АВТОР
системи інформаційної безпеки

Программное обеспечение «CryptoFiles»

Руководство пользователя

АЧСА.32248356.00187 96-01

Листов 23

2014

Оглавление

1. Введение

Документ содержит описание программного обеспечения «CryptoFiles», а также порядок эксплуатации носителей ключевой информации – электронных ключей «Secure Token-337F» (далее - «Secure Token-337F») и программных ключей при взаимодействии с данным программным обеспечением.

1.1 Назначение

Программное обеспечение «CryptoFiles» предназначено для создания и редактирования защищенных файлов (контейнеров), а также управления доступом к информации, содержащейся в них, с помощью носителей ключевой информации.

1.2 Область применения

Программное обеспечение «CryptoFiles» поддерживает работу под управлением следующих операционных систем: Windows XP/Vista/7/8/8.1 и Windows Server 2000/2003/2008/2012.

1.3 Определения и сокращения

- НКИ – носитель ключевой информации;
- ПК – персональный компьютер;
- ЭЦП – электронная цифровая подпись;
- АЦСК – аккредитованный центр сертификации ключей;
- ОС – операционная система;

Сертификат открытого ключа (далее – «сертификат») — цифровой документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Используется для шифрования данных, посылаемых владельцу сертификата.

2. Программное обеспечение «CryptoFiles»

Программное обеспечение «CryptoFiles» позволяет организовать:

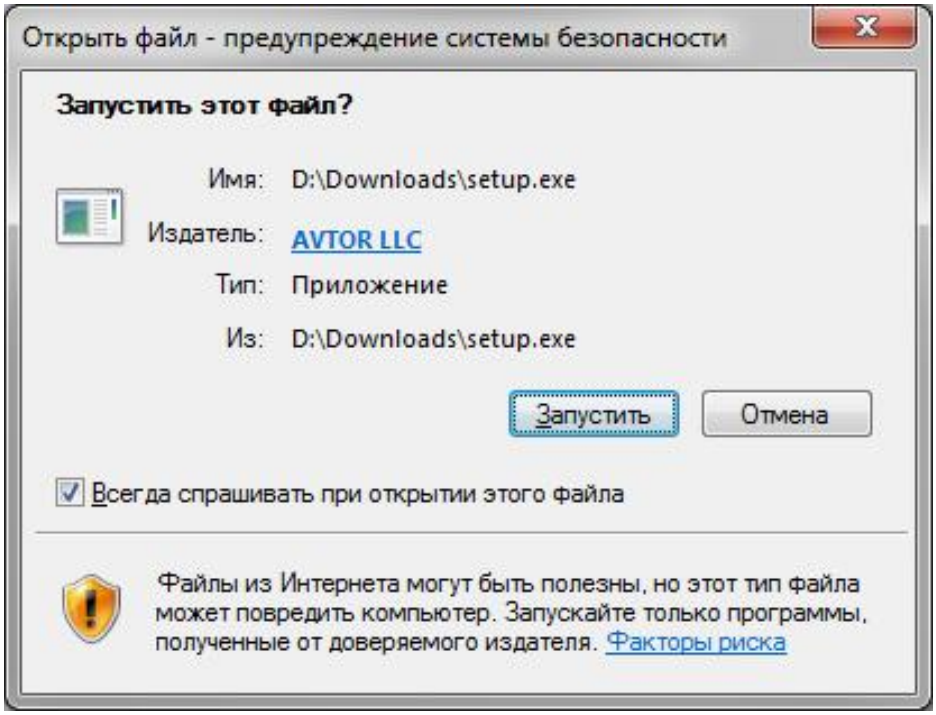
- надежно защищенное хранение важных файлов в зашифрованном виде, в том числе в общедоступных облачных хранилищах;
- обмен сертификатами с помощью облачного сервиса «CryptoFiles»;
- синхронизацию сертификатов с помощью облачного сервиса «CryptoFiles»;
- обмен файлами в зашифрованном виде между устройствами пользователя (рабочий компьютер, домашний компьютер, ноутбук, планшет, мобильный телефон);
- обмен файлами в зашифрованном виде с другими пользователями, с возможностью групповой (файлы предназначены для нескольких получателей) и индивидуальной (файлы предназначены только для конкретного получателя) адресации;
- возможность хранения в одном зашифрованном файле (контейнере) различных пользовательских файлов, в том числе структурированных по разным папкам;
- возможность создания полноценного зашифрованного диска[1].

Зашифрованный контейнер открывается как новый диск в системе, с которым могут работать любые программы пользователя. Возможен запуск программ с этого диска и их работа с данными, находящимися в зашифрованном контейнере. После выхода из программы «CryptoFiles» измененные пользователем файлы и новые файлы, которые пользователь записал на диск стандартными средствами, сохраняются в зашифрованном контейнере.

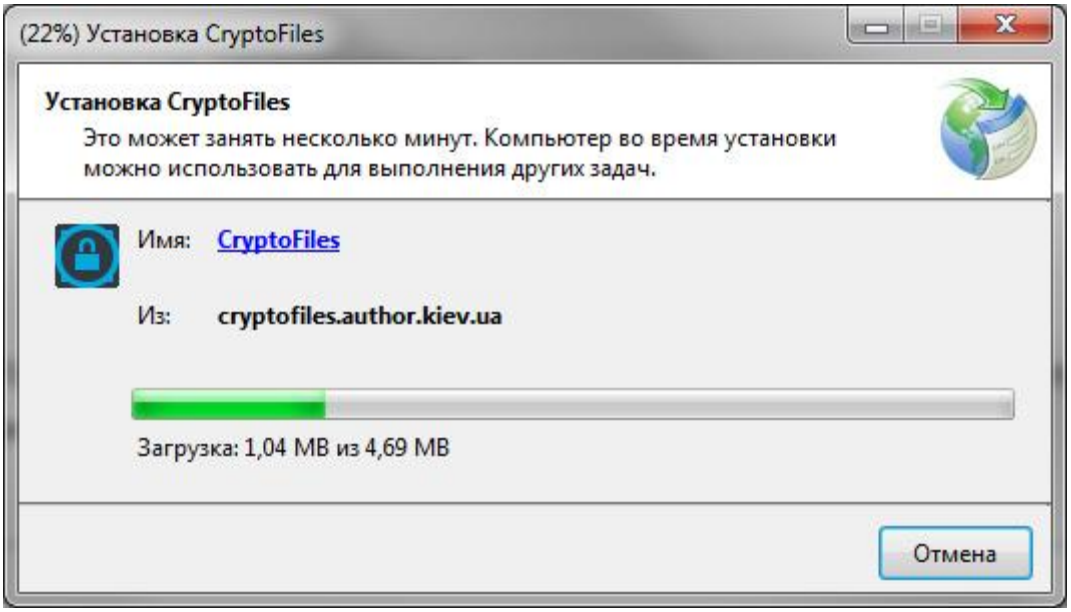
[1] Для создания зашифрованного диска используются ресурсы системного диска.

2.1 Установка программного обеспечения «CryptoFiles»

Для установки программного обеспечения «CryptoFiles» перейдите по ссылке: http://cryptofiles.author.kiev.ua/setup.exe, загрузите и выполните запуск **setup.exe**.



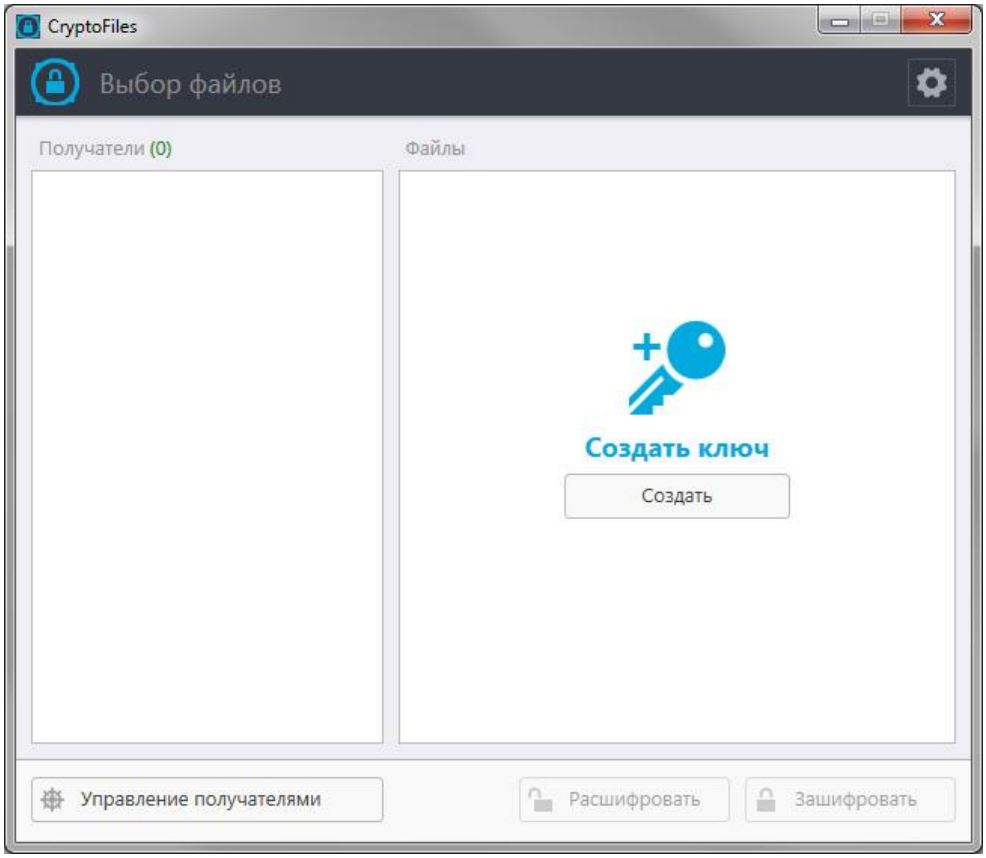
Запустите установку и выполните необходимые действия.



