АВТОР
системи інформаційної безпеки

Програмне забезпечення «CryptoFiles»

Настанова користувача

АЧСА.32248356.00187 96-01

Аркушів 23

2014

Зміст

1. Вступ

Документ містить опис програмного забезпечення «CryptoFiles», а також порядок експлуатації носіїв ключової інформації – електронних ключів «Secure Token-337F» (далі - «Secure Token-337F») і програмних ключів при взаємодії з даним програмним забезпеченням.

1.1. Призначення

Програмне забезпечення «CryptoFiles» призначене для створення і редагування захищених файлів (контейнерів), а також управління доступом до інформації, що міститься в них, за допомогою носіїв ключової інформації.

1.2. Сфера застосування

Програмне забезпечення «CryptoFiles» підтримує роботу під управлінням наступних операційних систем: Windows XP/Vista/7/8/8.1 і Windows Server 2000/2003/2008/2012.

1.3. Визначення і скорочення

НКІ – носій ключової інформації;

ПК – персональний комп'ютер;

ЕЦП – електронний цифровий підпис;

АЦСК – акредитований центр сертифікації ключів;

ОС – операційна система;

Сертифікат відкритого ключа (далі – «сертифікат») — цифровий документ, підтверджуючий відповідність між відкритим ключем і інформацією, що ідентифікує власника ключа. Використовується для шифрування даних, які посилаються власникові сертифікату.

2. Програмне забезпечення «CryptoFiles»

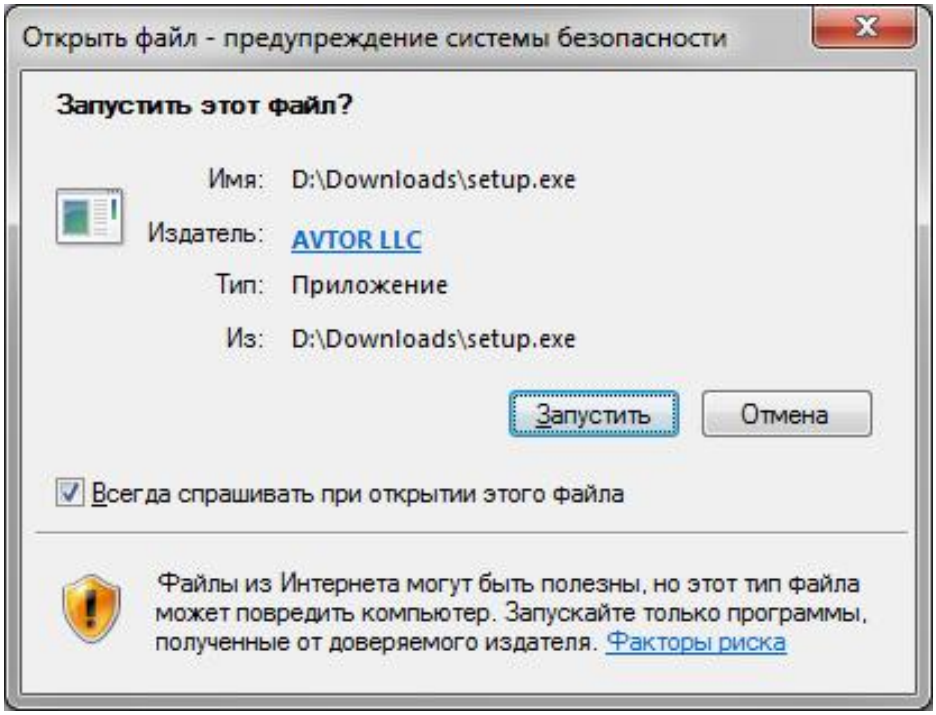
Програмне забезпечення «CryptoFiles» дозволяє організувати:

- надійно захищене зберігання важливих файлів в зашифрованому вигляді, у тому числі в загальнодоступних хмарних сховищах;
- обмін сертифікатами за допомогою хмарного сервісу «CryptoFiles»;
- синхронізацію сертифікатів за допомогою хмарного сервісу «CryptoFiles»;
- обмін файлами в зашифрованому вигляді між пристроями користувача (робочий комп'ютер, домашній комп'ютер, ноутбук, планшет, мобільний телефон);
- обмін файлами в зашифрованому вигляді з іншими користувачами, з можливістю групової (файли призначені для декількох одержувачів) і індивідуальної (файли призначені лише для конкретного одержувача) адресації;
- можливість зберігання в одному зашифрованому файлі (контейнері) різних призначених для користувача файлів, у тому числі структурованих по різних папках;
- можливість створення повноцінного зашифрованого диска[1]. Зашифрований контейнер відкривається в системі як новий диск, з яким можуть працювати будь-які програми користувача. Можливий запуск програм з цього диска і їх робота з даними, що знаходяться в зашифрованому контейнері. Після виходу з програми «CryptoFiles» файли, змінені користувачем, і нові файли, які користувач записав на диск стандартними засобами, зберігаються в зашифрованому контейнері.

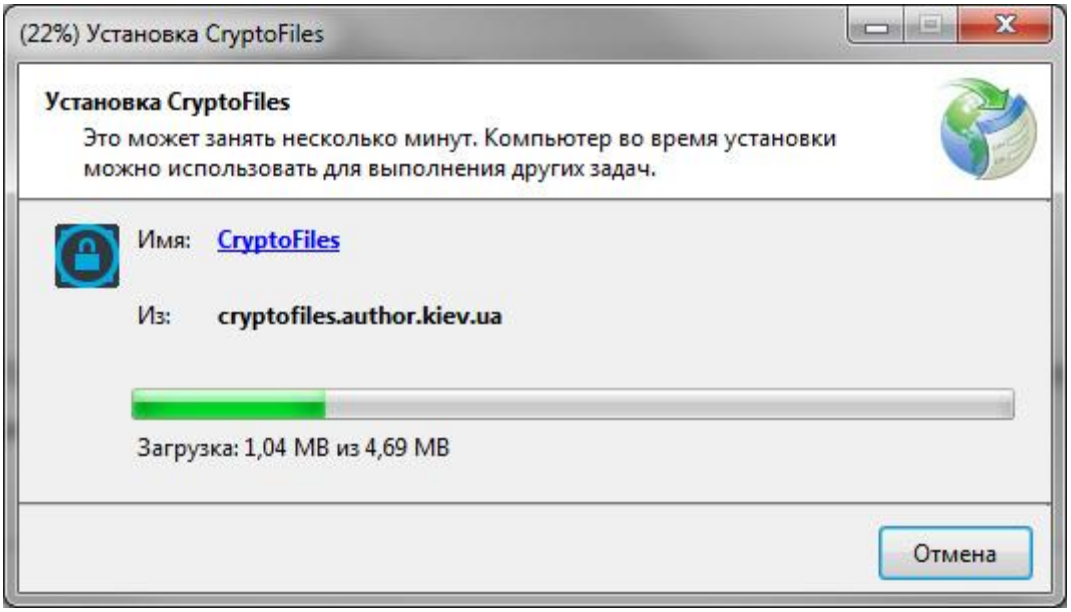
[1] Для створення зашифрованого диска використовується ресурс системного диска.

2.1 Установка програмного забезпечення «CryptoFiles»

Для установки програмного забезпечення «CryptoFiles» перейдіть по посиланню: http://cryptofiles.author.kiev.ua/setup.exe, завантажте і виконайте запуск **setup.exe**.



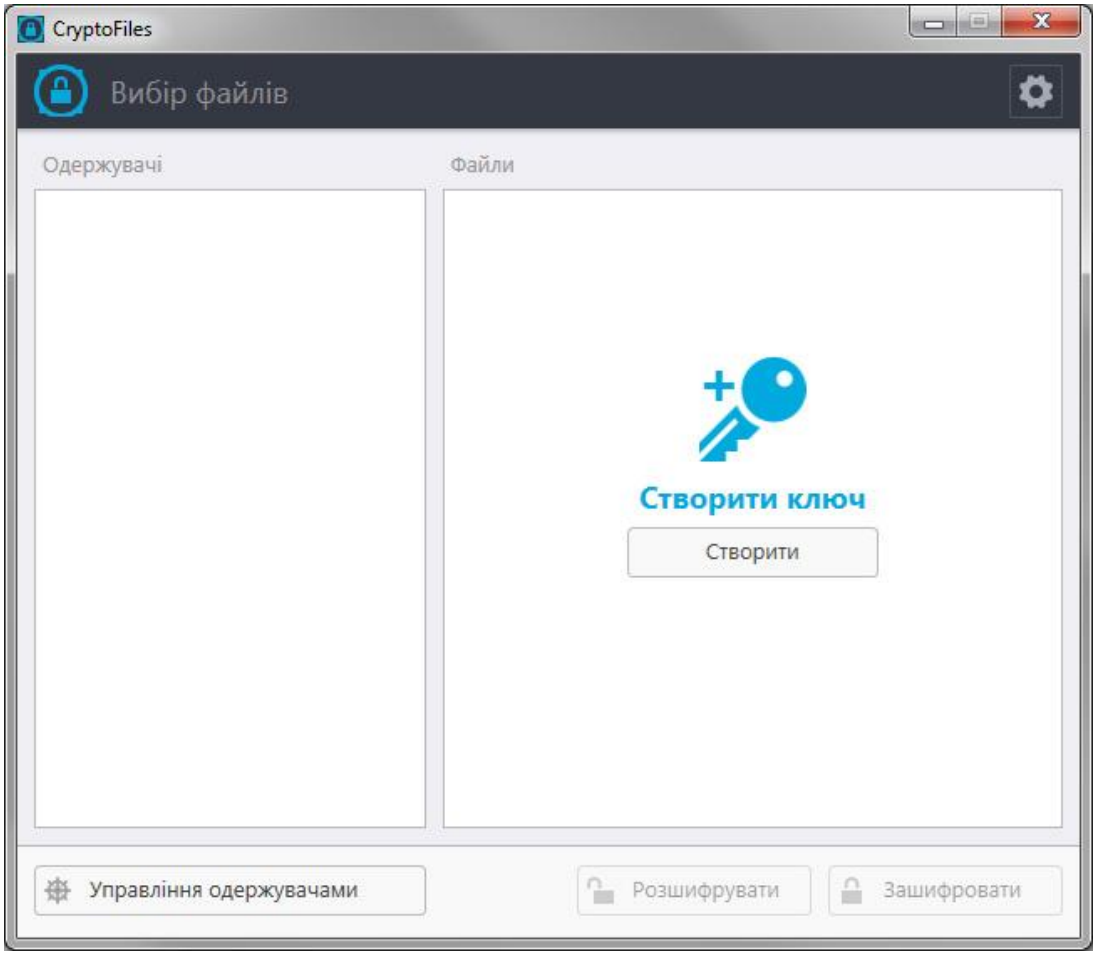
Запустить установку і виконайте необхідні дії.



