Secret Disk Server NG

Справочное руководство

Версия	Версия 3.13
Статус	Публичный
Дата	06.03.2019
Номер	ID-номер

Аннотация

Система защиты корпоративной конфиденциальной информации на серверах от несанкционированного доступа "Secret Disk Server NG" (версия 3.x.y.zz, где 3 – номер версии, x.y.zz – версия сборки) представляет собой специализированный программно-аппаратный комплекс, предназначенный для обеспечения безопасности данных, хранящихся на серверах.

Настоящий документ представляет собой справочное руководство Secret Disk Server NG (далее – SDS NG) и предназначено для операторов сервера (-ов), на которые установлено приложение SDS NG.

В документе содержатся сведения, необходимые оператору для установки, настройки приложения и дополнительных компонентов, сведения для работы с приложением, порядок работы оператора с компонентами системы защиты.

1. 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 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 будет преследоваться по закону.

2. Список терминов и определений

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
Защищённое хранилище	Файл или файлы с настройками приложения SDS NG, содержащие учётные записи администраторов, списки защищаемых ресурсов, параметры доступа к ресурсам, криптокопии ключей доступа и т.д.
ОС	Операционная система
Приёмник	С точки зрения программы – это сервер, который реагирует на сигнал "тревога"
Радиоприёмник	Устройство, которое принимает сигнал от сигнала "тревога" в виде радиобрелока
Источник	USB-адаптер кнопки "тревога"
Радиокнопка	Устройство, которое передает сигнал "тревога"
Сертификат открытого ключа	Электронный документ, подтверждающий принадлежность открытого ключа и определённых атрибутов конкретному пользователю
Secret Disk Crypto Extension Pack (SD CEP)	Пакет расширения, который позволяет использовать алгоритм шифрования ГОСТ 28147-89, предоставляемый сторонними криптопровайдерами.
КриптоПро CSP	Программа для предоставления алгоритмов шифрования по ГОСТ. Поставляется компанией КриптоПРО.
ViPNet CSP	Программа для предоставления алгоритмов шифрования по ГОСТ. Поставляется компанией Инфотекс.
eToken PKI Client	Программа для обеспечения работы USB-ключей и смарт-карт eToken на операционных системах семейства Windows до версии 7. Поставляется компанией Aladdin.
DDS (Сервис депонирования)	Распределённая база данных с хранением табличных данных в оперативной памяти, предназначенная для обеспечения взаимодействия компонентов SDS NG находящихся в разных узлах сети
SL (Сервис лицензирования)	Компонент Secret Disk Server NG, предназначенный для удалённого подключения электронных ключей с лицензиями сервера
Консоль управления Microsoft (Microsoft Management Console, MMC)	Компонент операционной системы Windows 2000 и более поздних версий Windows. Позволяет системным администраторам и продвинутым пользователям с помощью гибкого интерфейса конфигурировать и отслеживать работу системы. Консоль управления предоставляет более широкие

	возможности для управления компьютером. Основной принцип действия заключается в оснастках — небольших подпрограммах, позволяющих настроить разные аспекты операционной системы.
Лицензия администратора	Объект, хранящийся в памяти электронного ключа администратора. Наличие лицензии позволяет использовать электронный ключ для управления Secret Disk Server
Лицензия сервера приложений	Объект, хранящийся в памяти электронного ключа сервера и позволяющий запрещать сетевой доступ к зашифрованным дискам
Лицензия файл-сервера	Объект, хранящийся в памяти электронного ключа сервера и содержащий информацию о максимальном количестве клиентских подключений
Мастер-ключ зашифрованного диска	Уникальный секретный параметр алгоритма шифрования диска. Хранится в зашифрованном виде, для доступа к этому ключу используется закрытый ключ, соответствующий сертификату пользователя
Лицензия администратора	Объект, хранящийся в памяти электронного ключа администратора. Наличие лицензии позволяет использовать данный электронный ключ для управления Secret Disk Server
СКЗИ	Средства криптографической защиты информации.
Электронный ключ администратора	Электронный ключ, в памяти которого содержится лицензия администратора. Для каждого из используемых криптопровайдеров в памяти электронного ключа администратора должен присутствовать сертификат с закрытым ключом для защиты мастер-ключей зашифрованных дисков, шифруемых с помощью данного криптопровайдера, и аутентификации
Электронный ключ сервера	Электронный ключ с лицензией файл-сервера, лицензией сервера приложений или комбинированной лицензией. Электронный ключ сервера должен быть подсоединен к серверу Secret Disk Server NG напрямую или к серверу лицензирования

3. Общие сведения

3.1 Назначение

Программно-аппаратный комплекс SDS NG обеспечивает безопасную работу с конфиденциальной информацией, хранящейся на корпоративном сервере. Защита осуществляется путем шифрования дисков (томов), что делает невозможным доступ к ним посторонних лиц.

3.2 Характеристики

ПАК SDS NG позволяет зашифровывать, подключать и отключать диски.

Для управления зашифрованными дисками используется персональный электронный ключ в виде смарт-карты или USB-ключа (токена).

Шифрование и подключение зашифрованных ресурсов, резервное копирование и восстановление копий мастер-ключей осуществляется после успешного прохождения двухфакторной аутентификации.

В SDS NG встроена функция резервного копирования защищенного хранилища, в котором содержаться зашифрованные копии мастер-ключей и информация об администраторах серверов SDS NG.

Для чрезвычайных ситуаций предусмотрен инструмент "Тревожная кнопка". Он позволяет удаленно отключать защищённые ресурсы. При определенных настройках нажатие "Тревожной кнопки" может привести к удалению с сервера ключевой информации. В результате, если злоумышленники завладеют нужным токеном, ПИН-кодом токена, паролем для доступа к серверу и будут обладать полным доступом к серверу, то они не смогут прочесть информацию, не располагая резервной копией защищенного хранилища.

SDS NG использует несколько средств шифрования:

1. Криптографический драйвер ОС Microsoft Windows, применяется для шифрования дисков алгоритмом AES.
2. Криптопровайдер Microsoft Enhanced CSP (алгоритмы RSA и SHA), применяется для работы с ключевыми парами и сертификатами при аутентификации и шифровании с помощью токенов.
3. Российские криптографические средства (СКЗИ) ViPNet CSP или КриптоПРО CSP, применяются для шифрования дисков алгоритмом ГОСТ 28147-89 и для работы с ГОСТ-сертификатами и ключами, хранящихся на токенах.
4. Драйверы шифрования, реализованные в компоненте Secret Disk Crypto Extension Pack (SD CEP):
    - Triple DES;
    - Advanced Encryption Standard (AES);
    - Twofish.

