Secret Disk 5

Руководство администратора

Версия	2.0
Статус	Публичный
Дата	23.04.2019
Номер	ID-номер

Аннотация

Система защиты информации от несанкционированного доступа "Secret Disk 5" (версия 5.x.y.zz, где 5 – номер версии, x.y.zz – версия сборки), далее по тексту "SD5", представляет собой специализированный программно-аппаратный комплекс, далее по тексту "ПАК", предназначенный для обеспечения безопасности информации в автоматизированных системах на базе персональных компьютеров.

Настоящий документ представляет собой руководство администратора ПАК SD5 и предназначен для администраторов компьютеров, на которых установлено приложение SD5. В документе содержатся сведения, необходимые администратору для установки приложения и дополнительных компонентов, сведения для работы с приложением, а также приводится порядок работы администратора с компонентами системы защиты.

Авторские права и торговые знаки

Названия продуктов и логотипы Secret Disk, Секрет Диск, JaCarta являются зарегистрированными товарными знаками ЗАО "Аладдин Р.Д."

Все другие товарные знаки, обозначения и названия изделий, используемые в документе, являются или могут быть товарными знаками соответствующих владельцев.

Документ и содержащаяся в нём информация являются собственностью компании ЗАО "Аладдин Р.Д."

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, знаки обслуживания и т.д.), связанные или имеющие отношение к настоящему документу и приложениям, все содержащиеся в них данные, являются собственностью компании ЗАО "Аладдин Р.Д."

Все права на описываемый Продукт являются и будут являться собственностью исключительно компании ЗАО "Аладдин Р.Д."

ЗАО "Аладдин Р.Д." не передаёт вам права ни на это описание, ни на информацию, содержащуюся в нём или в описываемом Продукте, а лишь предоставляет ограниченное право на его использование в строгом соответствии с описанием.

Любое несанкционированное использование, разглашение или воспроизведение является нарушением прав интеллектуальной собственности и/или прав собственности ЗАО "Аладдин Р.Д.", и в полной мере преследуется по закону.

1. Список терминов и определений

ПО	Программное обеспечение.
ОС	Операционная система.
ПК	Персональный компьютер.
Токен	Электронное устройство (USB-ключ или смарт-карта), предназначенное для аппаратной реализации процедур ассиметричного шифрования, необходимых для систем шифрования, электронной подписи и двухфакторной аутентификации с использованием сертификатов открытого ключа.
Пользователь ПК	Субъект, который имеет пользовательскую учётную запись в системе Windows на ПК.
Локальный администратор ПК	Привилегированный пользователь ОС Windows (учётная запись с правами администратора ОС).
Администратор SD5	Локальный администратор ПК, обладающий собственным токеном с действующей лицензией SD5, произведший установку и первичную настройку SD5.
Пользователь SD5	Пользователь ПК, обладающий собственным токеном с действующей лицензией SD5 и являющийся владельцем зашифрованных ресурсов.
Алгоритм шифрования	Набор логических правил (математических преобразований), определяющих способ преобразования информации из открытого состояния в зашифрованное (процесс зашифрования) и наоборот, из зашифрованного состояния в открытое (процесс расшифрования).
JaCarta, eToken	Используемые в ПАК SD5 марки токенов.
Идентификация	Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем.
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдаёт.
Двухфакторная аутентификация	Двухфакторная аутентификация (2FA) — расширенная аутентификация, метод контроля доступа к компьютеру или информационной системе, в котором пользователю для получения доступа к информации необходимо предъявить более одного "доказательства механизма аутентификации". К категориям таких доказательств относят: ***Знание*** — информация, которую знает субъект. В случае с токенами – это PIN-код. ***Владение*** — вещь, которой обладает субъект. В случае SD5 речь идёт о токене.
Виртуальный диск	Логическое устройство, воспринимаемое ОС как обычный диск, но отличающееся тем, что все его данные хранятся в файле на одном из доступных физических дисков.
Зашифрованный диск (том)	Логический том или виртуальный диск, предназначенный для безопасного хранения конфиденциальной информации в зашифрованном виде с помощью SD5.

CSP	Cryptographic Service Provider, криптопровайдер или поставщик криптографии – программный модуль, реализующий один или несколько алгоритмов шифрования через системную шину ОС CryptoAPI.
Secret Disk Crypto Extension Pack (SD CEP)	Пакет расширения, который позволяет использовать алгоритм шифрования ГОСТ 28147-89 (ГОСТ 34.12-2015), предоставляемый сторонними криптопровайдерами.
КриптоПро CSP	Программа для предоставления симметричных и асимметричных алгоритмов шифрования по ГОСТ. Поставляется компанией КриптоПРО.
ViPNet CSP	Программа для предоставления симметричных и асимметричных алгоритмов шифрования по ГОСТ. Поставляется компанией Инфотекс.
eToken PKI Client	Программа для обеспечения работы USB-ключей и смарт-карт eToken на ОС семейства Windows не старше версии 7. Поставляется компанией Aladdin.
SafeNet Authentication Client (SAC)	Программа для обеспечения работы USB-ключей и смарт-карт eToken на ОС семейства Windows с версии 7 и старше. Поставляется компанией SafeNet.
JaCarta Unified Client	Программный комплекс, предназначенный для настройки и работы со всеми моделями USB-токенов и смарт-карт семейства JaCarta и поддерживаемых ПАК SD5 моделей eToken в ОС Microsoft Windows. Поставляется компанией "Аладдин Р.Д."
Сертификат открытого ключа	Электронный документ, подтверждающий принадлежность открытого ключа и определенных атрибутов конкретному пользователю.
Криптокопия	Зашифрованное значение параметра.
Крипто-хранилище	Файл или файлы с настройками приложения SD5, содержащие учётные записи пользователей, списки защищаемых ресурсов, параметры доступа к ресурсам, криптокопии ключей доступа и т.д.

2. Общие сведения

2.1 Назначение

ПАК SD5 защищает от посторонних лиц информацию, расположенную на дисках персонального компьютера. Защита осуществляется путём шифрования данных, что делает невозможным доступ к ним постороннего лица даже когда встроенные средства защиты ОС не действуют. Например, если данные пытаются скопировать подключив жёсткий диск к другому компьютеру, или обращаясь к данным от имени другого пользователя ОС.

Программно-аппаратный комплекс SD5 защищает информацию на внутренних и внешних устройствах хранения информации. Например, на компьютере с двумя дисками можно защитить системный диск (диск C:), логический том (диск D:) и внешний USB флэш-накопитель (диск E:).

> *SD5 не защищает информацию на оптических дисках CD и DVD.*

SD5 создает и позволяет использовать специальные защищённые ресурсы: виртуальные диски и файлы-контейнеры, а также защищать отдельные папки на обычных дисках.

При работе SD5 не использует учётные записи пользователей ОС. Администратор регистрирует пользователей SD5 в самом приложении, после чего сам администратор и пользователи аутентифицируются в нём при помощи специального электронного ключа – токена. Без подключения токена и ввода его пароля (PIN-кода) защищённый диск или другой ресурс подключить невозможно.

Данные на защищённых дисках всегда хранятся только в зашифрованном виде, даже когда с ними работает пользователь. Расшифрование данных для пользователя и приложений происходит только во время работы с ними и в расшифрованном виде данные находятся только в оперативной памяти компьютера. Если компьютер будет внезапно выключен или перейдёт в спящее состояние, информация на дисках останется зашифрованной и недоступной для посторонних.

2.2 Компоненты ПАК SD5

При работе с SD5 администратор использует следующие компоненты:

1. *Панель SD5* – приложение для управления пользователями и защищёнными ресурсами SD5. Панель SD5 можно запустить из меню (экрана) Пуск Windows. Основное окно приложения может быть закрыто. Запущенное приложение будет доступно в области уведомлений Windows.
2. *Загрузчик Secret Disk* – специальное приложение, которое запускается при включении компьютера и работает до загрузки ОС. Загрузчик Secret Disk устанавливается при включении защиты системного диска. Он осуществляет двухфакторную аутентификацию пользователя при помощи закрытого ключа сертификата на его токене и обеспечивает загрузку ОС Windows с зашифрованного диска, если пользователь имеет право на запуск ОС.

   В SD5 используются два вида загрузчиков – для режима загрузки LEGACY BIOS и для режима загрузки UEFI BIOS. Токен используется для аутентификации пользователя SD5. На токене пользователя хранятся следующие данные:

   - сертификат открытого ключа пользователя – его электронное удостоверение личности;
   - закрытый ключ пользователя (обеспечивает аутентификацию пользователя и шифрование ключевой информации);
   - защищённый файл с лицензией SD5, разрешающей использование ПАК SD5 владельцу токена.
3. *Программное обеспечение (клиент) для работы с токенами*. Это программное обеспечение используется незаметно для пользователя и требуется для работы с сертификатами и ключами на токене.

4. *Пакет расширенной криптографии (CEP)*, который позволяет использовать дополнительные драйверные алгоритмы шифрования, а также применять в SD5 алгоритмы шифрования ГОСТ внешних криптопровайдеров.

3. Характеристики SD5

3.1 Требования к операционной системе

SD5 может быть установлен на компьютер, работающем под управлением одной из следующих ОС:

- Microsoft Windows 7 SP1 Professional/Enterprise (x86 и x64);
- Microsoft Windows 8 Pro/Enterprise (x86 и x64);
- Microsoft Windows 8.1 Pro/Enterprise (x86 и x64);
- Microsoft Windows 10 Pro/Enterprise (x86 и x64).

Для загрузки ОС должен использоваться **стандартный** загрузчик Windows, установленный на системный диск в процессе инсталляции ОС. Разбиение дисковых накопителей должно быть сделано средствами устанавливаемой ОС. Тип разметки системного диска должен соответствовать выбранному режиму работы встроенного загрузчика (разметка MBR для режима LEGACY BIOS и тип GPT для режима UEFI BIOS).

3.2 Требования к компьютеру

Процессор (CPU)	• процессоры Intel с архитектурой EM64T и поддержкой команд SSE2 (процессоры поколения Core 2 и новее, кроме процессоров Itanium); • процессоры AMD с архитектурой IA64 и поддержкой команд SS2 (процессоры поколения K8 и новее).
Оперативная память (RAM)	• объём памяти, рекомендуемый для работы установленной ОС не менее 2 ГБ.
Свободное место на системном диске	• не менее 120 МБ.
Встроенное ПО компьютера	• LEGACY BIOS; • UEFI BIOS; • UEFI в режиме LEGACY BIOS (без CSM).
Внешние интерфейсы	• один свободный порт USB 1.1/2.0/3.0 для подключения токенов; • считывающее устройство для смарт-карт (если необходимо).

3.2.1 Поддерживаемые модели токенов

ПАК SD5 работает с перечисленными ниже моделями токенов. Токены разных моделей могут использоваться одновременно на одном компьютере. На компьютере должно быть установлено программное обеспечение (клиент) для используемых моделей токенов.

- JaCarta PKI (USB-ключ и смарт-карта);
- JaCarta PKI/ГОСТ (USB-ключ и смарт-карта);
- JaCarta PRO (USB-ключ и смарт-карта);
- JaCarta PRO/ГОСТ (USB-ключ и смарт-карта);
- eToken PRO Anywhere (USB-ключ);
- eToken PRO (Java) (USB-ключ и смарт-карта).

3.2.2 Криптопровайдеры алгоритмов шифрования ГОСТ

SD5 может использовать дополнительные криптоалгоритмы (AES 128, Twofish 256, AES 256) и внешних поставщиков криптографии, реализующие алгоритмы шифрования, определенные стандартами ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012, ГОСТ 28147-89, ГОСТ Р 34.12-2015 (Magma).

> *С 1 января 2019 года запрещено формирование электронной подписи с помощью ключей ГОСТ 34.10-2001.*

При применении в SD5 шифрования ГОСТ у пользователей SD5 должны быть ключи и сертификаты в формате ГОСТ, выпущенные с помощью установленного внешнего криптопровайдера.

> *Алгоритмы шифрования ГОСТ могут быть использованы только после загрузки ядра ОС и неприменимы для защиты системного диска.*
>
> *Установка одного из клиентов для работы с токеном необходима для корректной работы токенов eToken и JaCarta.*
>
> *Установка одного из криптопровайдеров для шифрования ГОСТ не обязательна к установке, но необходима, если требуется данный вид шифрования.*
>
> *Установка приложения SD CEP необходима и обязательна к установке, если требуются дополнительные драйверные алгоритмы или взаимодействие с криптопровайдерами. SD CEP необходимо установить после установки приложения ViPNet CSP или КриптоПРО CSP.*

Совместимое с SD5 программное обеспечение представлено в Таблица 1.

Таблица 1 – Совместимое ПО

Производитель	Название ПО	Рекомендуемая версия
ООО "КРИПТО-ПРО"	КриптоПРО CSP	4.0 R3, R4
ОАО "ИнфоТеКС"	ViPNet CSP	4.2

3.2.3 Работа SD5 при перезагрузке и в "спящих" режимах

SD5 обеспечивает защиту от потери данных в случае прерывания работы компьютера, включая штатные ситуации (перезагрузка, ждущий и спящий режимы) и нештатные (сбои в ОС сбои в электропитании и т.п.).

При подключённых зашифрованных дисках недопустима параллельная установка или удаление программ, способных подключать файлы-образы компакт-дисков в качестве виртуальных дисков.

> *Прежде чем устанавливать или удалять такие программы, необходимо отключить все зашифрованные диски, исключая системный.*

3.3 Лицензирование

Используемый электронный ключ (USB-токен или смарт-карта) должен содержать лицензию SD5 с актуальным сроком действия. Срок действия лицензии можно проверить с помощью дополнительной утилиты, входящей в дистрибутив – SD5LicRead.exe.

Подробное описание всех утилит, входящих в дистрибутив, находится в **Приложении 5**.

4. Дистрибутив SD5

Стандартная поставка ПО включает:

- файл лицензии;
- информационный листок;
- гарантийный талон.

> *Для работы продукта необходимо приобрести электронный ключ из числа совместимых.*

Дистрибутив включает

1. Документацию в электронном виде.
2. Клиентское ПО для работы с электронными ключами и криптографическими алгоритмами.
3. Установочные файлы SD5.
4. Утилиты для работы с лицензией (**Приложение 5**).

5. Установка и удаление SD5

> *Для установки и удаления ПО необходимы полномочия локального администратора.*

5.1 Порядок установки SD5

Перед установкой SD5 необходимо установить дополнительные программы:

	Приложение
Клиент для работы с токенами (**обязателен к установке**, должен соответствовать используемой модели токенов и версии ОС)	Программный комплекс "Единый клиент JaCarta" (процесс установки описан в Приложении 1)
	Приложение eToken PKI Client v. 5.1 (процесс установки описан в Приложении 2)
	Приложение SafeNet Authentication Client[1]
Криптопровайдеры ГОСТ (установка **обязательна при использовании алгоритмов шифрования ГОСТ**)	ViPNet CSP (процесс установки описан в Приложении 3)
	КриптоПРО CSP (Процесс установки описан в Приложении 4)
Secret Disk Crypto Extension Pack (SD CEP) установка обязательна при использовании алгоритмов шифрования ГОСТ и при необходимости использовании дополнительных драйверных криптоалгоритмов.	Secret Disk Crypto Extension Pack (SD CEP) (Вся необходимая информация о продукте представлена в отдельном файле).

> *Установка одного из клиентов для работы с токеном необходима для корректной работы токенов eToken и JaCarta.*
>
> *Установка одного из криптопровайдеров для шифрования ГОСТ не обязательна к установке, но необходима, если требуется данный вид шифрования.*
>
> *Установка приложения SD CEP необходима и обязательна к установке, если требуются дополнительные драйверные алгоритмы или взаимодействие с криптопровайдерами. SD CEP необходимо установить после установки приложения ViPNet CSP или КриптоПРО CSP.*

5.2 Установка SD5

Установка приложения SD5 производится с помощью инсталлятора sd-5.0.x.x-ru.exe, который подходит и для 64-битных и 32-битных ОС.

Установка SD5 завершается перезагрузкой ОС.

После установки SD5 рекомендуется сделать следующее:

- войти в Windows с учётной записью привилегированного пользователя;
- создать первого пользователя SD5 (в будущем администратора SD5) и зарегистрировать его сертификат (на токене с лицензией);
- настроить (создать) защищённые ресурсы, для создания которых необходимы полномочия привилегированного пользователя;

[1]Скачать лицензионную версию программы можно с официального сайта safenet.gemalto.com/

- при необходимости включить защиту системного диска;
- зарегистрировать сертификаты других пользователей SD5, которые будут работать в ОС Windows как непривилегированные пользователи и предоставить им соответствующие права на подключение защищённых ресурсов и загрузку ОС (если включена защита системного диска).

5.2.1 Установка инсталлятором SD5

Устанавливайте SD5 только на системный диск!

1. Запустите файл установки SD5: sd-5.x.x.xx-ru.(-x64 или –x86).msi.
2. Измените корневую папку установки программы (по желанию) нажатием кнопки **Изменить.**
3. Прочитайте лицензионное соглашение и примите его условия. Нажмите **Установить**.

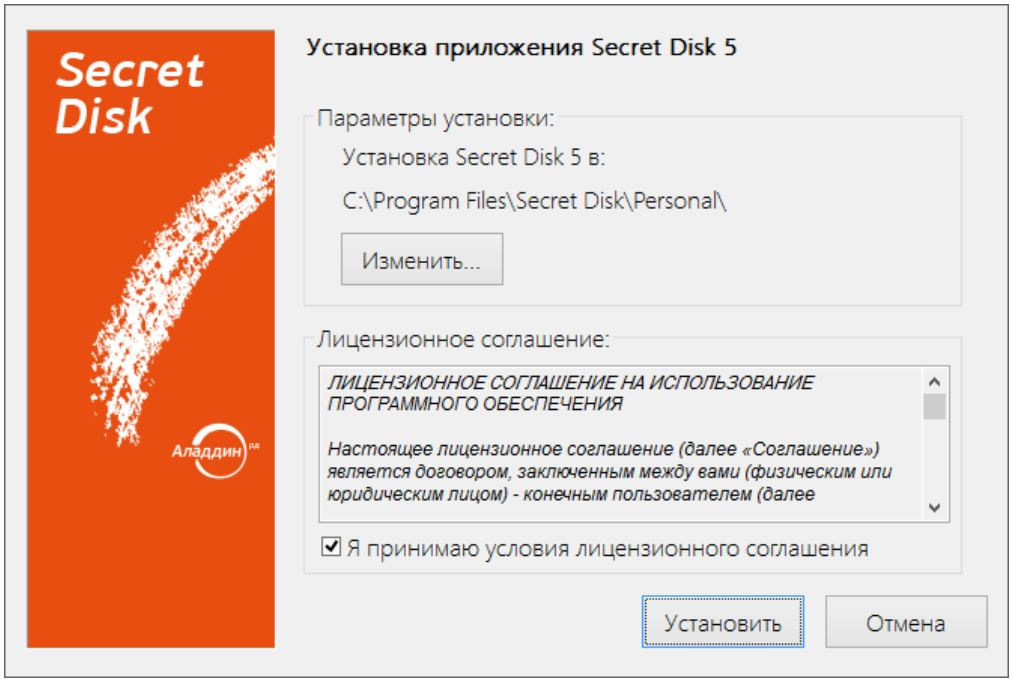

Рисунок 1. Окно мастера установки

4. Дождитесь окончания установки компонентов программы на компьютер.

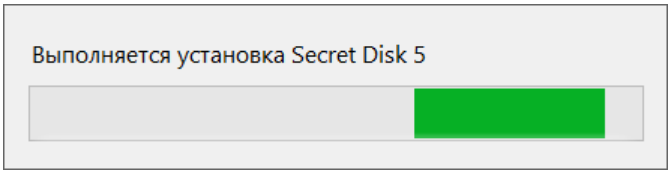

Рисунок 2. Процесс установки

5. Нажмите **Перезагрузка** для немедленной перезагрузки компьютера. Нажмите **Закрыть** для завершения программы установки.

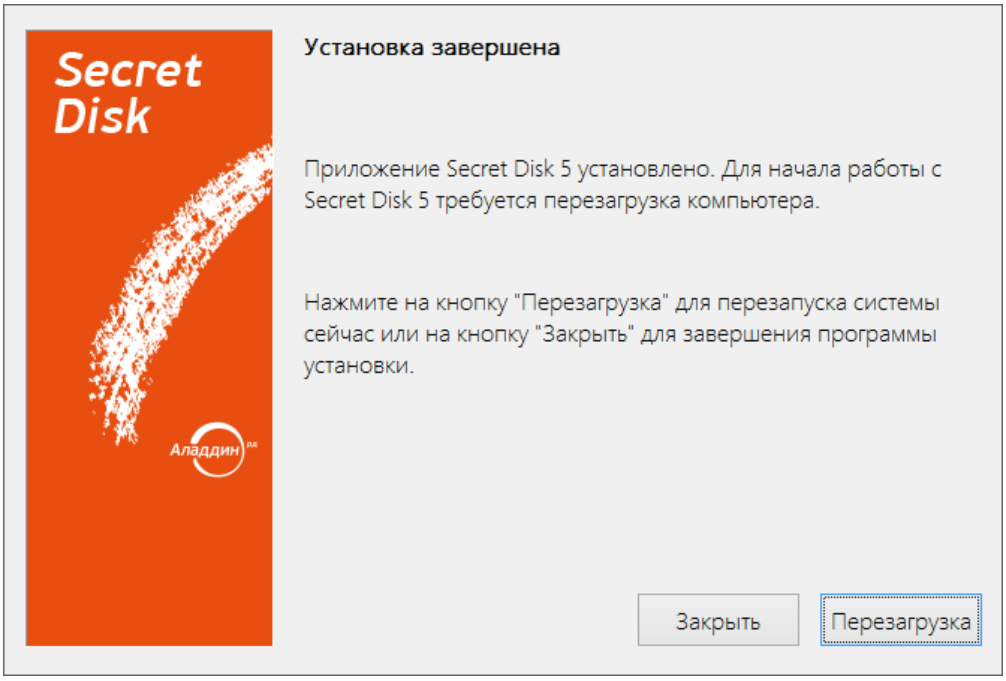

Рисунок 3. Окно уведомления о завершении установки

6. Управление пользователями SD5

Добавление пользователя – это регистрация имени пользователя, запись комментария и соответствующих сертификатов в крипто-хранилище.

> *У каждого пользователя должен быть хотя бы один сертификат.*
>
> *Для добавления пользователя необходимы полномочия администратора SD5 на компьютере.*

6.1 Регистрация первого пользователя – администратора SD5.

1. Откройте меню **Пуск → Программы → SD5**.
2. Нажмите **Зарегистрируйтесь**.

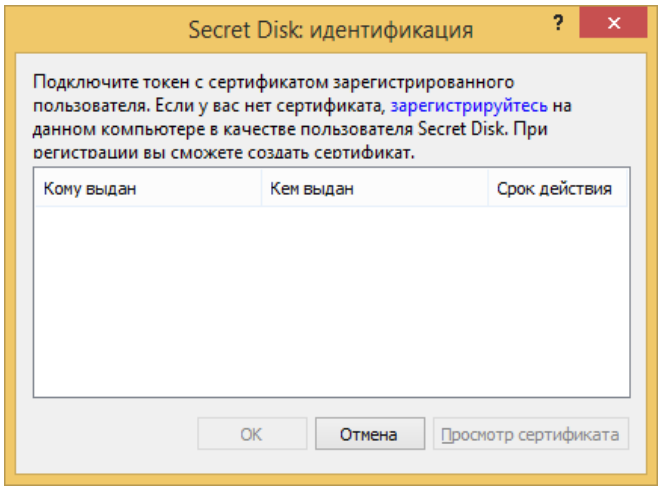

Рисунок 4 – Окно идентификации

3. Заполните необходимые поля и выберите поставщика криптографии. Нажмите **Выбрать.**

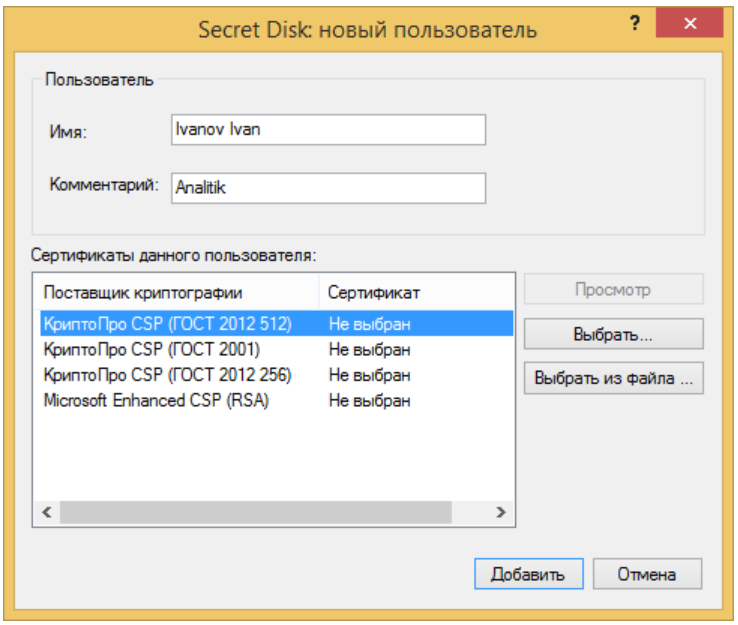

Рисунок 5 – Окно создания нового пользователя

4. В окне выбора сертификата нажмите **Создать**.

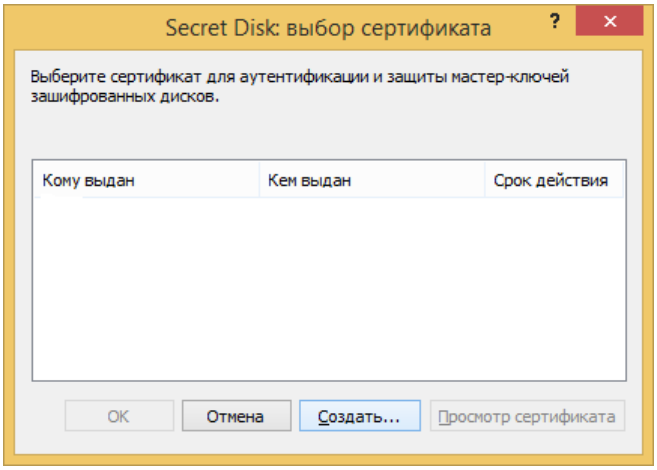

Рисунок 6 – Окно выбора/создания сертификата

5. Заполните данные для идентификации и выберите параметры шифрования. Нажмите **OK**.

