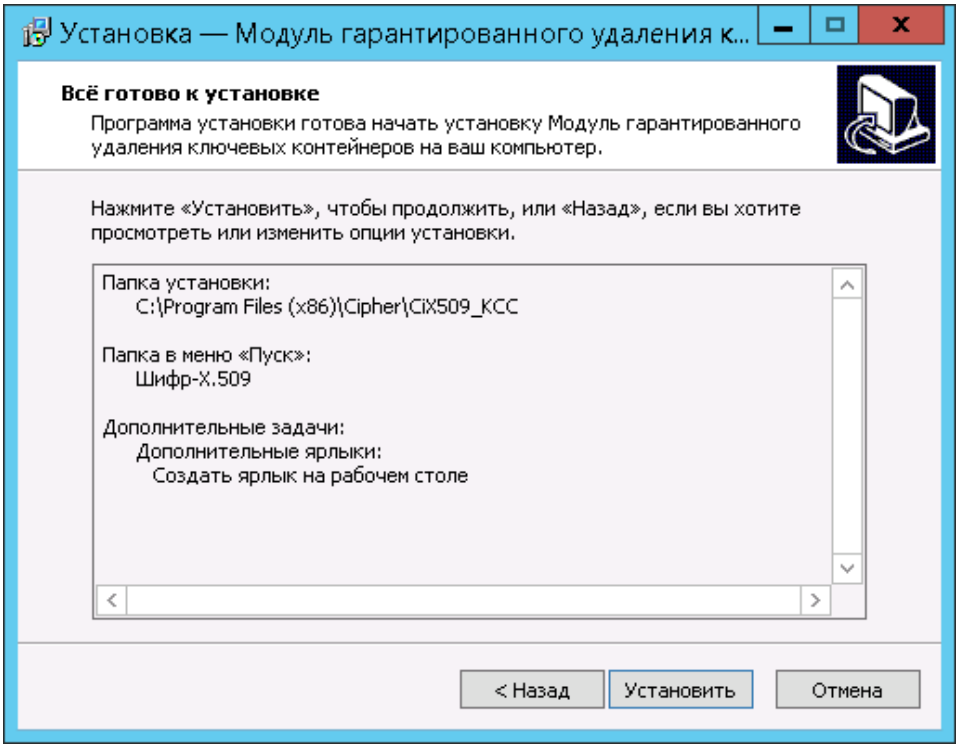

Рис. 6. Діалог перегляду налаштувань встановлення

Наступний діалог **Установка**, дозволяє продемонструвати процес копіювання файлів у систему користувача та налаштування застосування, Рис. 7. Процес встановлення можна перервати натисканням кнопки **Отмена**.