Для работы с алгоритмами, указанными в п. 3 и 4 должен быть установлен компонент Secret Disk Crypto Extension Pack. Компонент входит в комплект поставки SDS NG.

Российские СКЗИ КриптоПРО CSP и ViPNet CSP в комплект поставки SDS NG не входят и приобретаются отдельно.

При применении SDS NG без дополнительных российских СКЗИ по умолчанию будут использоваться средства, встроенные в ОС Microsoft Windows.

3.3 Компоненты

Программный комплекс SDS NG состоит из следующих компонентов:

- сервер Secret Disk;

- консоль администрирования Secret Disk;
- сервис депонирования данных;
- сервис лицензирования;
- Crypto Extension Pack.

Компоненты комплекса могут быть установлены на одном или нескольких компьютерах, подключенных к общей локальной сети передачи данных. Эти компьютеры могут работать под управлением домена Windows Active Directory (далее AD), либо быть независимыми.

Ниже перечислены основные рекомендации по выбору места установки компонентов комплекса:

1. Сервер Secret Disk (SDS):
   - устанавливается на компьютер, выполняющий роль файл-сервера, либо сервера приложения (например, сервер базы данных). В первом случае SDS, обычно, защищает данные, к которым открыт доступ по сети. Во втором случае – данные приложения, например, файлы базы данных;
   - Консоль управления рекомендуется **устанавливать** вместе с SDS, даже если она также будет установлена на другом компьютере;
   - Вместе с SDS **нельзя** установить Сервис лицензирования, все остальные компоненты комплекса могут быть установлены вместе с SDS на один компьютер.
2. Консоль управления:
   - если SDS установлен на компьютере, входящим в домен AD, Консоль управления должна быть установлена также на доменном компьютере;
   - для работы Консоли управления **необходимо** программное обеспечение (клиент) для работы с токеном.
3. Сервис лицензирования:
   - **должен** быть установлен на том компьютере (или компьютерах), к которому (которым) будут физически подключаться серверные токены с лицензиями;
   - вместе с Сервисом лицензирования **должен** быть установлен Сервис депонирования данных (DDS);
4. Сервис депонирования данных:
   - **может** устанавливаться отдельно от других компонентов SDS;
   - установка **невозможна** на контроллере домена;
   - если Сервис депонирования данных будет использовать аутентификацию Windows authentication то у компьютера должен быть сертификат, выданный по шаблону "Компьютер".

3.4 Управление комплексом

В SDS NG используются бессрочные лицензии двух типов – лицензия сервера и лицензия администратора. Лицензии хранятся в памяти токена в виде специального файла, который привязан к серийному номеру токена.

Лицензия администратора позволяет запускать Консоль администрирования одному оператору (администратору) сервера.

Лицензия сервера позволяет запускать один экземпляр компонента SDS в одном из трех режимов, описанных ниже.

В минимальный комплект поставки комплекса входит:

1. Дистрибутив программных компонентов и документация.
2. Токен администратора сервера.
3. Токен сервера.

> *Токены имеют соответствующую маркировку на корпусе: Administrator – токен оператора сервера, Server – токен сервера. Возможности, предоставляемые лицензиями разных типов указаны в таблице.*

Таблица 1 – Типы лицензий SDS NG

Тип лицензии	Особенности	Расположение	Примечания
Лицензия файл-сервера	Позволяет разрешить доступ к диску по сети	Токен сервера	
Лицензия сервера приложений	Позволяет установить ограничение на доступ к диску по сети	Токен сервера	
Комбинированная лицензия	Совмещает возможности лицензий сервера приложений и файл-сервера	Токен сервера	Представлен в памяти токена в виде двух лицензий: 1. Лицензии файл-сервера. 2. Лицензии сервера приложений.
Лицензия администратора	Доступ к функциям управления ПК SDS NG	Токен администратора	

Администраторов может быть несколько – по количеству токенов с лицензией администратора. Один и тот же токен с лицензией администратора можно использовать при администрировании нескольких серверов (Рисунок 1).

> *Пользователям для доступа к серверу лицензия не требуется.*

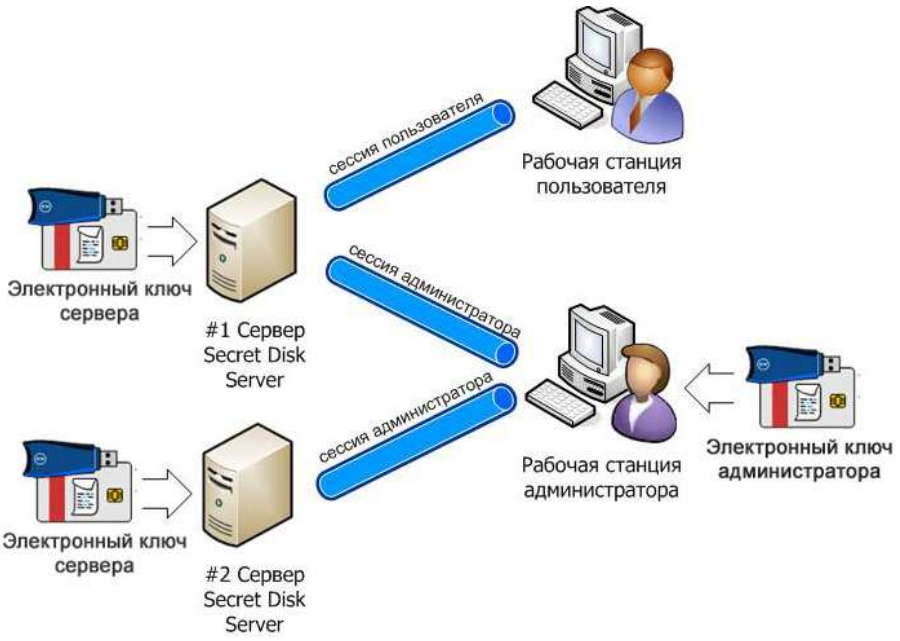


Рисунок 1 – Пример администрирования нескольких серверов

Если один и тот же компьютер является одновременно и рабочей станцией оператора и сервером, то можно использовать один токен с двумя лицензиями – Сервера и Администратора. Такой токен поставляется по специальному заказу.

4. Параметры установки SDS NG

4.1 Требования к среде исполнения

Операционные системы	Microsoft Windows Server 2016 Microsoft Windows Server 2012 R2 Microsoft Windows Server 2012 Microsoft Windows Server 2008 R2 Microsoft Windows Server 2008 Microsoft Windows Server 2003 R2 Microsoft Windows Server 2003 Microsoft Windows 7 Microsoft Windows 8/8.1 Microsoft Windows 10
Типы поддерживаемых дисков	Основные разделы и логические диски (тома) дисков накопителей Тома динамических дисков Внешние съёмные накопители (USB-диски, флэш-диски) Внешние сетевые хранилища (SAN)
Типы файловых систем	NTFS FAT32 FAT16 exFAT
Размер защищаемых дисков	До 64 ТБ (для NTFS) До 8 ТБ (для FAT32) До 4 ГБ (для FAT16)

Защищаемые диски (тома) должны иметь букву диска. Тома, монтируемые без назначения буквы, нельзя защитить с помощью SDS.