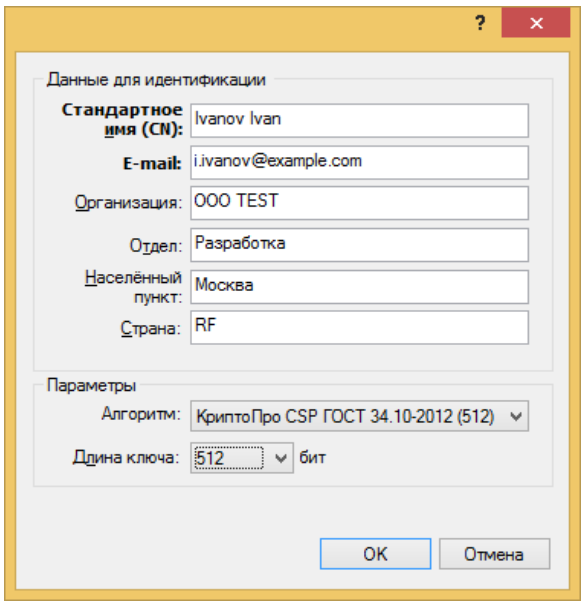

Рисунок 7 – Окно заполнения данных для идентификации

6. Для сохранения резервной копии сертификата нажмите **OK**.

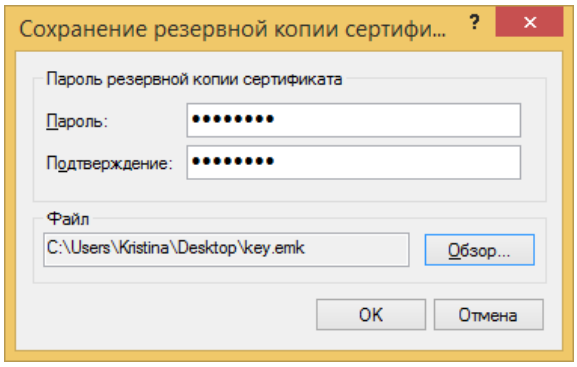

Рисунок 8 – Окно сохранения резервной копии сертификата пользователя

7. Выберите токен (если подключено несколько) и нажмите **OK**.

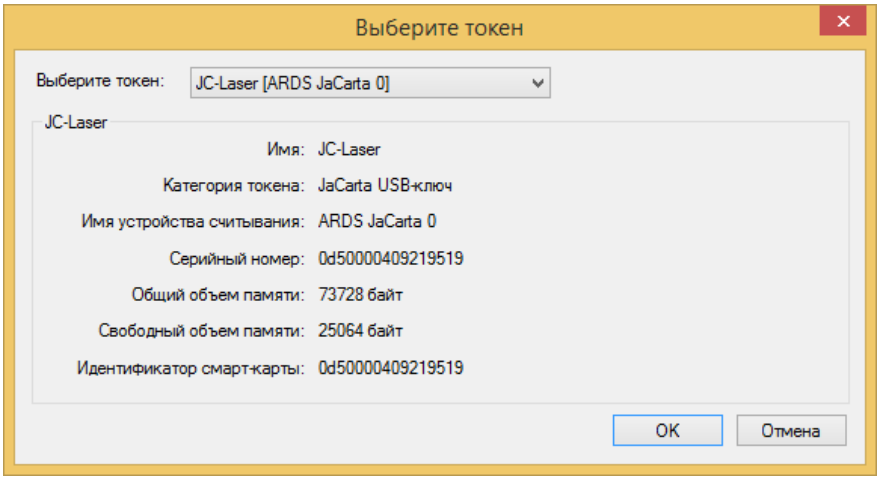

Рисунок 9 – Окно выбора токена

8. Введите PIN-код токена. Нажмите **OK**.

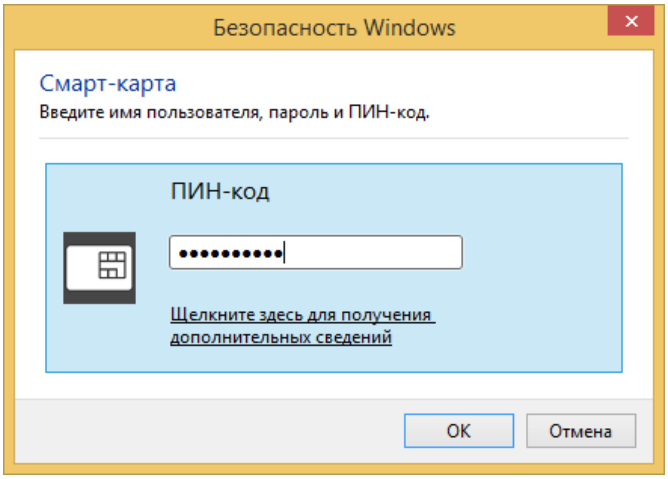

Рисунок 10 – Окно ввода ПИН-кода токена

9. Нажмите **OK**.

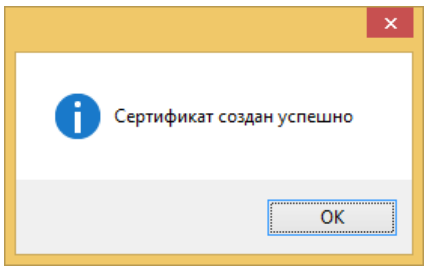

Рисунок 11 – Окно уведомления

10. В окне выбора сертификата появится созданный сертификат. Выберите его и нажмите **OK**.

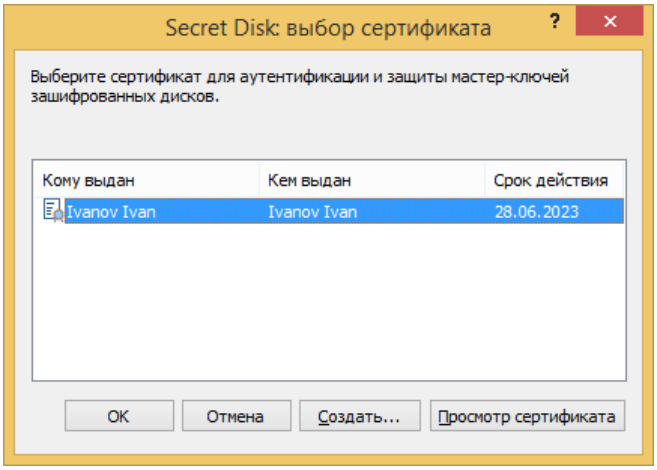

Рисунок 12 – Окно выбора сертификата пользователя

11. В окне регистрации пользователя нажмите **Добавить**.

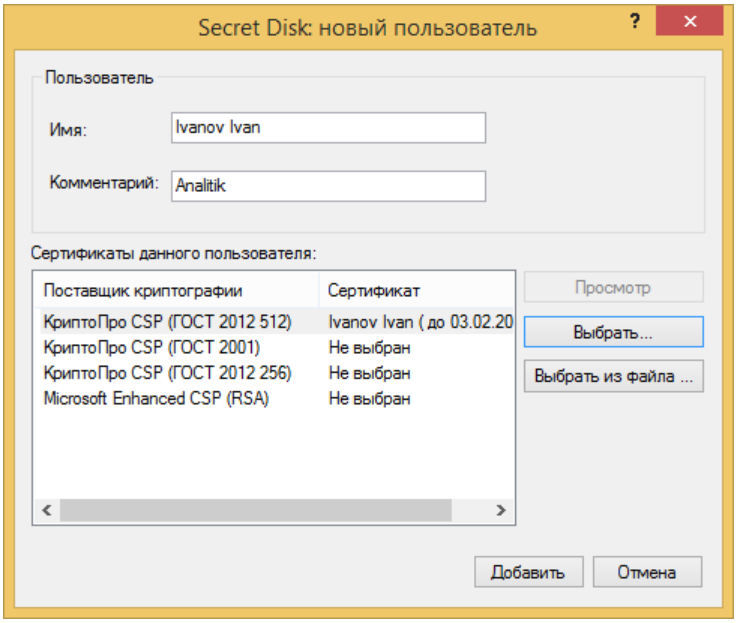

Рисунок 13 – Окно создания нового пользователя

12. Нажмите **OK**.

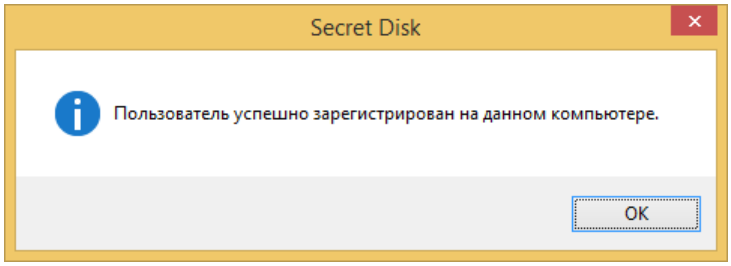

Рисунок 14 – Окно уведомления

13. В окне идентификации выберите созданного пользователя и нажмите **OK**.

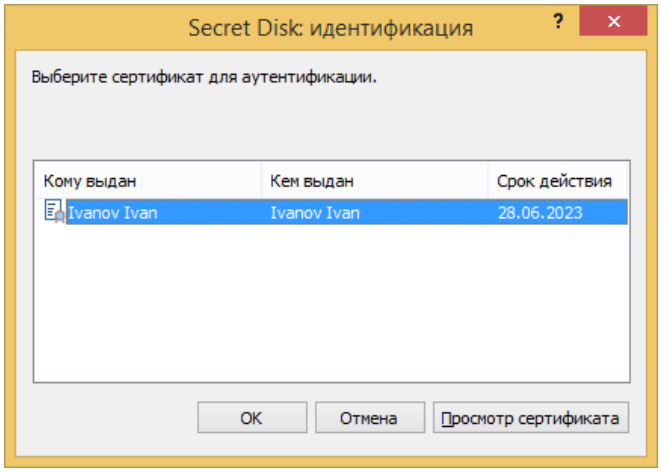

Рисунок 15 – Окно идентификации нового пользователя

> *У одного пользователя может быть несколько сертификатов. Но один сертификат не может принадлежать нескольким пользователям, т.е. выдать новому пользователю уже используемый сертификат невозможно.*

6.2 Создание нового пользователя администратором SD5

> *Список всех зарегистрированных и имеющих хотя бы один сертификат пользователей можно просмотреть в панели SD5 на вкладке Пользователи.*
>
> *Либо при выборе пользователя при запуске программы.*
>
> *Права на создание нового пользователя есть только у администратора SD5.*

Процедура создания нового пользователя другим пользователем аналогична описанной выше. Создать пользователя можно в панели SD5 во вкладке **Пользователи**.

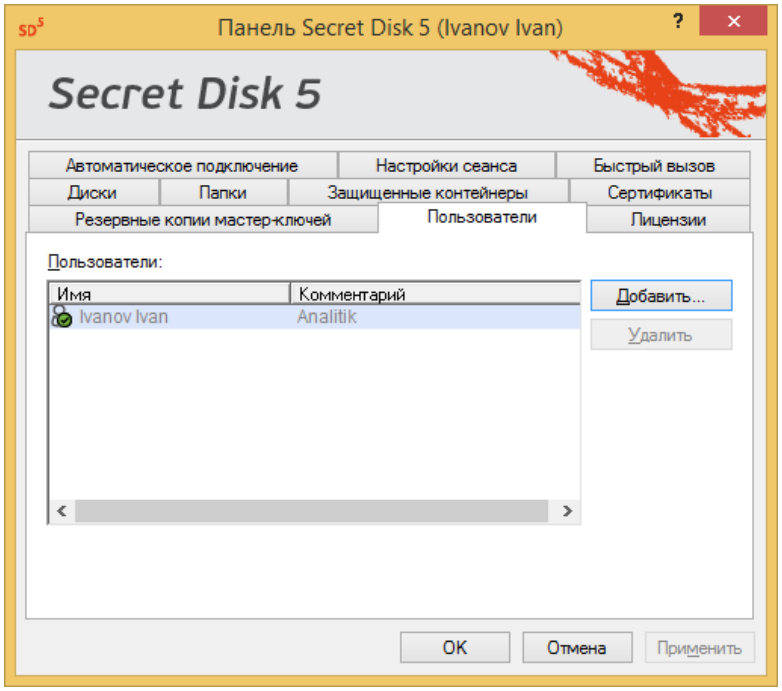

Рисунок 16 – Панель Secret Disk. Пользователи

6.3 Удаление пользователя SD5

> *Перед удалением данных пользователя убедитесь, что у этого пользователя не осталось зашифрованных ресурсов.*
>
> *При удалении пользоватлея его сертификат не удаляется. Процедура удаления сертификата описана в параграфе* ***Удаление сертификата****.*
>
> *Права на удаление пользователя есть только у администратора SD5.*

Для удаления пользователя выполните следующие действия:

1. В сеансе пользователя во вкладке **Пользователи** выберите нужного пользователя и нажмите **Удалить**.

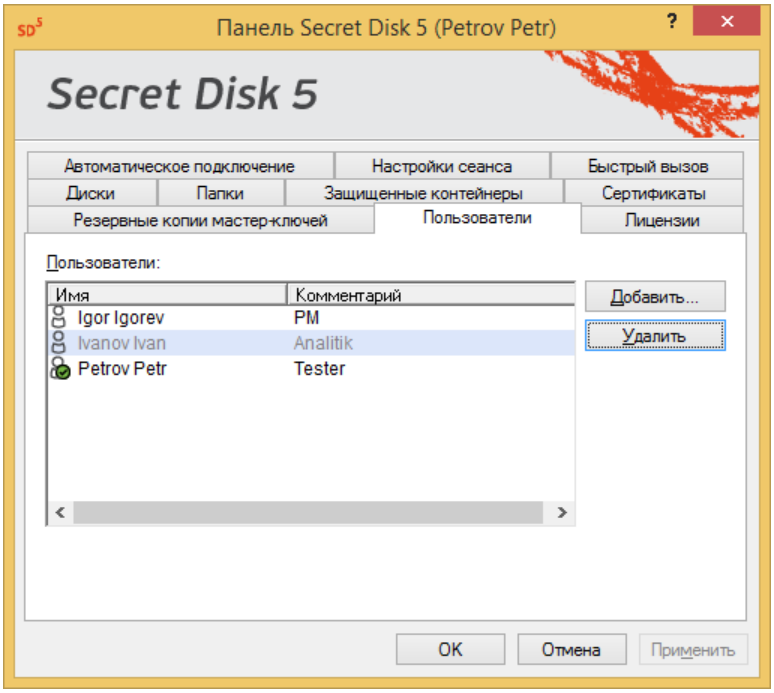

Рисунок 17 – Панель Secret Disk. Пользователи

2. Если у пользователя есть зашифрованные диски – программа покажет сообщение об ошибке и прервёт процесс удаления пользователя.

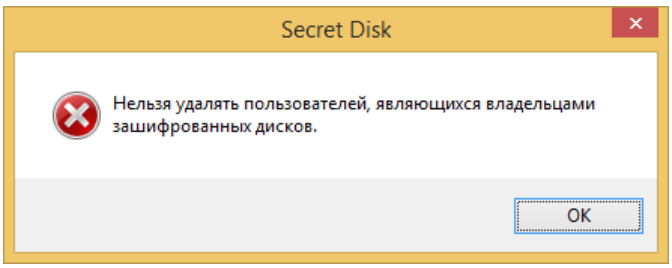

Рисунок 18 – Уведомление об ошибке удаления пользователя

3. Если у пользователя нет зашифрованных ресурсов – программа удалит выбранного пользователя без уведомления.

7. Работа с системным диском

7.1 Свойства системного диска

> *Защита системного диска доступна только пользователю с правами администратора Windows. Обычному пользователю эта функция недоступна.*

При установке защиты системного раздела необходимо учитывать следующие дополнительные ограничения:

1. Если на ПК установлено несколько жёстких дисков, то защиту можно устанавливать на загрузочный раздел (boot partition), расположенный на первом жёстком диске.
2. После установки защиты системного раздела не используйте диспетчеры загрузки, меняющие порядок загрузки ОС. SD5 поддерживает только стандартный загрузчик Windows 7 / Windows 8 и 8.1 / Windows 10.

> *ПК имеющие режим UEFI BIOS не должны использовать режим загрузки LEGACY BIOS.*
>
> *Внимание! На компьютерах использующих UEFI необходимо отключить режим SECURE BOOT.*

3. При наличии на защищаемом системном диске программ, производящих перезапись главной загрузочной записи (Master Boot Record), защищённая часть диска считываться не будет. Изменения главной загрузочной записи возможны также при установке на диск следующих типов программ:
   - программы шифрования дисков, отличные от SD5;
   - программы редактирования разделов жёсткого диска;
   - диспетчеры загрузки (мультизагрузчики);
   - ОС, отличные от Windows 7/Windows 8/8.1 /Windows 10, устанавливающие свои диспетчеры загрузки.

> *Необходимо снять атрибут сжатия для корневой папки и для всех вложенных.*
>
> *Если атрибут сжатия был снят только для корневой папки, без учёта вложенных, этот атрибут нужно установить вновь, затем снять для корневой папки и всех вложенных.*

4. Мастер-ключ загрузки ОС может храниться в памяти токена владельца, а его резервная копия в текстовом виде (на бумаге или в текстовом файле).

> *Для системного раздела нет возможности сохранить резервную копию мастер-ключа в защищённый паролем файл с расширением *.emk.*
>
> *Не выполняйте преобразование защищённого базового системного раздела в динамический – это приведёт к невозможности загрузки ОС!*

Перед конвертацией базового системного раздела в динамический необходимо снять с него защиту.

Несоблюдение условий при установке защиты системного раздела может привести к сбою загрузки ОС.

7.2 Предварительная проверка перед установкой защиты

Перед установкой защиты на системный раздел SD5 производит следующие проверки:

1. Тип используемого пользователем токена.
2. Возможность установки защиты.
3. При невозможности установки защиты могут появиться следующие сообщения:
   - системный раздел может быть защищён только если расположен на первом физическом диске;
   - загрузочный раздел не может быть защищён, так как установлен менеджер разделов;
   - раздел не может быть защищён, так как он является несистемным и на нём расположен загрузчик;

– системный диск с активным атрибутом сжатия файлов не может быть защищён.

7.3 Установка защиты на системный диск

Для установки защиты на системный диск выполните следующие действия

1. Откройте сеанс пользователя.
2. На вкладке **Диски** выберите **Системный диск** (C:), нажмите по нему правой кнопкой мыши и выберите пункт **Защитить диск**.

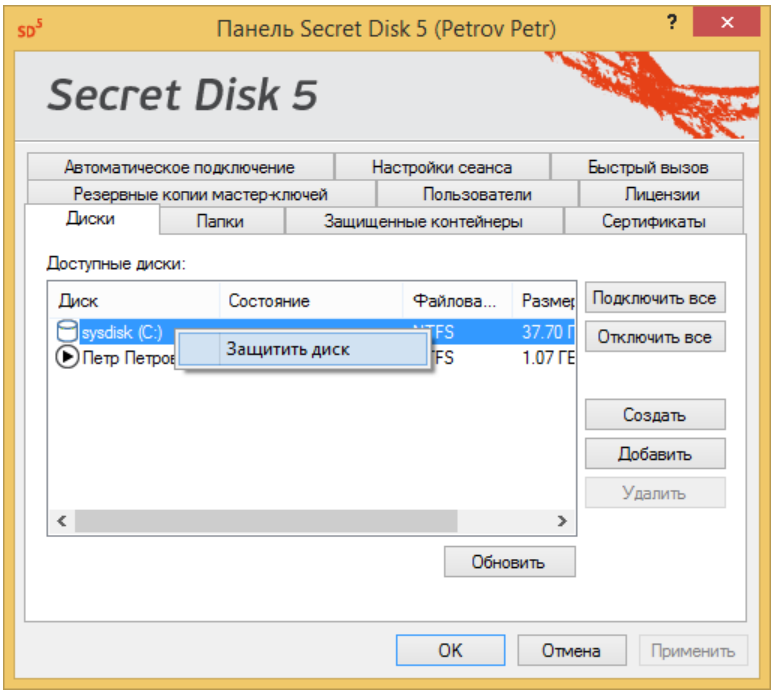

Рисунок 19 – Панель Secret Disk. Диски

3. Введите метку диска или оставьте ту, которая была задана при форматировании. После этого нажмите **OK**.

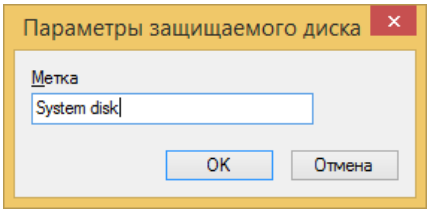

Рисунок 20 – Параметры защищаемого диска

> *При установке защиты системного диска допускается задавать только метку. Изменить букву системного диска нельзя.*

4. В окне **Резервное копирование** мастер-ключа нажмите **Распечатать** для вывода мастер-ключа защиты системного диска на принтер.
5. Для продолжения без сохранения копии мастер-ключа (это можно будет сделать позже в любое время в процессе работы) нажмите **Закрыть**.

> *Рекомендуется сохранить копию мастер-ключа **незамедлительно**.*
>
> *Распечатанную копию мастер-ключа необходимо хранить в защищённом месте, например, в сейфе.*

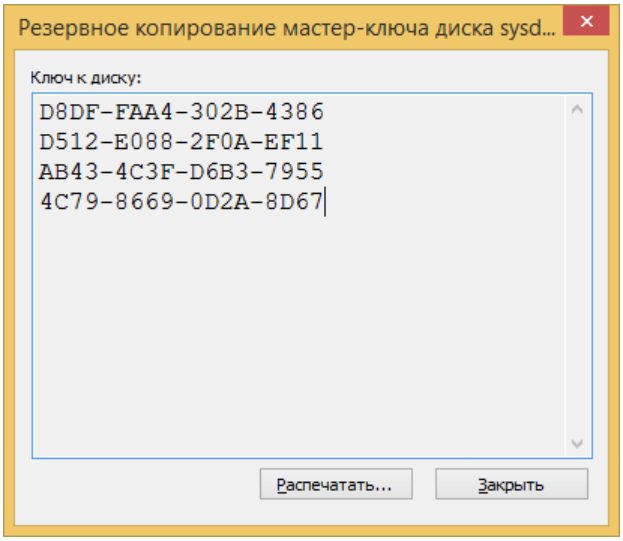

Рисунок 21 – Окно сгенерированного мастер-ключа для восстановления доступа к системному диску

6. Для продолжения защиты Системного диска и выполнения тестовой загрузки перезагрузите компьютер. Нажмите **Да**.

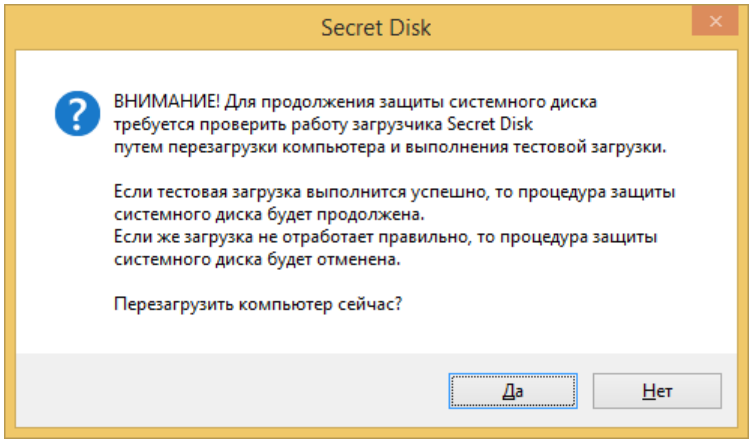

Рисунок 22 – Окно предупреждения о перезагрузке компьютера

7. При повторной загрузке на экране появится окно с предложением подключить электронный ключ.

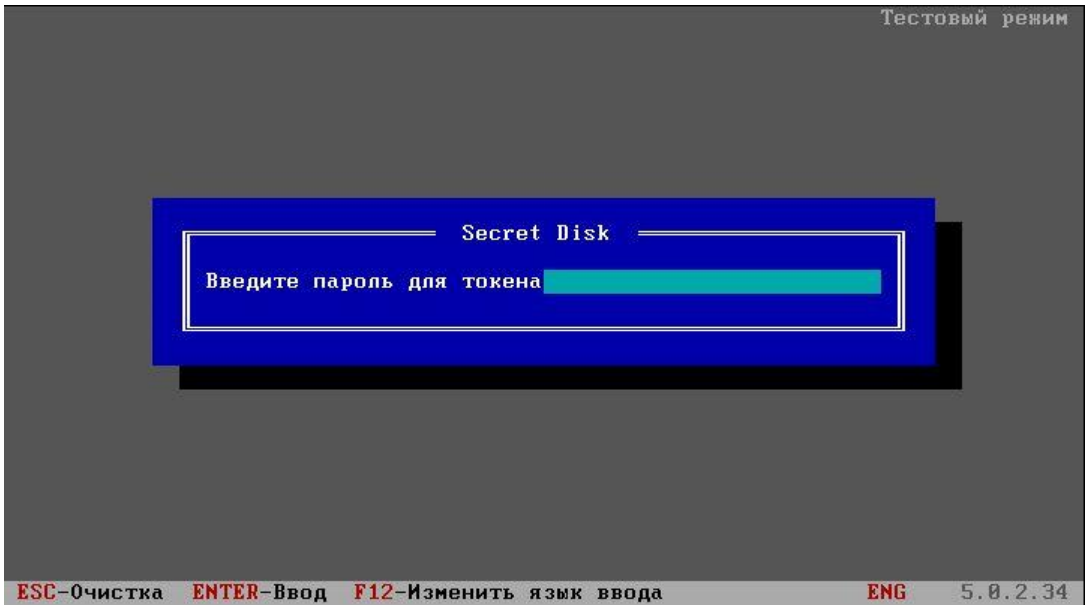

Рисунок 23 – Окно ввода ПИН-кода токена перед началом загрузки ОС Windows

8. Если электронный ключ уже подключён, то автоматически появится окно для ввода пароля.
9. Введите пароль электронного ключа и нажмите **Enter**.
10. После загрузки системы на экране появится предупреждение об успешном завершении тестовой загрузки.

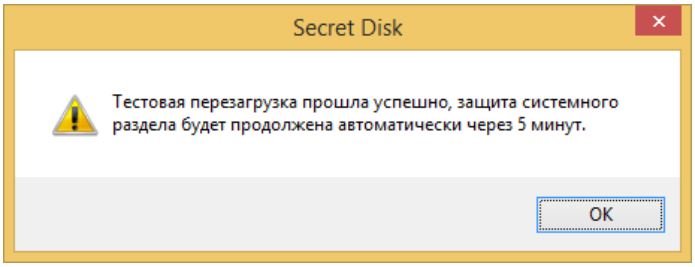

Рисунок 24 – Окно уведомления об успешной перезагрузке

Во время установки защиты системный диск остаётся полностью доступным для работы – на нём можно создавать и удалять файлы, выполнять проверку, определять права доступа пользователей к файлам и папкам и т.д.