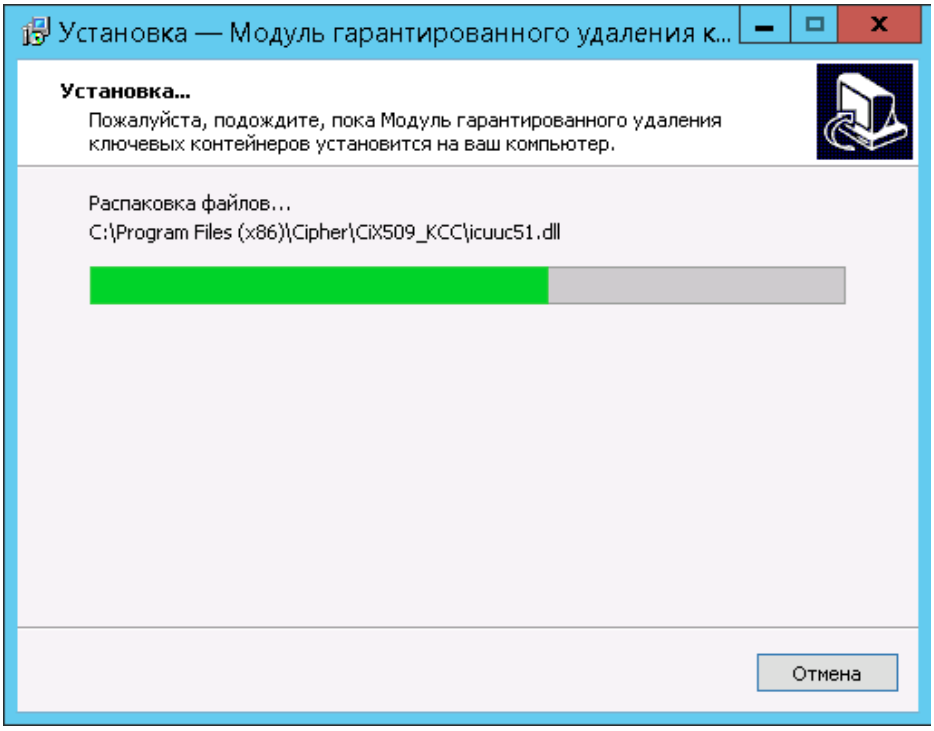

Рис. 7. Діалог відображення процесу встановлення

Після успішного копіювання файлів модуль та наступні налаштування його для роботи в ОС, відображається діалог, з пропозицією провести запуск модуля, Рис. 8.

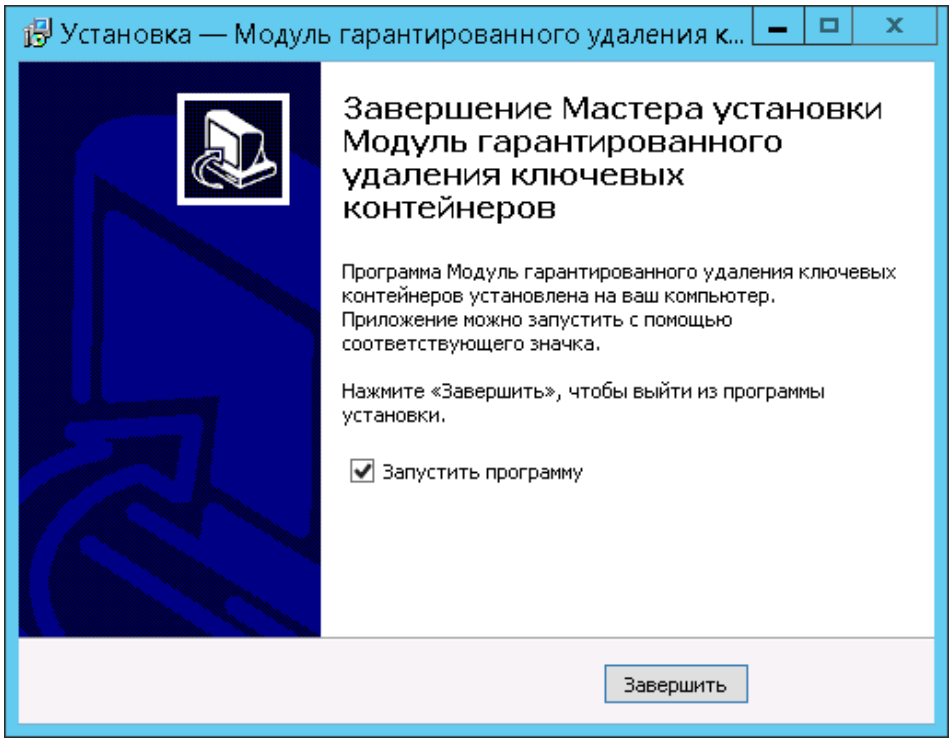

Рис. 8. Діалог завершення установки

Налаштування

Модуль гарантованого видалення ключових контейнерів не вимагає налаштування та готовий до роботи одразу після встановлення.

Робота з програмою

Запуск

Запуск модуля здійснюється із меню «Пуск->Шифр-X.509->Модуль гарантированного удаления ключевых контейнеров».

Після запуску, відображається головне меню застосування, Рис. 9.