4.2 Требования к программному обеспечению

При использовании системы резервного копирования Symantec Backup Exec 2010, необходимо установить её до установки SDS NG.

При установке SDS NG на ОС с Microsoft Hyper-V, убедитесь, что система виртуализации используется в стандартном режиме.

5. Использование шифрования ГОСТ

Администратор может управлять диском, защищенным алгоритмом шифрования ГОСТ, в случае, если у него есть сертификат типа ГОСТ. Для управления диском с любым другим типом шифрования нужен сертификат типа RSA. Чтобы один администратор мог управлять дисками и с шифрованием ГОСТ и с любым другим шифрованием, у него должны быть два сертификата обоих типов – ГОСТ и RSA. Оба сертификата должны быть зарегистрированы в одной учетной записи администратора SDS.

Если у администратора есть только один сертификат, то он не сможет управлять дисками с шифрованием неподходящего типа.

> *В консоли администрирования SDS пользователь может выбрать любой из своих сертификатов для аутентификации.*

При необходимости использования шифрования ГОСТ Р 34.10-2012, Р 34.11-94 и ГОСТ Р 34.11-2012, ГОСТ 28147-89, требуется установка стороннего программного обеспечения. Комплекс SDS NG может работать совместно со следующими средствам криптографической защиты информации (СКЗИ):

1. ViPNet CSP (v. 4.2 и выше).
2. КриптоПРО CSP (v. 4.0 и выше).

> *Нельзя одновременно устанавливать два СКЗИ в одной системе.*
>
> *С 1 января 2019 года запрещено формирование электронной подписи с помощью ключей ГОСТ 34.10-2001.*

СКЗИ должен быть установлен вместе с SDS и, также, вместе Консолью администрирования.

При использовании алгоритмов шифрования ГОСТ обязательна установка утилиты дополнительных драйверных алгоритмов шифрования – Secret Disk Crypto Extension Pack (SD CEP).

Процесс установки Secret Disk Crypto Extension Pack (SD CEP) описан в отдельном файле.

6. Установка и настройка SDS NG

6.1 Варианты развёртывания комплекса

Ниже кратко описаны три типовых варианта развертывания комплекса SDS NG: минимальная конфигурация с одним сервером, управляемых локально, конфигурация с удалённым сервером и использование SDS в отказоустойчивом кластере.

1. **Минимальная конфигурация**. Один сервер SDS, все компоненты SDS установлены на один компьютер. Токен сервера с лицензией физически подключается к серверу. Консоль администрирования может быть установлена вместе с сервером или находиться на другом компьютере.
2. **Удаленный сервер**. Один сервер SDS, к которому затруднён доступ для подключения токена. Поэтому токен сервера с лицензией физически не подключается к серверу, а доставляется с помощью Сервера лицензирования и Службы Депонирования данных, установленных на другом компьютере, к которому подключен серверный токен. Служба депонирования данных устанавливается также на сервере SDS.
3. **Отказоустойчивый кластер**. SDS и Служба депонирования данных, устанавливаются на 2-х и более компьютерах, входящих в кластер Windows Server Failover Cluster. Защищённый диск размещён во внешней системе хранения данных (СХД) и подключён к одному из серверов кластера, который в данный момент времени является активным. Активный сервер кластера, работающий с диском, может смениться в любой момент, и новый каждый экземпляр SDS должен быть постоянно готов к работе. Поэтому ключ шифрования диска после его подключения с помощью Службы Депонирования данных доставляется всем SDS.

6.2 Установка SDS NG в минимальной конфигурации

Минимальная конфигурация установки SDS с одним сервером представлена на Рисунок 2.

Рисунок 2 – Минимальная конфигурация установки SDS NG

Для такой конфигурации необходимо установить компонент SDS и консоль администратора на один сервер. При удалённом управлении сервером необходимо установить консоль управления администратора на любом другом компьютере.

6.3 Установка сервиса лицензирования

Сервис лицензирования предназначен для удалённого подключения серверных токенов и их лицензий к SDS. Сервис должен быть установлен на тех компьютерах, к которым планируется физически подключать токены.

Особенности установки Сервиса лицензирования:

- сервис лицензирования нельзя установить вместе с SDS на один компьютер;
- для работы сервиса лицензирования необходима установка сервиса DDS (компонент DDS должен быть установлен на компьютер вместе с сервисом лицензирования, а также на всех компьютерах SDS, которые будут получать лицензии от сервиса лицензирования);
- несколько сервисов лицензирования могут работать одновременно, объединенные одной службой депонирования. Это позволяет подключать серверные токены к разным компьютерам сервиса лицензирования и обеспечить доставку лицензий к серверам при отключении или неисправности некоторой части компьютеров.

6.4 Настройка сервиса лицензирования

1. Откройте Консоль управления службой лицензирования через меню **Пуск → Все программы → Secret Disk → Server → Управление сервисом лицензирования**.

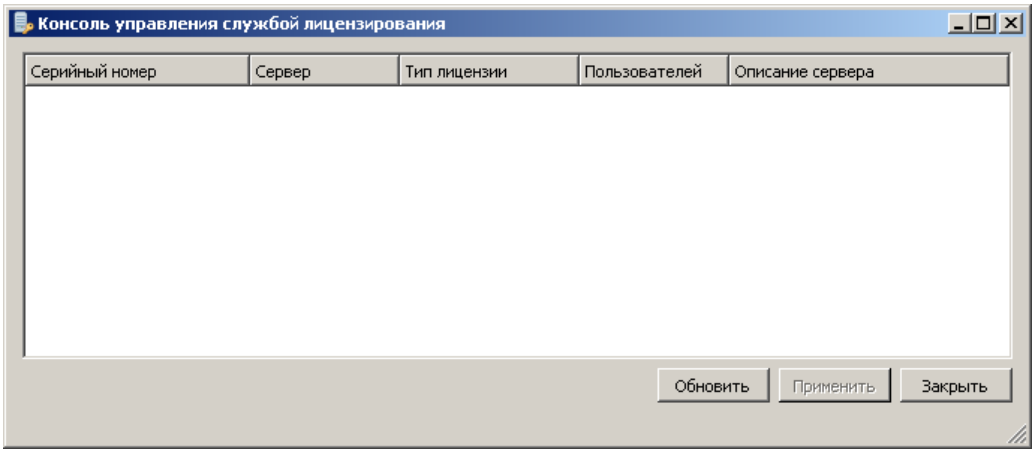


Рисунок 3 – Консоль управления службой лицензирования

2. Вставьте токен с лицензией Secret Disk Server и нажмите **Обновить**. В консоли будут отражены все лицензии, имеющиеся на токене.