При перезагрузке защиту системного раздела можно будет запустить вручную, либо она будет продолжена через 5 минут автоматически после загрузки компьютера.

> *Отключение (размонтирование) системного диска невозможно.*

Строка **Установка защиты** с указанием количества процентов готовности в ячейке **Состояние** показывает, что процесс установки защиты активен.

Сообщение об ошибке тестовой перезагрузки может появится в нескольких случаях

1. Во время тестовой перезагрузки отключалось питание компьютера.
2. Установлен неизвестный сторонний загрузчик системы.

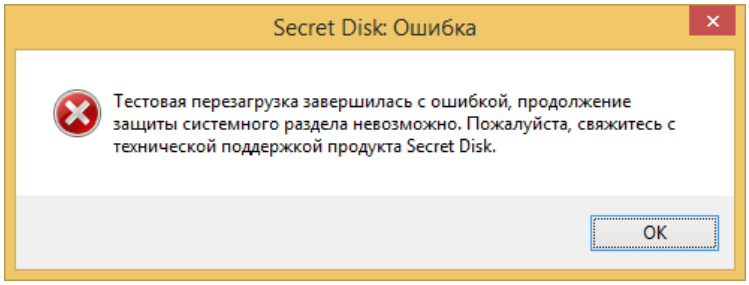

Рисунок 25 – Ошибка тестовой загрузки

После того как защита будет установлена на системный диск, поле *Состояние* сменит значение на *Защищён*.

Кнопка контекстного меню	Действие
Открыть в проводнике	Путь к системному диску откроется в проводнике
Переустановить защиту диска	Начало процесса переустановки защиты диска
Снять защиту диска	Снятие защиты с диска
Свойства	Открытие свойств защищённого диска
Сохранить мастер-ключ	Сохранение копии мастер-ключа защищённого диска
Защитить диск	Возобновление процесса защиты диска
Остановить процесс	Остановка процесса зашифрования/перешифрования диска

Для корректного восстановления ОС, создайте новую точку восстановления системы сразу после защиты системного раздела.

Для этого в меню **Пуск** выберите **Программы** → **Стандартные** → **Служебные** → **Восстановление системы** и создайте точку восстановления.

> *Пользователь, авторизованный в системе как не привилегированный, не может зашифровывать ресурсы (системный диск, логические тома, виртуальные диски, съёмные носители).*

7.4 Загрузка компьютера после установки защиты на системный диск

После установки защиты Системного диска меняется порядок загрузки ОС. При включении (перезагрузке) компьютера выдаётся начальное окно аутентификации SD5. В окне требуется подключить токен пользователя, которому разрешена загрузка ОС.

Для загрузки ОС необходимо подключить токен и ввести PIN-код.

На этом этапе можно вручную ввести мастер-ключ диска (который был сформирован и распечатан на этапе установки защиты). Это позволит произвести аутентификацию без токена.

Для ввода мастер-ключа вручную:

1. Нажмите **F2**.
2. Введите мастер-ключ.
3. Нажмите **Enter**. После ввода мастер-ключа загрузка ОС продолжится в обычном режиме.

> *После установки защиты системного диска не используйте диспетчеры загрузки, меняющие порядок загрузки ОС. SD5 поддерживает только стандартный загрузчик Windows 7/Windows 8/Windows 10.*

7.5 Перешифрование системного диска

1. Откройте сеанс пользователя.
2. На вкладке **Диски** нажмите правой кнопкой мыши на диск и выберите пункт **Переустановить защиту**.
3. Можно скопировать значение ключа шифрования на любой другой носитель или распечатать его, нажав кнопку **Распечатать**.
4. Для продолжения нажмите **Закрыть**.

> *Для установки защиты на системный диск используется только один криптографический алгоритм – AES-256.*

В процессе переустановки защиты в поле **Состояние** напротив Системного диска отобразится значение **Переустановка защиты** (с указанием процентных пунктов от выполненной задачи).

7.6 Расшифрование системного диска (снятие защиты)

Для снятия защиты с системного диска необходимо расшифровать диск.

1. Откройте сеанс пользователя.
2. На вкладке **Диски** нажмите правой кнопкой мыши на диске и выберите пункт **Снять защиту диска**.

> *В процессе снятия защиты в поле Состояние напротив системного диска отобразится значение Снятие защиты (с указанием процентных пунктов от выполненной задачи).*

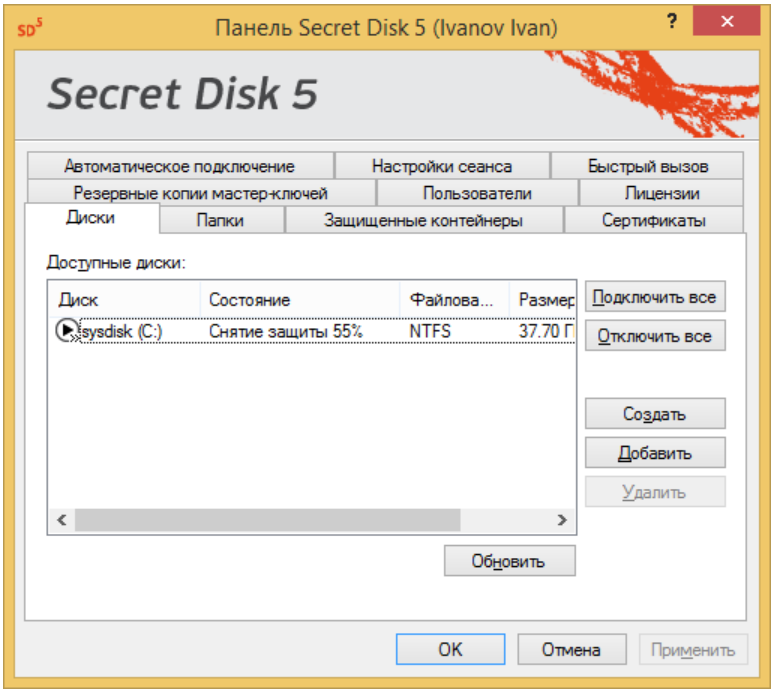

Рисунок 26 – Панель Secret Disk. Диски

7.7 Восстановление доступа к защищённому системному диску

> *Восстановление доступа к зашифрованному системному диску возможен при наличии сохранённой резервной копии мастер-ключа этого диска.*
>
> *При отсутствии резервной копии мастер-ключа восстановление невозможно!*

При невозможности подключения токена к компьютеру, используйте ранее сохранённую копию мастер-ключа системного диска.

Для восстановления доступа к системному диску и загрузке ОС выполните следующие действия.

1. Включите компьютер.
2. В окне запроса SD5 на подключение токена нажмите **F2**.

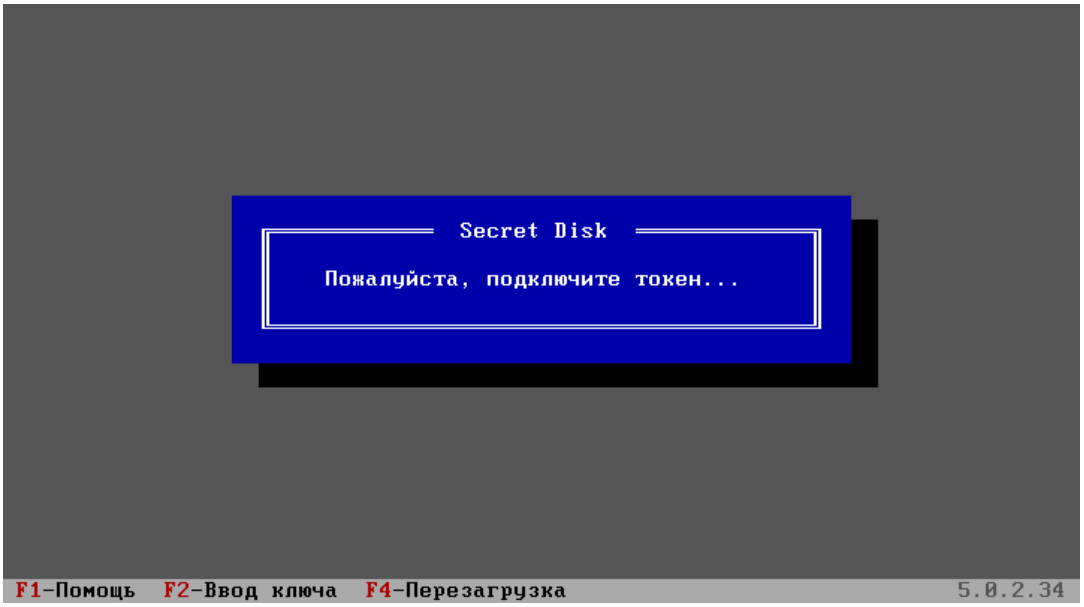

Рисунок 27 – Окно уведомления SD5 о подключении токена

3. Введите копию мастер-ключа и нажмите **Enter**.

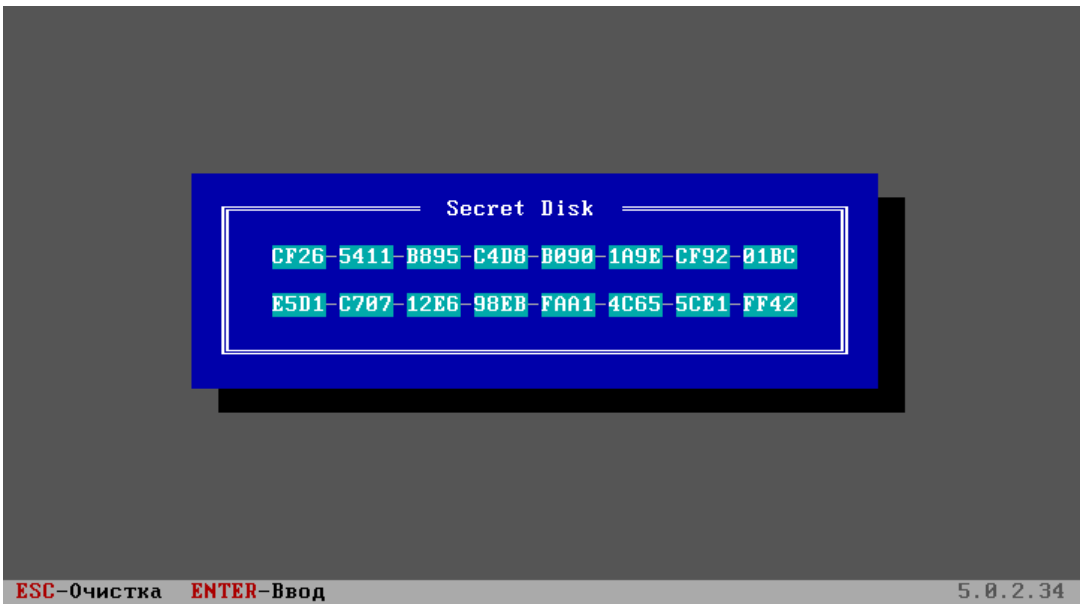

Рисунок 28 – Окно ввода мастер-ключа системного диска

4. Дождитесь окончания загрузки ОС.

Восстановить доступ к оставшимся защищённым ресурсам возможно при наличии сохранённых копий мастер-ключей.

Для этого необходим другой токен с лицензией SD5. С помощью этого токена и копий мастер-ключей возможно восстановить доступ к защищённым ресурсам. Процесс восстановления доступа к ресурсам описан в главе Восстановление доступа к защищённым ресурсам.

8. Работа с логическим томом

8.1 Особенности работы

Подключённые в SD5 ресурсы, которые ОС распознает как подключённые устройства: логические, физические, виртуальные тома и контейнеры, - доступны всем пользователям, одновременно работающим на компьютере (параллельная сессия).

8.2 Зашифрование логического тома

Чтобы зашифровать логический том, выполните следующие действия.

1. Откройте сеанс пользователя.

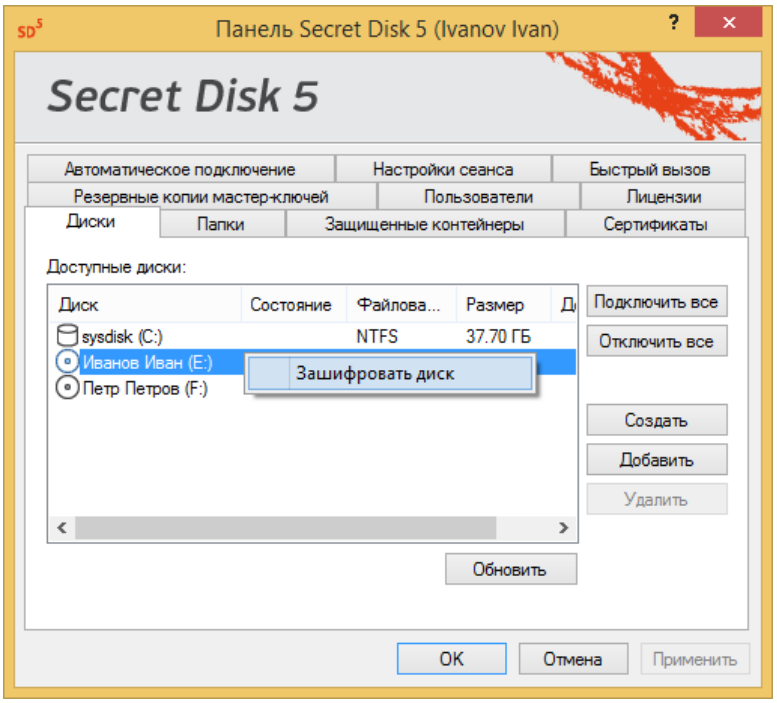

Рисунок 29 – Панель Secret Disk. Диски

2. Выберите во вкладке **Диски** нужный незашифрованный логический том. Нажмите правой кнопкой мыши по диску → **Зашифровать диск**.
3. Назначьте метку и выберите букву диска в окне **Параметры зашифрованного диска** (если вы хотите изменить значения, присвоенные по умолчанию).
4. Выберите алгоритм шифрования.

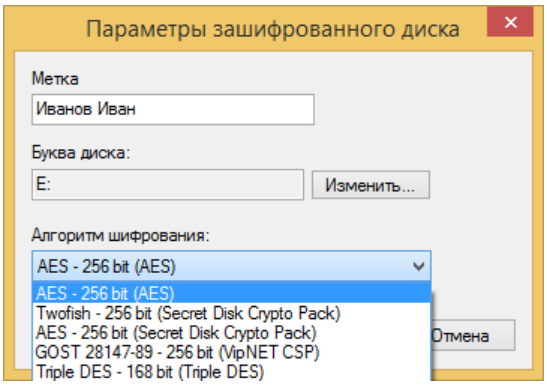

Рисунок 30 – Окно выбора параметров зашифрованного диска

В списке Алгоритм шифрования в скобках указывается компонент поставщика криптографии.

Для успешного зашифрования диска необходимо выбрать соответствующий поставщику криптографии сертификат открытого ключа.

5. Нажмите **OK**.
6. После завершения шифрования диска рекомендуется сохранить резервную копию мастер-ключа.

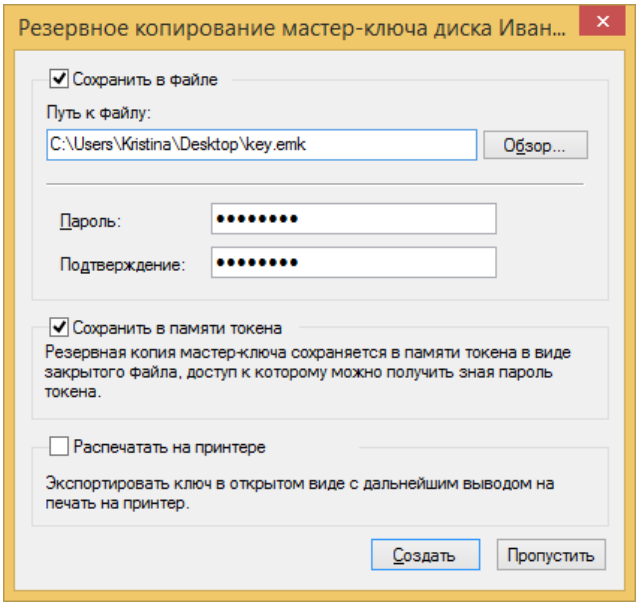

Рисунок 31 – Окно сохранения резервной копии мастер-ключа диска

Резервное копирование мастер-ключа зашифрованного диска возможно в любое время.

Можно сохранить резервную копию мастер-ключа в файле, на электронный ключ или распечатать на принтере.

Резервная копия на электронном ключе находится в закрытой области памяти электронного ключа и защищена паролем пользователя электронного ключа.

Резервная копия на съёмной носителе должна хранится в надёжном месте (например, сейфе).

Резервная копия ключа на бумажном носителе должна храниться в надёжном месте (например, сейфе).

7. После выбора места хранения резервной копии мастер-ключа нажмите **Создать**.
8. Для отмены создания резервной копии нажмите **Пропустить**.

Если в качестве места хранения резервной копии выбран электронный ключ, введите PIN-код ключа.

9. В окне сообщения об успешном сохранении резервной копии мастер-ключа нажмите **OK**.

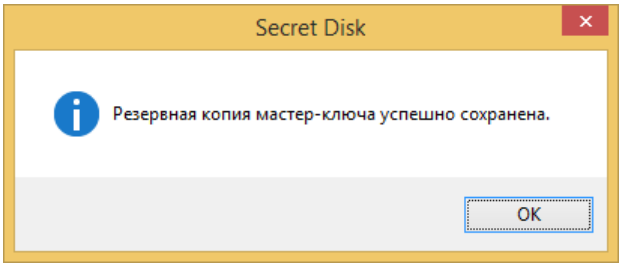

Рисунок 32 – Окно уведомления об успешном сохранении мастер-ключа диска

10. Строка *Шифрование* (с указанием количества процентов готовности) в ячейке *Состояние* свидетельствует, что процесс зашифрования активен.

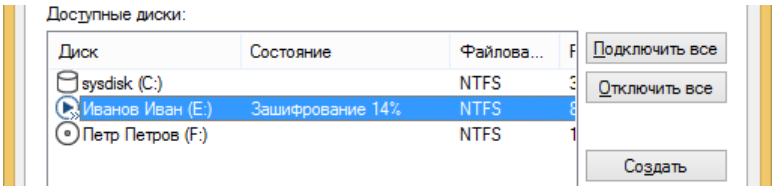

Рисунок 33 – Процесс зашифрования логического тома

- для остановки/прерывания процесса, нажмите на строку **Состояние** правой кнопкой мыши → **Остановить процесс**;
- продолжить зашифрование можно в любое другое время, выбрав пункт контекстного меню **Зашифровать диск**;
- для отмены защиты выберите **Расшифровать диск**.

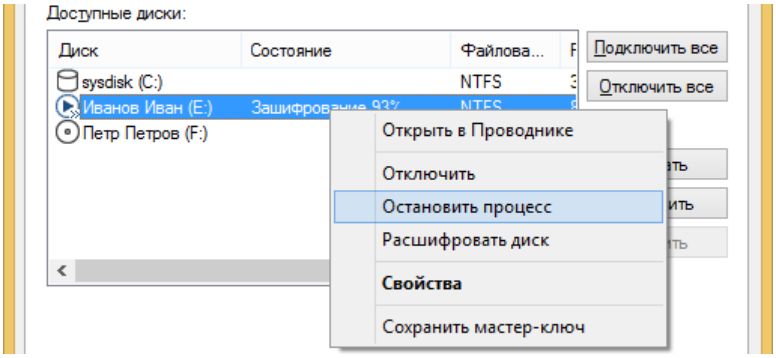

Рисунок 34 – Остановка процесса зашифрования

В процессе зашифрования диск полностью готов к работе. На нём можно:

- создавать и удалять файлы;
- выполнять проверку;
- работать с файлами;
- определять права доступа.

При использовании съёмных дисков необходимо, чтобы процедура шифрования была доведена до конца именно на том компьютере, где она была начата.

> *При попытке завершить шифрование на другом компьютере и/или другой ОС, данные будут безвозвратно утеряны.*

Когда диск полностью зашифрован и готов к работе, значок диска в ячейке **Диск** приобретёт вид  , а ячейка *Состояние* примет значение *Зашифрован*.

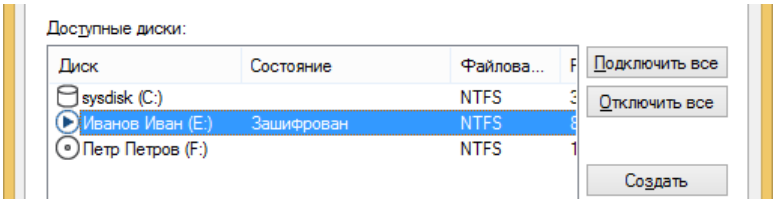

Рисунок 35 – Вид окна с зашифрованным логическим томом

8.3 Перешифрование логического тома

Для перешифрования логического тома выполните следующие действия.

1. Откройте сеанс пользователя.
2. На вкладке **Диски** нажмите правой кнопкой мыши на нужный логический том и выберите пункт **Перешифровать диск**.

Можно изменить метку, букву диска и алгоритм шифрования, выбрав необходимые значения в соответствующих полях.

3. Для подтверждения заданных параметров нажмите **OK**.

> *В процессе перешифрования в поле Состояние напротив выбранного диска будет отображаться значение Перешифрование (с указанием процентных пунктов от выполненной задачи).*

8.4 Расшифрование логического тома

Для снятия защиты с логического тома выполните следующие действия.

1. Выберите нужный зашифрованный логический том.
2. Нажмите правой кнопкой мыши → **Расшифровать диск**.
3. Дождитесь окончания процесса расшифрования.

8.5 Восстановление доступа и доступ пользователей к зашифрованному логическому тому

> *Восстановление доступа к зашифрованным ресурсам возможно при наличии сохранённых копий мастер-ключей этих ресурсов.*
>
> *При отсутствии сохранённых копий мастер-ключей восстановление доступа к защищённым ресурсам невозможно.*

Процедура восстановления доступа к логическому тому описана в главе "Восстановление доступа к зашифрованным ресурсам".

Процедура открытия доступа к логическому тому описана в главе "Доступ пользователей SD5 к защищённым ресурсам".

9. Работа с виртуальным томом

9.1 Особенности работы

Подключённые в SD5 ресурсы (те, которые ОС распознает как подключённые устройства (логические, физические, виртуальные тома и контейнеры)) доступны всем пользователям, одновременно работающим на компьютере (параллельная сессия).

> *Нельзя создать файл виртуального диска на уже зашифрованном логическом томе, на защищённом системном диске или внутри другого виртуального тома.*
>
> *Виртуальные тома создаются сразу зашифрованными. Расшифрование недоступно.*

9.2 Создание виртуального тома

Для создания зашифрованного виртуального диска выполните следующие действия.

1. Откройте сеанс администратора.
2. На вкладке **Диски** нажмите **Создать** (или в меню SD5 в области уведомлений выберите пункт Создать зашифрованный виртуальный диск).
   - введите путь к файлу виртуального диска, либо выберите путь с помощью кнопки Обзор и введите имя виртуального диска;

     По умолчанию файл будет иметь расширение *.vd.
   - выберите алгоритм шифрования из списка доступных алгоритмов;
   - по желанию измените метку диска;
   - по желанию измените букву диска;
   - выберите файловую систему (FAT, FAT32, exFAT или NTFS);
   - выберите тип диска (по умолчанию выбран расширяемый диск, объём которого варьируется в зависимости от содержимого. Максимальный размер будет соответствовать значению поля *Ёмкость диска*. Пункт Фиксированный – размер диска всегда равен указанному в поле *Ёмкость диска*);
   - выберите нужный размер диска (в гигабайтах).

> *В списке Алгоритм шифрования в скобках указывается компонент поставщика криптографии.*
>
> *Для успешного создания зашифрованного виртуального диска необходимо выбрать соответствующий поставщику криптографии сертификат открытого ключа.*
>
> *Объём доступного места на зашифрованном виртуальном диске будет несколько меньше размера файла. Величина этой разницы зависит от выбранной файловой системы.*

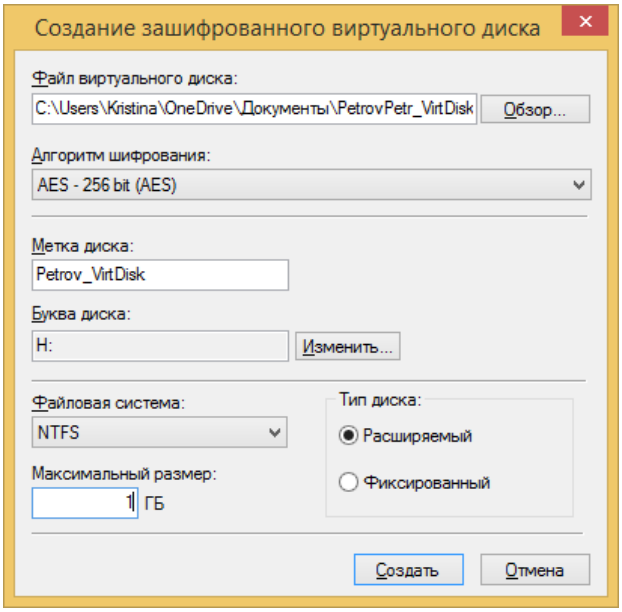

Рисунок 36 – Окно создания виртуального тома

3. Нажмите **Создать**.

Создание виртуального диска отображается в виде шкалы с комментариями по каждому этапу процесса.

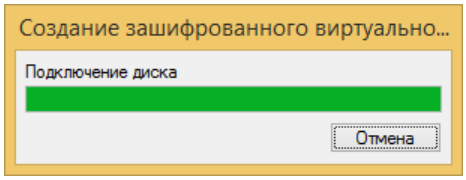

Рисунок 37 – Окно процесса создания виртуального тома

Рекомендуется сохранить копию мастер-ключа созданного диска.

4. Чтобы создать резервную копию, нажмите **Да**. Для отказа создания резервной копии нажмите **Нет**. Процесс создания резервной копии мастер-ключа описан в разделе "Сохранение резервной копии мастер-ключа".

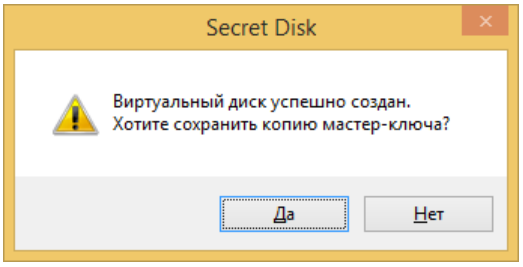

Рисунок 38 – Окно уведомления об успешном создании виртуального тома

5. В области уведомлений появится сообщение, что виртуальный диск создан. Новая запись появится на вкладке **Диски**.