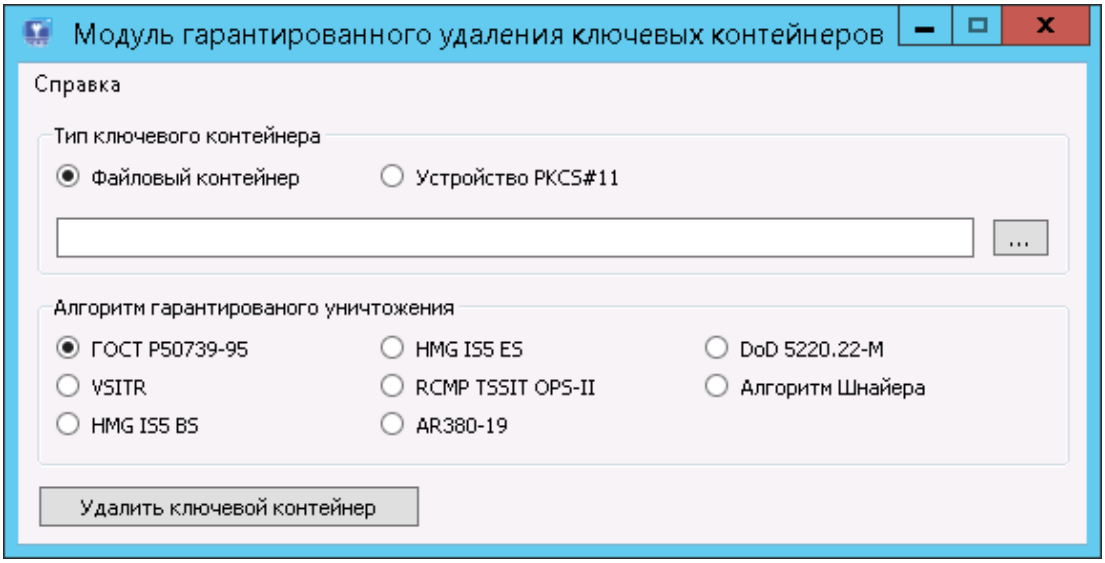

Рис. 9. Вигляд головного вікна модулю

Робота з файловими контейнерами

Модуль працює, як з файловими ключовими контейнерами, так і з захищеними носіями, що підтримують інтерфейс PKCS#11.

Для роботи з файловими контейнерами, необхідно обрати тип ключового носія, як «Файловый контейнер» та натиснути кнопку «…» після чого буде відображено діалог обрання ключового контейнера, Рис. 10.