Після завершення установки відбудеться запуск програми.

2.2 Запуск програмного забезпечення «CryptoFiles»

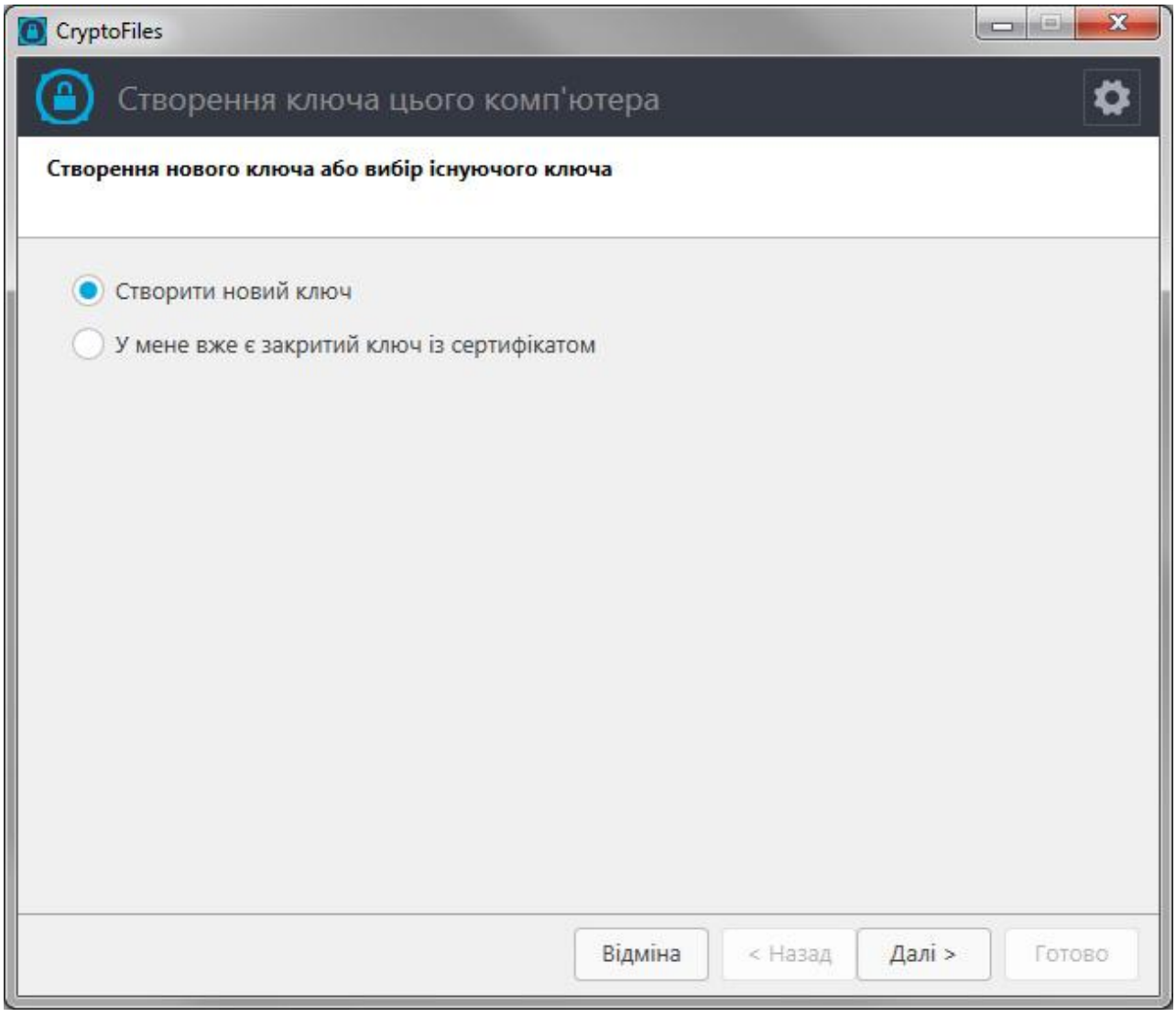
Для запуску програмного забезпечення «CryptoFiles» можна скористатися меню «Пуск» > «Avtor» > «CryptoFiles», або ярликом на робочому столі.



3. Робота з програмним забезпеченням «CryptoFiles»

3.1 Створення криптографічного ключа

Для роботи з програмним забезпеченням «CryptoFiles» необхідно створити ключ, який буде використовуватися для обміну захищеною інформацією. Натисніть кнопку «Створити…» в головному вікні програмного забезпечення для запуску майстра створення ключа і додержуйтесь подальших вказівок.

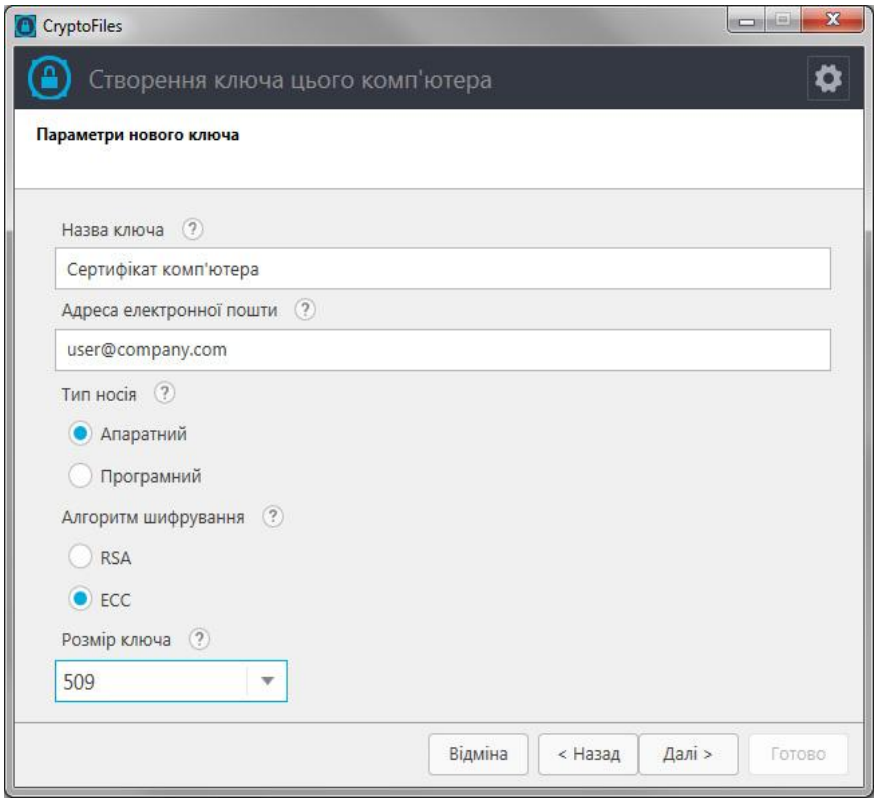


3.1.1 Створення нового ключа

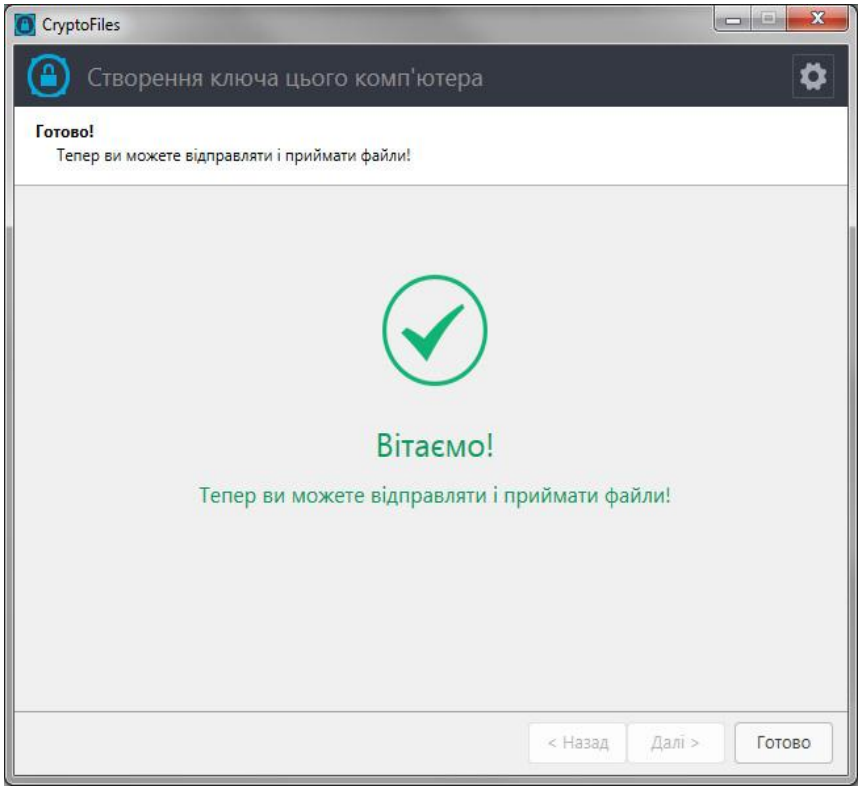
Для створення нового ключа необхідно заповнити обов'язкові поля, вказати алгоритм шифрування і вибрати НКІ. Параметри ключа з описом вказані в таблиці 1.