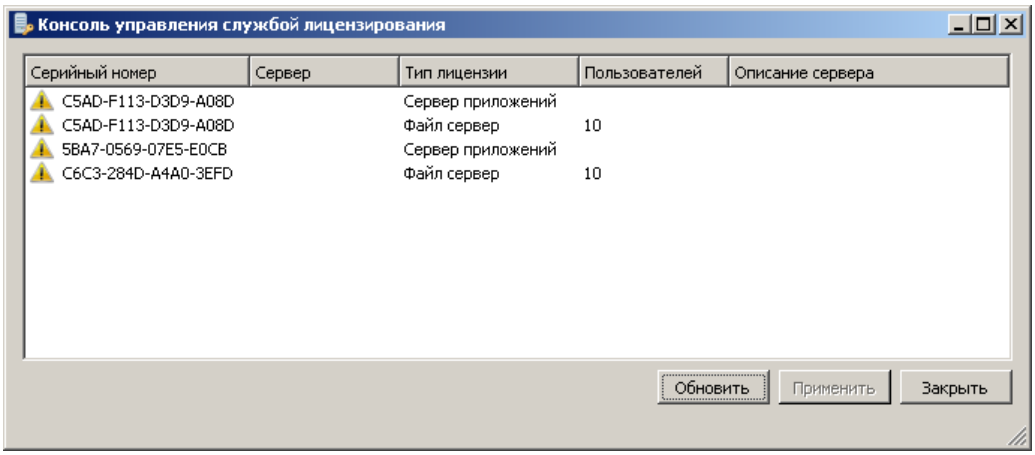


Рисунок 4 – Консоль управления службой лицензирования

3. Выберите лицензию и двойным щелчком мыши откройте ее свойства.

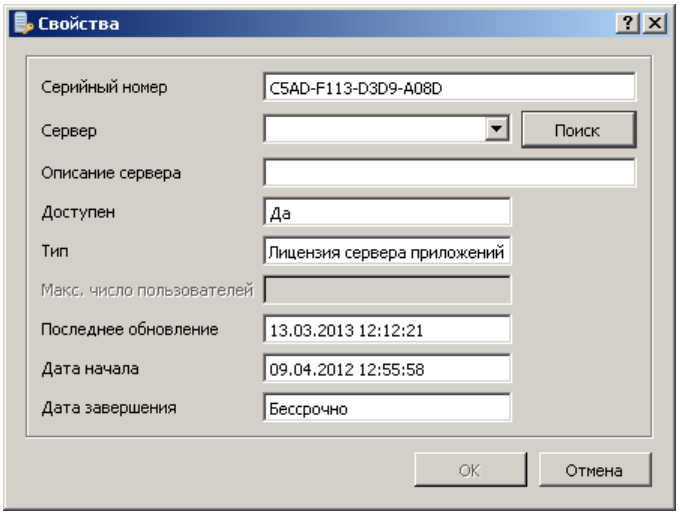


Рисунок 5 – Окно свойств лицензии

4. Чтобы назначить выбранную лицензию серверу нажмите **Поиск**. Будет выполнен поиск серверов в домене.

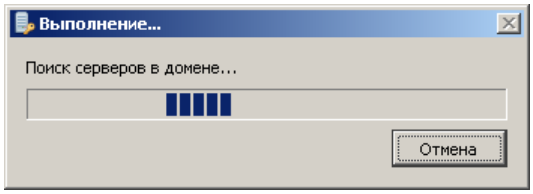


Рисунок 6 – Окно процесса выполнения поиска серверов в домене

5. В поле **Сервер** выберите сервер, которому будет назначена лицензия и нажмите **OK**.

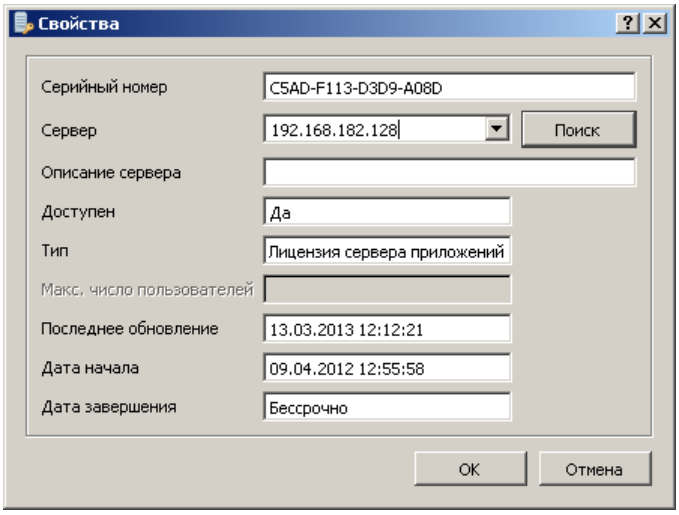


Рисунок 7 – Окно свойств лицензии

6. В консоли управления нажмите **Применить**. Настройка сервиса лицензирования закончена.

По умолчанию сервис лицензирования позволяет работать с серверами и зашифрованными дисками в случае, если токен отключён в течение 7 дней.

Компьютер, на который устанавливается сервис лицензирования, должен работать бесперебойно. В случае его отключения/перезагрузки необходимо подсоединить токен с лицензиями и обновить список лицензий в Консоли администрирования службой лицензирования.

7. Установка консоли управления

Установить консоль управления сервером можно, запустив файл-установщик SDS NG. Консоль администрирования можно установить, либо как самостоятельный компонент, либо как дополнительный.

В первом случае, выбор опции "Консоль администрирования Secret Disk" следует сделать в первом окне установщика (Рисунок 8), во втором случае – в окне выбора дополнительных компонент (Рисунок 9).