По завершению установки произведется запуск программы.

2.2 Запуск программного обеспечения «CryptoFiles»

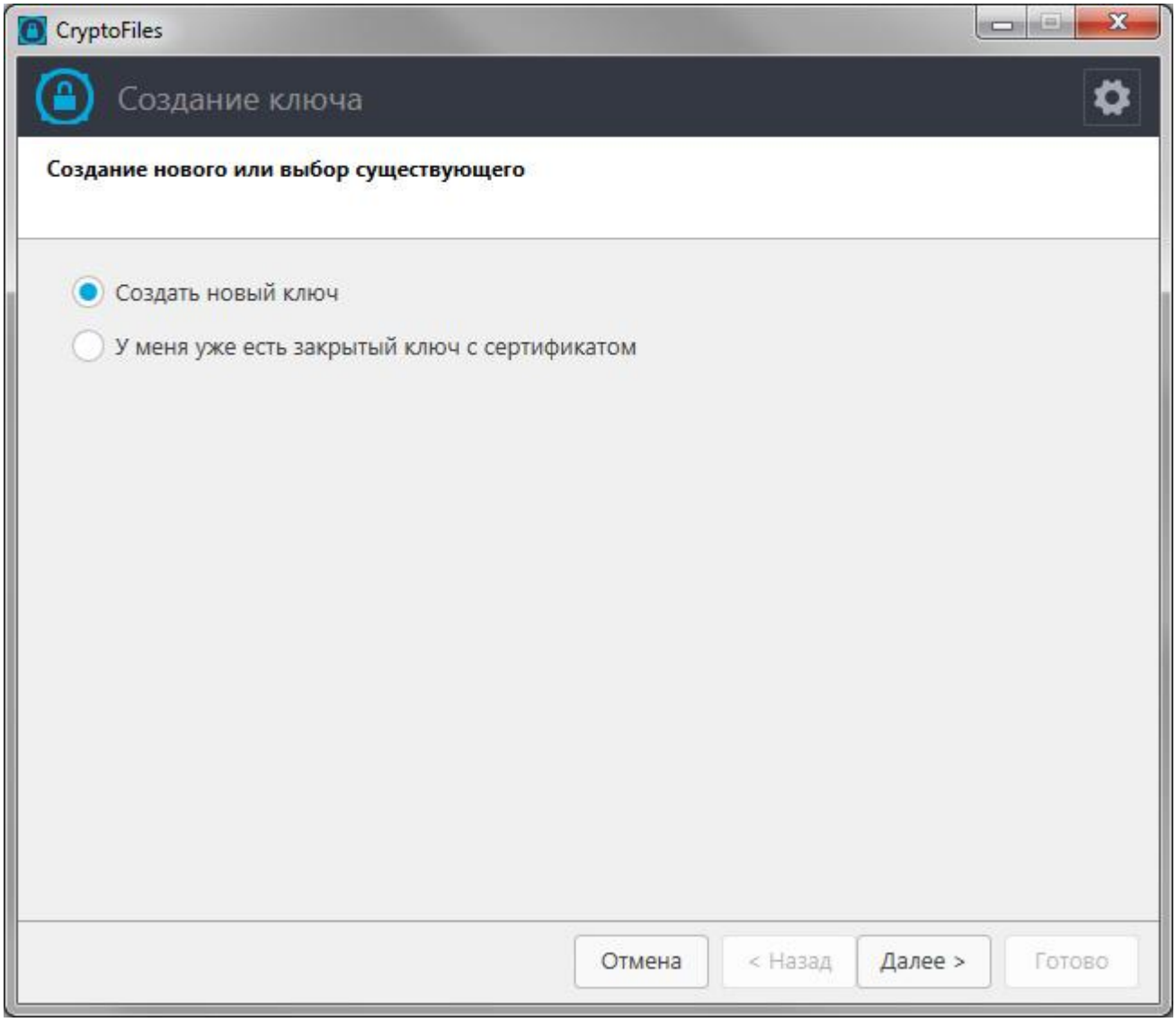
Для запуска программного обеспечения «CryptoFiles» можно воспользоваться меню «Пуск» > «Avtor» > «CryptoFiles», либо ярлыком на рабочем столе.



3. Работа с программным обеспечением «CryptoFiles»

3.1 Создание криптографического ключа

Для работы с программным обеспечением «CryptoFiles» необходимо создать ключ, который будет использоваться для обмена защищенной информацией. Нажмите кнопку «Создать……», в главном окне программного обеспечения, для запуска мастера создания ключа и следуйте дальнейшим указаниям.

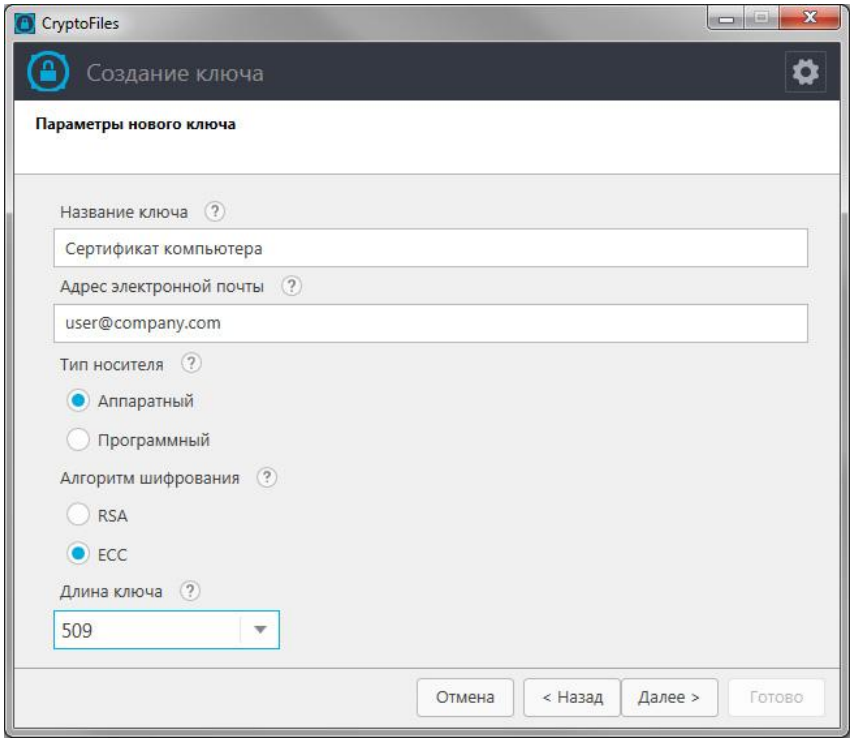


3.1.1 Создание нового ключа

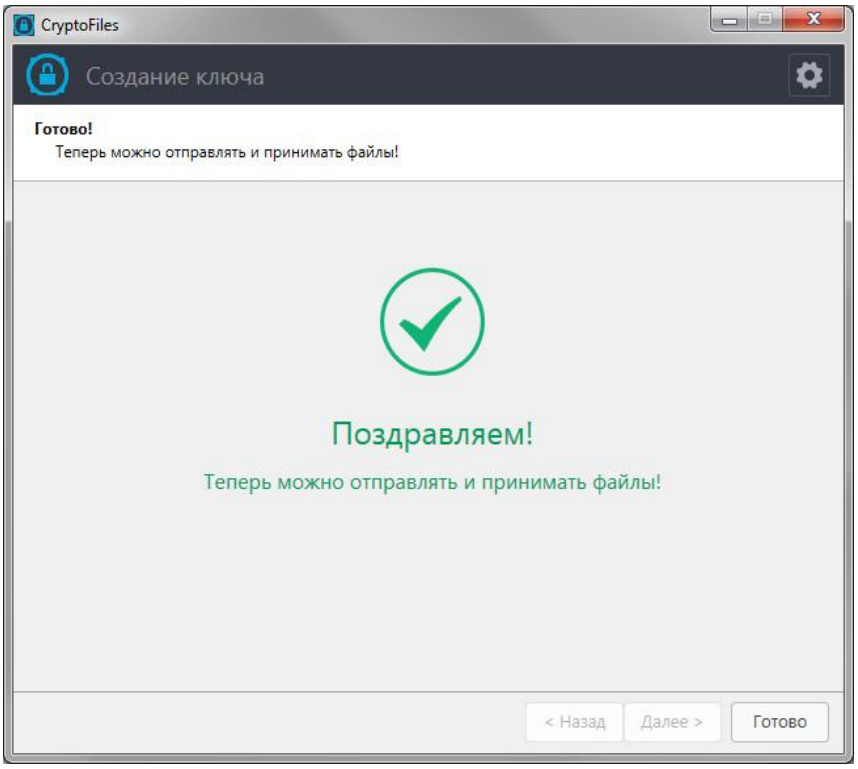
Для создания нового ключа необходимо заполнить обязательные поля, указать алгоритм шифрования и выбрать НКИ. Параметры с описанием указаны в таблице 1.