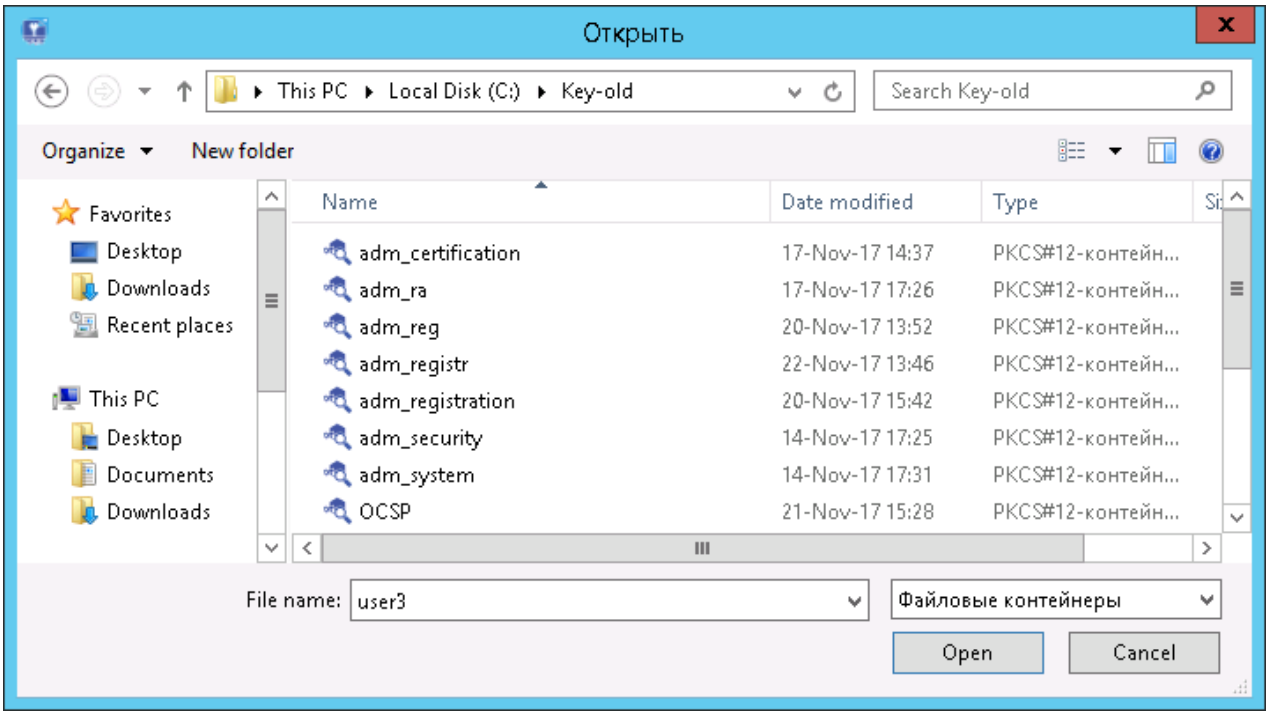

Рис. 10. Діалог вибору файлу ключового контейнера

Далі необхідно обрати алгоритм видалення ключового контейнера та натиснути кнопку «Удалить ключевой контейнер». Далі буде відображено діалог з підтвердженням видалення контейнера. Для продовження видалення контейнера здійснити підтвердження, див. Рис. 11.

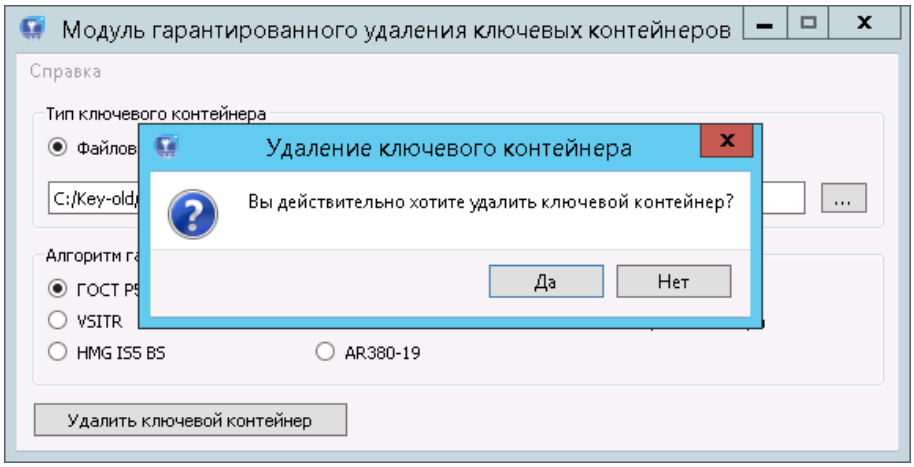

Рис. 11. Діалог підтвердження знищення контейнера

При успішному видаленні контейнера з’явиться повідомлення про успішне видалення, Рис. 12.

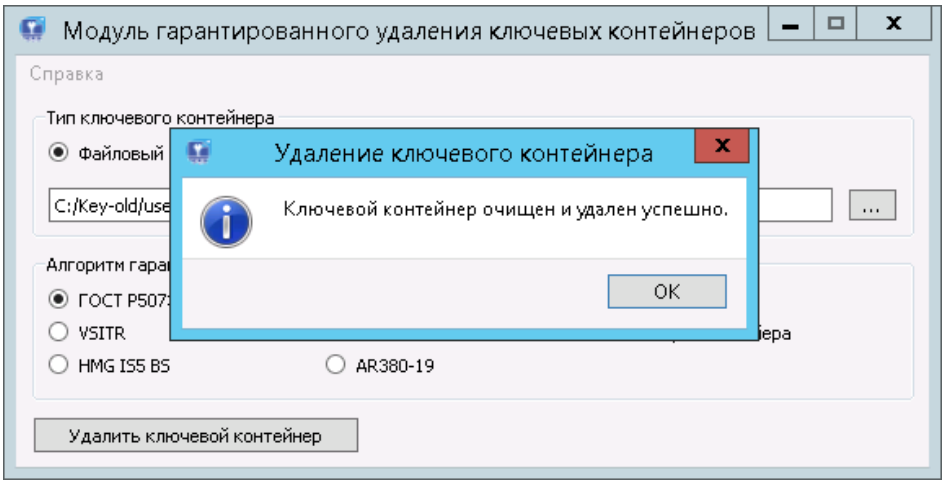

Рис. 12. Повідомлення про успішне видалення контейнера

У випадку видалення або читання контейнера буде відображено відповідне повідомлення, Рис. 13.