Таблиця 1

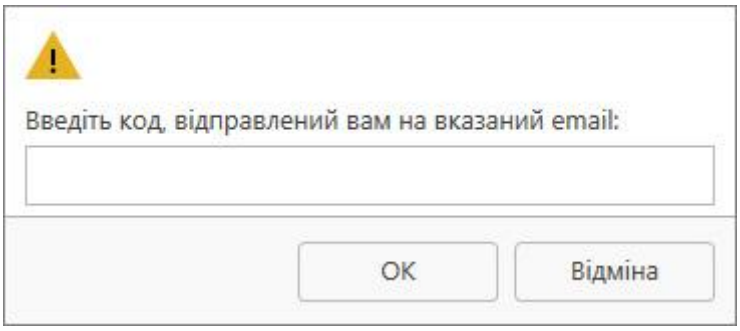
Параметр	**Опис**
Назва ключа	Cn (Common Name) – ім'я сертифікату ключа. Використовується для відображення користувача в хмарному сервісі
Адреса електронної пошти	E (Email) – електронна пошта користувача. Використовується для пошуку сертифікатів у хмарному сервісі. УВАГА: ЕЛЕКТРОННА ПОШТА ВЕРИФІКУЄТЬСЯ ШЛЯХОМ ВІДПРАВКИ ЗАХИСНОГО КОДУ НА ВКАЗАНУ АДРЕСУ
Тип носія	Тип носія визначає пристрій, на який буде записаний ключ користувача. За відсутності «Secure Token-337F» Ви можете скористатися програмним контейнером зберігання ключової інформації
Алгоритм шифрування	Алгоритм, за допомогою якого буде зашифрований Ваш персональний ключ:. RSA – міжнародний криптографічний алгоритм з відкритим ключем, що ґрунтується на обчислювальній складності завдання факторизації великих цілих чисел. Для шифрування використовується криптографічний алгоритм AES з довжиною ключа 256 біт ECC – криптографічні алгоритми, засновані на еліптичних кривих. У «CryptoFiles» використовується український стандарт ДСТУ 4145-2002. Для шифрування використовується криптографічний алгоритм відповідно до ДСТУ ГОСТ 28147:2009
Довжина ключа	Характеризує криптостійкість зашифрованих даних. Рекомендованими параметрами довжини є: – RSA – 2048 біт – ECC – 257 біт



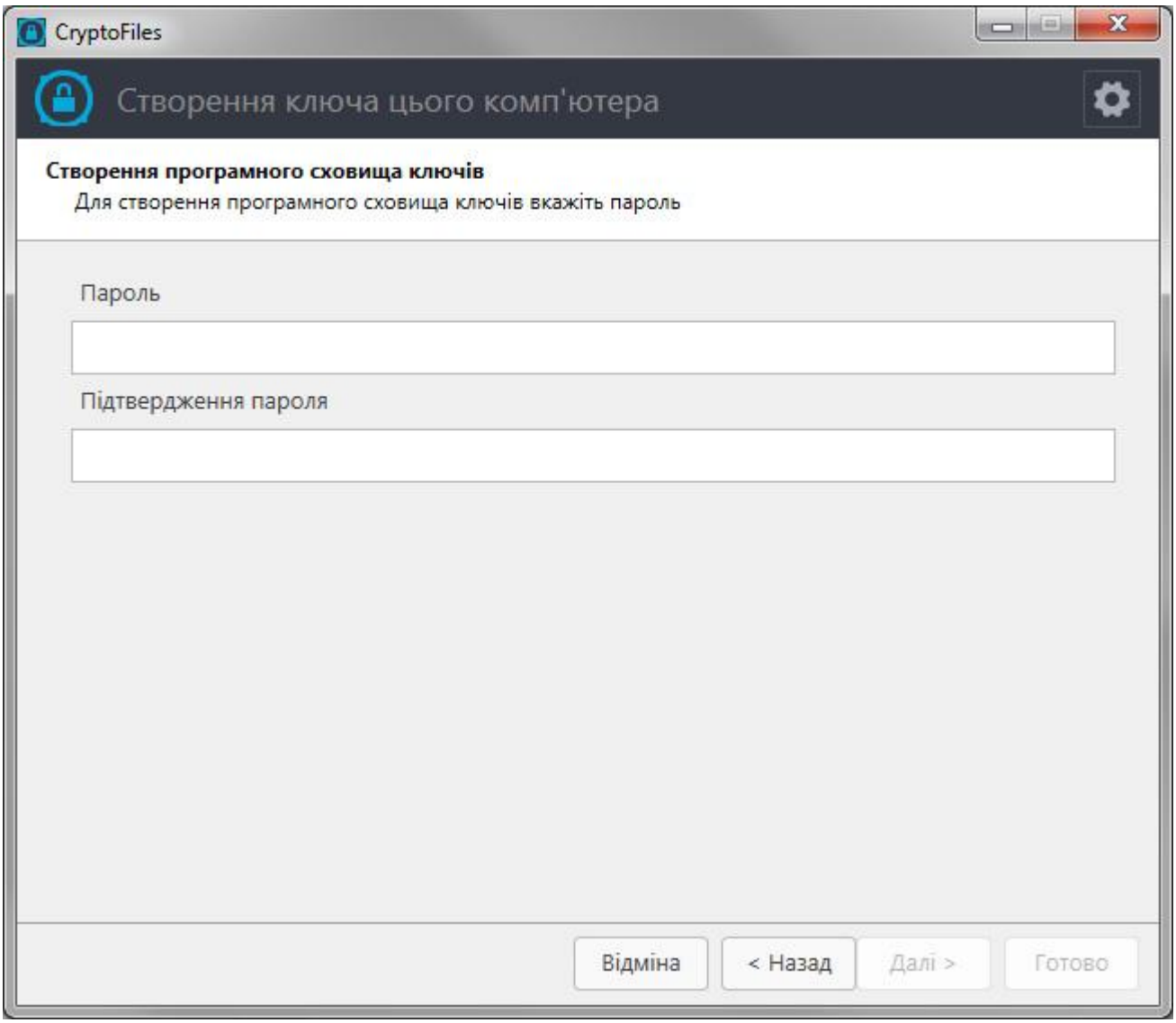
Після завершення заповнення параметрів натисніть кнопку «Далі» для створення ключа.



Для підтвердження адреси електронної пошти введіть код, який Ви отримаєте на вказану електронну пошту:

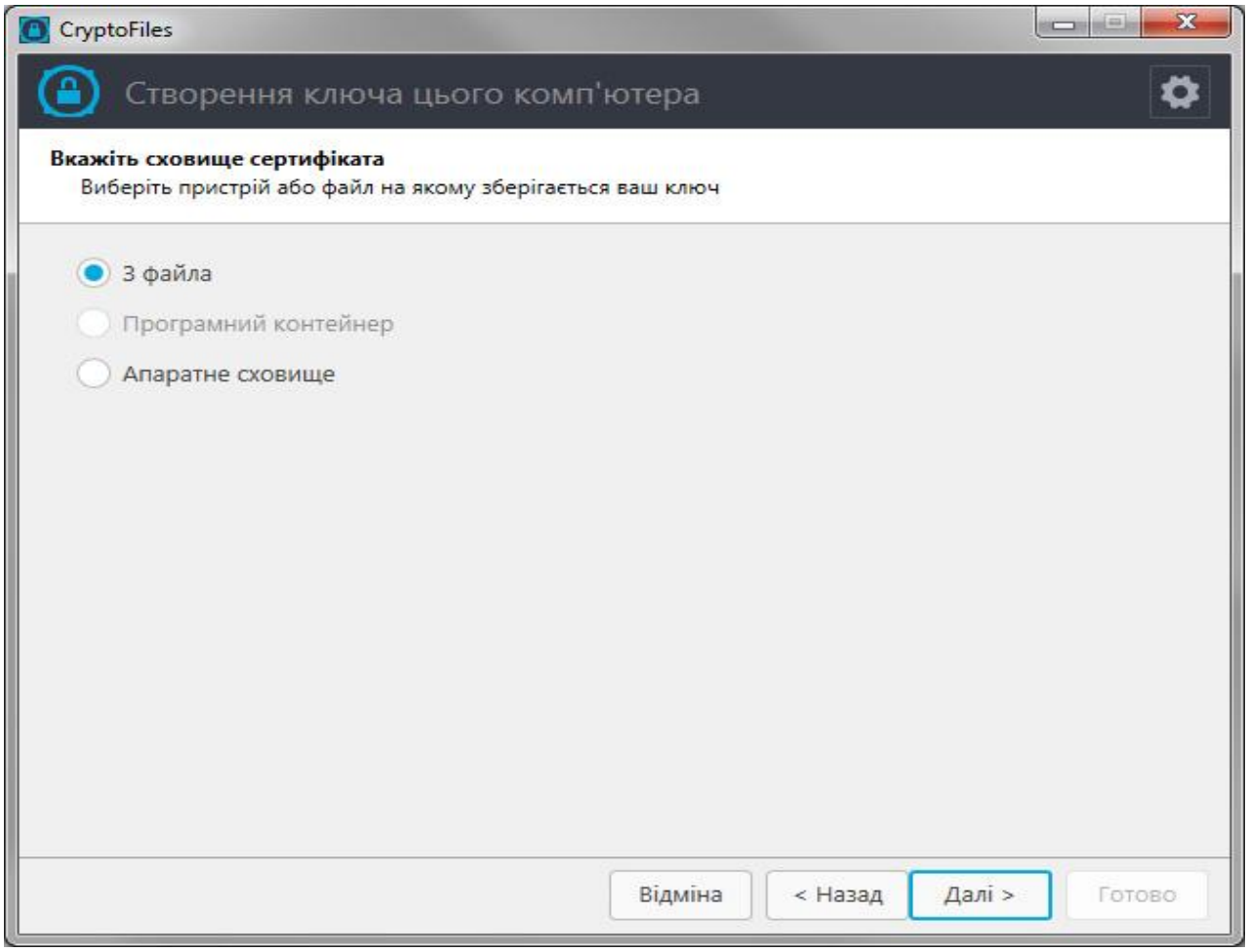


УВАГА: ПРИ ПЕРШОМУ СТВОРЕННІ ПРОГРАМНОГО КЛЮЧА, НЕОБХІДНО СТВОРИТИ ПРОГРАМНИЙ КОНТЕЙНЕР ЗБЕРІГАННЯ КЛЮЧІВ. ПРИ НАТИСНЕННІ КНОПКИ «ДАЛІ», КОРИСТУВАЧЕВІ НЕОБХІДНО ВВЕСТИ ПАРОЛЬ ДОСТУПУ ДО ПРОГРАМНОГО КОНТЕЙНЕРА.



3.1.2 Вибір існуючого ключа

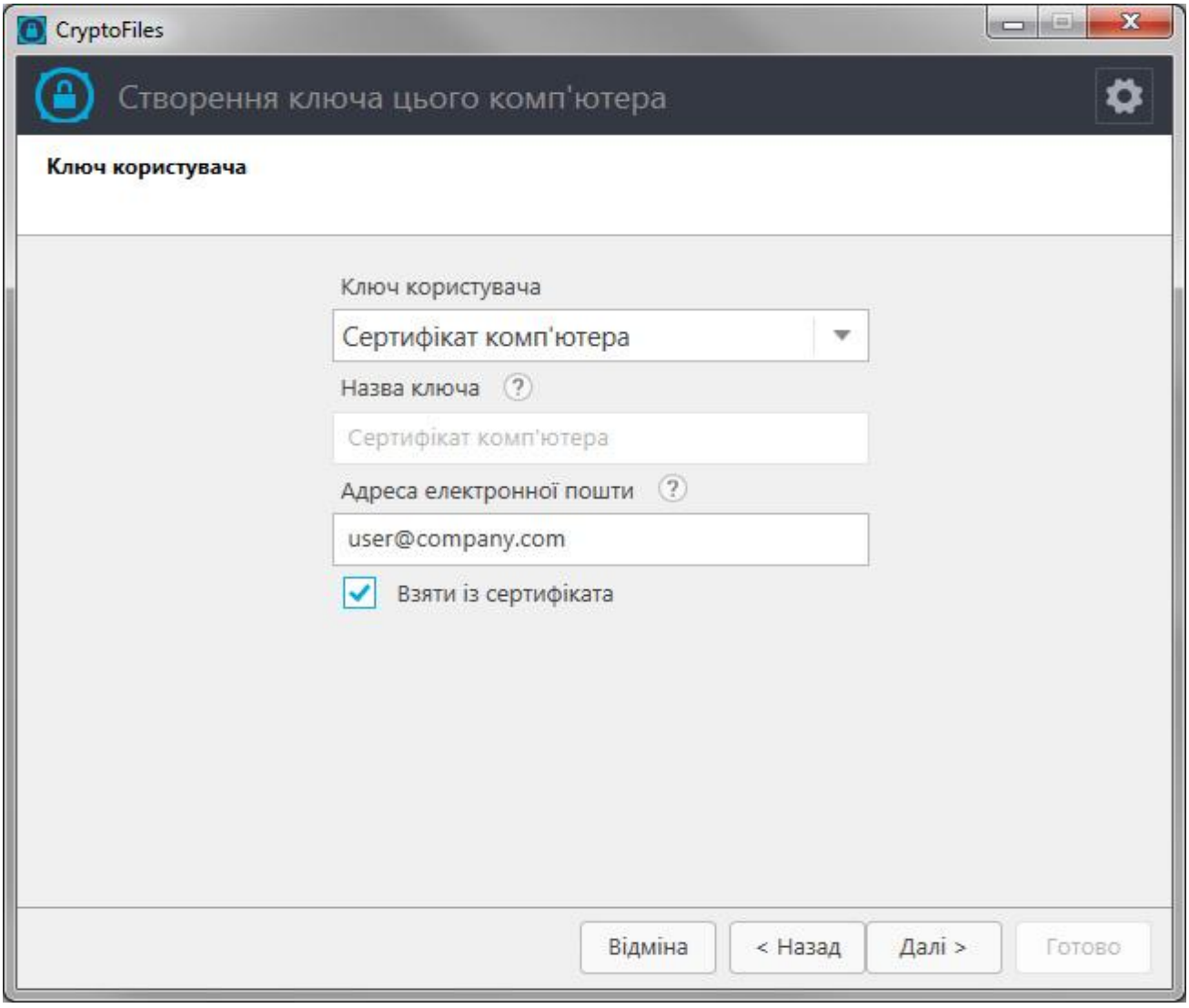
Вибір існуючого ключа виконується шляхом вказівки пристрою, на якому він зберігається, і заповнення відсутніх параметрів (таблиця 2).



Таблиця 2

Параметр	**Опис**
З файлу	Виконується витягання ключа з файлу обміну ключовою інформацією (PFX). Даний формат є одним з найскладніших криптографічних протоколів, але також залишається єдиним стандартним способом сьогодні для зберігання закритих ключів і сертифікатів в одному зашифрованому файлі
Програмне сховище	Використання закритого ключа з програмного контейнера компанії «АВТОР» УВАГА: ЦЯ ОПЦІЯ ДОСТУПНА ЛИШЕ ТОДІ, ЯКЩО ПРОГРАМНИЙ КОНТЕЙНЕР ВЖЕ ВСТАНОВЛЕНИЙ
Тип носія	Використання закритого ключа з НКІ «Secure Token-337F» компанії «АВТОР».

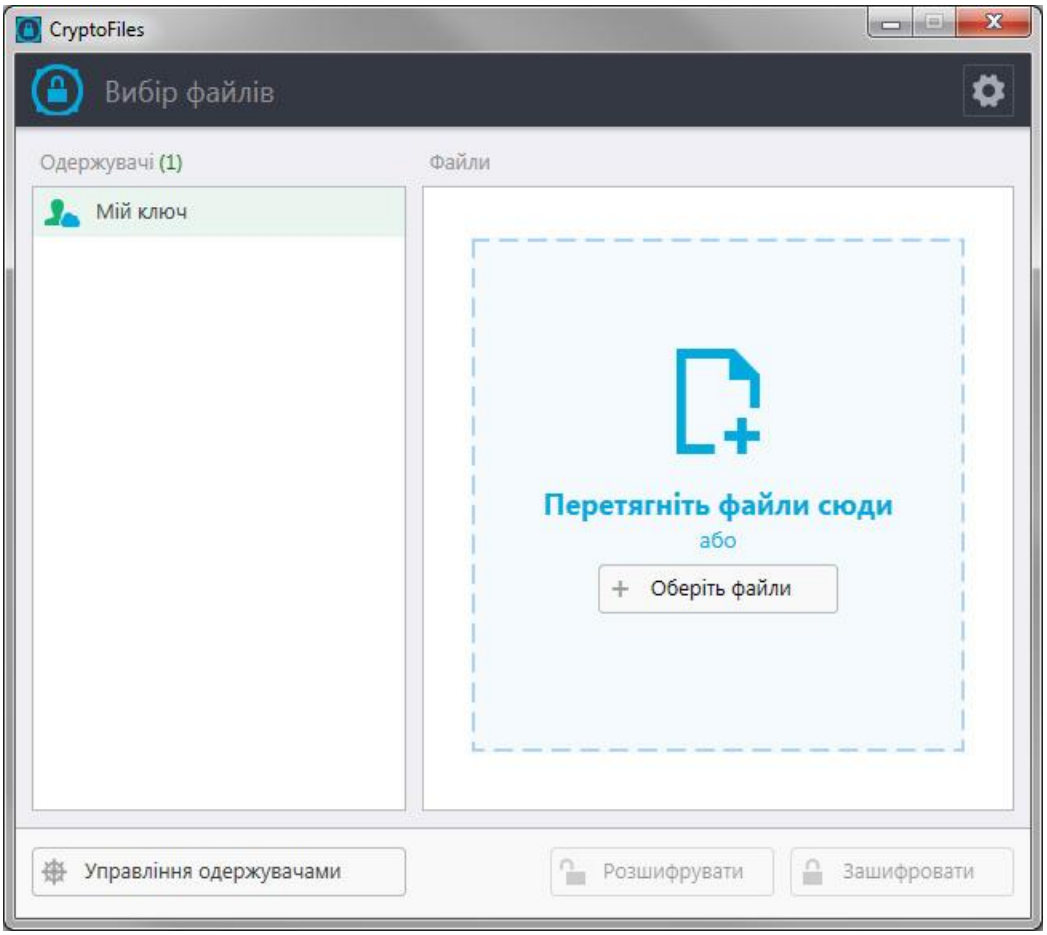
Після вибору типу пристрою[2] заповніть відсутні параметри:



Прапор «Взяти з сертифікату» заповнює поля даними, що знаходяться в сертифікаті закритого ключа при їх наявності.