Таблица 1

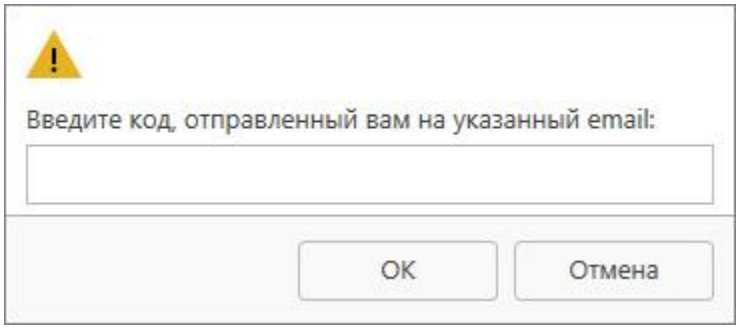
Параметр	**Описание**
Название ключа	CN (Common Name) – имя сертификата ключа, используется для отображения пользователя в облачном сервисе
Адрес электронной почты	E (Email) – электронная почта пользователя. Используется для поиска сертификатов в облачном сервисе. ВНИМАНИЕ: ЭЛЕКТРОННАЯ ПОЧТА ВЕРИФИЦИРУЕТСЯ ПУТЕМ ОТПРАВКИ ЗАЩИТНОГО КОДА НА УКАЗАННЫЙ АДРЕС
Тип носителя	Тип носителя определяет устройство, на которое будет записан ключ пользователя. При отсутствии «Secure Token-337F», вы можете воспользоваться программным контейнером хранения ключевой информации.
Алгоритм шифрования	Алгоритм, с помощью которого будет зашифрован Ваш персональный ключ. RSA – международный криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Для шифрования используется криптографический алгоритм AES с длиной ключа 256 бит ECC – криптографические алгоритмы, основанные на эллиптических кривых. В «CryptoFiles» используется украинский стандарт ДСТУ 4145-2002. Для шифрования используется криптографический алгоритм в соответствии с ДСТУ ГОСТ 28147:2009
Длина ключа	Характеризирует криптостойкость зашифрованных данных. Рекомендуемыми параметрами длины являются: – RSA – 2048 бит – ECC – 257 бит



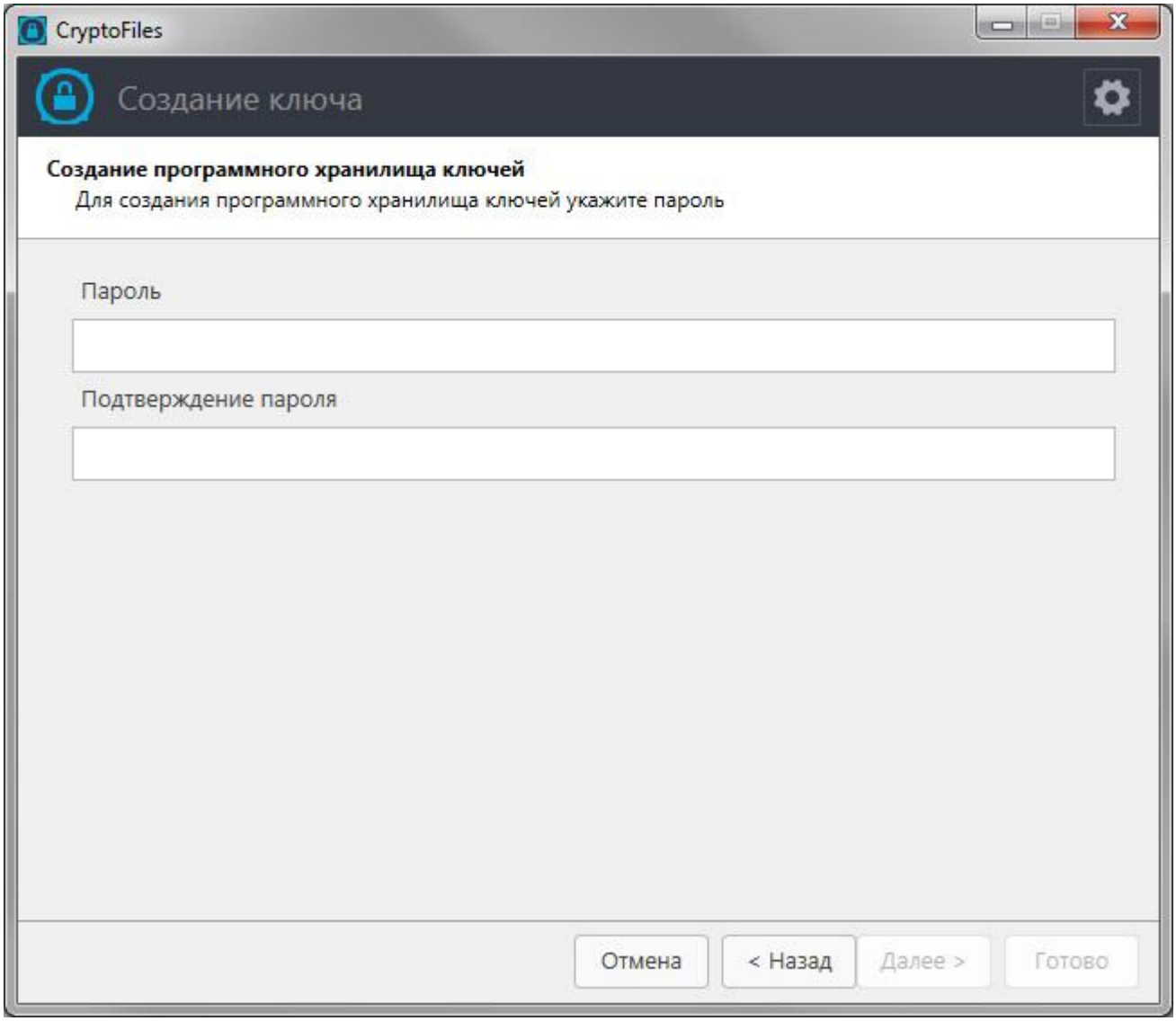
После завершения заполнения параметров нажмите кнопку «Далее» для создания ключа.



Для подтверждения адреса электронной почты, введите код, который Вы получите на указанную электронную почту:



ВНИМАНИЕ: ПРИ ПЕРВОМ СОЗДАНИИ ПРОГРАММНОГО КЛЮЧА, НЕОБХОДИМО СОЗДАТЬ ПРОГРАММНЫЙ КОНТЕЙНЕР ХРАНЕНИЯ КЛЮЧЕЙ. ПРИ НАЖАТИИ КНОПКИ «ДАЛЕЕ», ПОЛЬЗОВАТЕЛЮ НЕОБХОДИМО ВВЕСТИ ПАРОЛЬ ДОСТУПА К ПРОГРАММНОМУ КОНТЕЙНЕРУ.



3.1.2 Выбор существующего ключа

Выбор существующего ключа производится путем указания устройства, на котором он хранится и заполнения недостающих параметров (таблица 2).