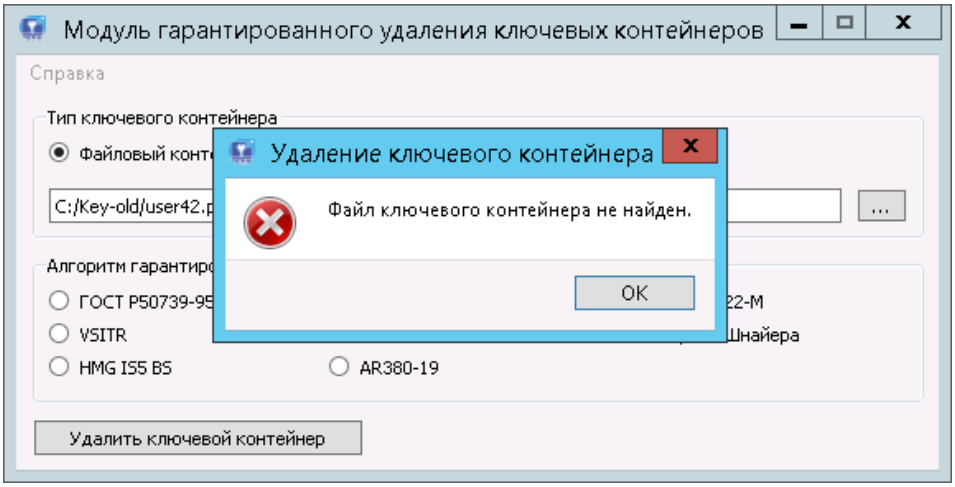

Рис. 13. Повідомлення про помилку

Робота із захищеними ключовими носіями, які підтримуються PKCS#11

Робота із захищеними носіями аналогічна до роботи із файловими контейнерами. Для цього необхідно змінити позначку на пристрій PKCS#11 та з випадаючого списку підключений носіїв обрати необхідний пристрій, див. Рис. 14, Рис. 15, Рис. 16.