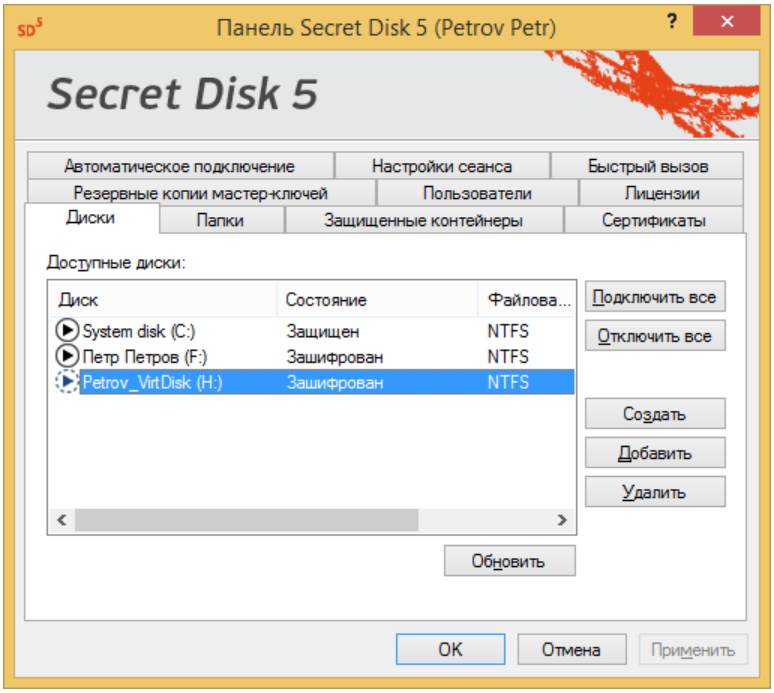

Рисунок 39 – Панель Secret Disk. Диски

> *При перешифровании виртуальных дисков необходимо, чтобы процедура шифрования была доведена до конца именно на том компьютере, где она была начата.*
>
> *В случае попытки завершения процедуры шифрования на другом компьютере и/или другой ОС данные будут безвозвратно потеряны.*

9.3 Удаление виртуального тома

Для удаления зашифрованного виртуального тома выполните действия:

1. Откройте сеанс пользователя.
2. На вкладке **Диски** выберите зашифрованный виртуальный том, который необходимо удалить, и нажмите **Удалить**.
3. Нажмите **Да**. В запросе на отключение диска нажмите **Да**, если диск в данный момент подключён.

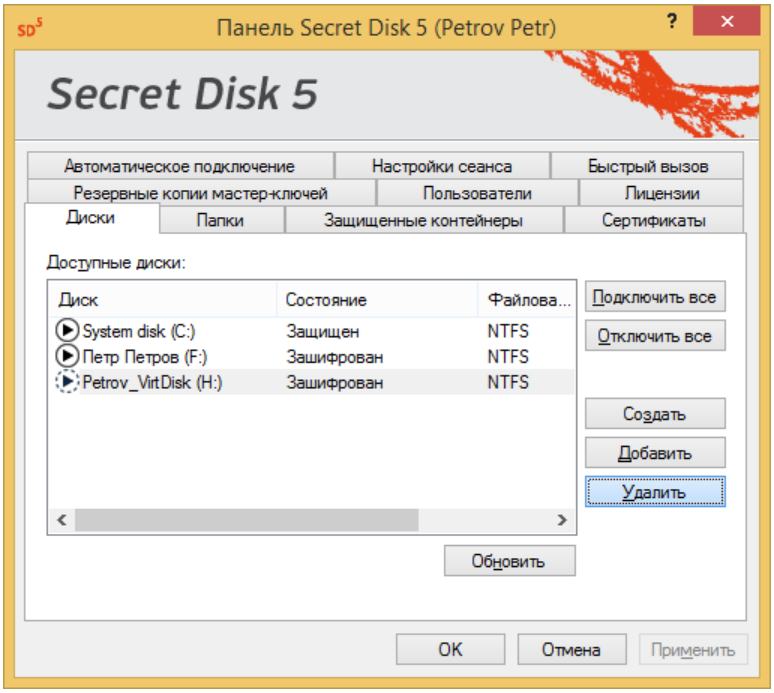

Рисунок 40 – Панель Secret Disk. Диски

Файл диска остается нетронутым

4. Если в дальнейшем диск будет нужен – необходимо его добавить.

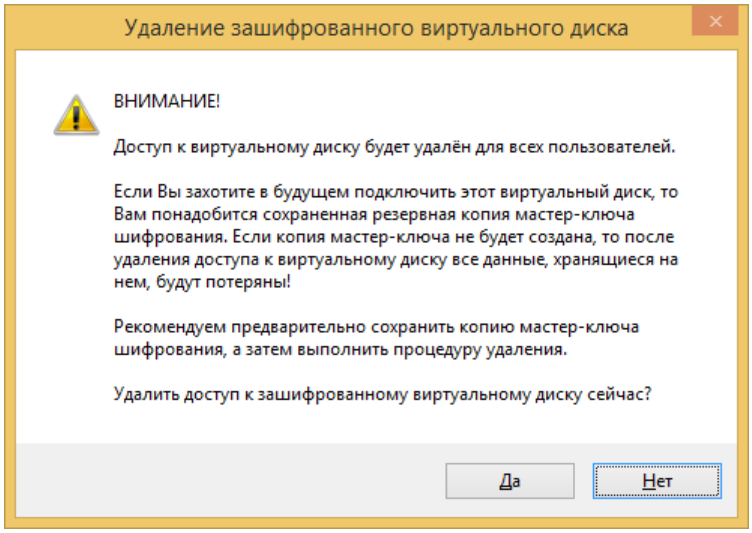

Рисунок 41 – Окно уведомления об удалении зашифрованного виртуального диска

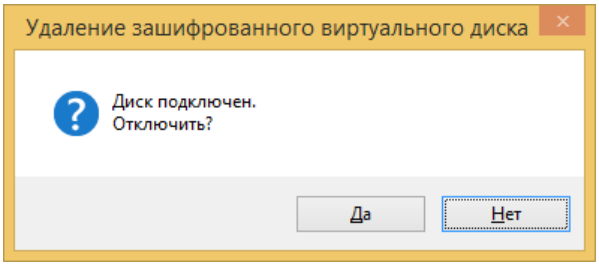

Рисунок 42 – Удаление зашифрованного виртуального диска

5. Для полного удаления виртуального диска необходимо дополнительно удалить файл диска из каталога, в который он был сохранён.

9.4 Добавление/восстановление виртуального тома

Чтобы добавить удалённый (потерянный) виртуальный том в список выполните следующие действия:

1. Откройте сеанс пользователя.
2. На вкладке **Диски** нажмите **Добавить**.
3. Укажите путь к файлу виртуального диска в окне **Добавление зашифрованного виртуального диска**.

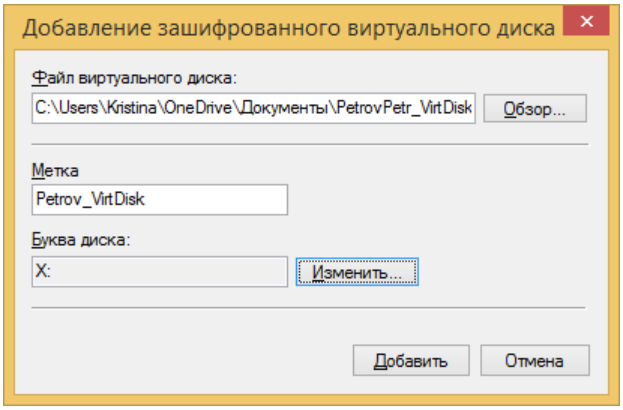

Рисунок 43 – Окно добавления зашифрованного виртуального диска

4. Для изменения метки и буквы диска:
   - отредактируйте поле **Метка диска**;
   - нажмите **Изменить**;
   - в окне **Назначение буквы диска** выберите букву диска из списка доступных букв и нажмите **ОК**.
5. Нажмите **Добавить**.
6. Укажите тип резервной копии мастер-ключа зашифрованного виртуального диска:
   - если резервная копия не хранится в памяти электронного ключа, введите путь к файлу и пароль;
   - если резервная копия хранится на бумажном носителе, выберите пункт меню **Ввести ключ диска вручную** с распечатанной копии и введите все символы при помощи клавиатуры.

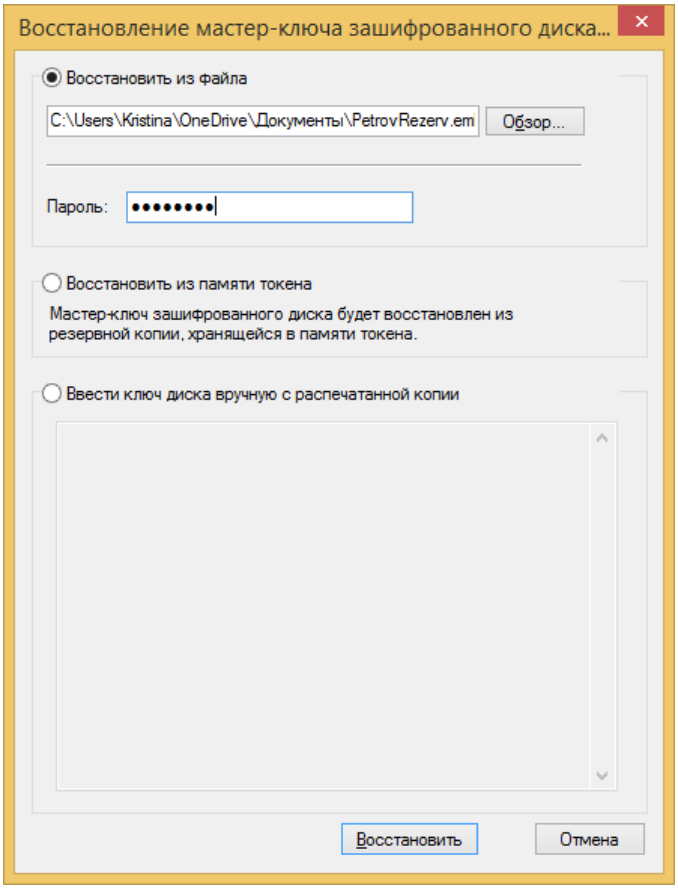

Рисунок 44 – Окно восстановления мастер-ключа зашифрованного виртуального диска

7. Нажмите **Восстановить**.

В области уведомлений появится подтверждающее сообщение. В списке на вкладке **Диски** появится соответствующая запись.

При необходимости выберите считыватель и введите PIN-код токена (интерфейс зависит от используемого криптографического средства).

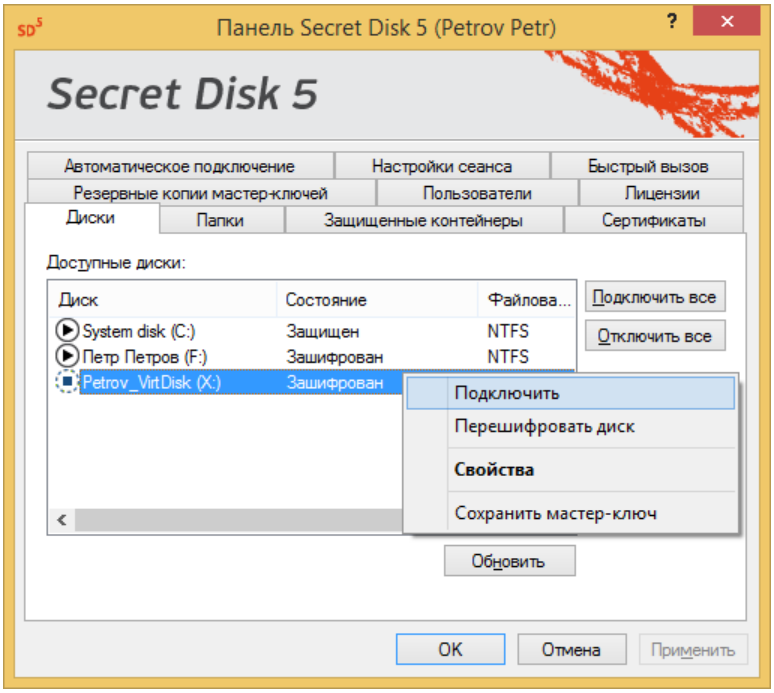

Рисунок 45 – Панель Secret Disk. Диски

> *Владельцем зашифрованного виртуального диска является тот, кто его создал.*
>
> *Если на компьютере у этого зашифрованного виртуального диска был другой владелец, то он (владелец) утрачивает свои полномочия по отношению к этому диску, сохраняя лишь право подключать его.*

9.5 Совместный доступ пользователей

Настройка совместного доступа к защищённому виртуальному тому описана в главе "Доступ пользователей SD5 к защищённым ресурсам".

9.6 Перешифрование виртуального тома

1. Откройте сеанс пользователя.
2. На вкладке **Диски** выберите нужный виртуальный диск.
3. Нажмите по нему левой кнопкой мыши → **Перешифровать диск**.

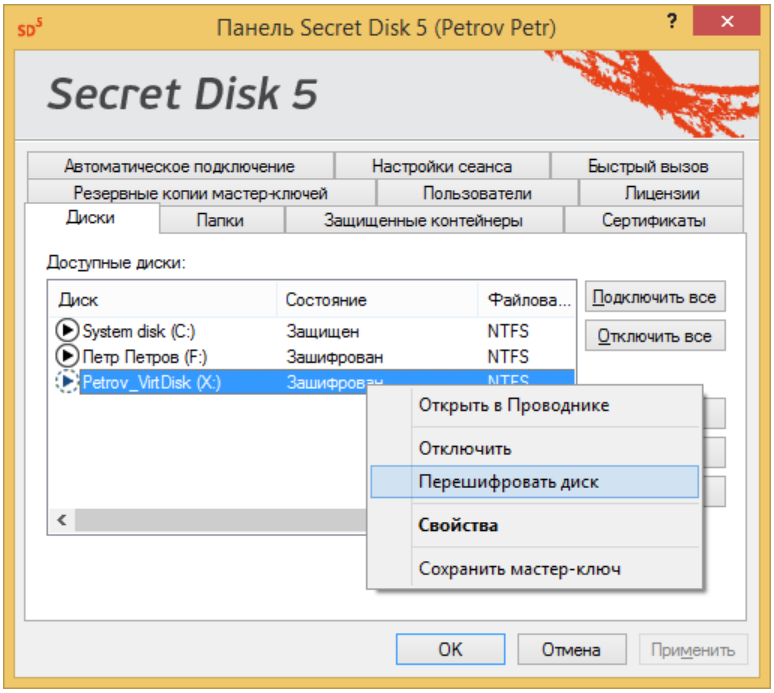

Рисунок 46 – Панель Secret Disk. Диски

4. Выберите новый алгоритм шифрования и нажмите **OK**.

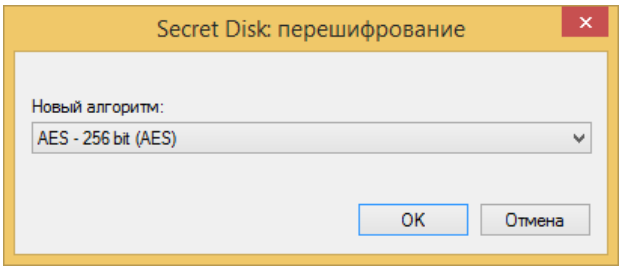

Рисунок 47 – Окно выбора нового алгоритма перешифрования виртуального диска

> *Рекомендуется создать резервную копию мастер-ключа диска. Процедура создания резервной копии мастер-ключа представлена в главе "Сохранение резервной копии мастер-ключа".*

5. Дождитесь окончания процесса установки.

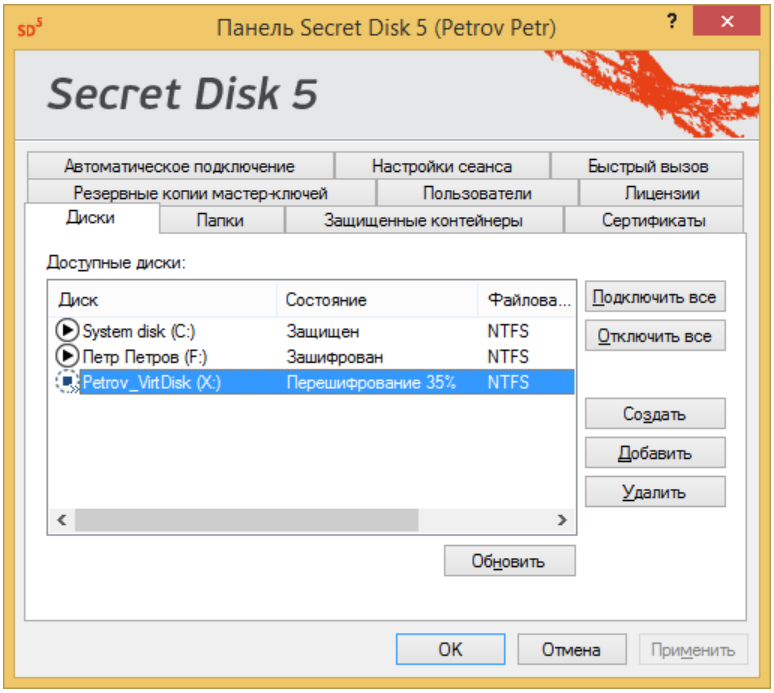

Рисунок 48 – Панель Secret Disk. Диски

10. Защита съёмного носителя

SD5 позволяет защитить данные на съёмных носителях (флэш-картах, съёмных жёстких дисках).

> *Защита съёмного носителя доступна только для пользователей с правами администратора на локальном компьютере.*

Для защиты съёмных носителей выполните следующие действия:

1. Подключите съёмное устройство к компьютеру.
2. В сеансе пользователя во вкладке **Диске** отобразится съёмное устройство.
3. Нажмите на поле съёмного устройства **правой кнопкой мыши → Зашифровать диск**.
4. Выберите метку диска, букву и алгоритм шифрования. Нажмите **OK**.

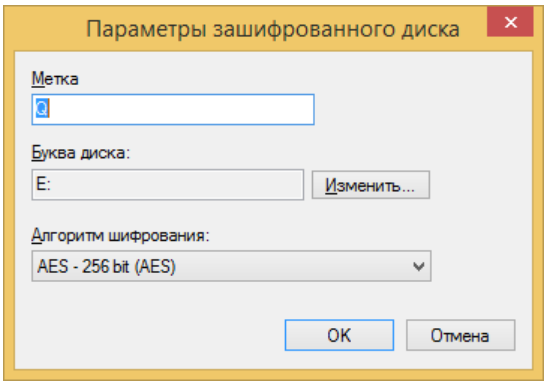

Рисунок 49 – Окно настройки параметров зашифрованного диска

> *Рекомендуется выполнить резервное копирование мастер-ключа диска.*

5. Дождитесь окончания процесса зашифрования.

11. Доступ пользователей SD5 к защищённым ресурсам

Настройка доступа пользователей к зашифрованным ресурсам предполагает, что владелец ресурса сам даёт другому пользователю право на просмотр и работу с этими защищёнными ресурсами.

Пользователь-владелец логического и виртуального томов может добавить другого пользователя, зарегистрированного в SD5, для совместного доступа.

> *Добавленный пользователь имеет доступ к зашифрованному логическому или виртуальному тому. Он может работать на нём (создавать, редактировать, удалять данные, но не может перешифровать или снять защиту с зашифрованного ресурса).*
>
> *Добавленный пользователь не имеет доступа к защищённым папкам, находящимся на зашифрованных томах.*

Чтобы добавить пользователя выполните следующие действия

1. Подключите токен другого пользователя к компьютеру.
2. Нажмите **правой кнопкой мыши по нужному тому → Свойства**.
3. Во вкладке **Доступ** нажмите **Добавить**.

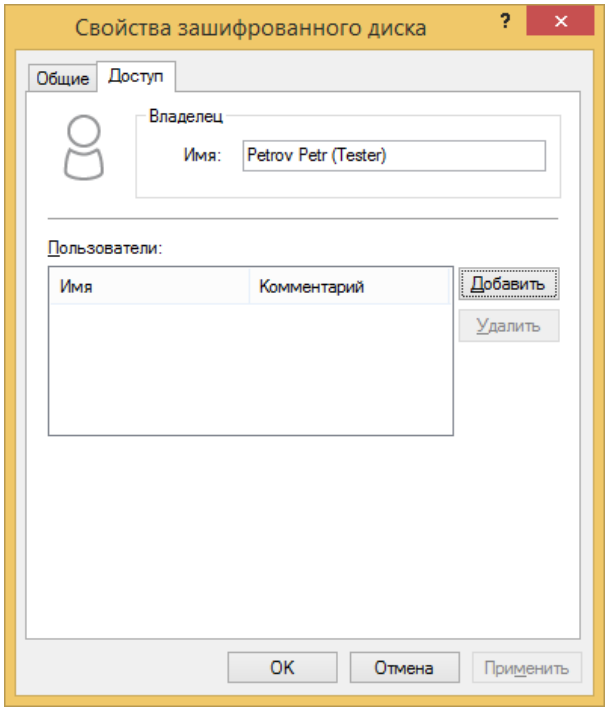

Рисунок 50 – Окно свойств зашифрованного диска

4. Выберите зарегистрированного в SD5 пользователя, которого необходимо добавить. И нажмите **Выбрать.** Если пользователя нет, **создайте его**.

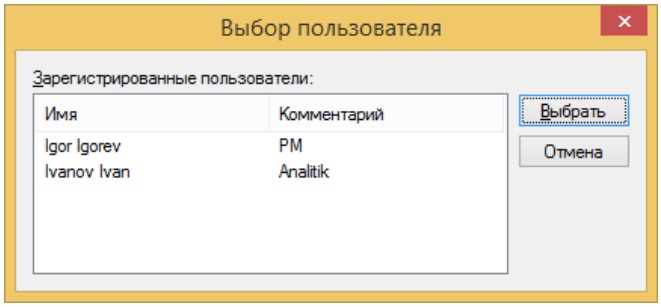

Рисунок 51 – Окно выбора пользователя

5. Пользователь добавлен. Нажмите **OK**.

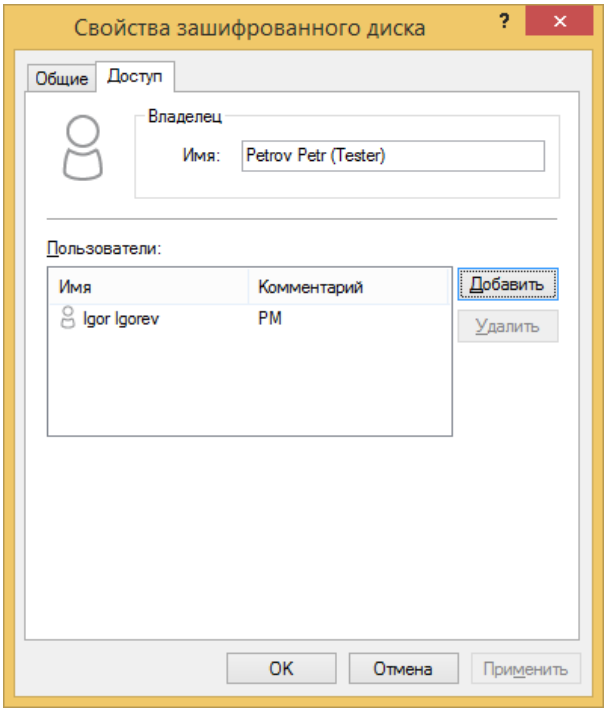

Рисунок 52 – Окно свойств зашифрованного диска

12. Работа с сертификатами

12.1 Общая информация

Для аутентификации пользователя на его токене должны находится:

1. Ключевая пара пользователя, состоящая из двух ключей – закрытого ключа пользователя и открытого ключа.
2. Сертификат открытого ключа.

Сертификат – это электронный документ, содержащий сведения о пользователе и его открытый ключ, заверенные (подписанные) электронной подписью Удостоверяющего центра. В SD5 можно использовать сертификаты любого формата, предназначенные для работы в "Инфраструктуре Открытых Ключей" (PKI).

Ключевая пара и сертификат для пользователя SD5 могут быть созданы в самом SD5, либо выпущены с помощью программного средства или специальной службы - Удостоверяющего центра, отвечающим требованиям PKI. Отличие состоит в том, что сертификаты, созданные внешним Удостоверяющим центром, могут использоваться для других задач (например, для цифровой подписи или шифрования сообщений), а не только служить аутентификаторами пользователей SD5.

В SD5 применяются следующие типы ключевых пар:

1. ГОСТ – необходима для работы с алгоритмами шифрования ГОСТ, но не позволяет включать защиту системного диска.
2. RSA – необходима для защиты системного диска и позволяет защищать все ресурсы любыми алгоритмами шифрования, кроме ГОСТ.

При необходимости защиты системного диска и использования алгоритмов шифрования ГОСТ для защиты других ресурсов, на токене пользователя SD5 должны находиться две ключевые пары разных типов и соответствующие им сертификаты. Если алгоритмы шифрования ГОСТ не используются, пользователю достаточно иметь ключевую пару и сертификат типа RSA.

12.2 Создание сертификата с помощью SD5

При регистрации пользователей SD5 позволяет создать новый сертификат и ключевую пару пользователя на его токене, если у пользователя нет ключей и сертификатов, выданных ему независимым Центром сертификации.

При работе с токенами SD5 может выполнять две операции:

1. Создавать закрытые ключи типа RSA и соответствующие им сертификаты в памяти токена.
2. Сохранять созданные ключи и сертификаты в виде файла формата PFX с целью сохранения резервной копии.

Для создания сертификата выполните следующие действия:

1. Запустите программу SD5.
2. Нажмите **Зарегистрируйтесь** в окне идентификации.

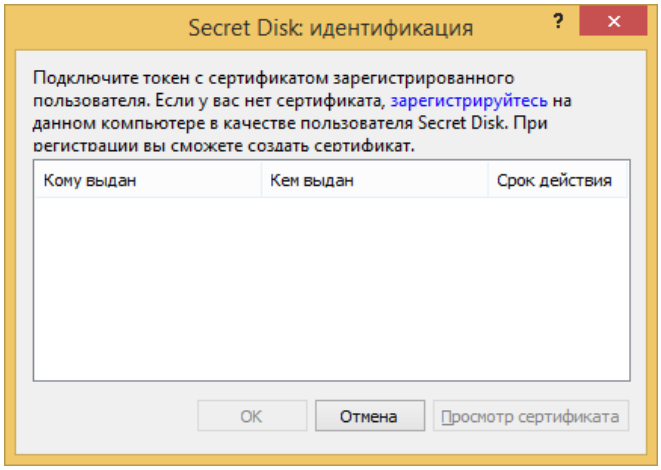

Рисунок 53 – Окно создания/выбора сертификата пользователя

3. Введите **Имя** и **Комментарий**.
4. Выделите поставщика криптографии и нажмите **Выбрать**, поскольку поставщиков криптографии может быть несколько.