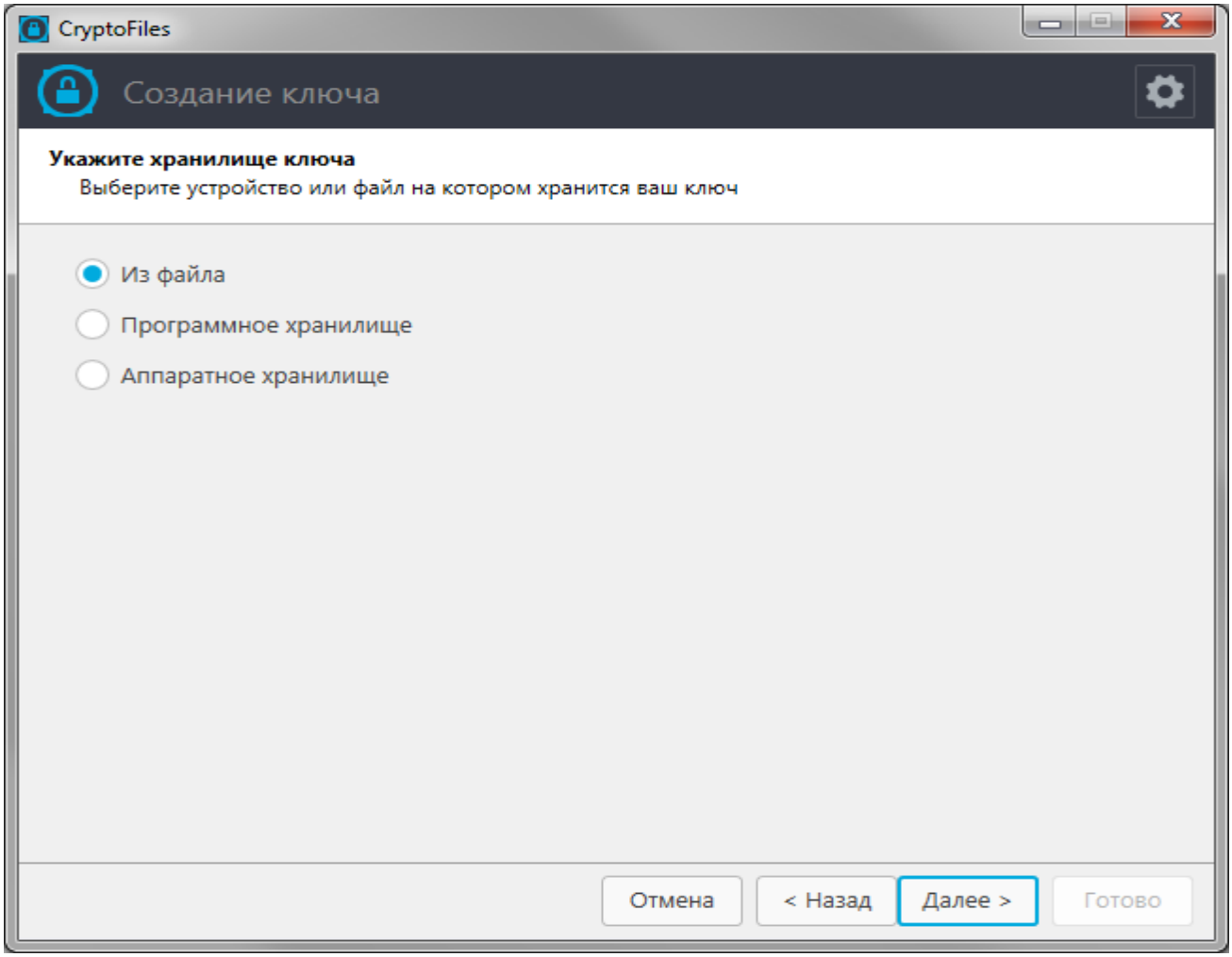
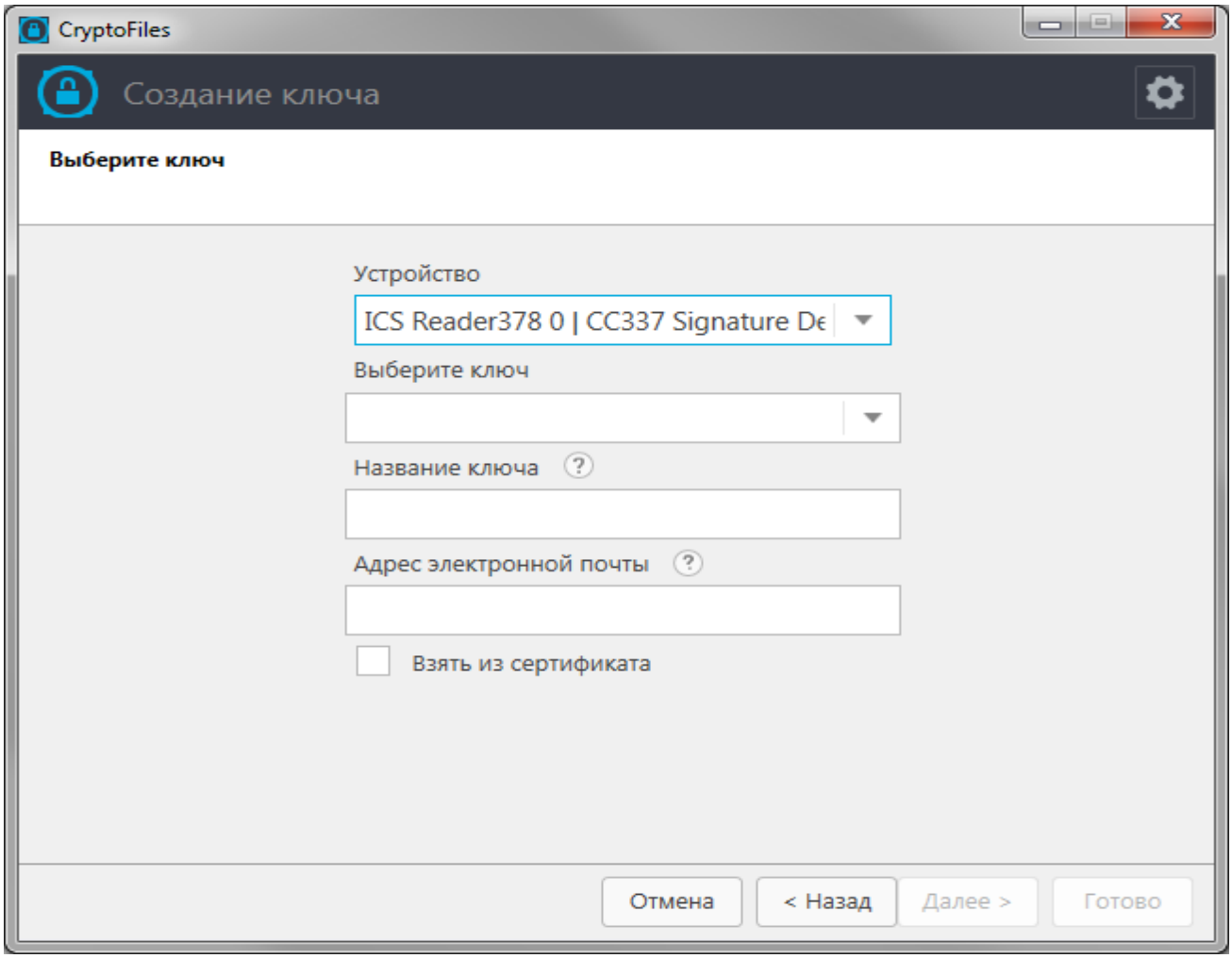


Таблица 2

Параметр	**Описание**
Из файла	Производится извлечение ключа из файла обмена ключевой информацией (PFX). Данный формат является одним из самых сложных криптографических протоколов, но, тем не менее, остается единственным стандартным способом сегодня для хранения закрытых ключей и сертификатов в одном зашифрованном файле
Программное хранилище	Использование закрытого ключа из программного контейнера компании «АВТОР». ВНИМАНИЕ: ЭТА ОПЦИЯ ДОСТУПНА ТОЛЬКО В СЛУЧАЕ, ЕСЛИ ПРОГРАММНЫЙ КОНТЕЙНЕР УЖЕ УСТАНОВЛЕН
Тип носителя	Использование закрытого ключа из НКИ «Secure Token-337F» компании «АВТОР».

После выбора типа устройства[2], заполните недостающие параметры:



Флаг «Взять из сертификата» – заполняет поля данными, находящимися в сертификате закрытого ключа при их наличии.

[2] При подключении только одного НКИ, выбор устройства отсутствует.

После успешного создания ключа, программное обеспечение имеет следующий вид (его описание - см. таблицу 3).

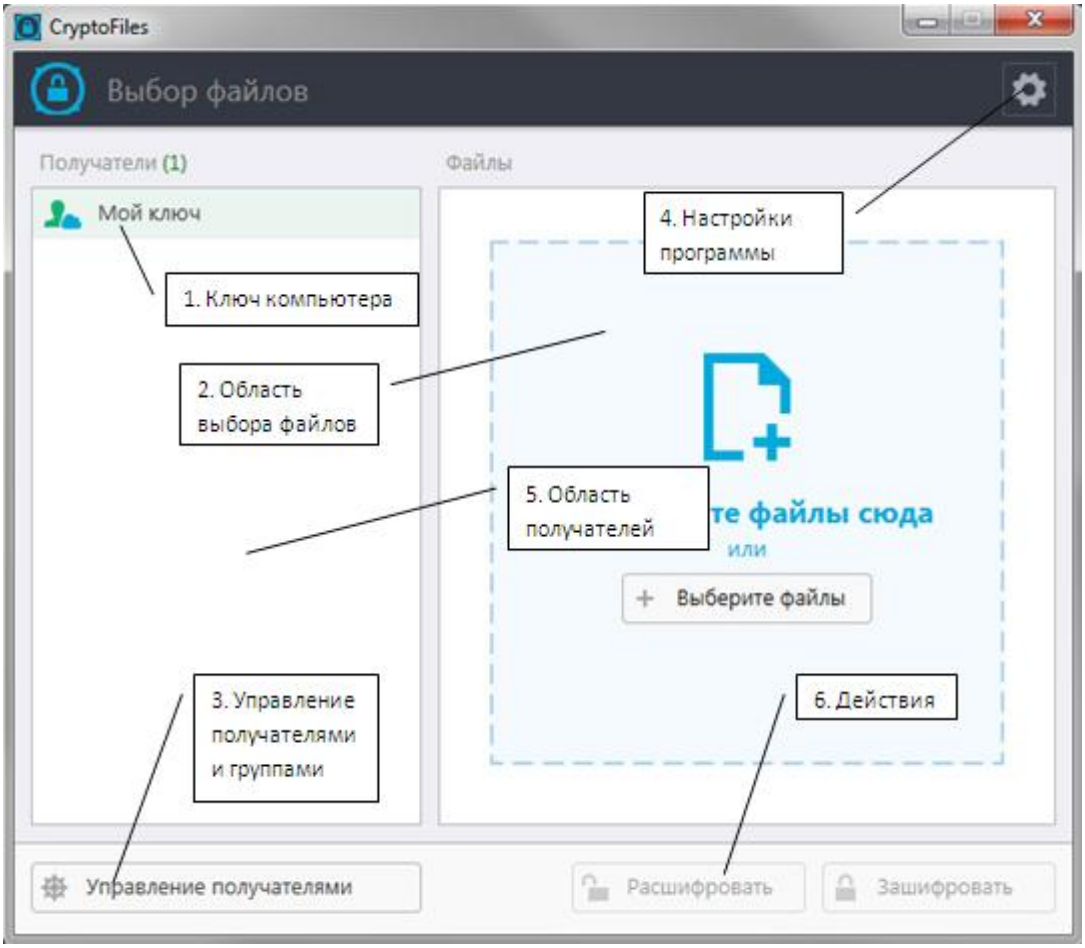


Таблица 3

Область	**Описание**
1. Ключ компьютера	Текущий ключ компьютера. Имеет отличительное выделение цветом. Значок облака указывает, что сертификат ключа помещён в облачное хранилище и доступен для поиска другими пользователями
2. Область выбора файлов	Область, поддерживающая технологию «Drag and Drop» для выбора файлов и последующей работы с ними
3. Управление получателями и группами	Менеджер получателей и групп, позволяющий добавлять, группировать, удалять и редактировать получателей. Все функции также доступны из контекстного меню