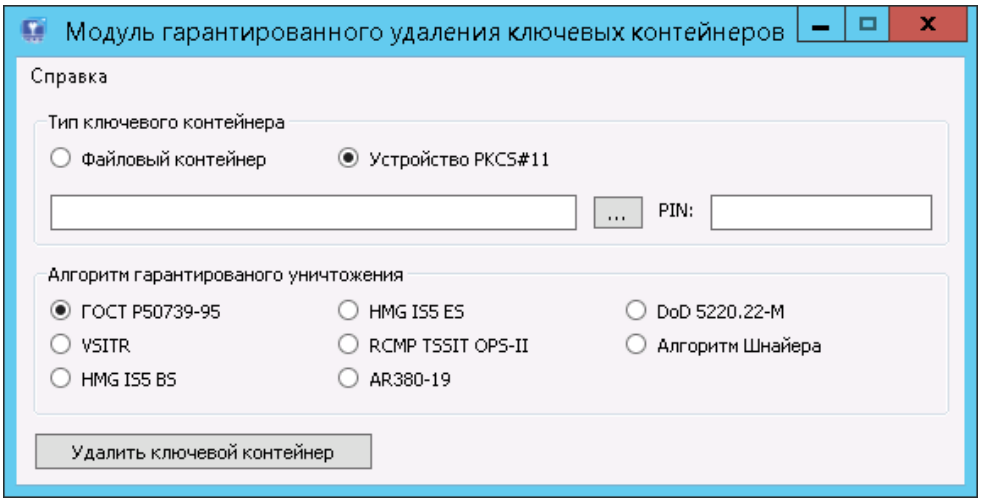

Рис. 14. Вказівка до використання PKCS#11 апаратного носія

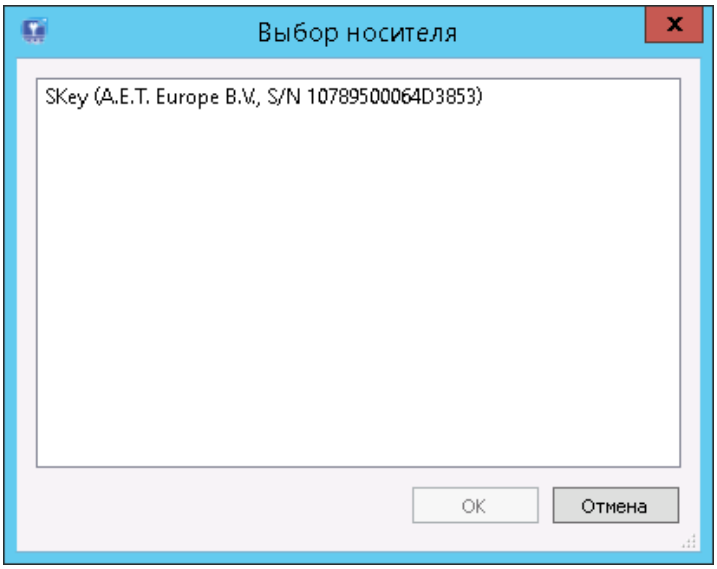

Рис. 15. Вибір PKCS#11 апаратного носія зі списку доступних

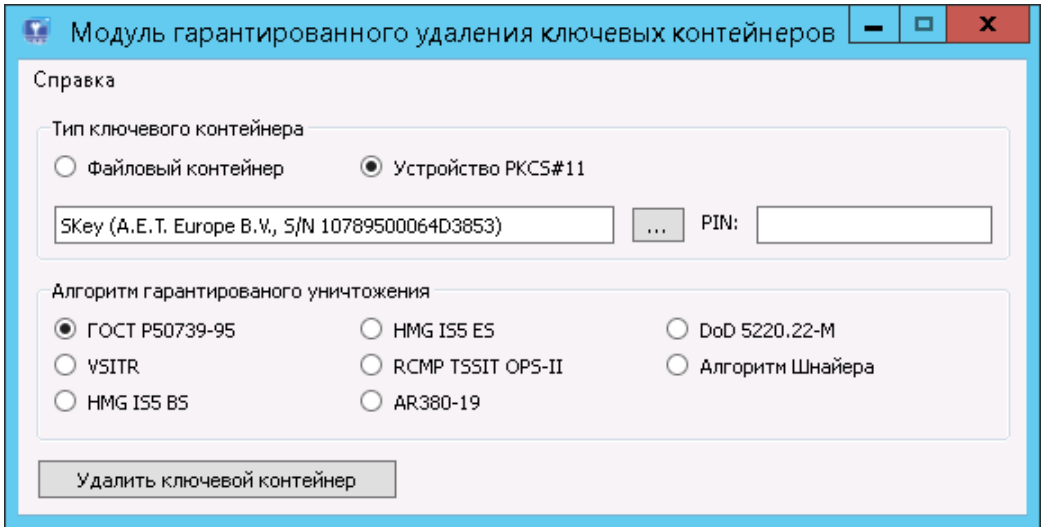

Рис. 16. Робота із захищеним носієм

Далі, необхідно ввести PIN-код для авторизації пристрою, обравши алгоритм видалення та натиснути кнопку «Удалить ключевой контейнер», Рис. 17.