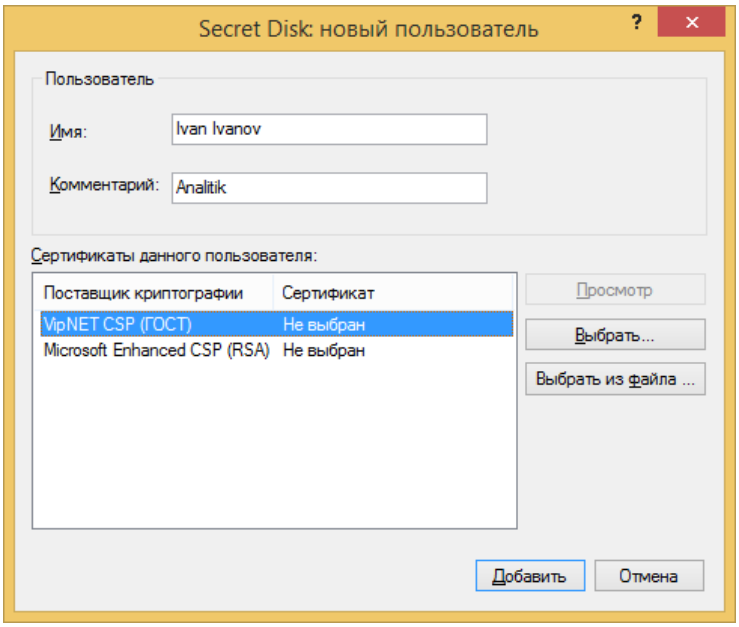

Рисунок 54 – Окно создания нового пользователя

5. Нажмите **Создать**... в окне выбора сертификата.

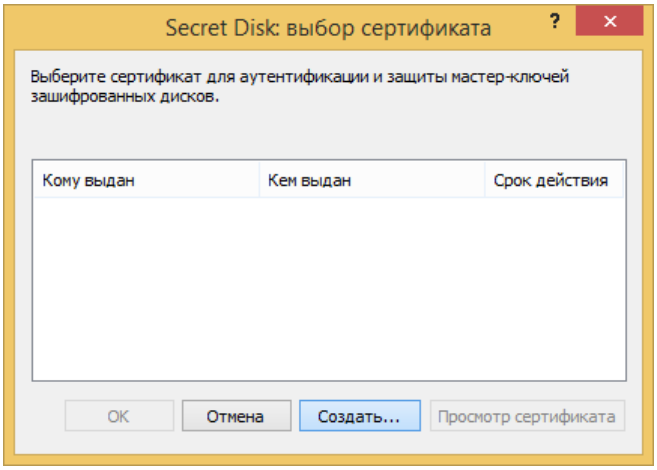

Рисунок 55 – Окно выбора сертификата

6. Заполните все обязательные поля, выделенные полужирным текстом и, по желанию, необязательные поля.

При заполнении поля Страна используйте буквы латинского алфавита.

При заполнении поля Организация используйте буквы латинского алфавита. Не используйте знаки препинания и кавычки.

7. Выберите алгоритм шифрования и длину ключа:

С 1 января 2019 года запрещено формирование электронной подписи с помощью ключей ГОСТ 34.10-2001.

– VipNET CSP (ГОСТ 34.10-1994) имеет длину ключа 1024 бит.

8. Нажмите **OK**.

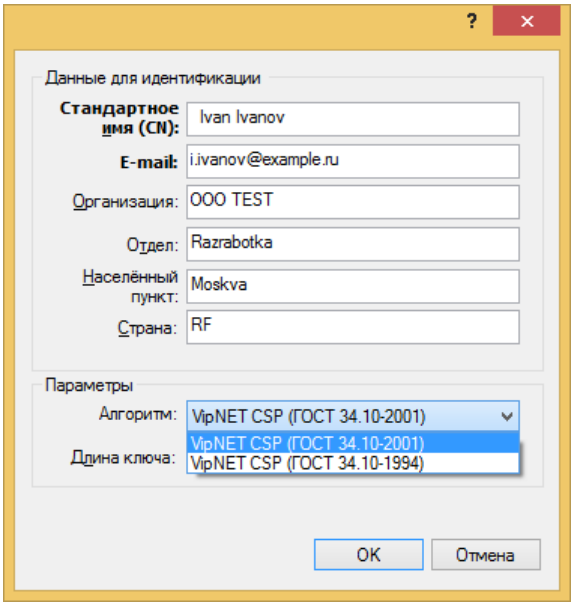

Рисунок 56 – Окно ввода данных для идентификации пользователя

9. Выберите устройство хранения контейнера ключей, если их несколько. Введите PIN-код токена.

Если подключённых к компьютеру устройств больше одного – внимательно выбирайте устройство хранения контейнера ключей!

10. Нажмите **OK**.

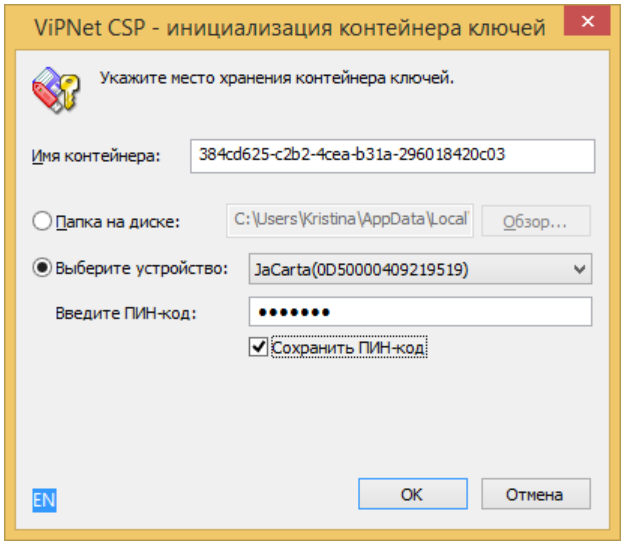

Рисунок 57 – Окно инициализации контейнера ключей

11. Перемещайте указатель мыши в пределах окна или нажимайте любые клавиши на клавиатуре для инициализации генератора случайных чисел.

Генерация случайных чисел будет производиться каждый раз при создании сертификата с алгоритмами шифрования по ГОСТу.

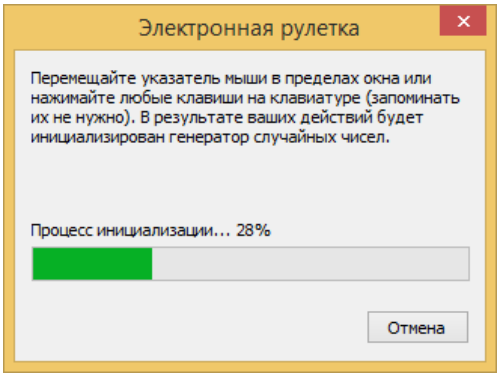

Рисунок 58 – Окно генерации случайных чисел

12. Сохраните резервную копию сертификата. Нажмите **OK**.

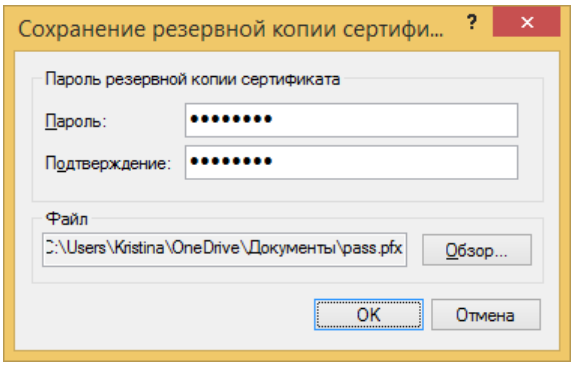

Рисунок 59 – Окно сохранения резервной копии сертификата

13. Сертификат успешно создан.

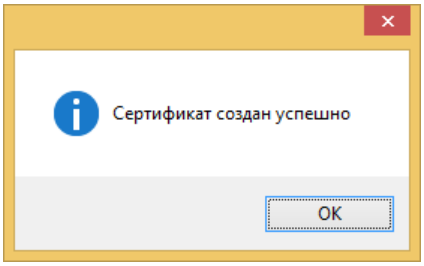

Рисунок 60 – Уведомление об успешном создании сертификата

14. Созданный сертификат появится в окне выбора сертификатов.

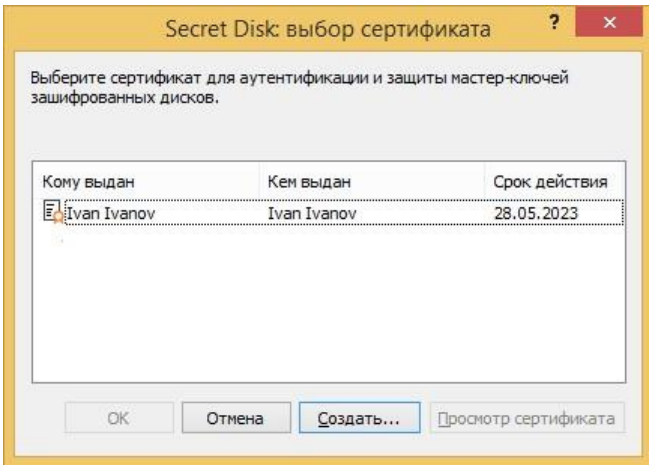

Рисунок 61 – Окно выбора сертификата

> *Если выбран алгоритм шифрования отличный от ГОСТа, то после сохранения резервной копии сертификата программа покажет окно выбора токена с информацией о каждом токене.*
>
> *Если их несколько, выберите необходимый.*

15. Нажмите **OK**.

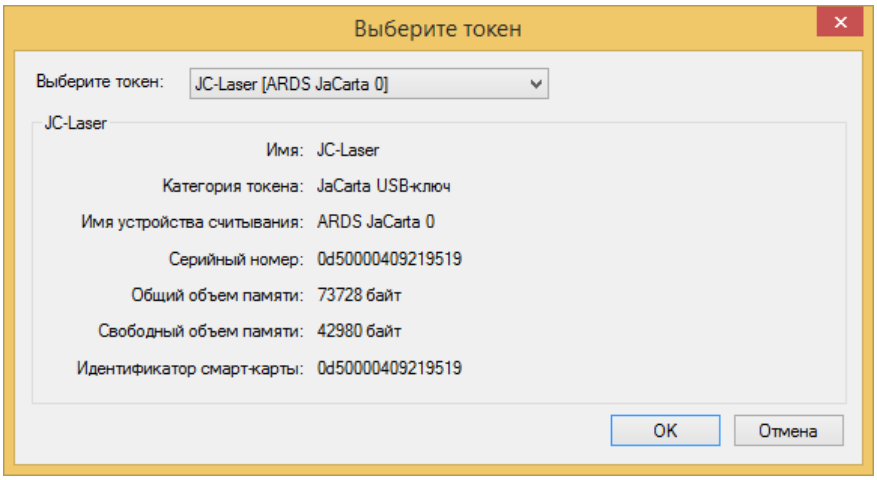

Рисунок 62 – Окно выбора токена пользователя

16. После успешного создания сертификата на экране появится окно с соответствующим сообщением. Нажмите **OK**.

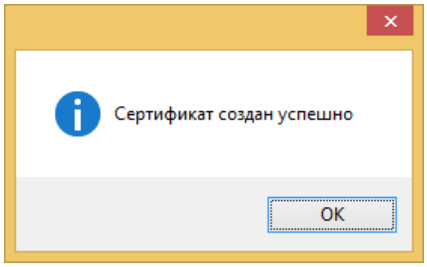

Рисунок 63 – Уведомление об успешном создании сертификата

12.3 Импорт резервной копии сертификата и удаление сертификата

С помощью SD5 нельзя сделать импорт сертификата и ключей из файла PFX, а также нельзя удалить ненужные ключи и сертификат из токена. Для выполнения этих действий следует использовать установленный ранее клиент для работы с токенами:

- Единый клиент JaCarta;
- eToken PKI Client;
- Safenet Authentication Client.

> *Для работы с ГОСТ-сертификатами следует использовать программные средства КриптоПро CSP или VipNet CSP.*

Для удаления сертификата с токена выполните следующие действия

5. Откройте Единый клиент JaCarta, вкладку PKI.

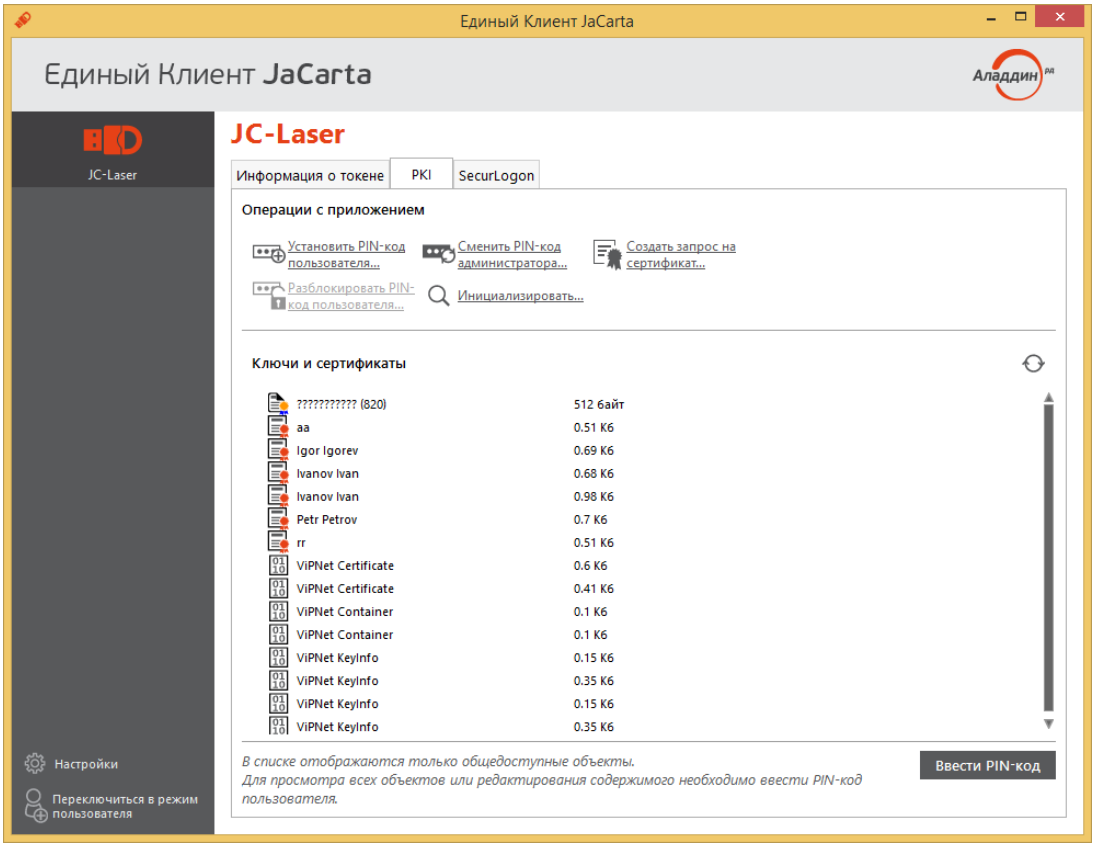

Рисунок 64 – Окно сертификатов токена

6. Введите PIN-код своего токена и нажмите OK.

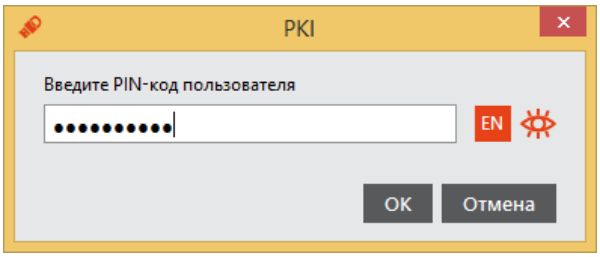

Рисунок 65 – Окно ввода ПИН-кода токена

7. Выберите нужный сертификат для удаления и нажмите по нему правой кнопкой мыши → **Удалить**.

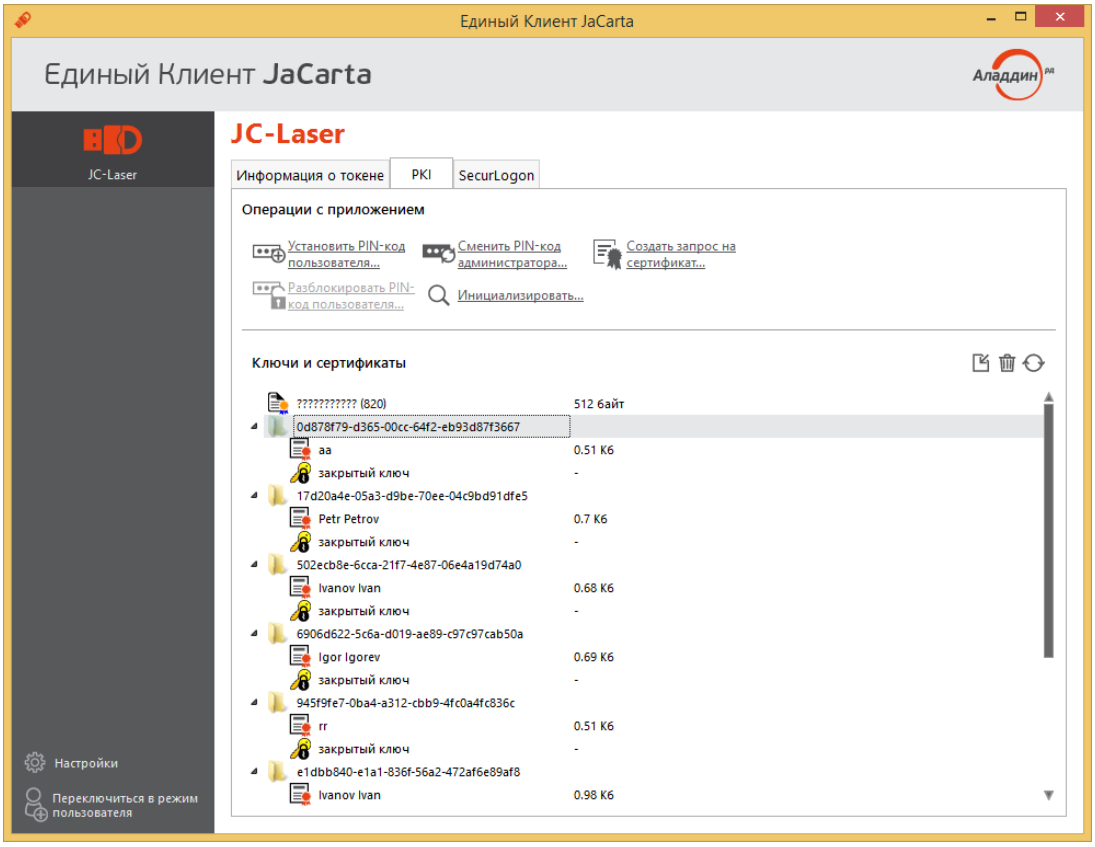

Рисунок 66 – Окно сертификатов токена

8. Подтвердите своё действие, нажав **Да**.

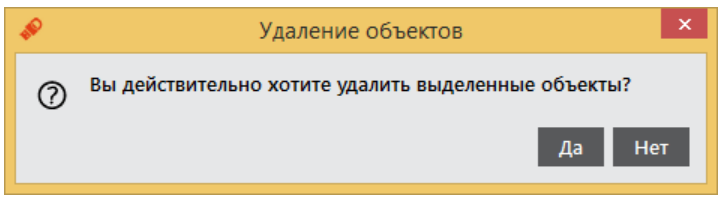

Рисунок 67 – Окно подтверждения удаления сертификата

13. Сохранение резервной копии мастер-ключа

13.1 Создание резервной копии мастер-ключа

> *Внимательно ознакомьтесь с этим разделом!*
>
> *Резервные копии мастер-ключей необходимы для восстановления доступа к защищённым ресурсам.*
>
> *При потере или не сохранении резервной копии мастер-ключа защищённого ресурса – доступ к этому ресурсу будет невозможен.*

Сохранение резервной копии мастер-ключей для всех ресурсов идентичен.

Для сохранения резервной копии мастер-ключей выполните следующие действия:

1. Нажмите по нужному ресурсу **правой кнопкой мыши → Сохранить мастер-ключ**.

> *Либо в процессе установки защиты программа автоматически предложит сохранить мастер-ключ.*

2. В окне резервного копирования выберите место хранения мастер-ключа.

Флаг	**Место сохранения**
Сохранить в файле	Копия мастер-ключа сохранится на компьютере пользователя. *Рекомендуется сохранение на флэш-карте.*
Сохранить в памяти токена	Копия мастер-ключа сохраняется в памяти токена в виде закрытого файла. Доступ к файлу можно получить зная PIN-код токена.
Распечатать на принтере	Копия мастер-ключа выводится на печать. Распечатанную копию мастер-ключа необходимо хранить в надёжном, защищённом месте (например, в сейфе).

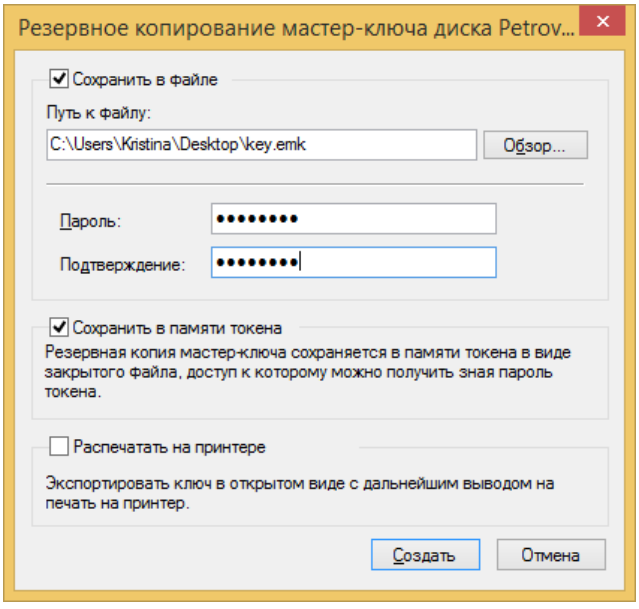

Рисунок 68 – Окно резервного копирования мастер-ключа защищённого ресурса

> *Рекомендуется сохранять копии мастер-ключей в файле и распечатывать на принтере.*
>
> *При распечатывании на принтере необходимо хранить ключ в защищённом месте, например в сейфе.*

3. Нажмите **Создать**.

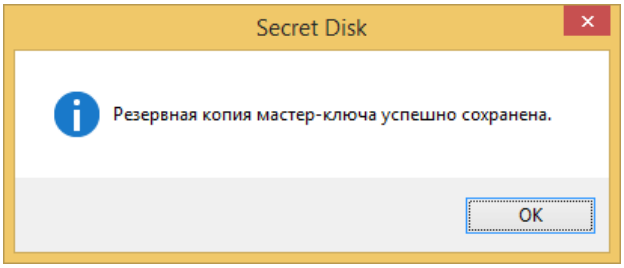

Рисунок 69 – Окно уведомления о сохранении резервной копии мастер-ключа диска

> *Сохранённую на токене копию мастер-ключа можно посмотреть на вкладке Резервные копии мастер-ключей.*

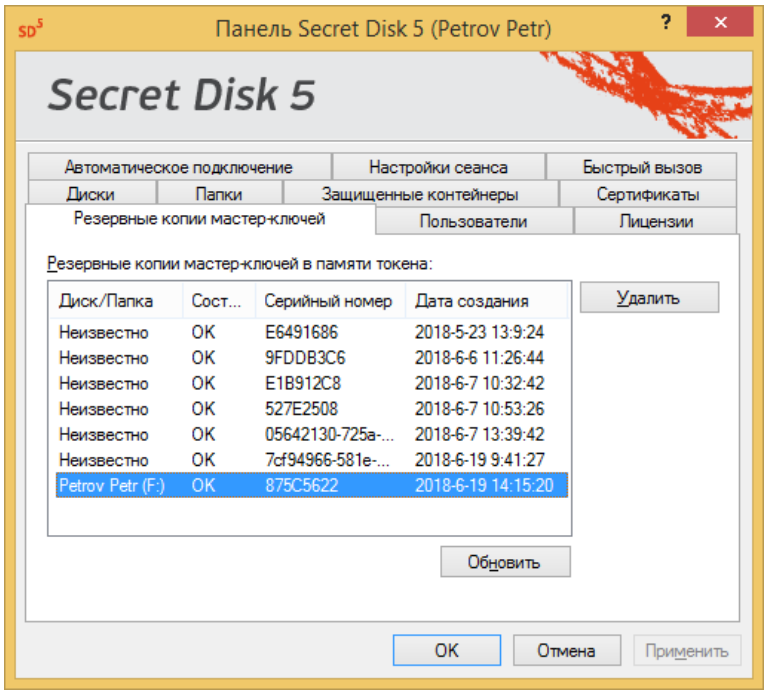

Рисунок 70 – Панель Secret Disk. Резервные копии мастер-ключей

13.2 Удаление резервной копии мастер-ключа

Удалить резервную копию мастер-ключа с токена можно во вкладке "*Резервные копии мастер-ключей*".

> *Восстановление резервной копии мастер-ключа после удаления невозможно!*

14. Восстановление доступа к защищённым ресурсам

> *Восстановление доступа к зашифрованным ресурсам возможен при наличии сохраненной резервной копии мастер-ключа.*
>
> *При отсутствии резервной копии мастер-ключа восстановление невозможно!*
>
> *Восстановление доступа к защищённым ресурсом идентично (кроме системного диска).*

14.1 Восстановление доступа

Для восстановления доступа к зашифрованному логическому тому выполните:

1. Нажмите во вкладке *Диски* по пустому полю **правой кнопкой мыши → Восстановить доступ к зашифрованному диску**.