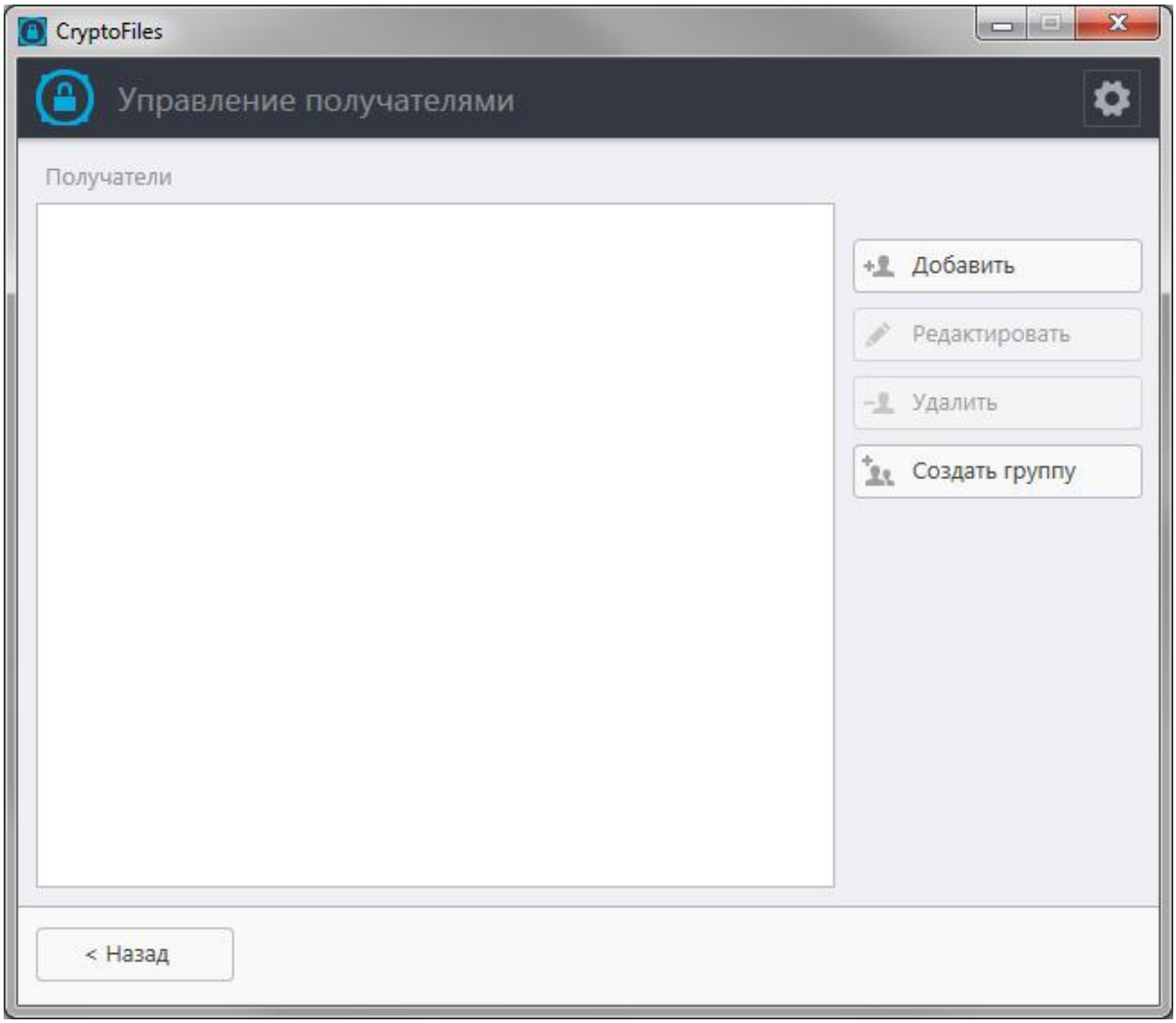
4. Настройки программного обеспечения	Настройки программного обеспечения и интерфейса
5. Область получателей	Список доступных получателей и групп
6. Действия	Возможность зашифровать либо расшифровать файл (файлы)

Теперь есть возможность у пользователя управлять, создавать и получать защищенные контейнеры, а также управлять получателями.

3.2 Управление получателями

Для добавления получателей и групп, воспользуйтесь кнопкой «Управление получателями» либо контекстным меню в «Области получателей».

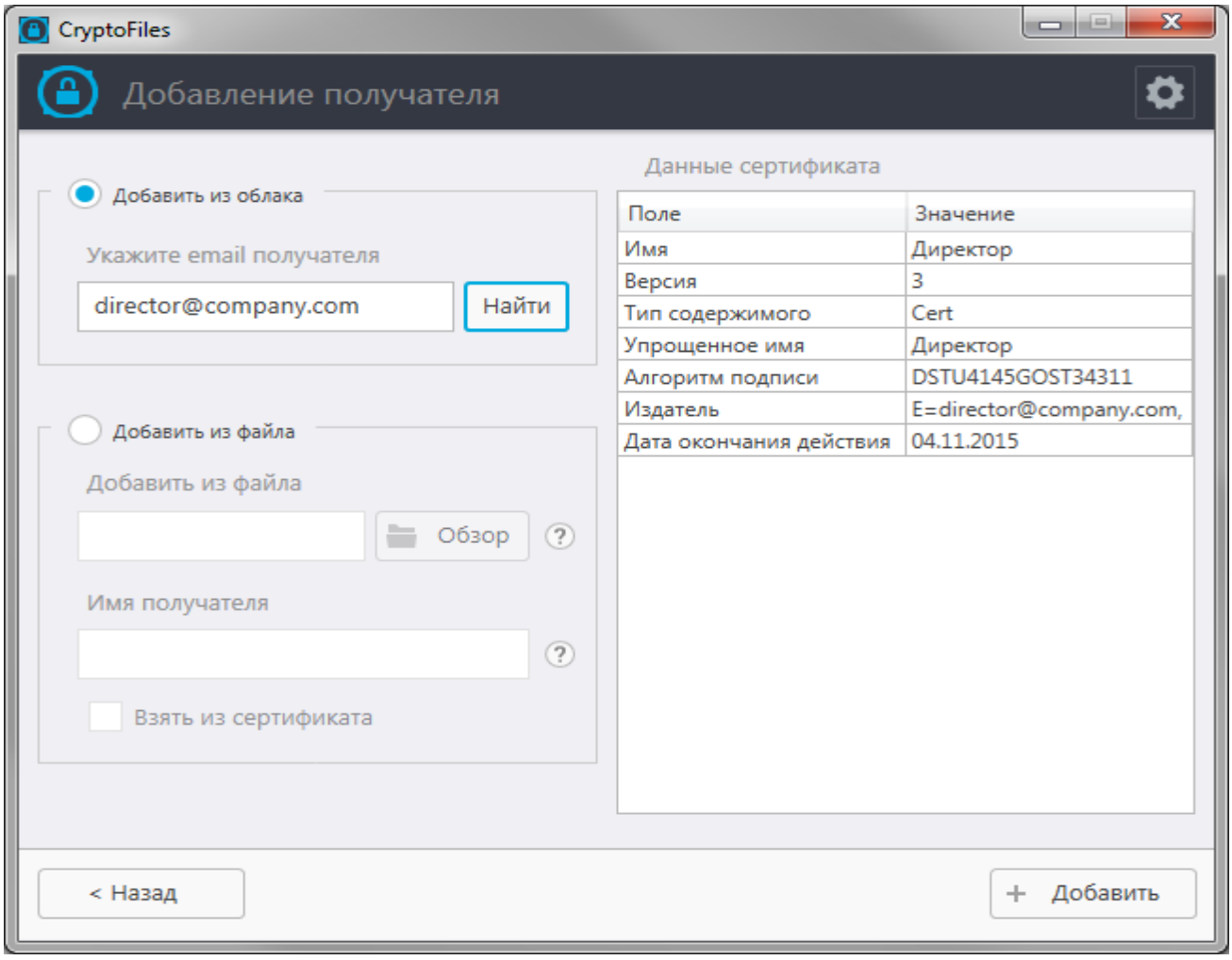
3.2.1 Добавление получателя



Для добавления получателя воспользуйтесь кнопкой «Добавить» либо выберите соответствующий пункт из контекстного меню. Добавление может быть произведено двумя способами:

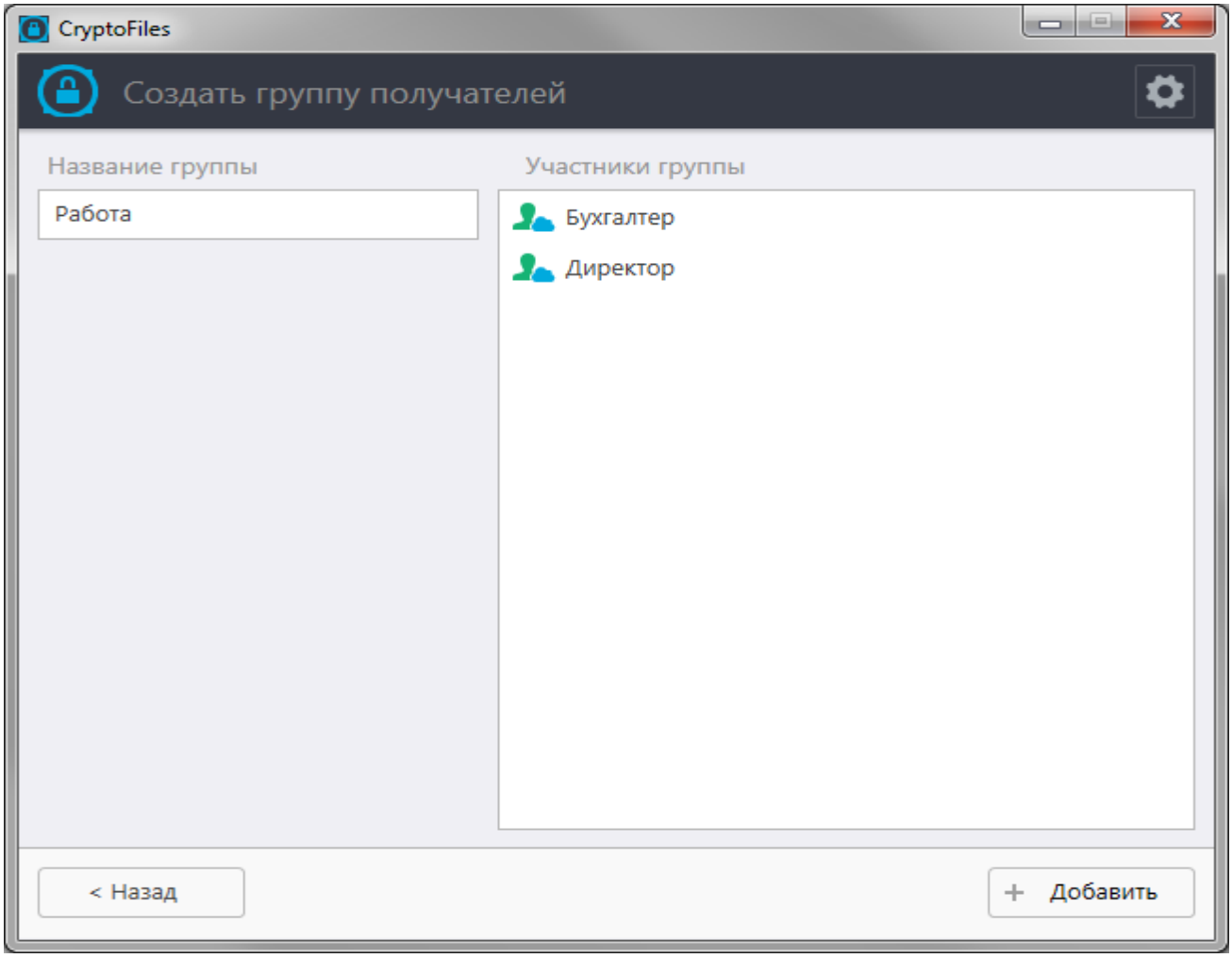
– добавлением из облачного хранилища (данный метод позволяет произвести поиск сертификата по электронному адресу в облачном хранилище; сертификат предварительно должен быть помещен в облачное хранилище)
– добавлением из файла (для этого необходимо получить сертификат ключа пользователя).

ВНИМАНИЕ: ЕСЛИ СЕРТИФИКАТ ПОЛЬЗОВАТЕЛЯ НЕ СОДЕРЖИТ АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ, ПОЯВИТСЯ ПОЛЕ ВВОДА АДРЕСА, КОТОРОЕ НЕОБХОДИМО ЗАПОЛНИТЬ.



3.2.2 Добавление группы

Для создания группы необходимо заполнить «Название группы», отметитьучастников в правой части экрана и нажать кнопку «Добавить».



3.2.3 Редактирование и удаление получателей и групп

Редактирование и удаление получателей и групп производится путём выбора получателя и нажатием соответствующей кнопки, либо соответствующим пунктом контекстного меню.

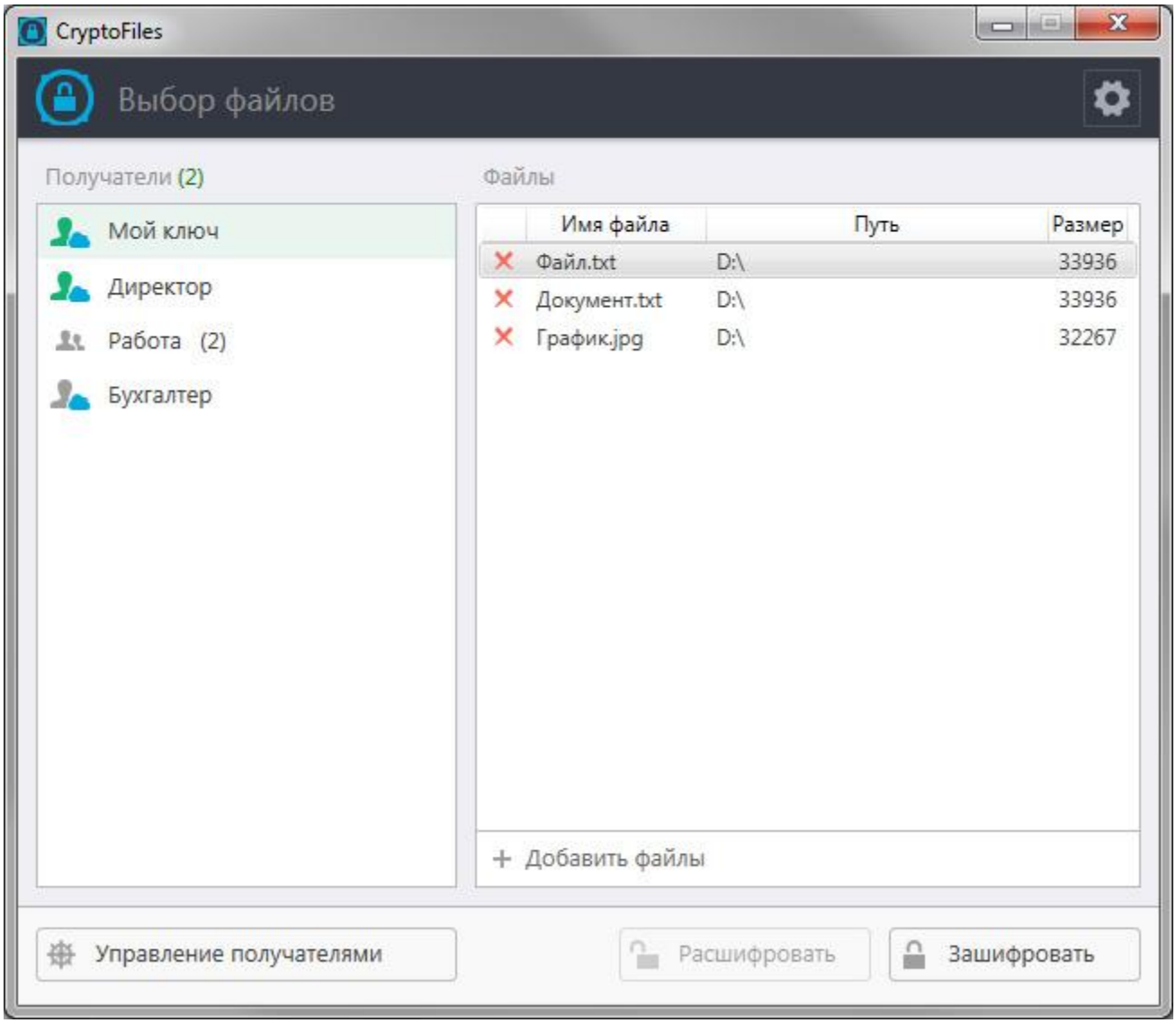
3.3 Создание защищенного контейнера и шифрование данных

Для создания защищенного контейнера необходимо выбрать получателей и файлы. Для выбора получателя или группы нажмите левую кнопку мыши на имя. Повторное нажатие отменит выбор получателя или группы.