[2] При підключенні тільки одного НКІ, вибір пристрою відсутній.

Після успішного створення ключа, програмне забезпечення має наступний вигляд, а його опис див. таблицю 3.



Таблиця 3

Параметр	**Опис**
1. Ключ комп'ютера	Поточний ключ комп'ютера. Має відмітне виділення кольором. Значок хмари вказує, що сертифікат ключа поміщений в хмарне сховище і доступний для пошуку іншими користувачами.
2. Область вибору файлів	Область вибору файлів Область, що підтримує технологію «Drag and Drop» для вибору файлів і подальшої роботи з ними.
3. Управління одержувачами і групами	Менеджер одержувачів і груп, який дозволяє додавати, групувати, видаляти і редагувати одержувачів. Усі функції також доступні з контекстного меню.

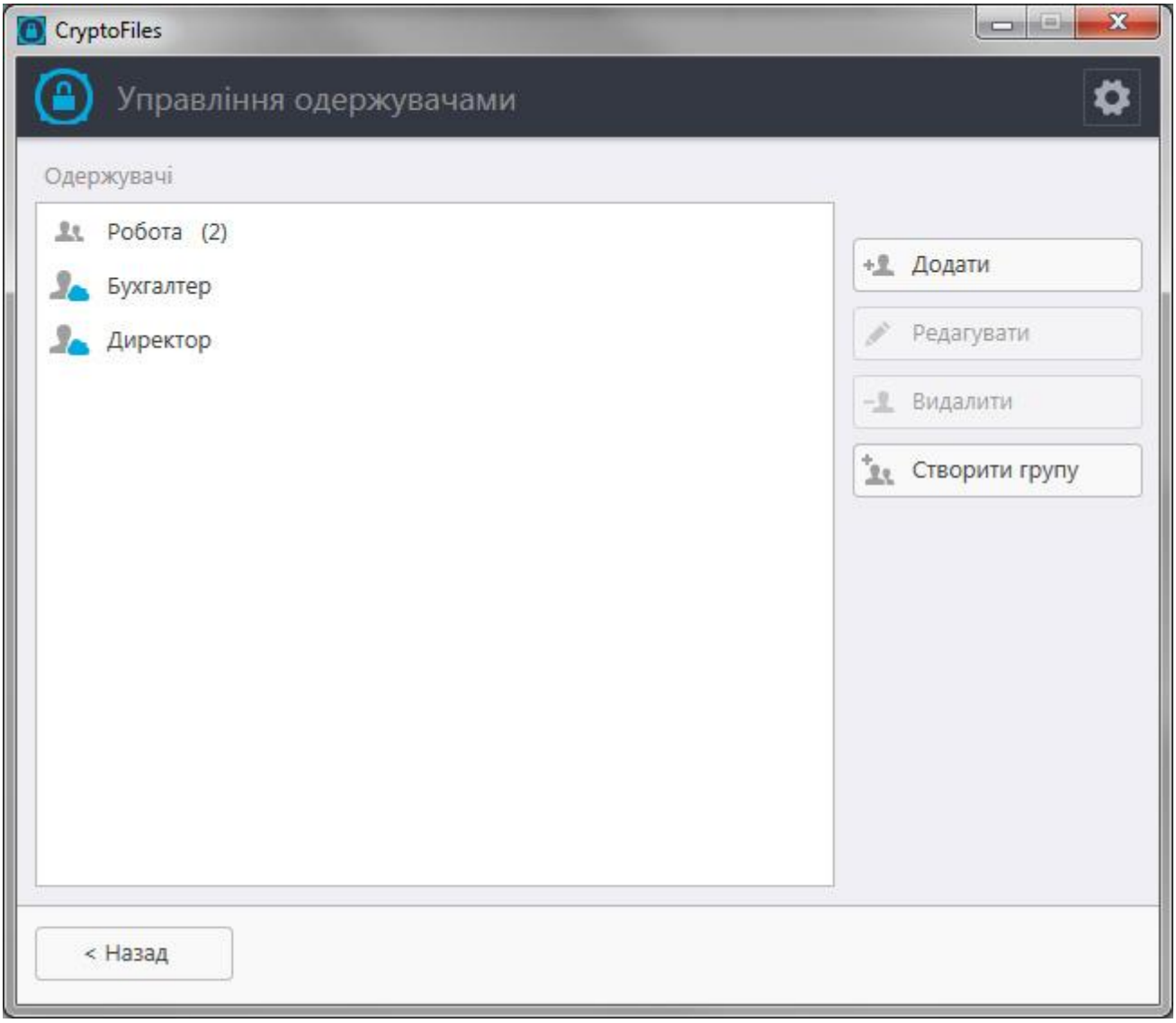
4. Налаштування програмного забезпечення	Настройки програмного забезпечення і інтерфейсу.
5. Область одержувачів	Список доступних одержувачів і груп.
6. Дії	Можливість зашифрувати або розшифрувати файл (файли).

Тепер є можливість у користувача управляти, створювати і отримувати захищені контейнери, а також управляти одержувачами.

3.2 **Управління одержувачами**

Для додавання одержувачів і груп скористайтеся кнопкою «Управління одержувачами» або контекстним меню в «Області одержувачів».

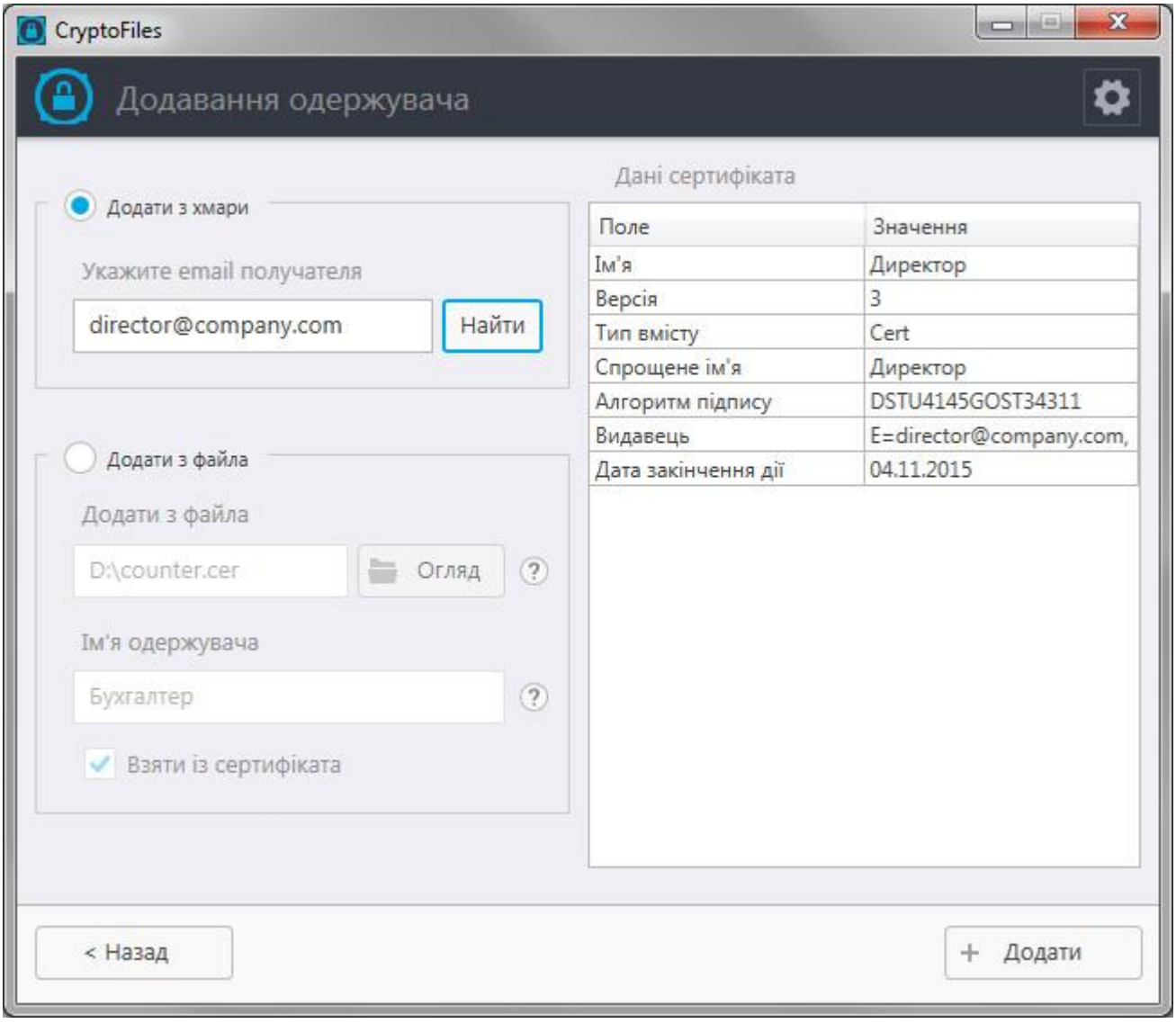
3.2.1 Додавання одержувача



Для додавання одержувача скористайтеся кнопкою «Додати» або виберіть відповідний пункт з контекстного меню. Додавання може бути виконане двома способами:

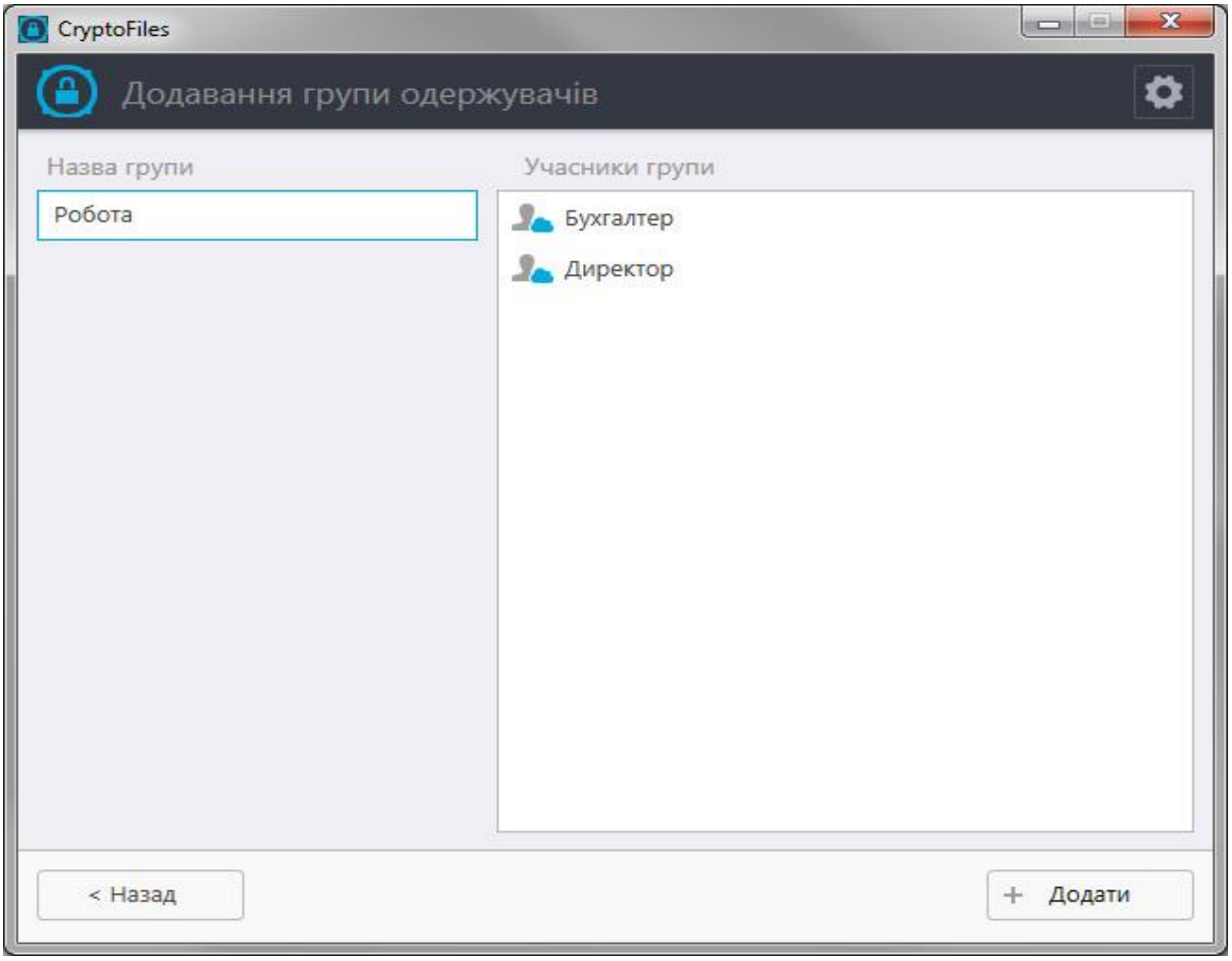
– додаванням з хмарного сховища (даний метод дозволяє виконати пошук сертифікату за електронною адресою в хмарному сховищі; сертифікат заздалегідь має бути поміщений в хмарне сховище);
– додаванням з файлу (для цього необхідно отримати сертифікат ключа користувача).

УВАГА: ЯКЩО СЕРТИФІКАТ КОРИСТУВАЧА НЕ МІСТИТЬ АДРЕСИ ЕЛЕКТРОННОЇ ПОШТИ, З'ЯВИТЬСЯ ПОЛЕ ВВЕДЕННЯ АДРЕСИ, ЯКЕ НЕОБХІДНО ЗАПОВНИТИ.



3.2.2 Додавання групи

Для створення групи необхідно заповнити «Назву групи», відзначити учасників в правій частині екрану і натискувати кнопку «Додати».



3.2.3 Редагування і видалення одержувачів і груп

Редагування і видалення одержувачів і груп виконується шляхом вибору одержувача і натисненням відповідної кнопки, або відповідним пунктом контекстного меню.

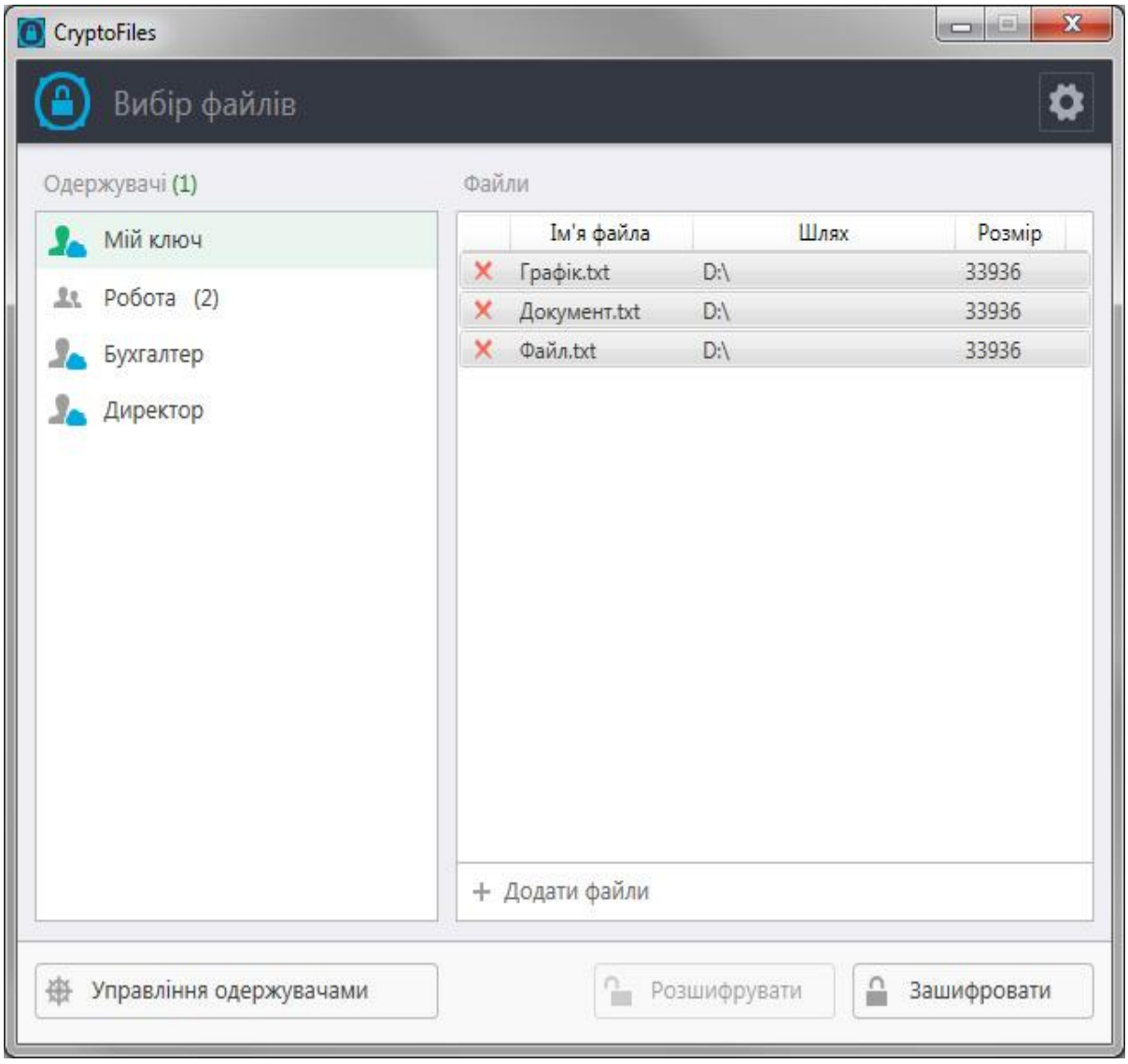
3.3 Створення захищеного контейнера і шифрування даних

Для створення захищеного контейнера необхідно вибрати одержувачів і файли. Для вибору одержувача або групи натисніть ліву кнопку миші на ім'я . Повторне натиснення відмінить вибір одержувача або групи.

УВАГА: ДЛЯ РОБОТИ ІЗ ЗАХИЩЕНИМ КОНТЕЙНЕРОМ КЛЮЧ КОМП'ЮТЕРА АВТОМАТИЧНО ЗАНОСИТЬСЯ В СПИСОК ОДЕРЖУВАЧІВ.