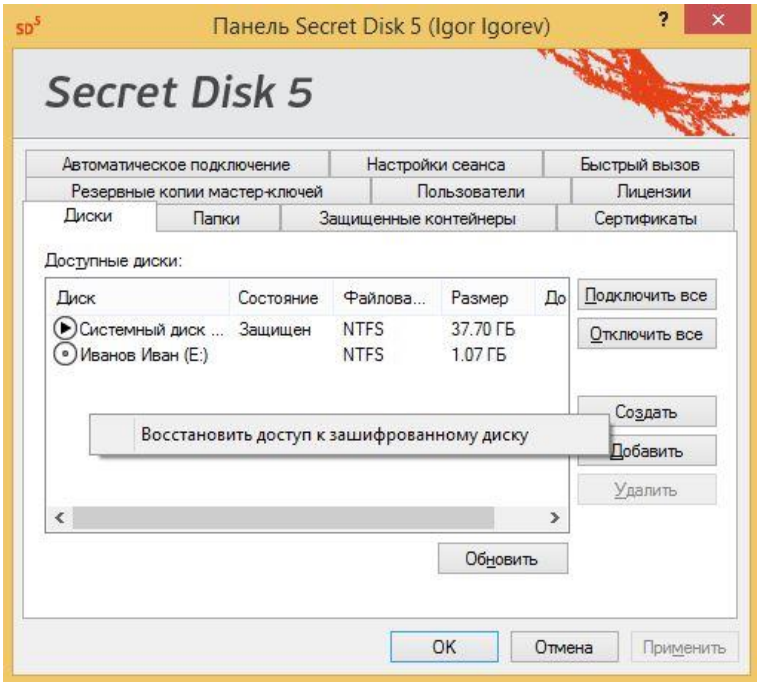

Рисунок 71 – Панель Secret Disk. Диски

2. Выберите способ восстановления. Нажмите **Восстановить**.

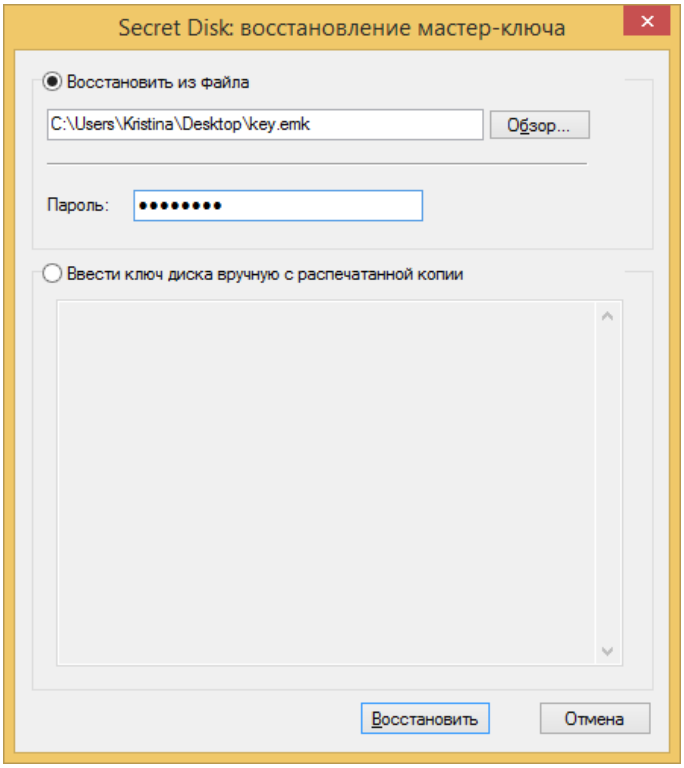

Рисунок 72 – Окно восстановления мастер-ключа

3. Восстановленный зашифрованный неподключенный логический том появится в списке дисков.

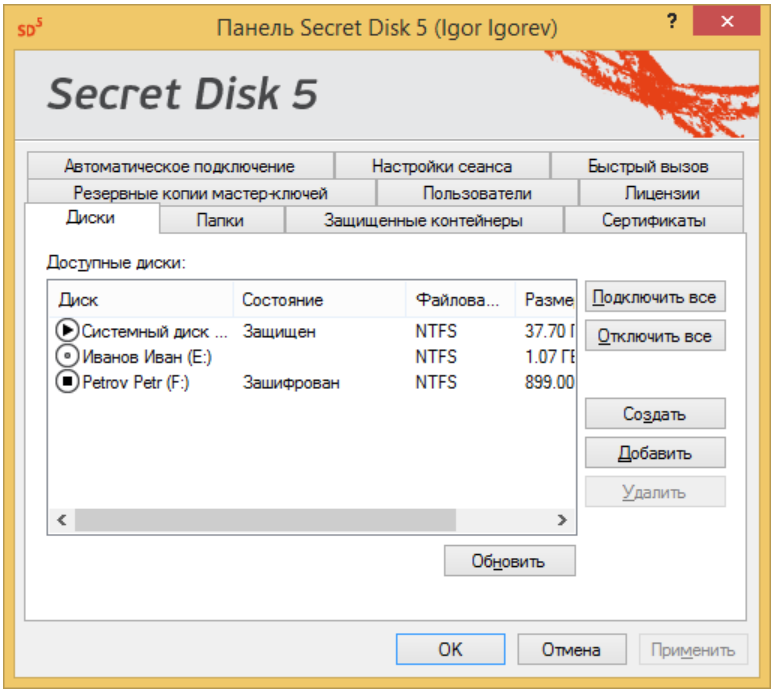

Рисунок 73 – Панель Secret Disk. Диски

Восстановление доступа к виртуальному тому и защищённой папке производится аналогично.

15. Обновление SD5

Обновлений с предыдущих версий не предусмотрено.

Для перехода на новую версию SD5 нужно:

- снять защиту со всех защищённых ресурсов;
- удалить (деинсталлировать) старую версию SD и CEP;
- установить новую версию SD и CEP.

16. Удаление SD5 (отказ от использования SD5)

16.1 Общее описание процесса удаления

> *Перед удалением SD5 следует расшифровать все защищённые ресурсы. При невозможности расшифрования (виртуальные диски/защищённые контейнеры) необходимо скопировать из них информацию.*

Для удаления программы необходим инструмент Windows "Удаление программы". Находится в Панели управления.

16.2 Удаление без расшифрования и переустановка SD5

Возможно удаление SD5 без расшифрования ресурсов. При этом доступ к зашифрованным данным теряется. Вернуть доступ можно несколькими способами:

1. Если крипто-хранилище не было удалено, то заново установить SD5 и вернуть доступ.
2. Если крипто-хранилище было удалено, то восстановление будет производиться по сохранённым мастер-ключам ресурсов.

> *Если резервные копии мастер-ключей не были сохранены и удалено крипто-хранилище, то восстановление доступа к зашифрованным ресурсом будет невозможно. Все данные будут безвозвратно утеряны.*
>
> *Загрузка ОС Windows с защищённого системного диска (при удалении программы) будет происходить без изменений.*

16.3 Полное удаление SD5

1. Откройте в меню **Пуск → Панель управления → Установка и удаление программ**.
2. Выберите в списке программ SD5, нажмите **Удалить**.
3. Нажмите **Да**.

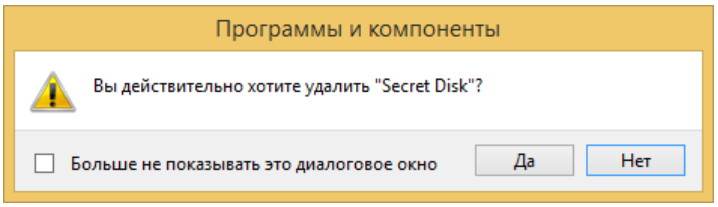

Рисунок 74. Окно уведомления

4. При необходимости закройте требуемые окна и нажмите **Повторить**.

> *Проверьте, что в системе не осталось зашифрованных ресурсов и ко всем ресурсам есть резервные копии мастер-ключей.*

5. Нажмите **Да** для удаления крипто-хранилища SD5.
6. Нажмите **Нет**, если крипто-хранилище не надо удалять.

> *Если потребуется заново установить SD5 на компьютер и использовать эти же зашифрованные ресурсы нажмите Нет. Крипто-хранилище останется на системном диске.*

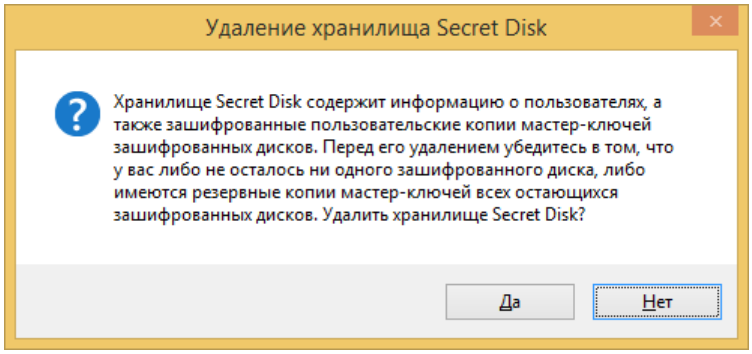

Рисунок 75. Удаление хранилища Secret Disk

7. Нажмите **Да**, чтобы перезагрузить компьютер немедленно. Нажмите **Нет**, чтобы выполнить перезагрузку позже.

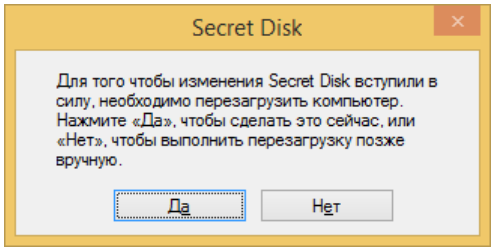

Рисунок 76. Окно перезагрузки компьютера

17. Сценарии использования

17.1 Персональное использование и персональное использование с дополнительным привилегированным пользователем

- пользователь(-ли) является(-ются) администратором(-ми) ресурсов. Доступны все функции по работе с ресурсами;
- в SD5 зарегистрирован либо только один пользователь, либо несколько пользователей с правами администратора.

17.2 Персональное использование с дополнительным непривилегированным пользователем

Пользователь устанавливает и запускает SD5, используя привилегированную учётную запись Windows. В SD5 он регистрирует учётную запись для себя и создаёт защищённые ресурсы. После этого он может работать с защищёнными ресурсами сам, дать доступ и управлять доступом к ним другого пользователя, который использует обычную (непривилегированную) учётную запись Windows.

Для этого первый пользователь регистрирует второго пользователя и его токен в SD5 и добавляет его в список пользователей тех дисков, которые ему разрешено самостоятельно подключать.

Второй пользователь сможет подключать и отключать диски, созданные первым пользователя, а также создавать защищённые папки и контейнеры. Но он не сможет создавать новые защищённые диски и регистрировать других пользователей SD5 в том случае, если его учётная запись Windows является обычной.

В таблице представлен пример разграничения прав доступа администратором и непривилегированными пользователями.

Диск C: могут подключить только администратор и Пользователь №3. Они могут загрузить ОС со своими токенами с вводом PIN-кода.

Пользователь №1 и Пользователь №2 не смогут запустить ОС со своими токенами, но они могут работать в уже загруженной системе.

Диск D: защита включена администратором, он может подключать его сам и предоставил право подключения Пользователю № 1.

Диск E: защита включена Пользователем №1, которые предоставил право подключения Пользователю №2. Администратор не может подключить этот диск или поменять доступ других пользователей к нему.

Диск F: создан администратором и его могут подключить все пользователи SD5.

Таблица 2 – Пример разграничения прав доступа к зашифрованным ресурсам

Пользователи	Диск C: (системный)	Диск D: (2 диск)	Диск E: (3 диск)	Диск F: (виртуальный)
Администратор	Владелец	Владелец	-	Владелец
Пользователь1	-	+	Владелец	+
Пользователь2	-	-	+	+
Пользователь3	+	-	-	+

18. Окончание срока действия лицензии на токене

По окончании срока действия лицензии необходимо обратиться в ЗАО "Аладдин Р.Д." по почте aladdin@aladdin-rd.ru.

18.1 Предупреждение о скором окончании срока действия

Предупреждение о скором окончании срока лицензии появится за 3 месяца до окончания срока лицензии.

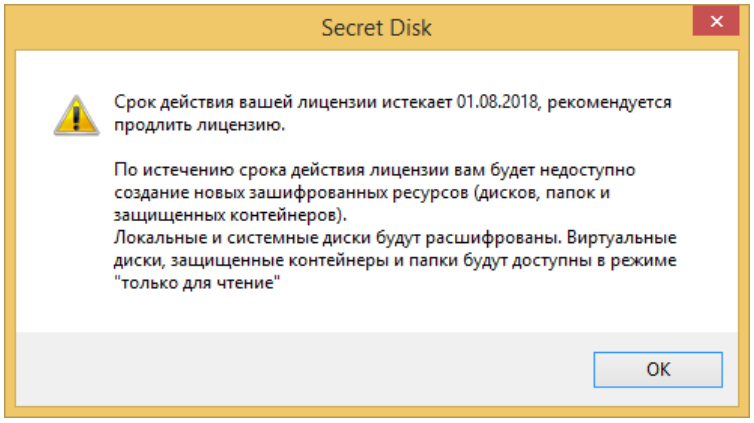

Рисунок 77 – Предупреждение о скором окончании срока действия лицензии

18.2 Работа SD5 после окончания действия лицензии

Если сессию SD5 открывает пользователь, чей токен содержит недействительную лицензию, то ему будет выведено следующее предупреждение:

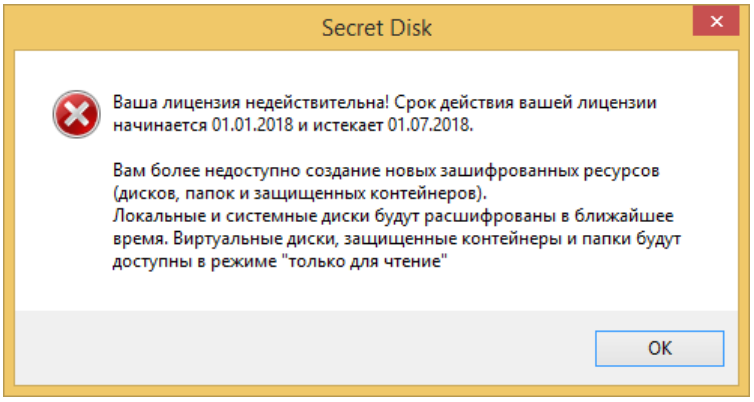

Рисунок 78 – Уведомление о недействительности лицензии

Для пользователя с недействительной лицензией начинают действовать следующие ограничения:

- пользователь не может создать новые зашифрованные ресурсы (диски, папки, защищённые контейнеры);
- запускается расшифрование дисков (в том числе системного диска), владельцем которых является этот пользователь;
- пользователь может подключить виртуальные диски, защищённые папки и контейнеры, но они будут доступны ему в режиме "только чтение".

Другие пользователи SD5, имеющие действительные лицензии, будут продолжать работать как обычно, если откроют сессию SD5 под своим именем и со своим токеном.

19. Особенности поведения SD5 в "спящих" режимах Windows

Таблица 3 – Виды режима ожидания в ОС Windows

Режим	Windows 7-10
Sleep mode (Stand-by) (спящий режим)	Все открытые документы и запущенные приложения хранятся в оперативной памяти и при выходе из режима компьютер моментально готов к работе.
Hibernate (гибернация)	Все открытые документы и приложения, включая "слепок" оперативной памяти сохраняются на жёсткий диск, и только после этого питание компьютера отключается.
Hybrid sleep (гибридный спящий режим)	Все открытые документы и запущенные приложения хранятся на жёстком диске, и при выходе из режима компьютер моментально готов к работе.

В настройках сеанса пользователя на панели SD5 можно установить флаг **Закрывать сеанс при отключении токена**.

При этом сеанс пользователя будет закрываться как при отключении электронного ключа, так и в случае ухода компьютера в режимы Sleep mode, Hibernate, Hybrid sleep.

Если системный диск не защищён (независимо от наличия или отсутствия флага **Закрывать сеанс при отключении токена**), сеанс пользователя закрывается при переходе компьютера в спящие режимы, при этом отключаются все защищённые диски.

Если системный диск защищён, то:

1. При выходе из режима Hibernate необходимо пройти аутентификацию с помощью электронного ключа (отсутствие или наличие флага **Закрывать сеанс при отключении токена** не влияет на степень безопасности на компьютере)
2. При выходе из режима Sleep mode аутентификации перед загрузкой ОС нет, но может потребоваться повторное открытие сеанса Secret Disk.

20. Журнал событий

> *Права на управление журналом событий есть только у локального администратора. Пользователь может только просматривать журнал.*

Посмотреть журналы событий SD5 можно в разделе **Администрирование → Управление компьютером → Просмотр событий**.

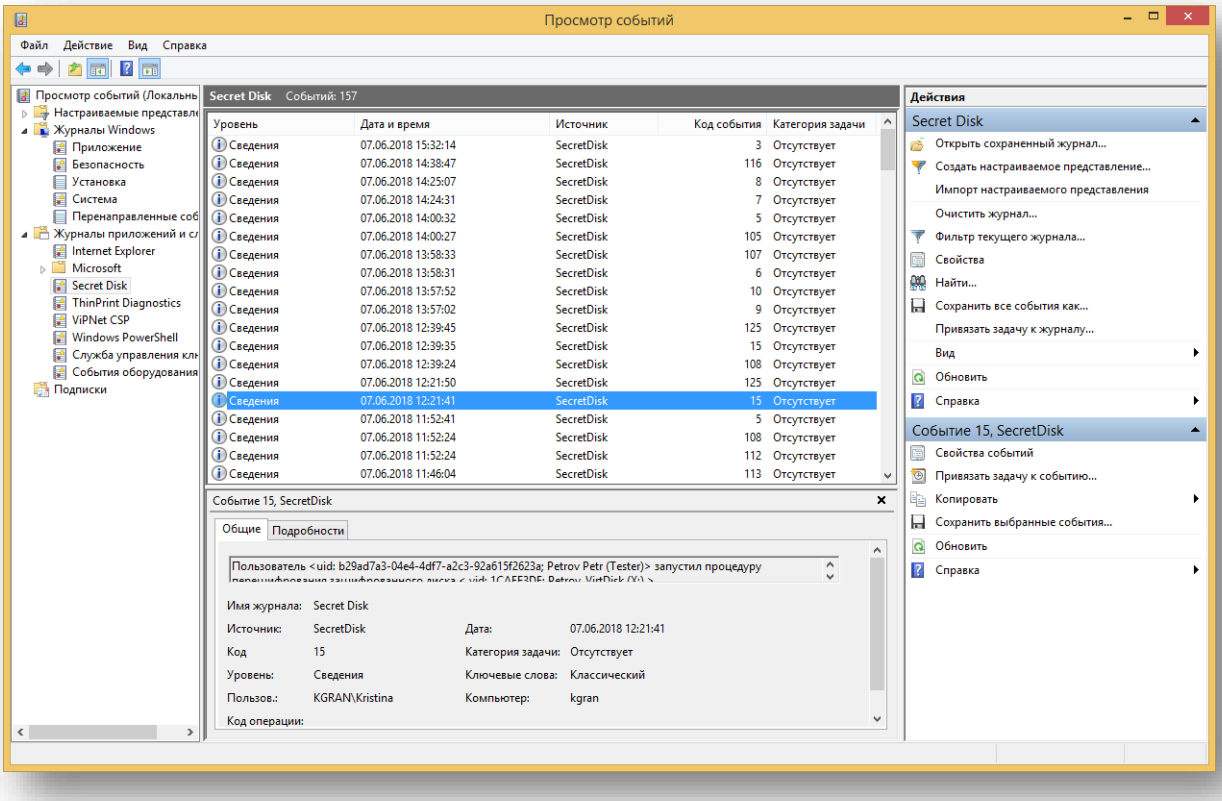

Рисунок 79. Журнал просмотра событий

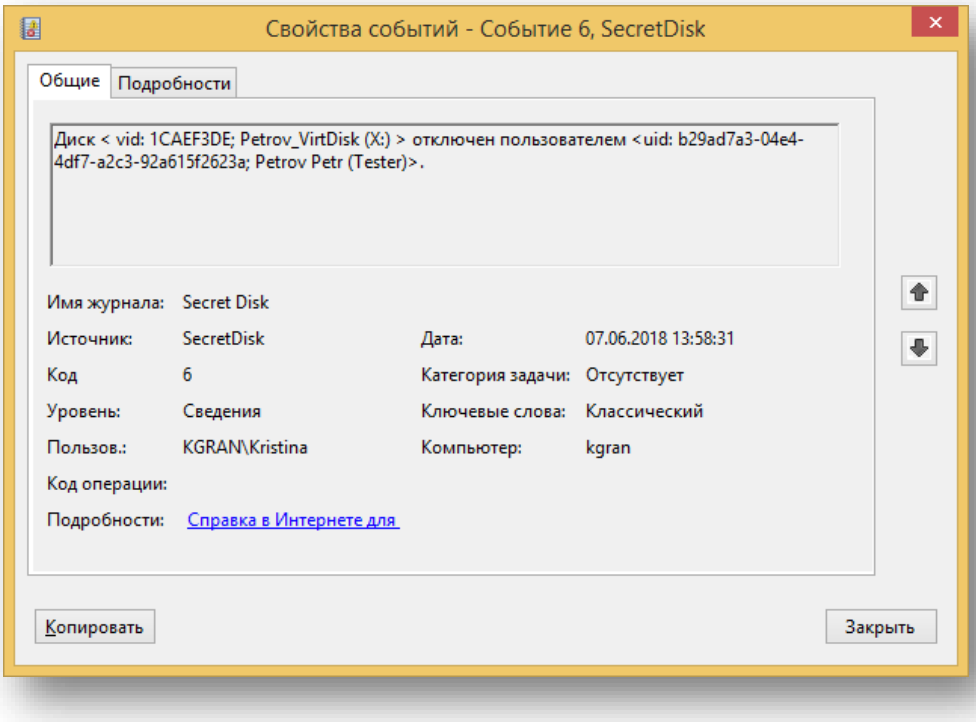

Рисунок 80. Свойства событий

Настроить протоколирование событий можно через параметр реестра

1. Запустите реестр сочетанием клавиш **Win+R**.
2. В поле введите **regedit** и нажмите **OK**.

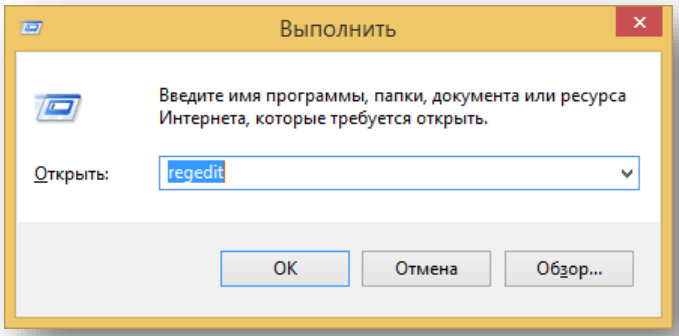

Рисунок 81. Командная строка

3. Перейдите в HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Secret Disk NG\EventLogging

- если значение = 1, то события записываются в журнал событий;
- если значение = 0 или параметр реестра не задан, то регистрация событий не ведётся.

4. Установите требуемое значение параметра.

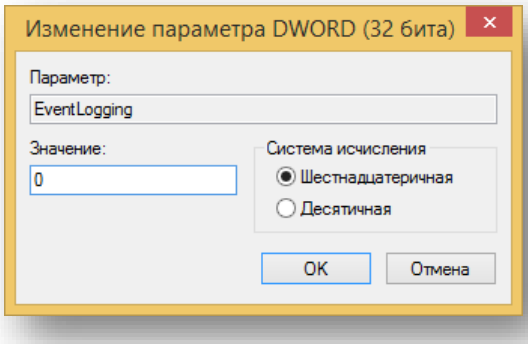

Рисунок 82. Изменение параметра DWORD

Приложение 1. Установка единого клиента JaCarta

1. В зависимости от разрядности ОС запустите файл установки "Единого клиента JaCarta".
2. Нажмите **Далее >**.

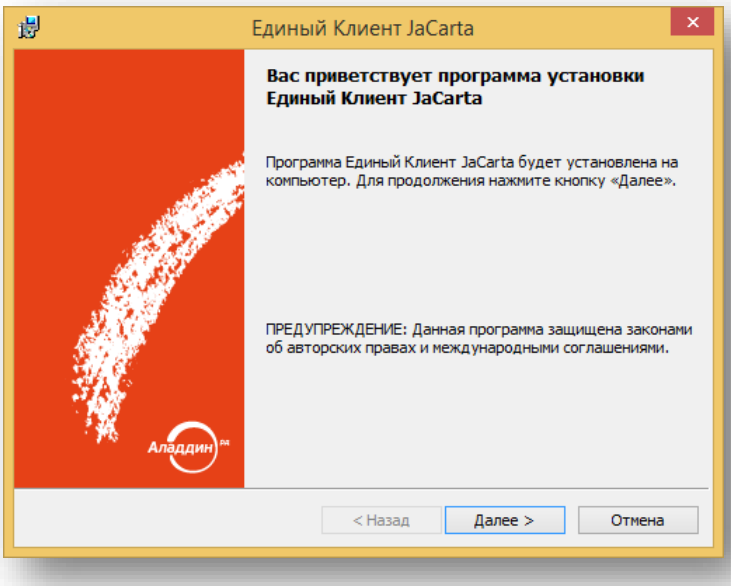

Рисунок 83. Мастер установки JaCarta

3. Прочитайте Лицензионное соглашение.

- Выберите пункт **Я принимаю условия лицензионного соглашения**, если вы согласны с его условиями.
- Нажмите **Отмена**, если вы не согласны с условиями лицензионного соглашения.

4. Нажмите **Далее >**.

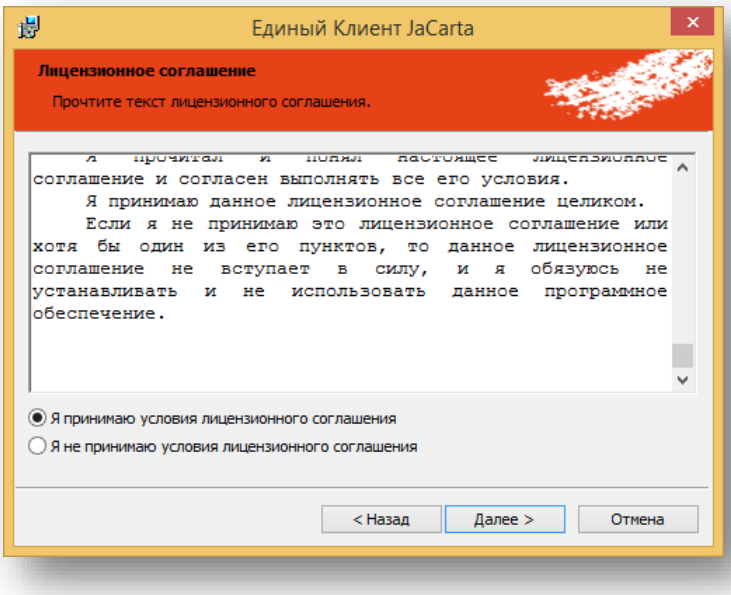

Рисунок 84. Лицензионное соглашение JaCarta

5. Выберите вид установки: **Стандартная** или **Выборочная**.