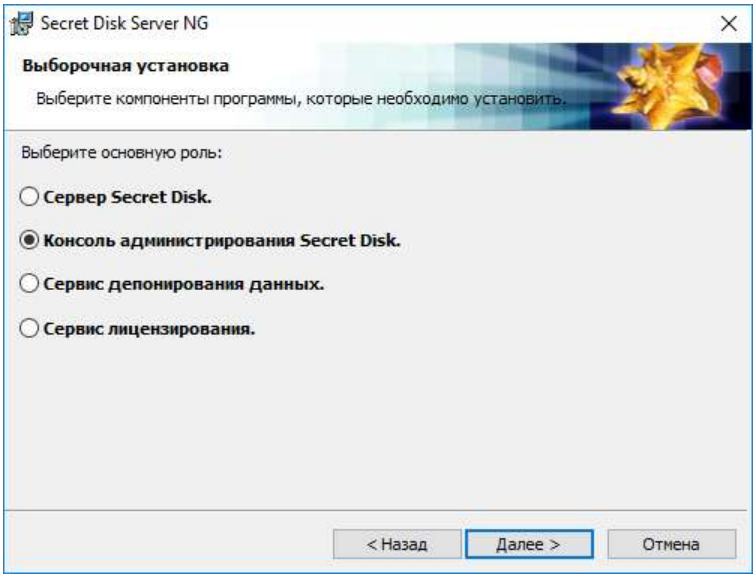


Рисунок 8 – Установка консоли администрирования отдельно

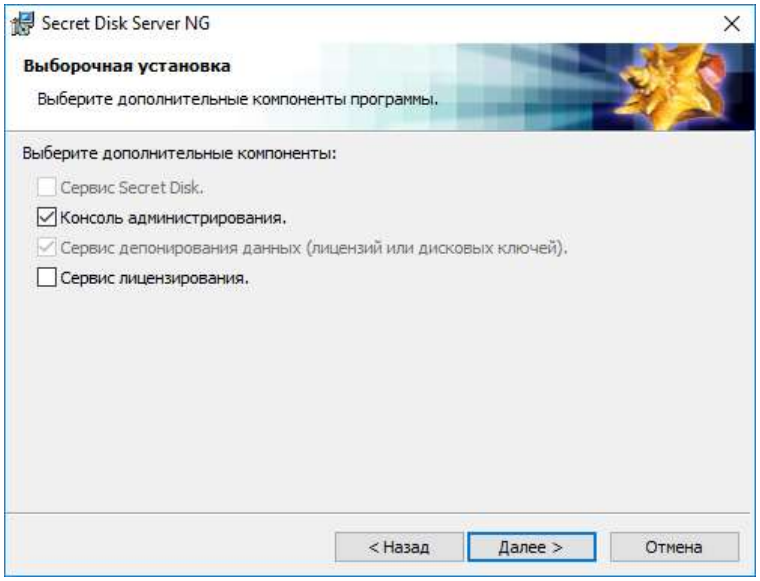


Рисунок 9 – Установка консоли администрирования дополнительно

Консоль администрирования Secret Disk устанавливается как специальное приложение – оснастка – для программы "Консоль управления Microsoft" (Micrsoft Managament Console, – MMC). После установки, оснастку Secret Disk можно добавить в любую консоль MMC, используемую на компьютере.

Также установщик создает новую консоль MMC с названием "Управление компьютером", которая содержит Консоль администрирования Secret Disk и несколько других стандартных оснасток для управления компьютером. Ярлык для запуска этой консоли MMC добавляется в меню запуска приложений "Пуск". Эту консоль можно запустить сразу после завершения установки без предварительной настройки.

7.1 Добавление оснастки

Запустите консоль через проводник, Панель управления или откройте новую консоль командой "mmc". Далее:

1. В меню *Файл* выберите *Добавить или удалить оснастку*.

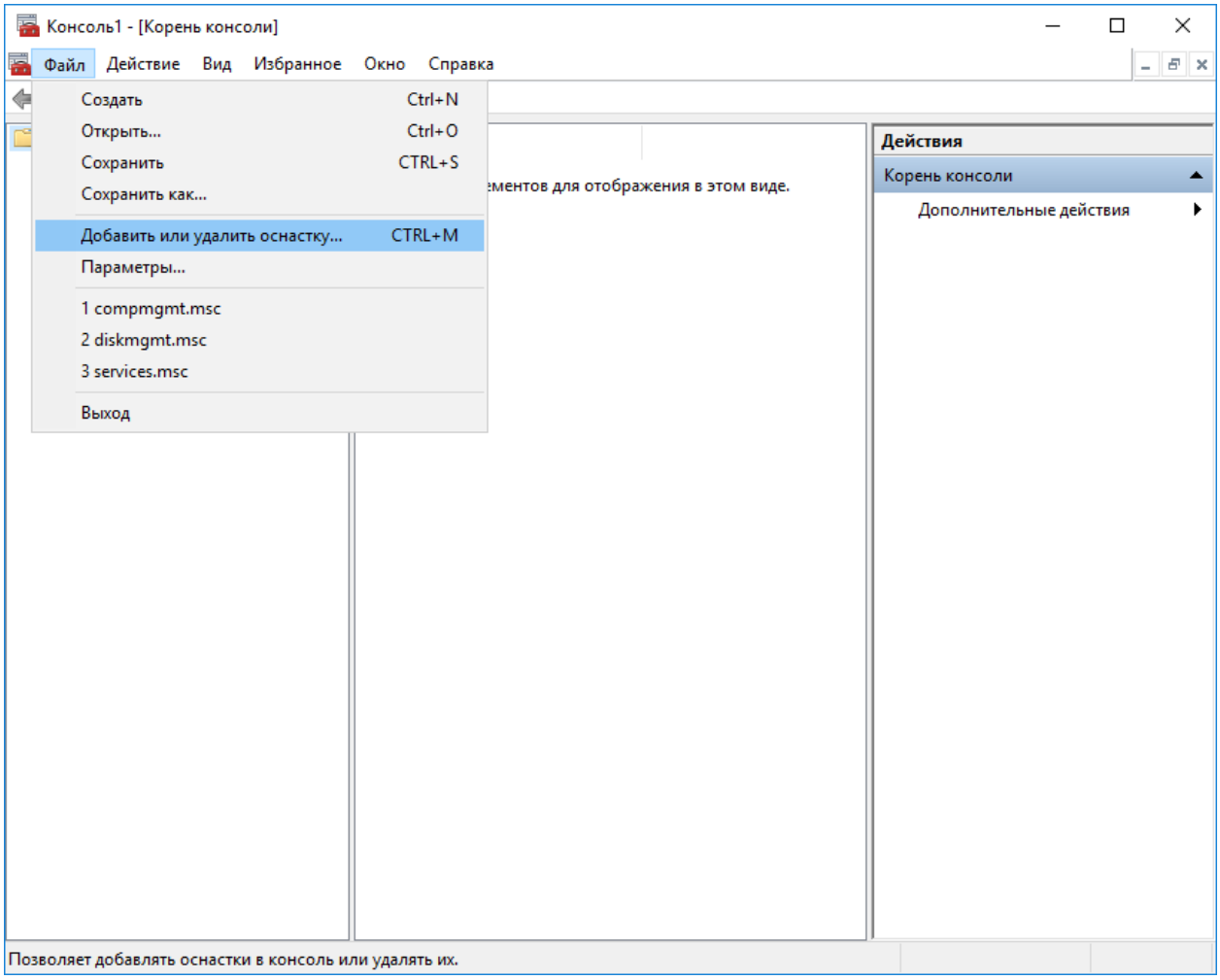


Рисунок 10 – Консоль администрирования

2. В окне **Добавление и удаление оснасток** выберите оснастку **Управление Secret Disk**. Нажмите **Добавить**.
3. На экране появится окно, сообщающее о том, что выполняется поиск доступных серверов.