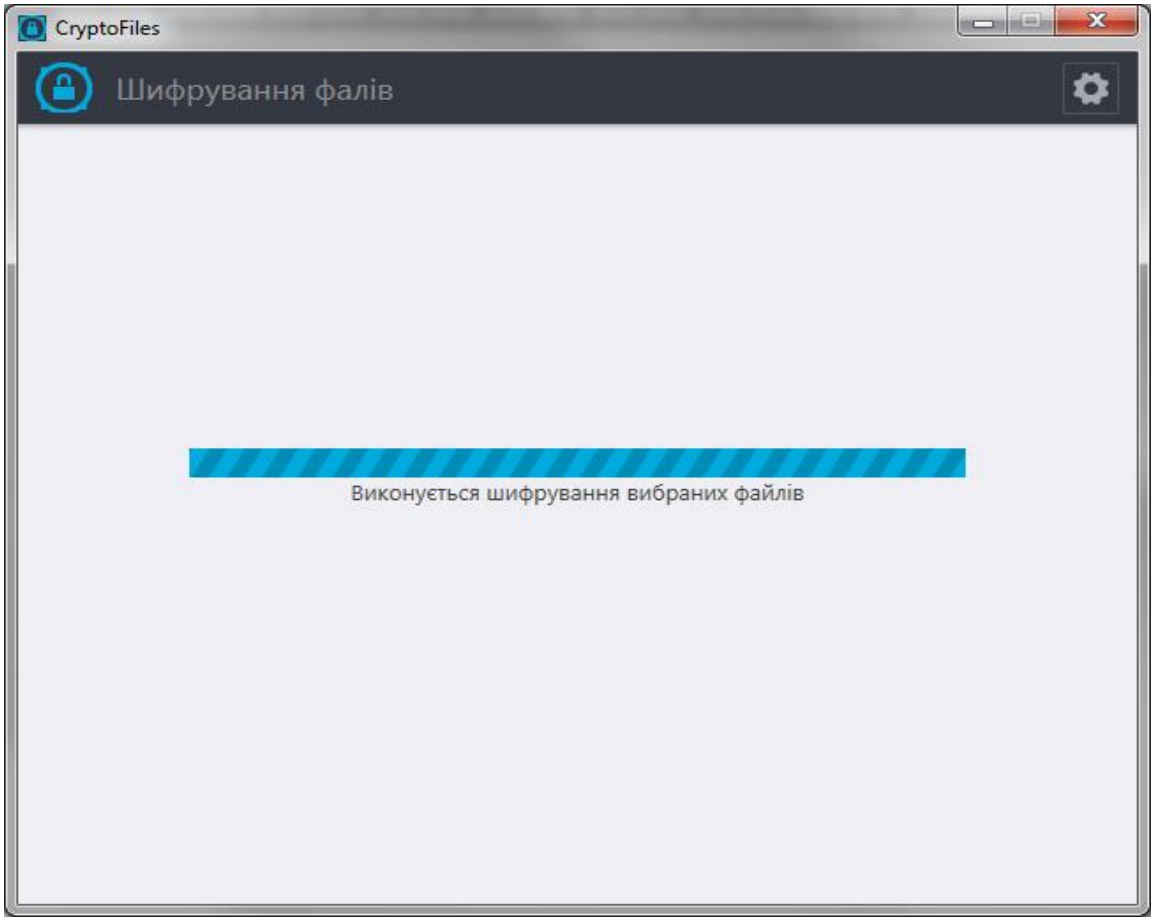
Додавання файлів в захищений контейнер може бути виконане декількома способами:

- перетягуванням файлів в область вибору файлів («Drag and Drop»);
- додаванням шляхом вибору файлів за допомогою діалогу («Open file»).

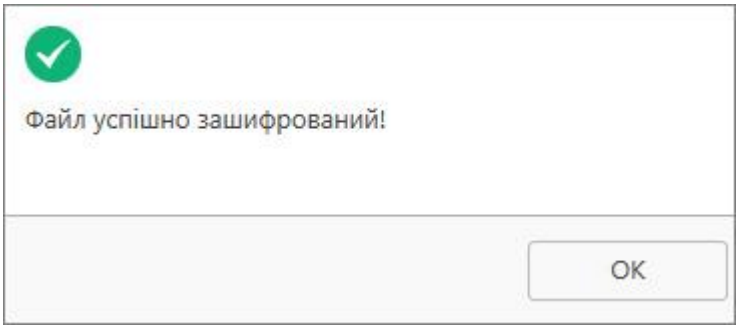


Якщо, з якої-небудь причини, Ви не хочете включати файл в захищений контейнер – видаліть його із списку, натиснув значок видалення зліва від файлу.

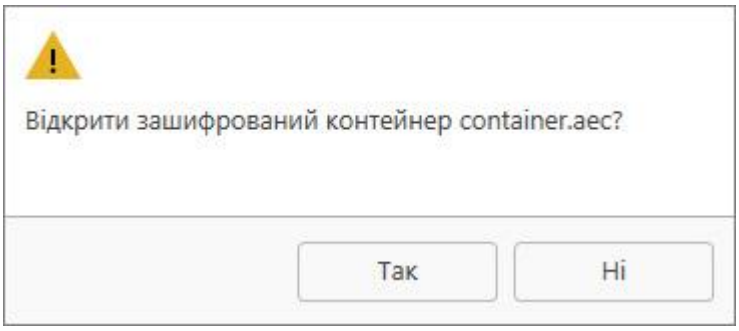
Після завершення вибору файлів, натисніть кнопку «Зашифрувати» і виберіть шлях до контейнера[3], аби почати шифрування.



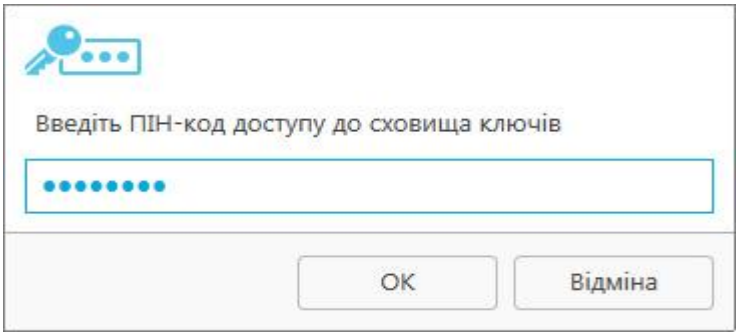
По завершенню операції з'явиться повідомлення користувача про успішне завершення, або про помилку під час виконання операції з подальшою пропозицією відкрити контейнер для подальшої роботи:



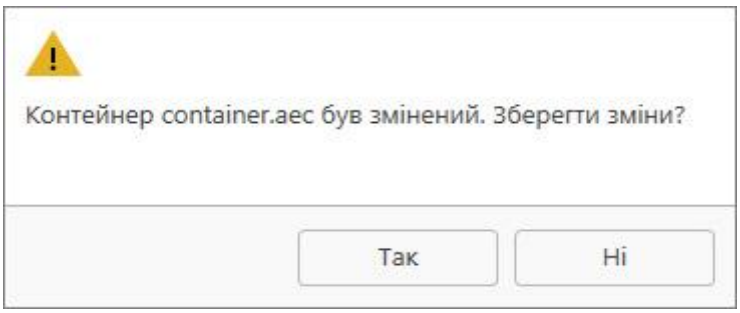
[3] Програма створить файл контейнера, якщо він відсутній, або замінить існуючий файл.



Для відкриття контейнера необхідно розшифрувати дані, які в нього поміщені. Для цих цілей використовується ПІН-код НКІ, або пароль до PFX контейнеру, якщо Ваш ключ знаходиться у файлі обміну ключовою інформацією.



При коректному введенні станеться розшифрування даних і монтування окремого жорсткого диска для роботи з файлами. При закритті програмного забезпечення з'явиться повідомлення про зміну контейнера з можливістю збереження:

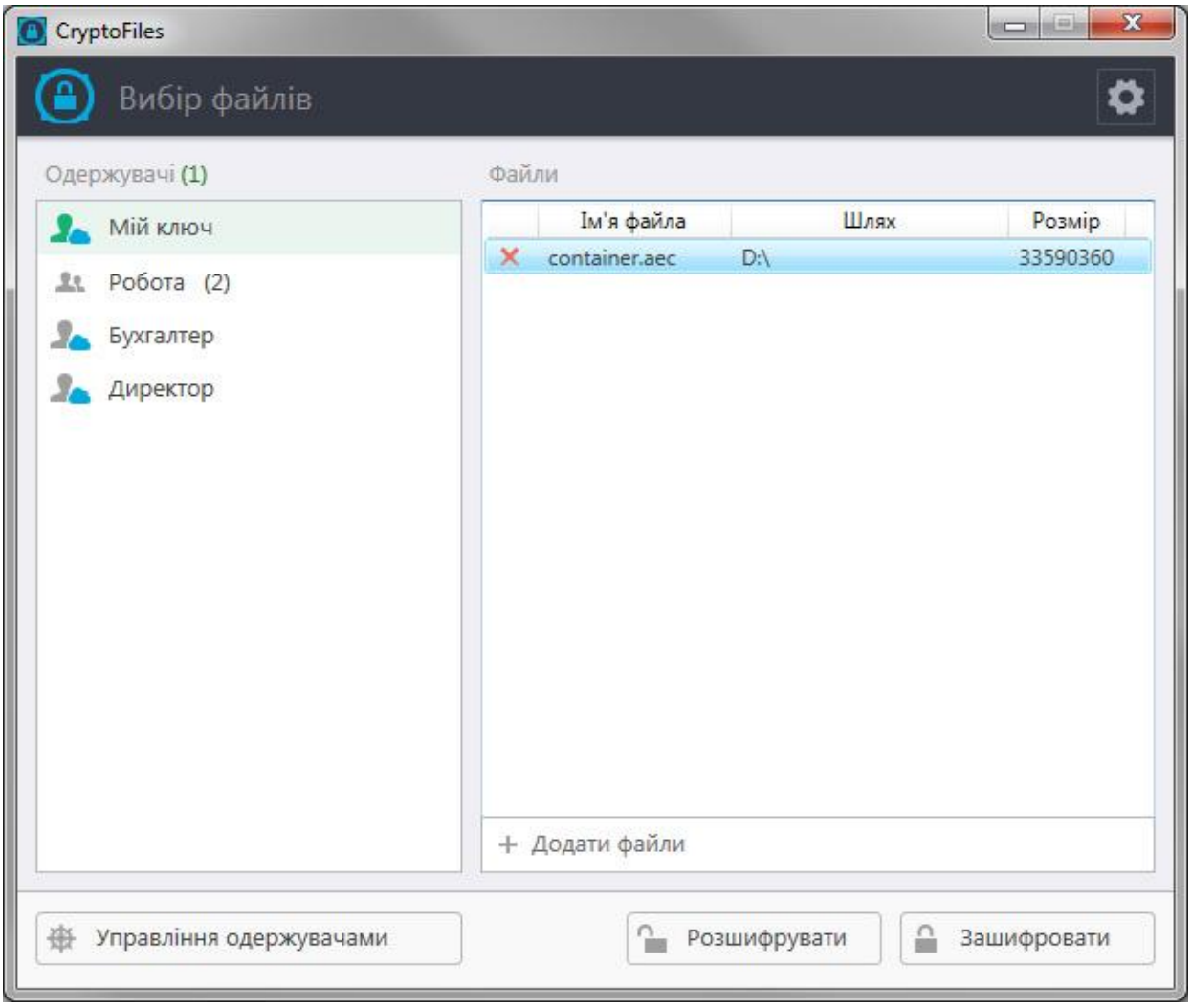


3.4 **Розкриття захищеного контейнера**

Розкриття захищеного контейнера може виконуватися наступними способами:

- за допомогою провідника Windows;
-
- за умовчанням, захищений контейнер має розширення «*.aec» і асоційований з програмою «CryptoFiles». У контекстному меню виберіть «Відкрити» або виконайте подвійне натискання на вибраному файлі;
- поміщенням контейнера в область файлів;

Перетягніть захищений контейнер в область файлів або скористайтеся кнопкою «Додати файли» і вкажіть файл.



При поміщенні захищеного контейнера в область файлів, в списку одержувачів відмічаються користувачі, яким адресований даний контейнер, якщо вони є у Вашому списку.

Для здійснення розшифрування файлів необхідно натиснуть кнопку «Розшифрувати». Подальші дії аналогічні п. 3.3.

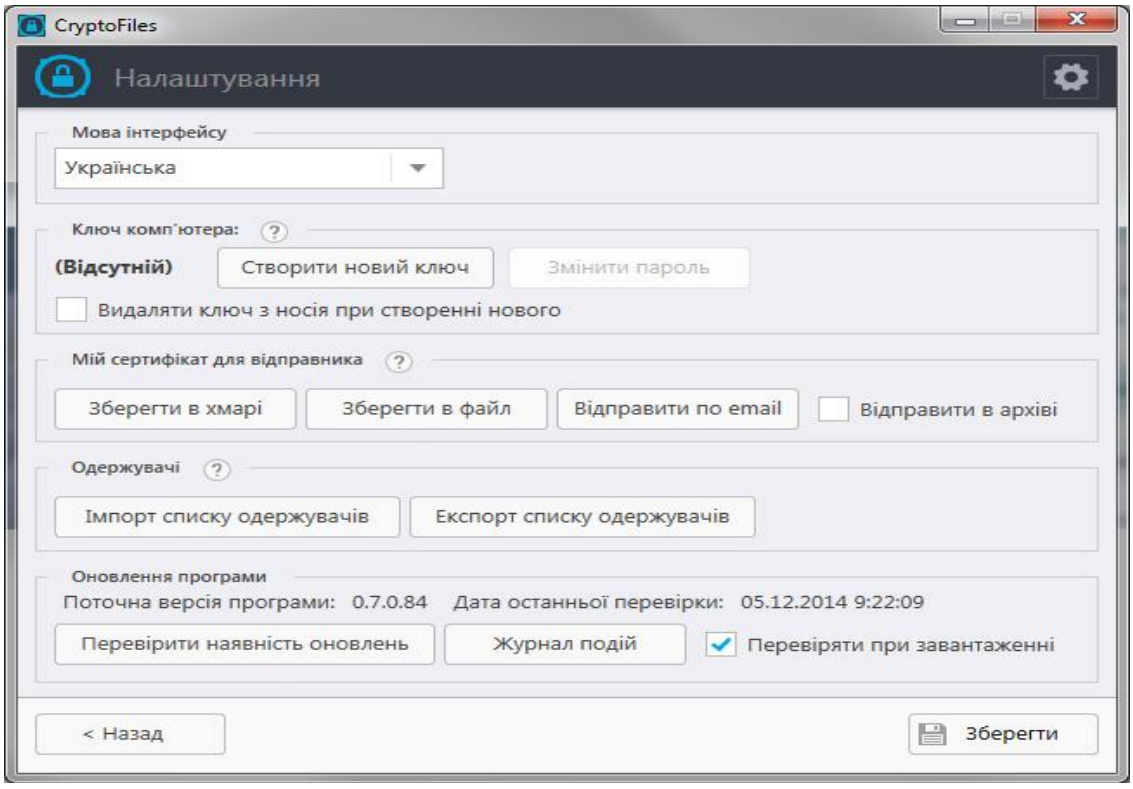
4. Налаштування програмного забезпечення

Основні налаштування програмного забезпечення приведені в таблиці 4.

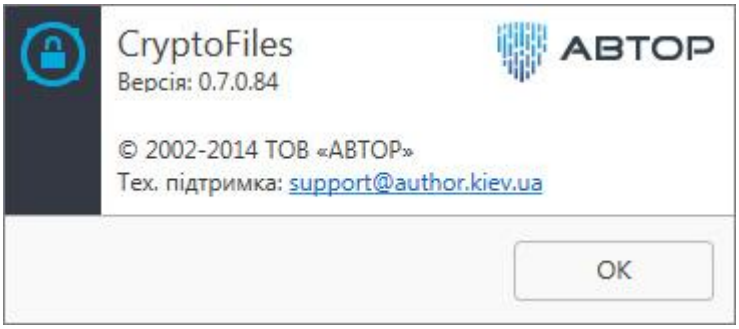
Таблиця 4

Параметр	**Опис**
Мова інтерфейсу	Мова інтерфейсу програмного забезпечення. Доступні 3 варіанти: – російська мова; – українська мова; – англійська мова
Створити новий ключ	Видаляє поточний ключ комп'ютера і запускає майстер створення ключа
Змінити пароль	Надання можливості зміни пароля носія ключової інформації, на якому знаходиться ключ комп'ютера
Видалити ключ з носія при створенні нового	Дана опція визначає, чи буде фізично видалений ключ з носія ключової інформації. УВАГА: ДАНА ОПЦІЯ НЕ ПОШИРЮЄТЬСЯ НА PFX ФАЙЛ
Додати в хмару/Видалити з хмари	Виконує поміщення (або видалення) сертифікату ключа комп'ютера в хмарне сховище. УВАГА: ДЛЯ ПОМІЩЕННЯ СЕРТИФІКАТУ В ХМАРНЕ СХОВИЩЕ ВИКОНУЄТЬСЯ ВЕРИФІКАЦІЯ АДРЕСИ ЕЛЕКТРОННОЇ ПОШТИ
Зберегти у файл	Збереження сертифікату ключа у файл для подальшого обміну з іншими користувачами.
Відправити по email	Відправка сертифікату ключа у файл, для подальшого обміну з іншими користувачами
Відправити до архіву	Оскільки деякі поштові клієнти не дозволяють додати файли сертифікатів, сертифікат поміщається в архів без пароля

Імпорт списку одержувачів	Надає можливість перенесення списку одержувачів з іншого комп'ютера або пристрою
Експорт списку одержувачів	Дозволяє зберегти поточний список одержувачів для подальшого імпорту на інший пристрій. УВАГА: З МЕТОЮ БЕЗПЕКИ, ЕКСПОРТ СПИСКУ ОДЕРЖУВАЧІВ НЕ ЗБЕРІГАЄ ВАШ ЗАКРИТИЙ КЛЮЧ КОМП'ЮТЕРА
Перевірити наявність нової версії	Дозволяє виробити пошук оновлень програмного забезпечення на сервері компанії «АВТОРА»
Перевіряти при завантаженні	Прапор, що вказує на необхідність перевірки наявності нової версії при кожному запуску програмного забезпечення



5. Про виробника



Програмне забезпечення «CryptoFiles» розроблене ТОВ «АВТОР».

Адреса: вул. Смоленська, 31-33, 03005 Київ, Україна

Телефон: (380 44) 538-00-89

Факс: (380 44) 538-00-89

WEB: http://author.kiev.ua, http://platimo.ua

E-mail: author@author.kiev.ua