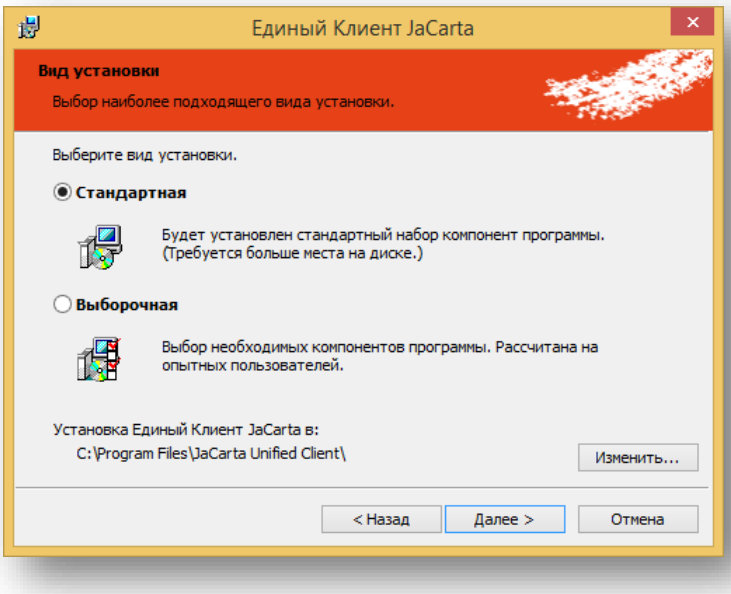

Рисунок 85. Выбор вида установки

6. Если выбран вид установки **Стандартная**, то будут установлены следующие компоненты:

- Единый клиент JaCarta;
- Управление токеном;
- Поддержка биометрии;
- Серверные компоненты RDP для биометрии;
- Установка Athena CSP в качестве криптопровайдера по умолчанию.

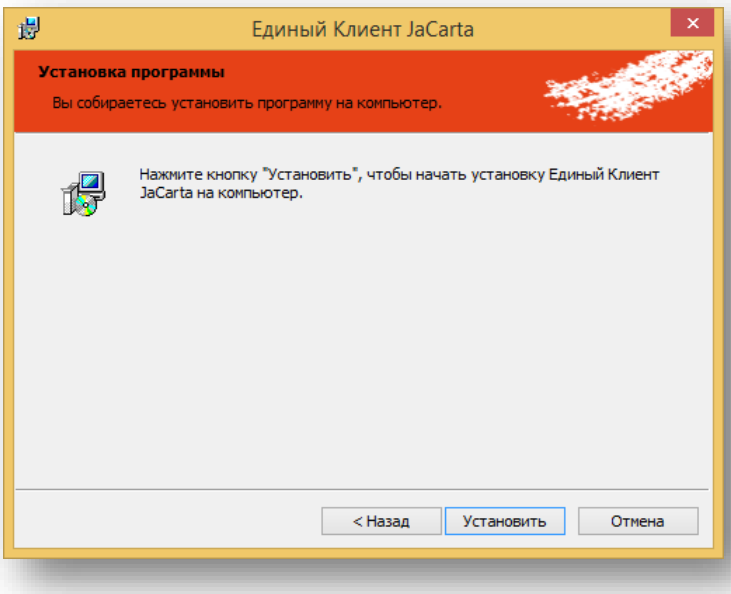

Рисунок 86. Установка программы

7. Если был выбран вид установки *Выборочная*, то при установке будет предоставлен выбор из следующего набора компонентов:

- JaCarta SecurLogin;
- JaCarta WebPass Tool;
- JaCarta АРМ УЦ;
- Управление токеном;
- Поддержка биометрии;
- Серверные компоненты RDP для биометрии;
- Установка Athena CSP в качестве криптопровайдера по умолчанию;
- Драйверы.

> *Компонент "Единый Клиент JaCarta" является обязательным и устанавливается всегда (независимо от выбранного типа установки).*

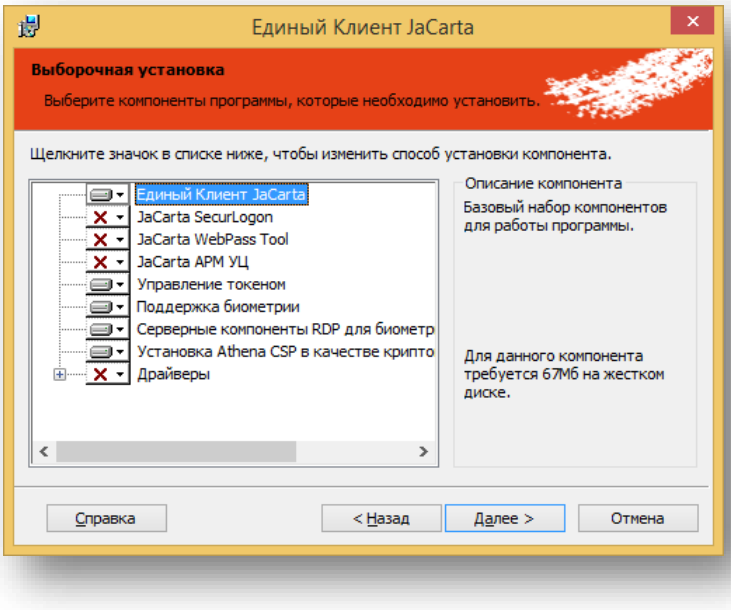

Рисунок 87. Выборочная установка

8. Нажмите **Изменить**... для выбора пути установки Единого Клиента JaCarta.
9. Для установки необходимого компонента в окне **Выборочная установка** в строке с названием требуемого компонента, нажмите значок  и выберите нужную опцию для установки.

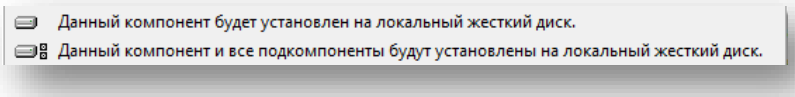

Рисунок 88. Параметры выборочной установки

10. При необходимости воспользуйтесь советами по выборочной установке: при нажатии на кнопку **Справка** появится окно.

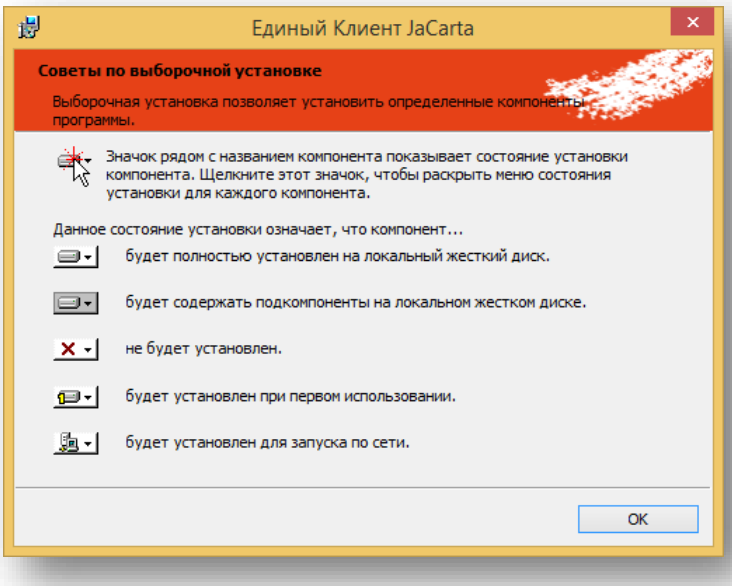

Рисунок 89. Советы по выборочной установке JaCarta

11. Нажмите **Далее >**.
12. Выберите нужный способ автоматического обновления при выборочной установке **"Единого Клиента JaCarta"**.

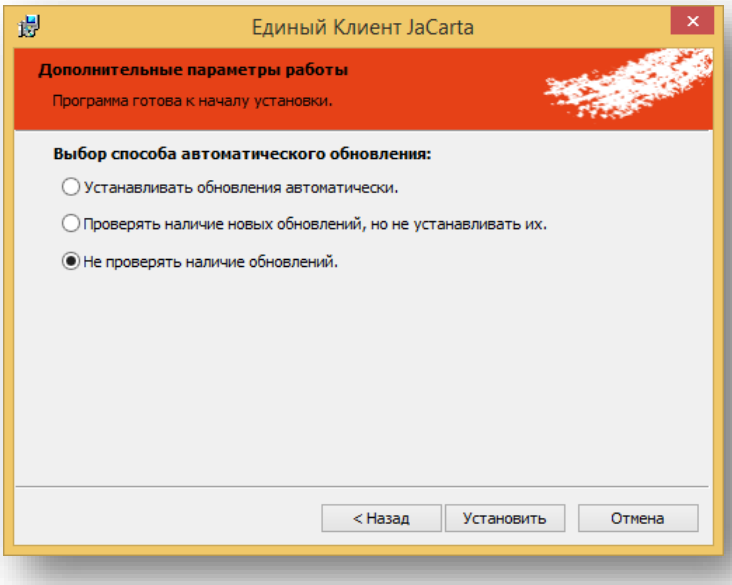

Рисунок 90. Дополнительные параметры

13. Нажмите **Установить** и дождитесь окончания установки.

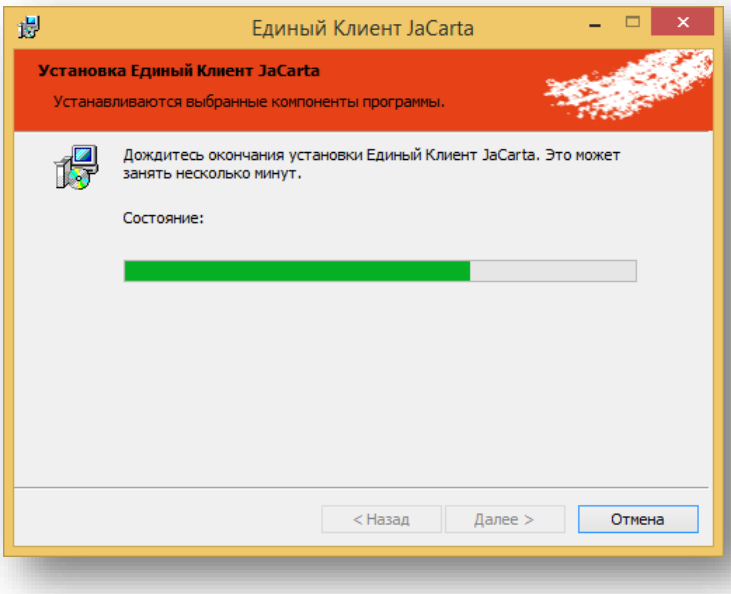

Рисунок 91. Установка Единого клиента

14. Нажмите **Готово**.

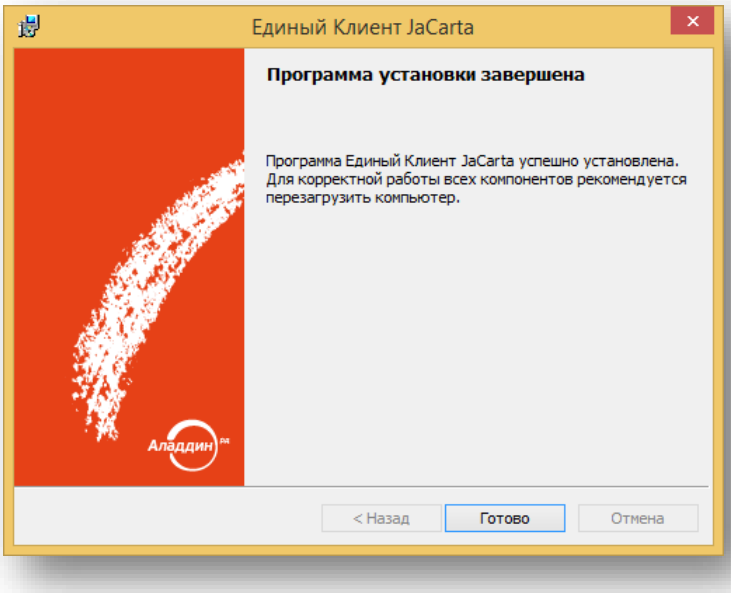

Рисунок 92. Уведомление об успешной установке Единого клиента

15. Для вступлений изменений в силу перезапустите компьютер.

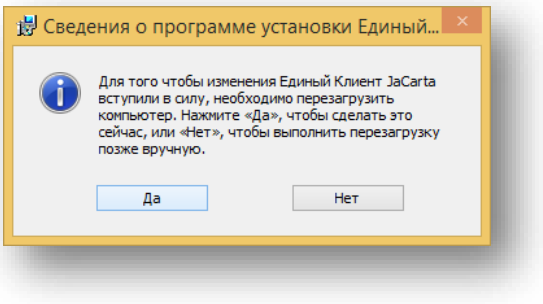

Рисунок 93. Окно уведомления о перезагрузке компьютера

Приложение 2. Установка приложения eToken PKI Client

1. В зависимости от разрядности ОС запустите соответствующий файл установки "eToken PKI Client".
2. Нажмите **Next >**.

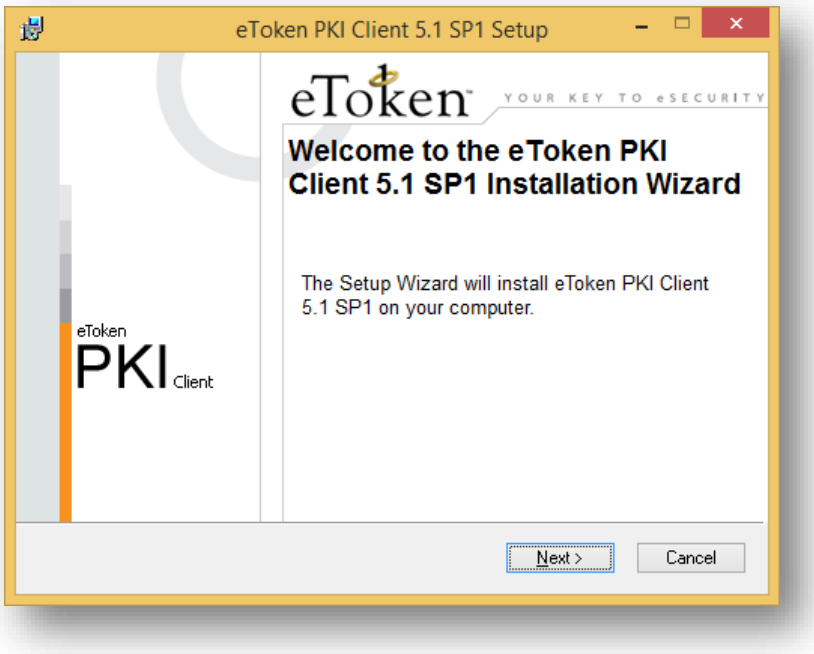

Рисунок 94. Окно приветствия мастера установки

3. Выберите язык программы и нажмите **Next >**.

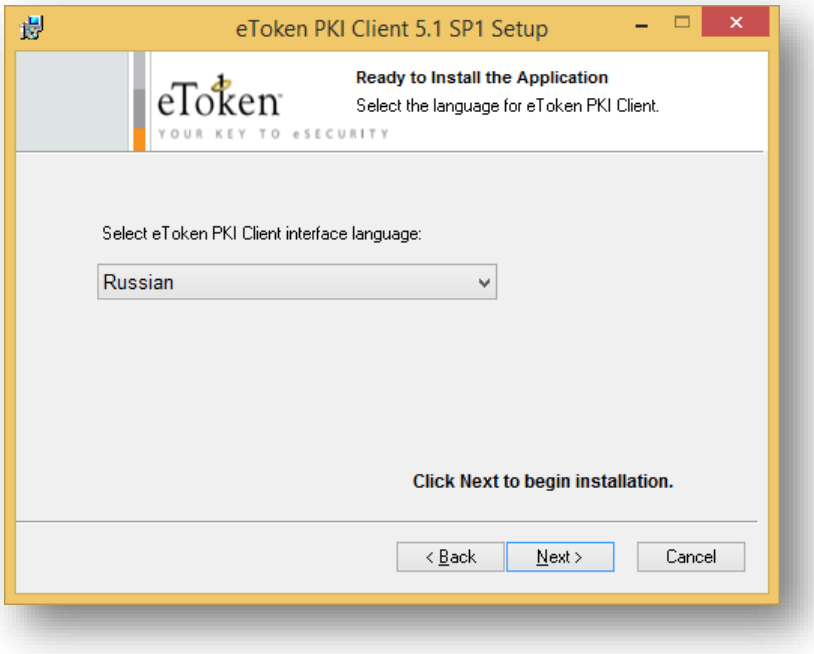

Рисунок 95. Окно выбора языка программы

4. Прочитайте Лицензионное соглашение.

- Выберите пункт **I accept the license agreement**, если вы согласны с его условиями. И нажмите **Next>**.
- Нажмите **< Back** , если вы не согласны с условиями лицензионного соглашения.

Рисунок 96. Окно ознакомления с лицензионным соглашением

5. Выберите папку установки и нажмите **Next >**.

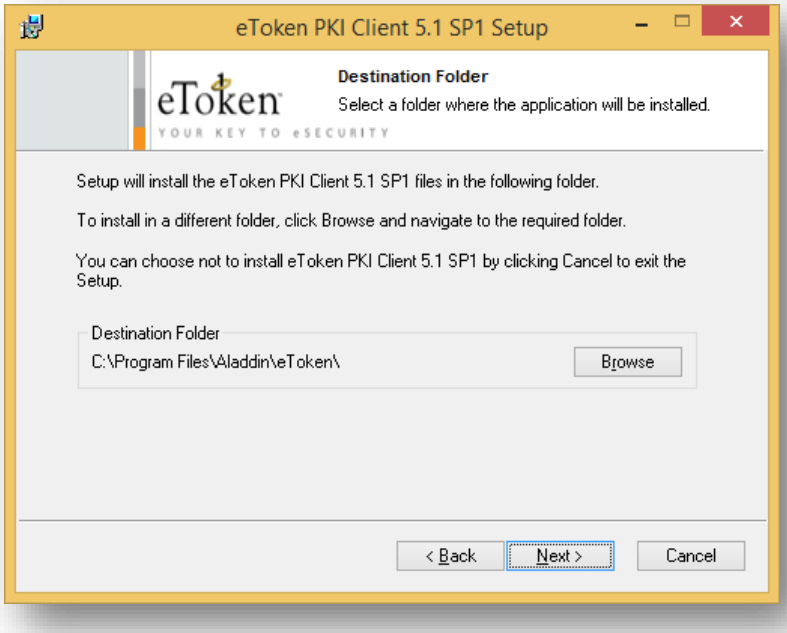

Рисунок 97. Окно выбора папки установки приложения

6. Дождитесь окончания установки.

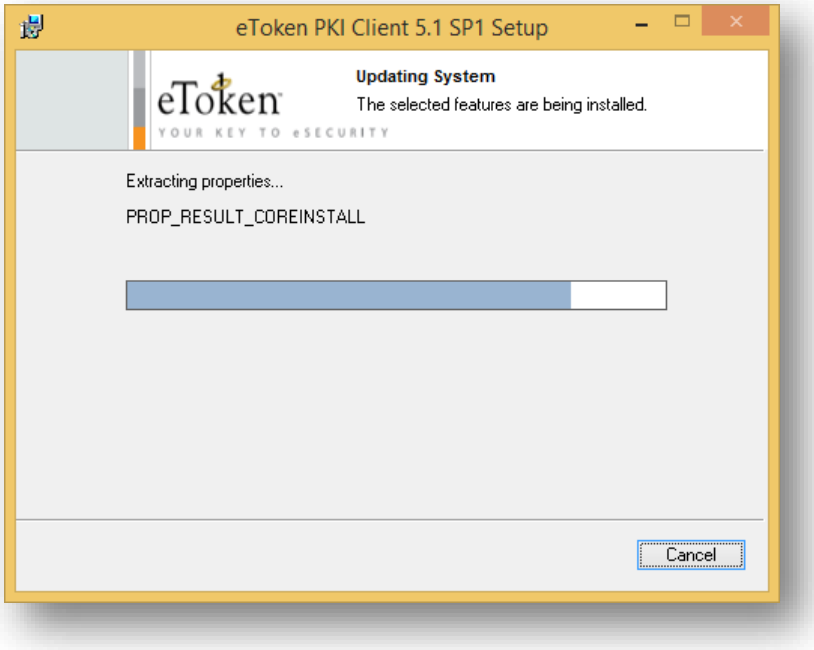

Рисунок 98. Процесс установки приложения

7. Нажмите **Finish** для завершения процесса установки.

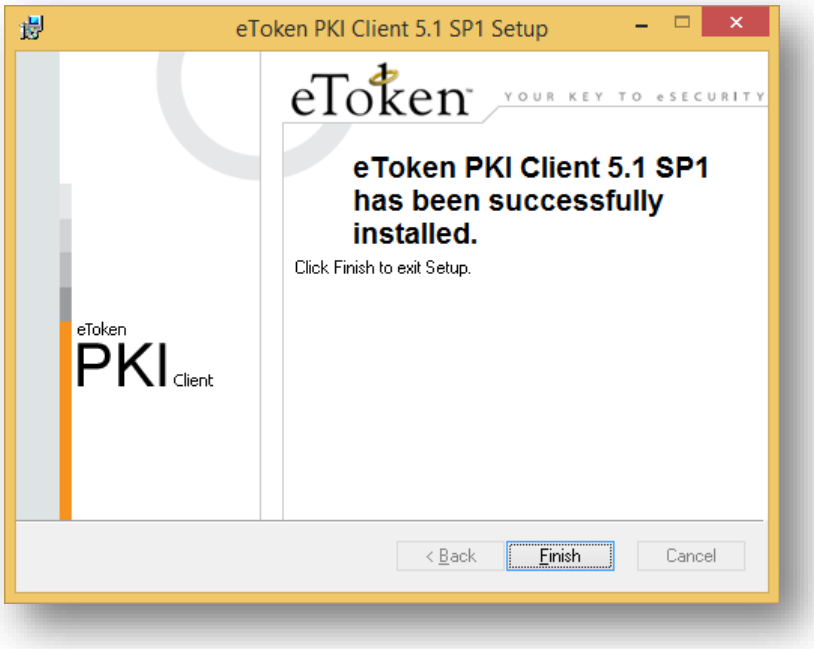

Рисунок 99. Окно уведомления об успешной установке приложения

8. Перезагрузите компьютер, чтобы изменения вступили в силу.

Приложение 3. Установка ViPNet CSP

1. В зависимости от разрядности ОС запустите соответствующий файл установки ViPNet_CSP.

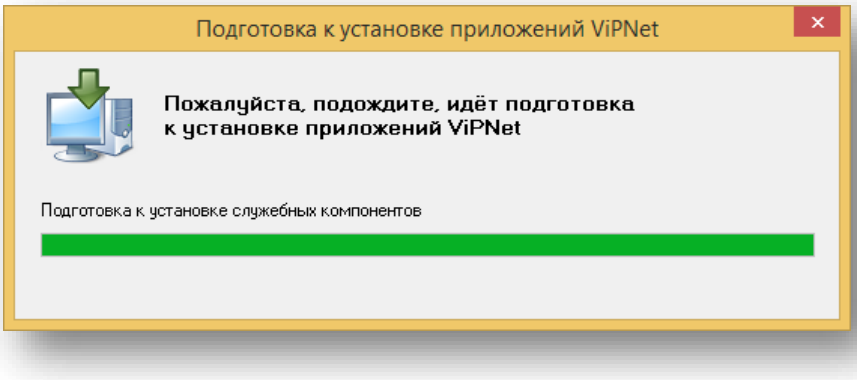

Рисунок 100. Подготовка к установке

2. Прочитайте текст лицензионного соглашения и примите его условия.
3. Нажмите **Продолжить**.

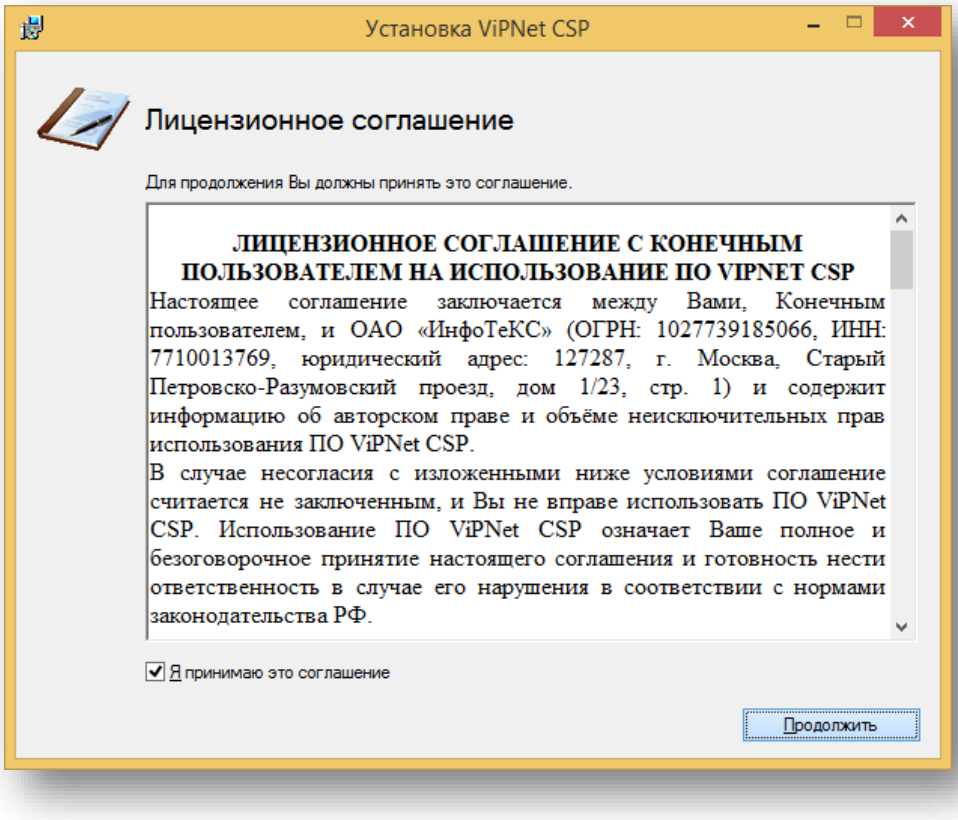

Рисунок 101. Лицензионное соглашение

4. Выберите флаг **Автоматически перезагрузить компьютер после завершения установки**.