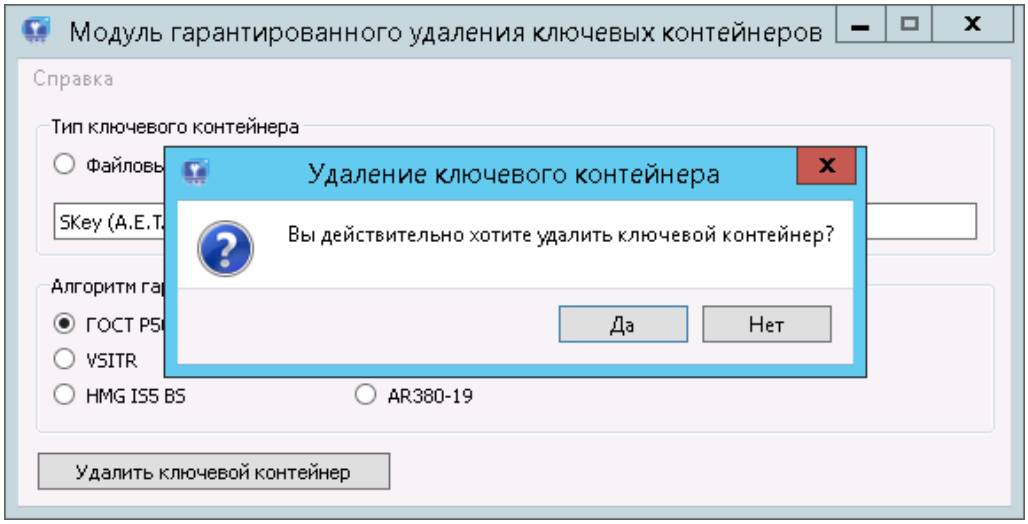

Рис. 17. Видалення контейнера з апаратного PKCS#11 носія

У випадку успішної операції буде відображено повідомлення про успішне видалення, Рис. 18, чи повідомлення з текстом помилки, Рис. 19.