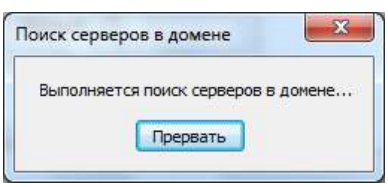


Рисунок 11 – Поиск серверов в домене

4. В окне **Управление Secret Disk Server** нажмите **Готово**.

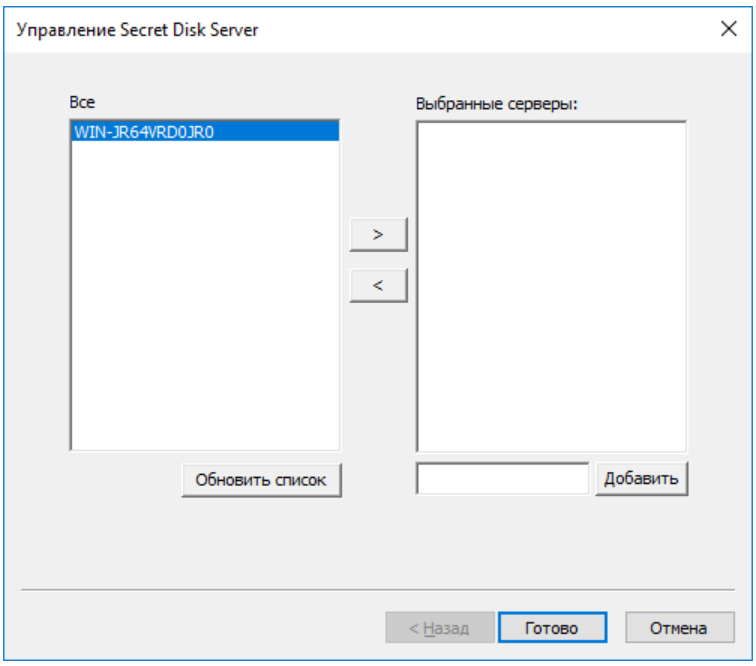


Рисунок 12 – Окно управления SDS

5. В окне **Добавить или удалить оснастку** нажмите **OK**. Нужная оснастка открыта.

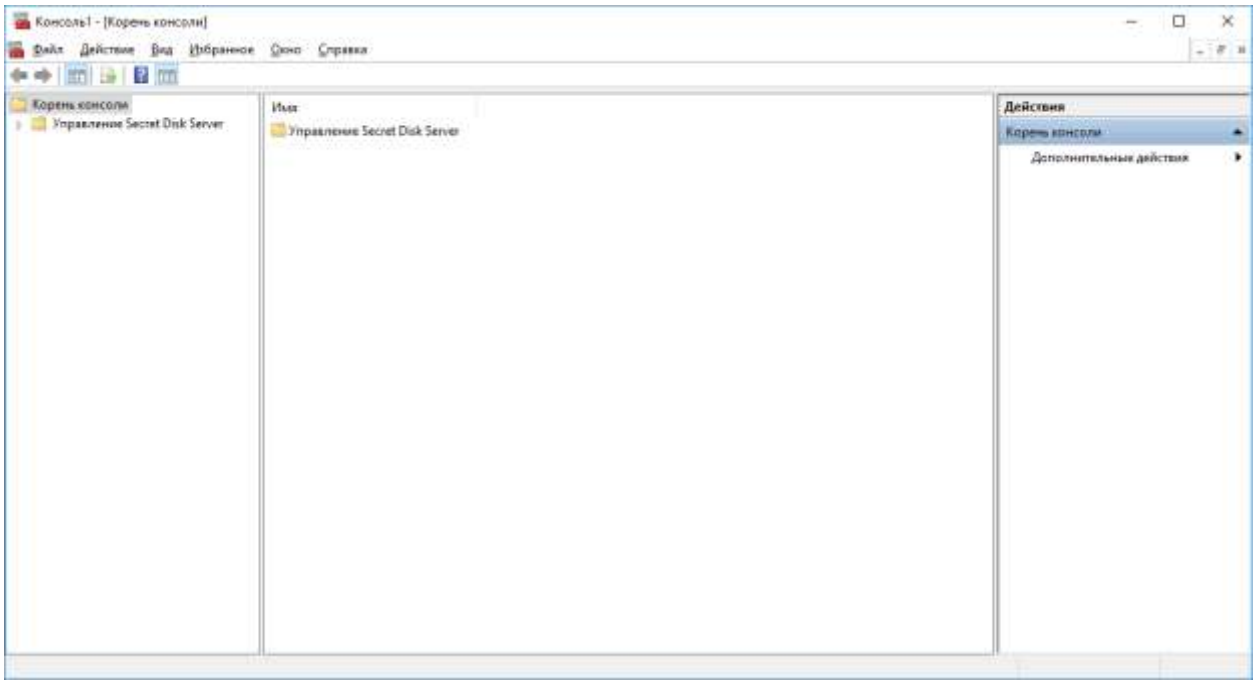


Рисунок 13 – Консоль администрирования

8. Установка SDS на отказоустойчивый кластер

8.1 Особенности

Для каждого узла кластера требуется токен с лицензией сервера. Лицензии, используемые на всех узлах кластера должны быть одного типа:

- файл-сервер;
- сервер приложений либо комбинированная лицензия.

Создание виртуального тома на отказоустойчивом кластере не рекомендуется.

В противном случае диски, зашифрованные на узле с одним типом лицензии, будут недоступны на узле с другим типом лицензии.

При выполнении операции зашифрования, перешифрования или расшифрования на одном из узлов кластера, необходимо довести ее до конца, а затем переходить к другому узлу кластера.

При выполнении операции зашифрования, перешифрования, расшифрования или других действий, которые ведут к изменению хранилища, должны работать все узлы, указанные в конфигураторе DDS.

Процедура восстановления хранилища выполняется на одном узле кластера, затем остальные узлы добавляются в кластер.

8.2 Установка SDS NG в отказоустойчивый кластер

Для корректной работы SDS NG в отказоустойчивом кластере необходимо установить:

- на каждый сервер (кроме контроллера домена) SDS и сервис депонирования данных (DDS);
- на доменный сервер сервис лицензирования (SL) и DDS;
- на рабочую станция администратора Консоль администрирования, DDS.