5. Выберите **Установить сейчас** для быстрой установки. Выберите **Настроить** для установки параметров настройки.

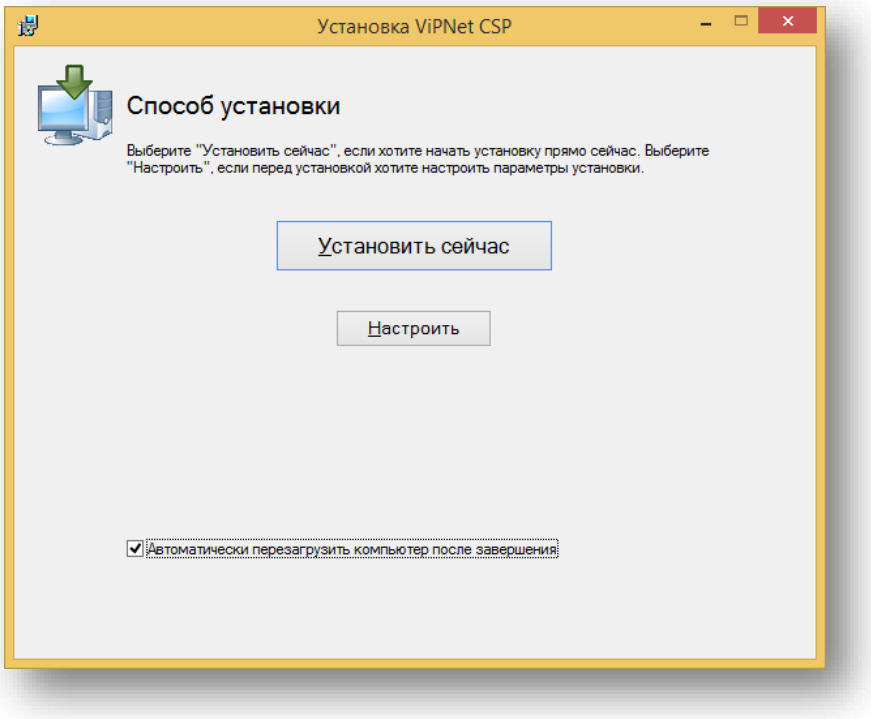

Рисунок 102. Выбор способа установки

6. Если выбрать **Установить сейчас**, то установка начнётся немедленно.
7. Если необходимо настроить параметры установки, нажмите **Настроить**.

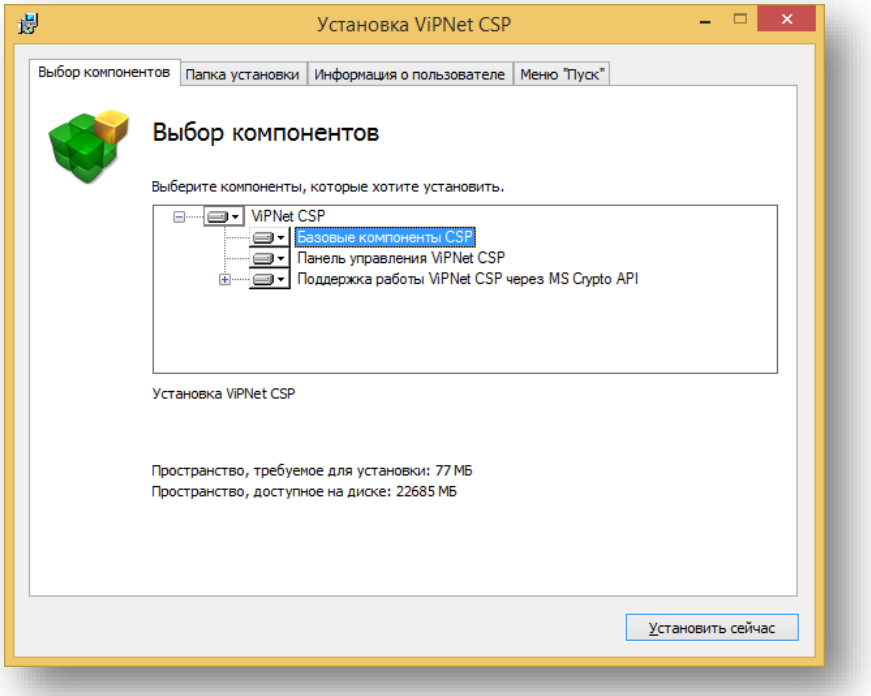

Рисунок 103. Выбор компонентов установки приложения

8. Для установки необходимого компонента во вкладке **Выбор компонентов** в строке с названием требуемого компонента, нажмите значок и выберите нужную опцию для установки.

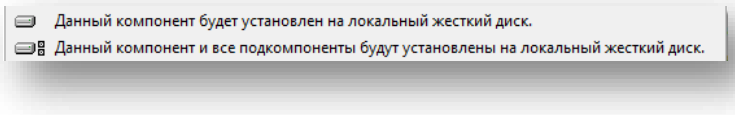

Рисунок 104. Компоненты установки приложения

9. Во вкладке **Папка установки** выберите нужную папку установки ViPNet CSP, нажав **Обзор**....

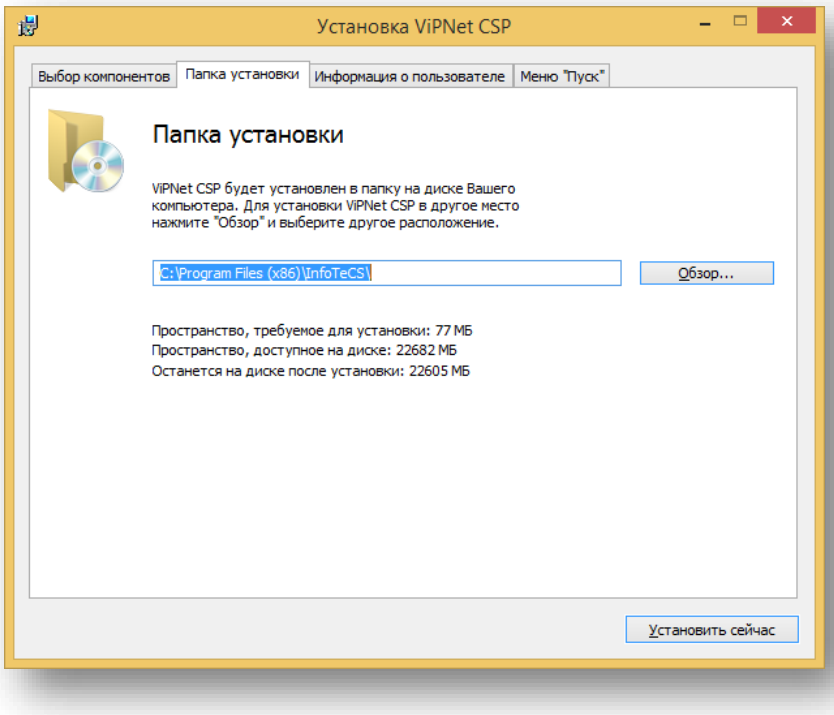

Рисунок 105. Выбор папки установки приложения

10. Во вкладке **Информация о пользователе** заполните необходимые поля.

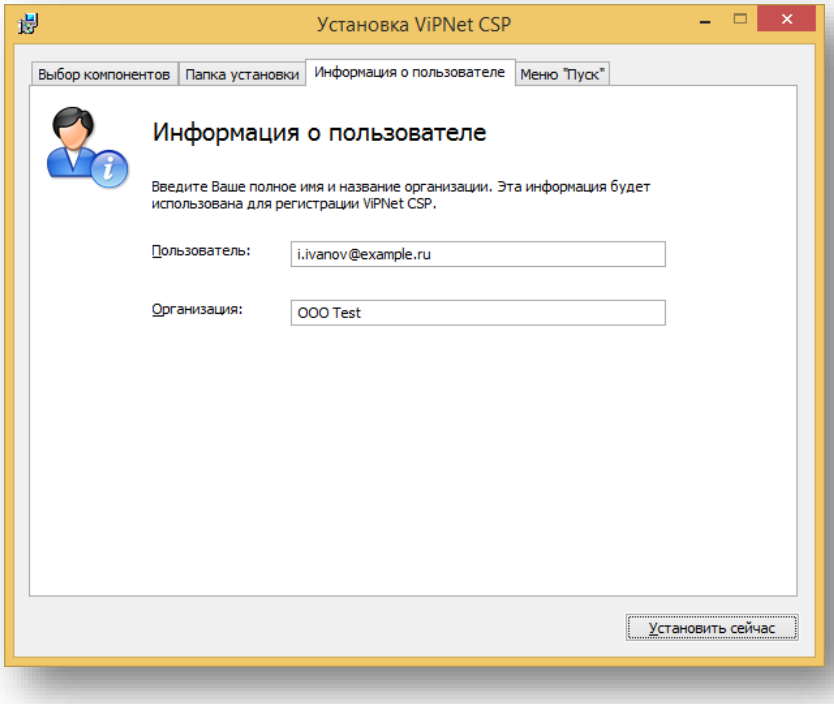

Рисунок 106. Внесение сведений о пользователе

11. Во вкладке меню **Пуск** настройте путь к папке и её название. Включите флаг **Создать ярлыки на рабочем столе**.

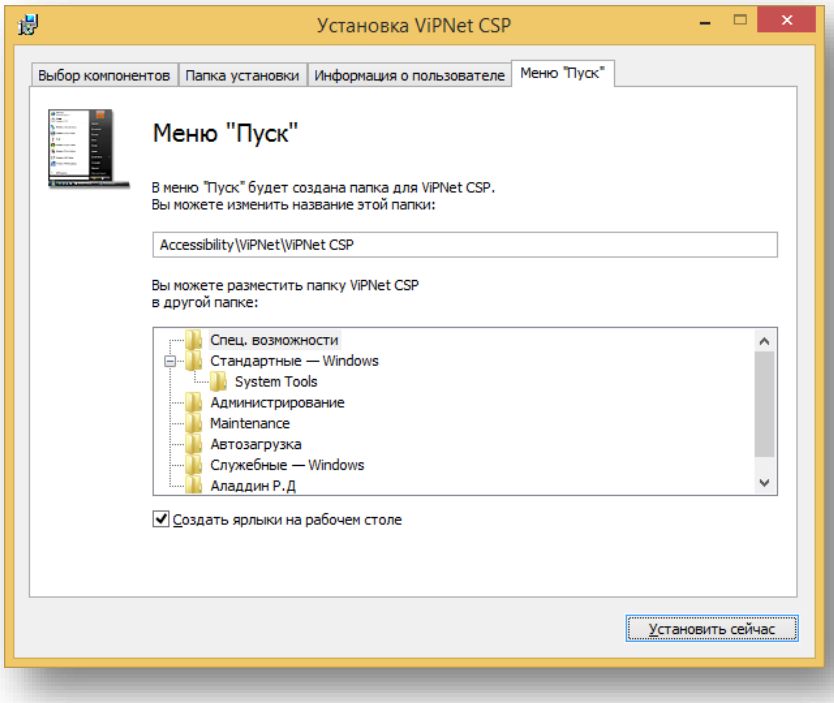

Рисунок 107. Настройка ярлыков

12. Нажмите **Установить сейчас**. Дождитесь окончания установки.

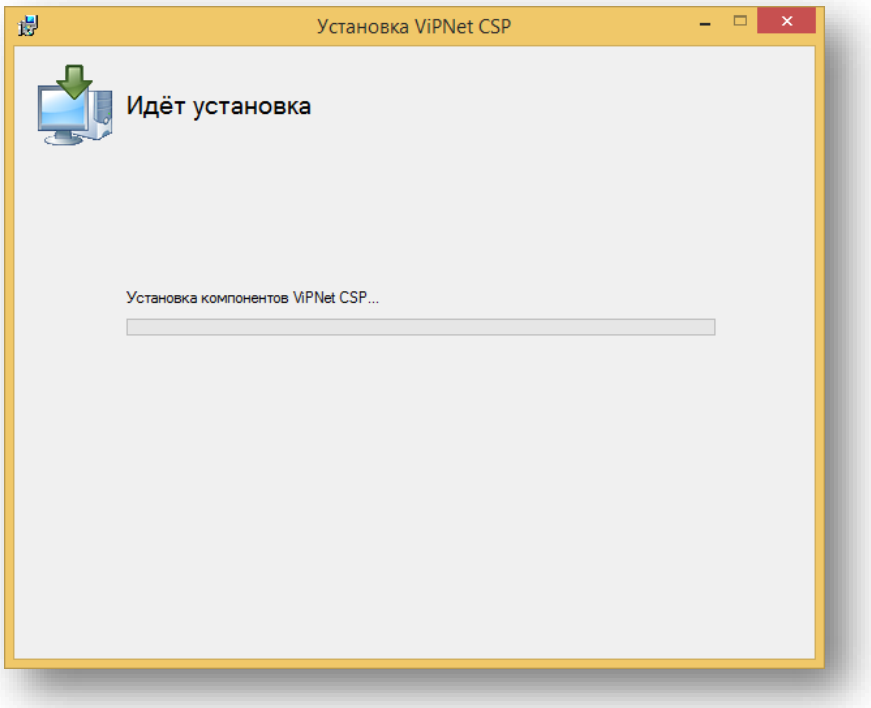

Рисунок 108. Процесс установки приложения

13. По окончании установки нажмите **Закрыть**.

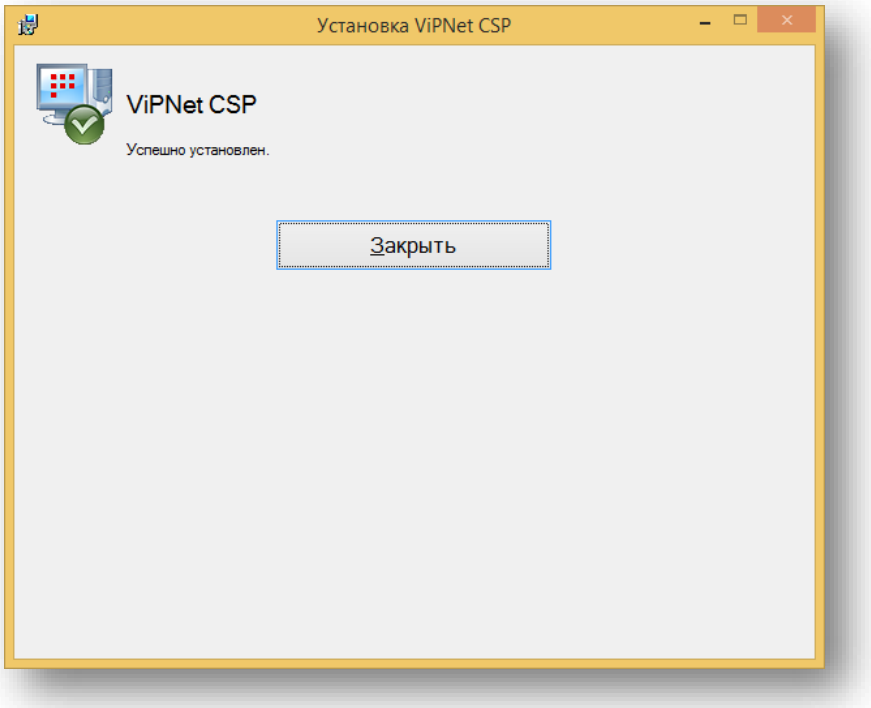

Рисунок 109. Окно уведомления об успешной установке приложения

14. Перезагрузите компьютер.

Приложение 4. Установка КриптоПро CSP

1. Запустите файл установки CSPSetup, соответствующий разрядности операционной системы.
2. Выберите **Установить (рекомендуется)** для установки стандартных параметров либо нажмите **Дополнительные опции** для выбора конфигурации и языка программы.

Флаг Установить корневые сертификаты необходима, если вам требуется установка этих сертификатов.

3. Дождитесь окончания процесса установки.
4. Нажмите **OK**.

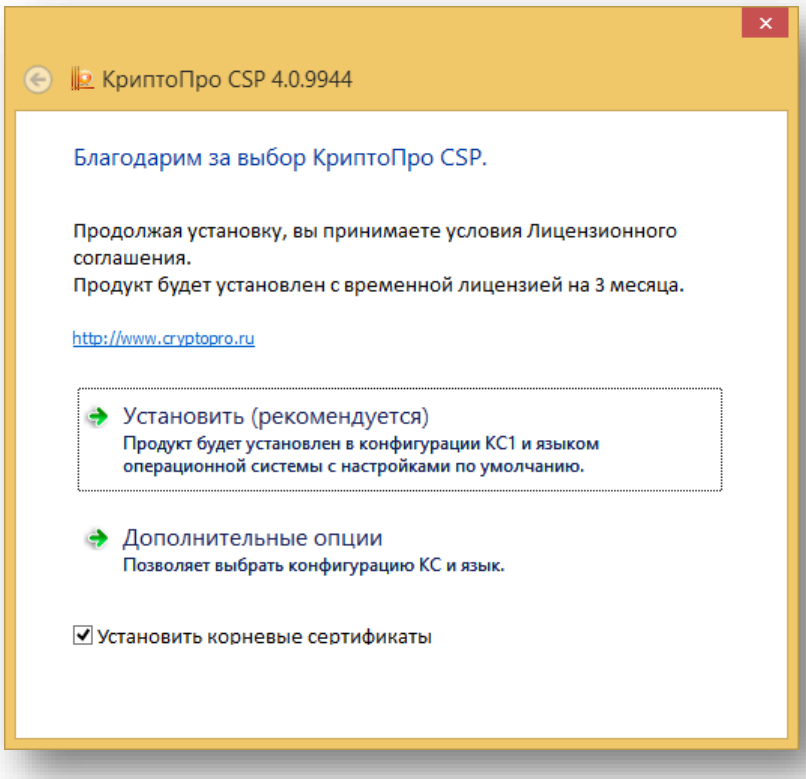

Рисунок 110. Окно выбора способа установки приложения

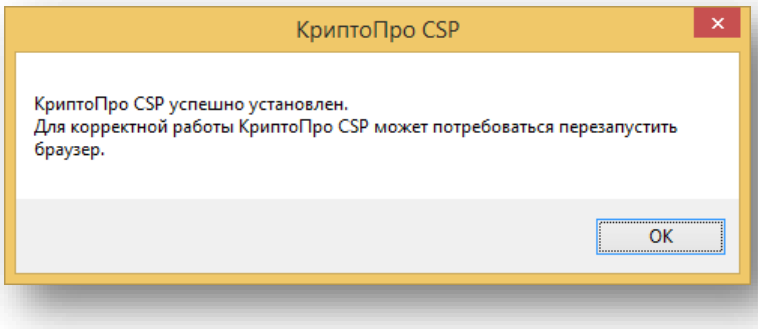

Рисунок 111. Уведомление об успешной установке приложения

Приложение 5. Описание утилит для работы с лицензиями SD5

В состав дистрибутива SD5 входят 2 утилиты для работы с лицензиями. Они позволяют прочитать параметры лицензии, записанной на электронный ключ, и записать лицензию на электронный ключ, если поставка не включала токен либо необходимо обновить/продлить лицензию на право использования SD5.

1. **SD5LicRead.exe** - утилита чтения параметров лицензии SD5.

Утилита запускается без ключей и выполняет сканирование текущего каталога на предмет файлов лицензий и подключенных токенов, содержащих лицензии. Рекомендуется для запуска данной утилиты использовать пакетный файл исполнения команд (*.cmd или *.bat), оканчивающийся командой "pause", чтобы результат выполнения команде не был скрыт автоматически закрывающимся окном выполнения программы.

> *Бинарный файл лицензии, полученной от партнёра компании-производителя имеет размер 512 байт и обычно имеет название sd5.xxxxxxxx.lic, где "xxxxxxxx" – номер SmartCard ID токена, на котором она записана или на который она может быть записана.*

2. **SD5LicWrite.exe** - утилита записи файлов лицензий на токен.
   При запуске без ключей программа сама выполняет поиск в текущем каталоге файлов лицензии и определяет подключенные к данному компьютеру токены. Пользователю нужно выбрать токен на который будет произведена запись и ввести его PIN-код.
   Утилита имеет следующие ключи командной строки:
   - p [PINCODE] – PIN-код токена. Код может быть указан заранее. Данный ключ не может быть использован одновременно с ключом "-o";
   - o [j; e] – PIN-коды новых токенов JaCarta или eToken, пришедших с производства. По умолчанию подставляет для JaCarta значение "11111111", а для eToken "1234567890". Ключ не совместим с ключом –p;
   - m [filename] – Записывает лицензию из файла с измененным именем. Имя по умолчанию sd5.[serial].lic.

> *Файл лицензии помимо параметров использования SD5 содержит SCID целевого токена. Утилита SD5LicWrite.exe выполнит запись лицензии только при полном совпадении номера SCID токена и номера SCID, записанного в лицензии.*

Список таблиц

Список рисунков

21. Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО "Аладдин Р.Д.".

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р.Д." обязательны.

Владельцем зарегистрированных товарных знаков "Аладдин", Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, "Крипто БД", логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены ЗАО "Аладдин Р.Д." без предварительного уведомления.

ЗАО "Аладдин Р.Д." не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

ЗАО "Аладдин Р.Д." не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе ЗАО "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

ЗАО "Аладдин Р.Д." НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ ЗАО "Аладдин Р.Д." БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

21.1 Лицензионное соглашение

Пожалуйста, внимательно прочитайте данное лицензионное соглашение прежде, чем использовать содержимое данного комплекта и/или прежде, чем загружать или устанавливать программное обеспечение.

Все указания по использованию программного обеспечения, предоставляемые Закрытым акционерным обществом "Аладдин Р. Д." (или любым его дочерним предприятием – каждое из них упоминаемое как "компания"), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на Ваш компьютер и/или используя данное программное обеспечение иным способом, Вы принимаете данное соглашение и соглашаетесь с его условиями.

Если Вы не согласны с данным соглашением, не загружайте и/или не устанавливайте данное программное обеспечение и незамедлительно (не позднее 7 (семи) дней с даты ознакомления с настоящим текстом) верните этот продукт в ЗАО "Аладдин Р.Д.", удалите данное программное обеспечение и все его части со своего компьютера и не используйте его никоим образом.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) — конечным пользователем (далее "Пользователь") — и ЗАО "Аладдин Р.Д." (далее "Компания") относительно передачи неисключительного права на использование настоящего программного обеспечения, являющегося интеллектуальной собственностью Компании.

Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как Программное обеспечение или ПО), и связанная с ним документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остаётся исключительной собственностью Компании.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтверждённые или включённые в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на ПО являются и будут являться собственностью исключительно Компании.

Данное соглашение не передаёт Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничто в данном Соглашении не подтверждает отказ Компании от прав на интеллектуальную собственность по какому бы то ни было законодательству.

Лицензия

Компания настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного **Соглашения:**

Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении.

Вы можете добавить/присоединить Программное обеспечение к программам для мобильных устройств с единственной целью, описанной в данном Соглашении. Принимая условия настоящего соглашения, Вы соглашаетесь:

- не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;

- не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;

- не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;

- не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (http://developer.aladdin-rd.ru/).

Использование ПО

Пользователь вправе:

- воспроизводить ПО путём записи его в память электронно-вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;

- встраивать ПО любым способом в продукты и решения Пользователя;

- распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Российской Федерации и импортом таких средств в другие страны. В частности, ограничения и дополнительные требования могут возникать при распространении ПО через магазины приложений, содержащие различные приложения для мобильных устройств.

Условия использования, изложенные в настоящем соглашении, действуют в отношении всего содержимого ПО, в частности в отношении:

- дизайна (графики, расположения элементов оформления и т.п.);

- всех иных элементов, в том числе изображений, фонограмм, текстов.

Получаемые Пользователем неисключительные имущественные права не включают права на передачу третьим лицам каких-либо прав на встраивание, воспроизведение, распространение и использование программ для ЭВМ не в составе продуктов и решений Пользователя.

Компания сохраняет за собой все исключительные права на ПО и входящие в него компоненты, включая права на предоставление неисключительных и исключительных прав третьим лицам.

Пользователь вправе осуществлять использование ПО в пределах, предусмотренных настоящим Соглашением, исключительно на территории Российской Федерации.

Обслуживание и поддержка

Компания не несёт обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов ПО.

Ограниченная гарантия

Компания гарантирует, что программное обеспечение с момента приобретения его Вами в течение 12 (двенадцати) месяцев будет функционировать в полном соответствии с его технической/эксплуатационной документацией, при условии, что ПО будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

Отказ от гарантии

Компания не гарантирует, что программное обеспечение будет соответствовать Вашим желаниям и требованиям, или что его работа будет бесперебойной или безошибочной. В объёме, предусмотренном законодательством РФ, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов

или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

Ограничение возмещения

В случае нарушения гарантии, оговоренной выше, Компания может по собственному усмотрению:

- заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;

- возместить стоимость, выплаченную Вами за ПО.

Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее 7 (семи) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Компанию. Всё ПО (все экземпляры, имеющиеся у Вас) должно быть возвращено Компании и отправлено возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Экземпляры ПО должны быть отправлены с копией платёжных документов и накладных.

Исключение косвенных убытков

Стороны признают, что Программное обеспечение не может быть полностью лишено ошибок. Компания не несёт ответственности (как в силу договора, гражданского правонарушения, включая халатность, так и в любой иной форме) перед Вами или любой третьей стороной за любые потери или убытки (включая косвенные, фактические, побочные или потенциальные убытки), включая, без ограничений, любые потери или убытки прибыльности бизнеса, потерю доходности или репутации, утраченную или искажённую информацию или документацию вследствие какого-либо использования данного программного обеспечения и/или любой компоненты данного по, даже если компания письменно уведомлена о возможности подобных убытков.

Ограничение ответственности

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких-либо дефектов или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного обеспечения не будет превышать суммы, выплаченной вами ЗАО "Аладдин Р.Д." за это ПО.

Прекращение действия соглашения

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

- лицензия, предоставленная Вам данным Соглашением, прекращает своё действие, и Вы после её прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;

- вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

Государственное регулирование и экспортный контроль

Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и реэкспорт ПО.

Разное

Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ. Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ. ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

22. Контакты

22.1 Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: https://www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

22.2 Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт: www.aladdin-rd.ru/support/index.php.

Регистрация изменений

Версия	Изменения
1.0	Полное обновление документа.

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru

Коротко о компании

Компания "Аладдин Р.Д." основана в апреле 1995 года и является российским разработчиком (вендором) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

Основные направления

- Обеспечение безопасного доступа к информационным ресурсам предприятия, веб-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация).
- Электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI.
- Защита персональных данных, данных на дисках компьютеров, серверов, баз данных.
- Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ и Министерства обороны (включая работу с гостайной до уровня секретности СС).

Лицензии

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа.
- Система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты.
- Система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.