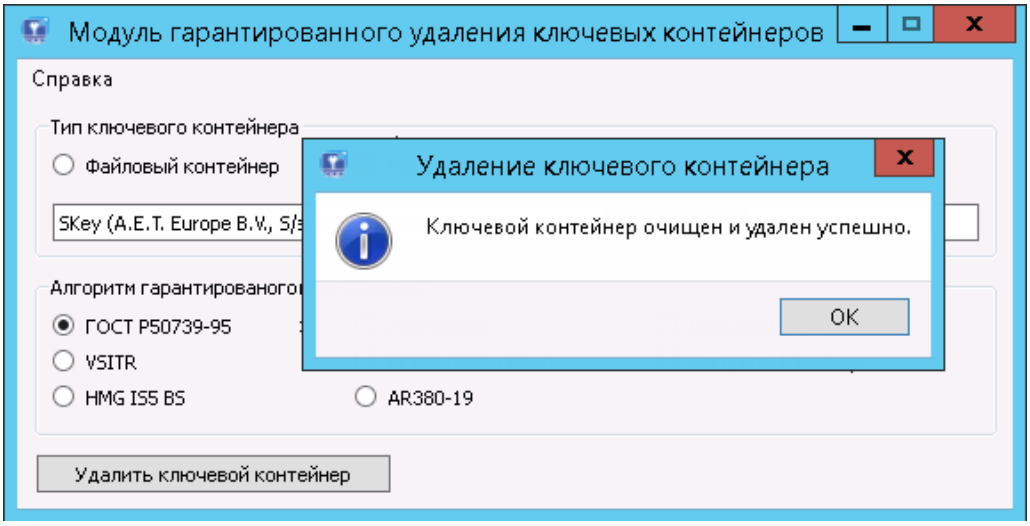

Рис. 18. Результат успішної очистки та видалення ключового контейнера

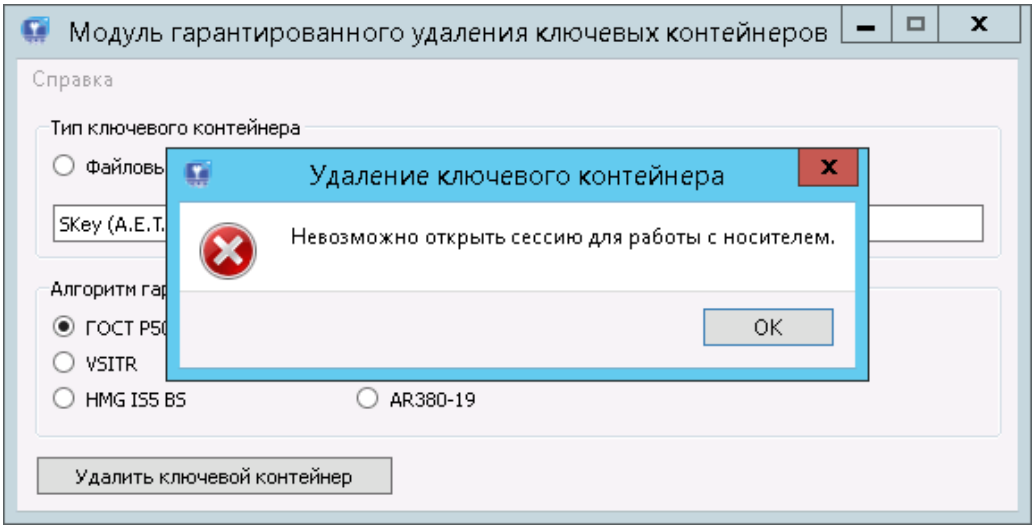

Рис. 19. Повідомлення про помилку

Інформація про програму

Для перегляду інформації про програму необхідно обрати пункт меню «Справка», далі «О Программе».

Дана функція дозволяє відобразити діалогове меню, на якому відображається логотип, назва, версія продукту, інформація про авторські права, Рис. 20.

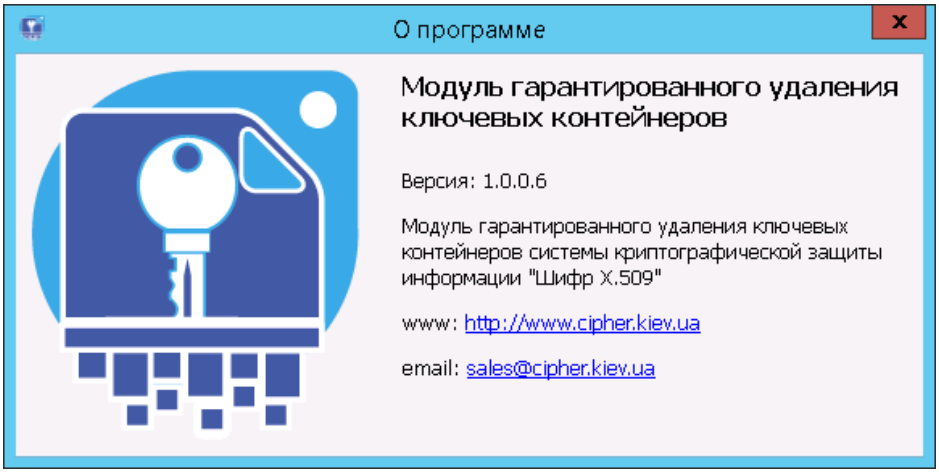

Рис. 20. Вікно «О программе»

Набір алгоритмів гарантованого видалення ключових носіїв

Для гарантованого видалення ключових носіїв використовуються наступні алгоритми:

- Британський HMG IS5 BS, ES [1].
- Російський ГОСТ Р50739-95 [2].
- Армія США AR380-19 [3].
- Міноборони США DoD 5220.22-M (E) [4].
- Канадський RCMP TSSIT OPS-II [5].
- Німецький VSITR [6].
- Алгоритм Шнайера [7].

Використовувані джерела

1. The HMG IS5 data sanitization method. URL: http://pcsupport.about.com/od/termshm/g/hmg-is5.htm
2. GOST R 50739-95. URL: http://pcsupport.about.com/od/termsg/g/gost-r-50739-95.htm
3. AR 380-19. URL: http://pcsupport.about.com/od/termsag/g/ar-380-19.htm
4. DoD 5220.22-M. URL: http://pcsupport.about.com/od/termsd/g/dod-5220-22-M.htm
5. RCMP TSSIT OPS-II. URL: http://pcsupport.about.com/od/termsr/g/rcmp-tssit-ops-ii.htm
6. VSITR. URL: http://pcsupport.about.com/od/termsv/g/vsitr.htm
7. Schneier method. URL: http://pcsupport.about.com/od/termss/g/schneier-method.htm