Рисунок 14 – Архитектура кластера

8.3 Конфигурация кластера

Компонент программы	**Место установки**
Серверный компонент	Узлы кластера
Интерфейс администратора	Рабочая станция администратора
ПО для подачи сигнала "тревога"	Сервер лицензирования

9. Сервис депонирования лицензий и ключей

9.1 Установка сервиса DDS

Установка службы DDS может производится несколькими способами. Установочный файл включен в дистрибутив SDS NG.

Для установки службы DDS выполните следующие действия:

1. Запустите файл-установщик SDS NG (sds-3.x.y.z-ru-x64.exe – для 64-битной системы или sds-3.x.y.z-ru-x86.exe – для 86-битной системы).
2. Нажмите **Далее >**.

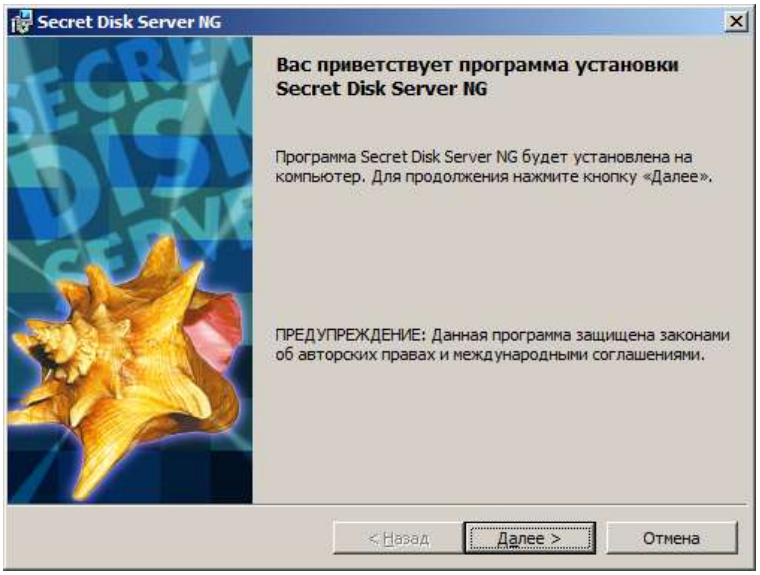


Рисунок 15 – Мастер установки программы

3. Прочитайте условия лицензионного соглашения. Выберите **Я принимаю условия лицензионного соглашения**, нажмите **Далее >**.

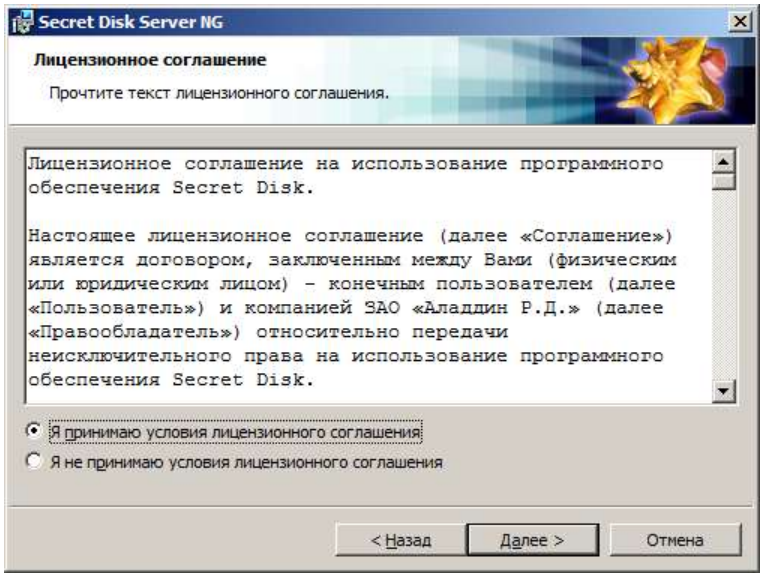


Рисунок 16 – Лицензионное соглашение установки SDS NG

4. Выберите папку для установки программы.

По умолчанию папка назначения **C:\Program Files\Secret Disk\Server**.
Нажмите **Далее >**.

5. Выберите пункт **Сервис депонирования данных** и нажмите **Далее >**.

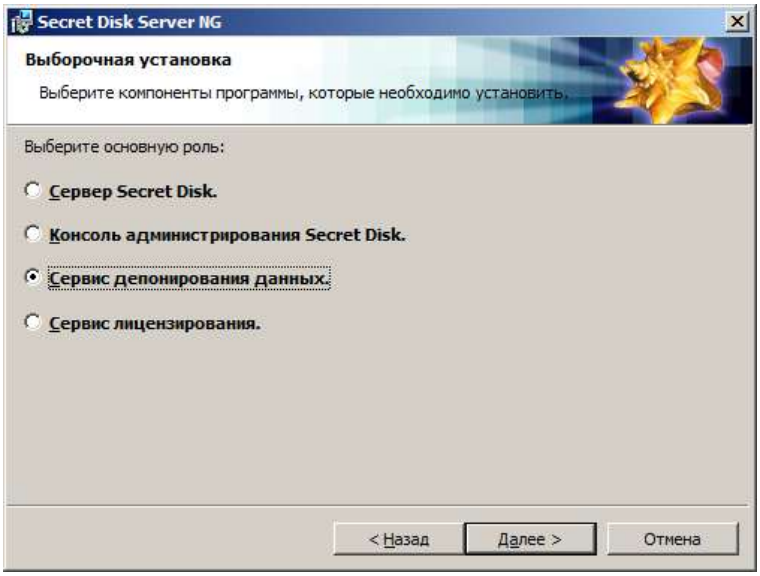


Рисунок 17 – Установка необходимого компонента программы

6. При необходимости выберите консоль администрирования и сервис лицензирования. Нажмите **Далее >**.