ВНИМАНИЕ: ДЛЯ РАБОТЫ С ЗАЩИЩЕННЫМ КОНТЕЙНЕРОМ КЛЮЧ КОМПЬЮТЕРА АВТОМАТИЧЕСКИ ВКЛЮЧАЕТСЯ В СПИСОК ПОЛУЧАТЕЛЕЙ.

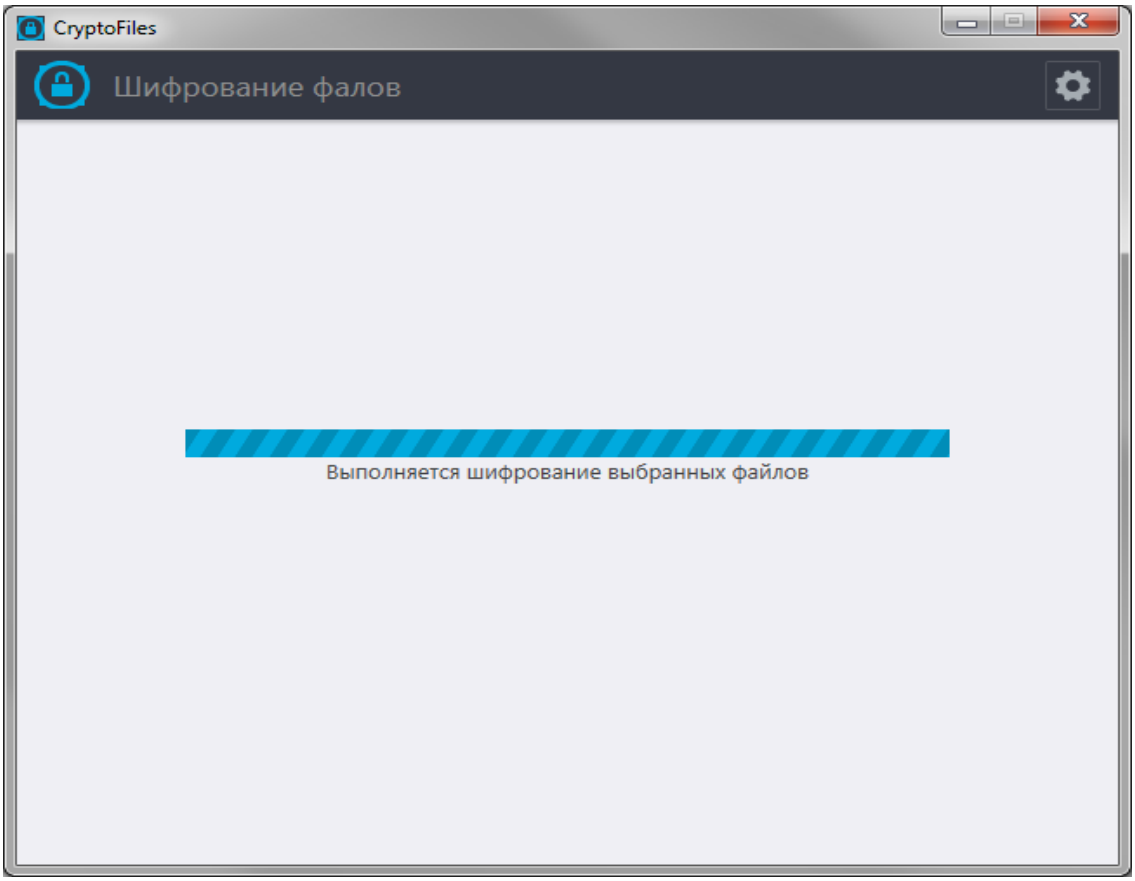
Добавление файлов в защищенный контейнер может быть произведено несколькими способами:

- перетаскиванием файлов в область выбора файлов («Drag and Drop»);
- добавлением, путем выбора файлов с помощью диалога («Open file»).

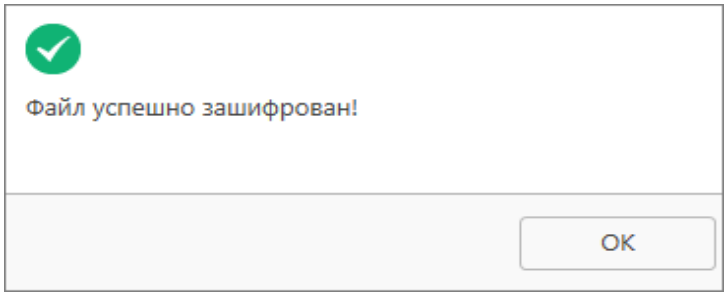


Если, по какой-либо причине, Вы не хотите включать файл в защищенный контейнер – удалите его из списка, нажав значок удаления слева от файла.

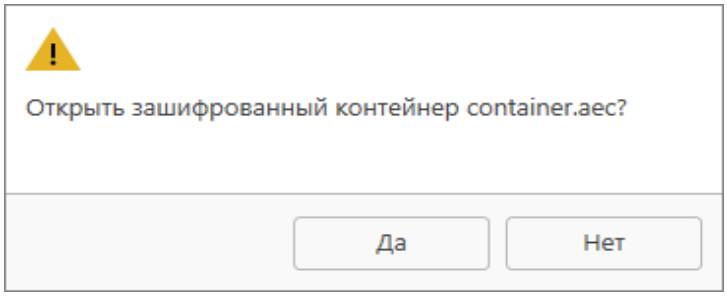
После завершения выбора файлов, нажмите кнопку «Зашифровать» и выберите путь к контейнеру[3], чтобы начать шифрование.



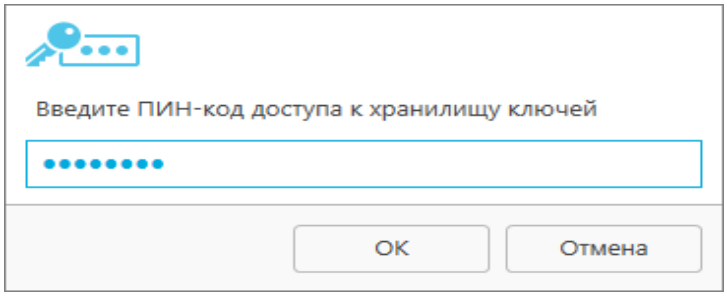
По завершению операции произойдет уведомление пользователя об успешном завершении, либо ошибке во время выполнения операции с последующим предложением открыть контейнер для дальнейшей работы:



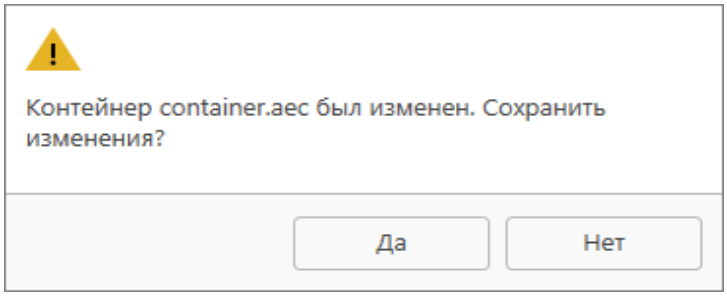
[3] Программа создаст файл контейнера, если он отсутствует, либо заменит существующий файл.



Для открытия контейнера необходимо расшифровать данные, которые в него помещены. Для этих целей используется ПИН-код НКИ, либо пароль к PFX контейнеру, если Ваш ключ находится в файле обмена ключевой информацией.



При корректном вводе произойдет расшифрование данных и монтирование отдельного жесткого диска для работы с файлами. При закрытии программного обеспечения появится уведомление об изменении контейнера с возможностью сохранения:

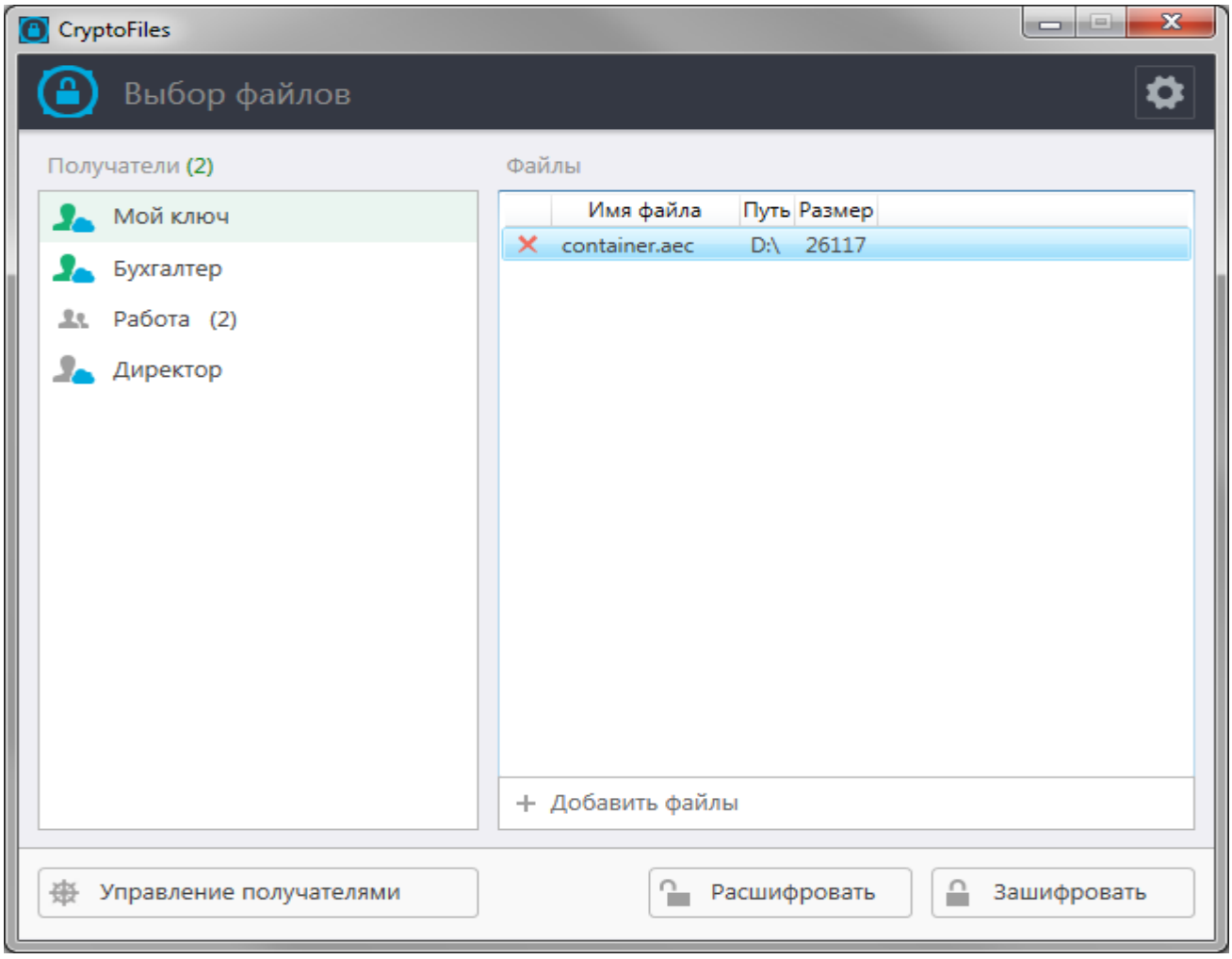


3.4 Открытие защищенного контейнера

Открытие защищенного контейнера может производиться следующими способами:

- с помощью проводника Windows;
- по умолчанию, защищенный контейнер имеет расширение «*.aec» и ассоциирован с программой «CryptoFiles». В контекстном меню выберите «Открыть» либо произведите двойной щелчок на выбранном файле;
- помещением контейнера в область файлов.

Перетяните защищенный контейнер в область файлов или воспользуйтесь кнопкой «Добавить файлы» и укажите файл.



При помещении защищенного контейнера в область файлов, в списке получателей отмечаются пользователи, которым адресован данный контейнер, если они есть в Вашем списке.

Для осуществления расшифрования файлов необходимо нажать кнопку «Расшифровать». Дальнейшие действия аналогичны п. 3.3.

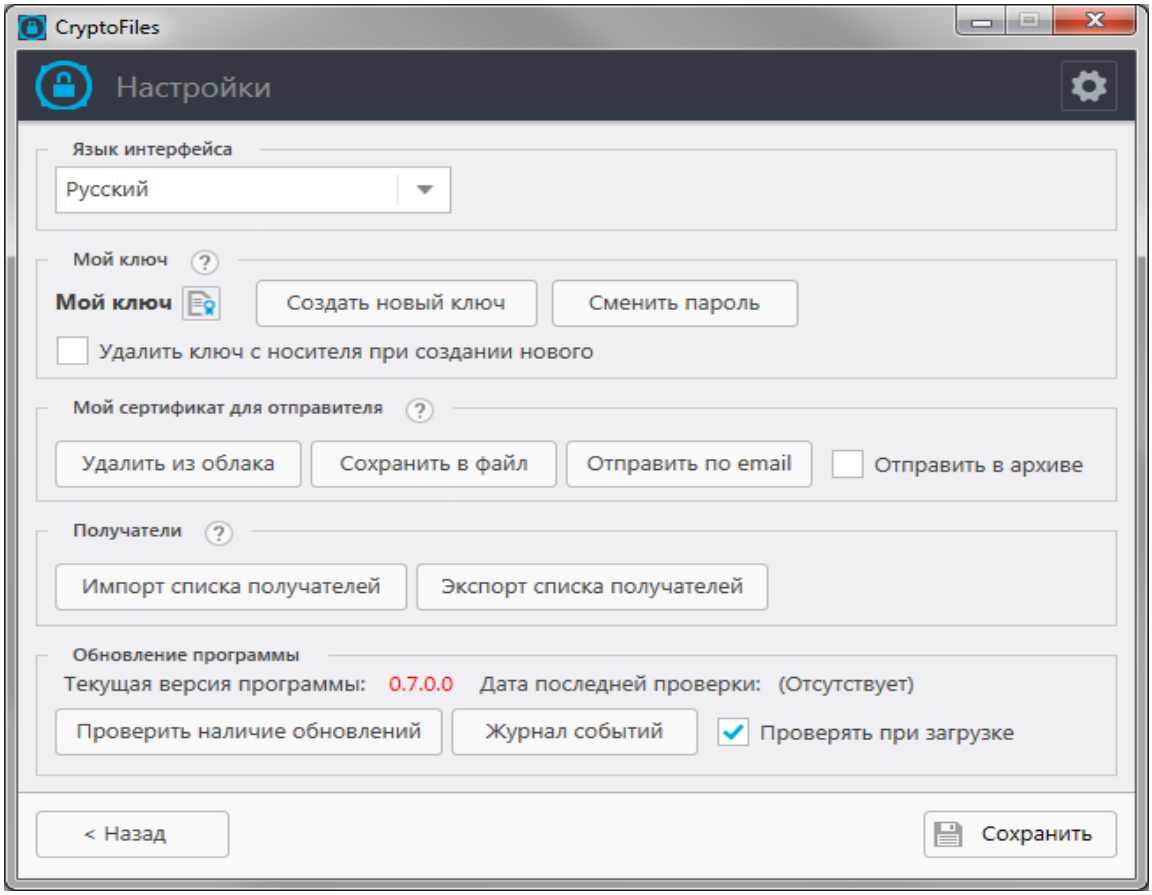
4. Настройки программного обеспечения

Основные настройки программного обеспечения приведены в таблице 4.

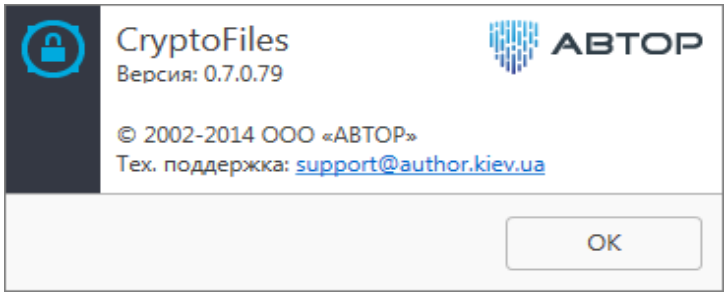
Таблица 4

Параметр	**Описание**
Язык интерфейса	Язык интерфейса программного обеспечения. Доступны 3 варианта: – русский язык; – украинский язык; – английский язык.
Создать новый ключ	Удаляет текущий ключ компьютера и запускает мастер создания ключа
Сменить пароль	Предоставление возможности смены пароля носителя ключевой информации, на котором находится ключ компьютера
Удалить ключ с носителя при создании нового	Данная опция определяет, будет ли физически удален ключ с носителя ключевой информации ВНИМАНИЕ: ДАННАЯ ОПЦИЯ НЕ РАСПРОСТРАНЯЕТСЯ НА **PFX-**ФАЙЛ
Добавить в облако/Удалить из облака	Производит помещение (либо удаление) сертификата ключа компьютера в облачное хранилище ВНИМАНИЕ: ДЛЯ ПОМЕЩЕНИЯ СЕРТИФИКАТА В ОБЛАЧНОЕ ХРАНИЛИЩЕ ПРОИЗВОДИТСЯ ВЕРИФИКАЦИЯ АДРЕСА ЭЛЕКТРОННОЙ ПОЧТЫ
Сохранить в файл	Сохранение сертификата ключа в файл для последующего обмена с другими пользователями
Отправить по email	Отправка сертификата ключа в файл, для последующего обмена с другими пользователями
Отправить в архив	Так как некоторые почтовые клиенты не позволяют добавить файлы сертификатов, сертификат помещается в архив без пароля

Импорт списка получателей	Предоставляет возможность переноса списка получателей с другого компьютера либо устройства.
Экспорт списка получателей	Позволяет сохранить текущий список получателей для последующего импорта на другое устройство. ВНИМАНИЕ:В ЦЕЛЯХ БЕЗОПАСНОСТИ, ЭКСПОРТ СПИСКА ПОЛУЧАТЕЛЕЙ НЕ СОХРАНЯЕТ ВАШ ЗАКРЫТЫЙ КЛЮЧ КОМПЬЮТЕРА
Проверить наличие новой версии	Позволяет произвести поиск обновлений программного обеспечения на сервере компании «АВТОР»
Проверять при загрузке	Флаг, указывающий на необходимость проверки наличия новой версии при каждом запуске программного обеспечения



5. О производителе



Программное обеспечение «CryptoFiles» разработано ООО «АВТОР».

Адрес: ул. Смоленская, 31-33, 03005 Киев, Украина

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