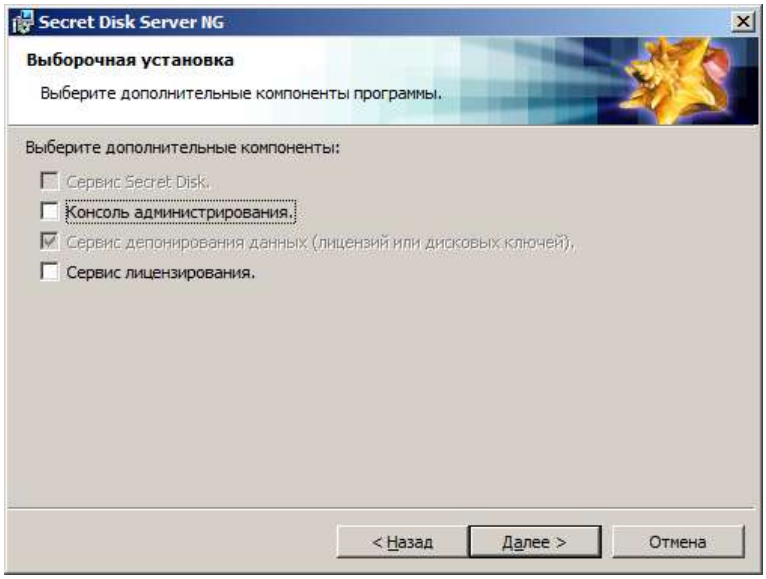


Рисунок 18 – Установка дополнительных компонентов программы

7. При необходимости выберите пункт **Выводить сообщения Secret Disk Server NG** в журнал событий и нажмите **Установить**.

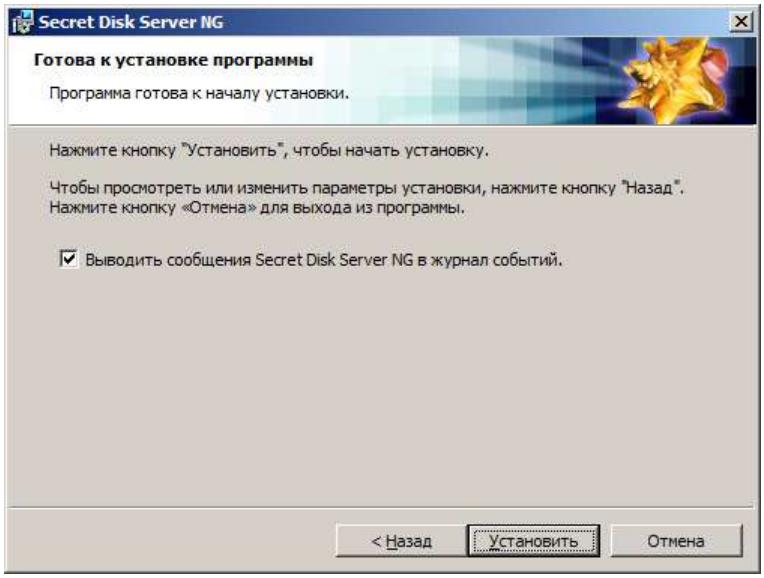


Рисунок 19 – Окно уведомления о готовности к установке программы

8. Дождитесь окончания процесса установки сервиса депонирования данных.

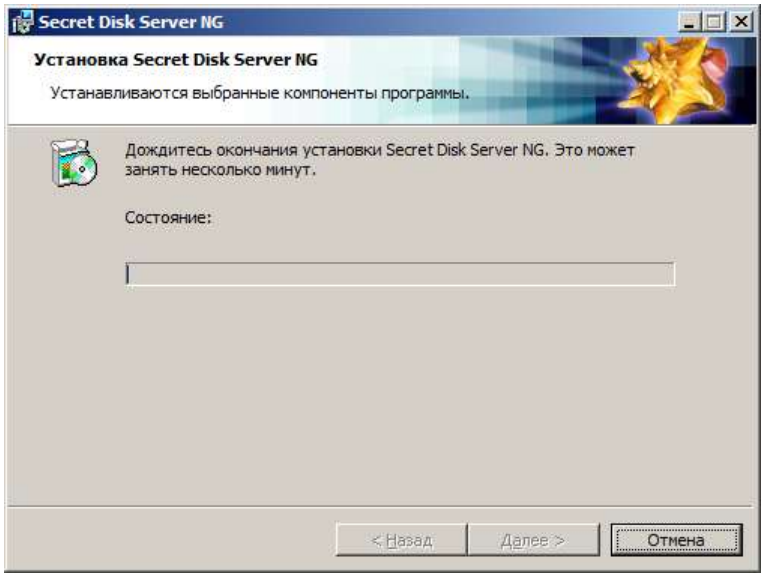


Рисунок 20 – Окно состояния установки программы

9. Нажмите **Готово**.

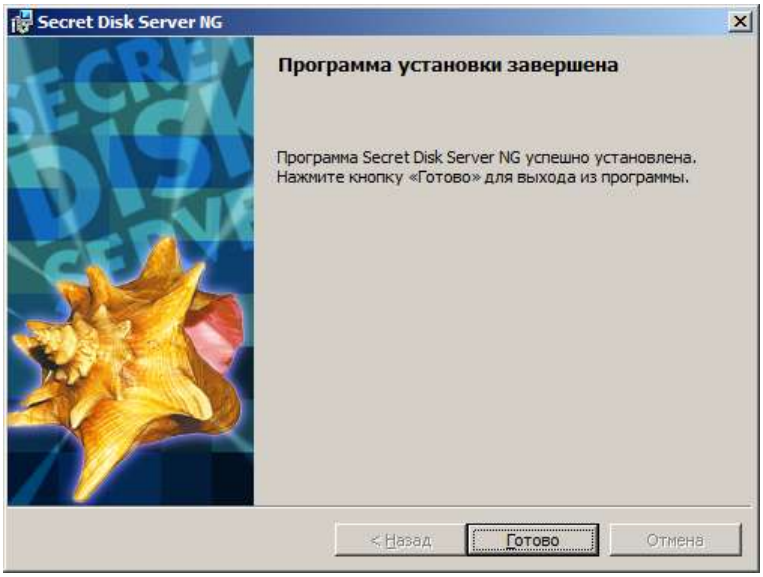


Рисунок 21 – Окно уведомления о завершении установки программы

9.2 Выбор типа соединения

9.2.1 Windows Authentication

Простой в использовании метод аутентификации серверов депонирования. Позволяет с минимальным числом настроек запустить сеть депонирования данных в организации с применением метода аутентификации Windows "по умолчанию".

9.2.2 Security Channel

Метод аутентификации с точной настройкой аутентификации серверов депонирования. Позволяет определить конкретный сертификат рабочих станции, применяемый для аутентификации, и гарантирует организацию защищенного канала между узлами депонирования по средствам выбранных сертификатов.

В качестве сертификатов рабочих станций могут быть выбраны сертификаты ГОСТ, сгенерированные доверенным УЦ. Для этого требуется установка и настройка УЦ сторонних поставщиков ГОСТ сертификатов: КриптоПРО или VipNET.

9.3 Настройка DDS для депонирования ключей в кластере

Для настройки депонирования лицензий необходимо установить сервис лицензирования.

Для настройки DDS выполните следующие действия:

1. Откройте службу **Data Distribution → Консоль управления службой Data Distribution**.

2. Нажмите **Добавить**.

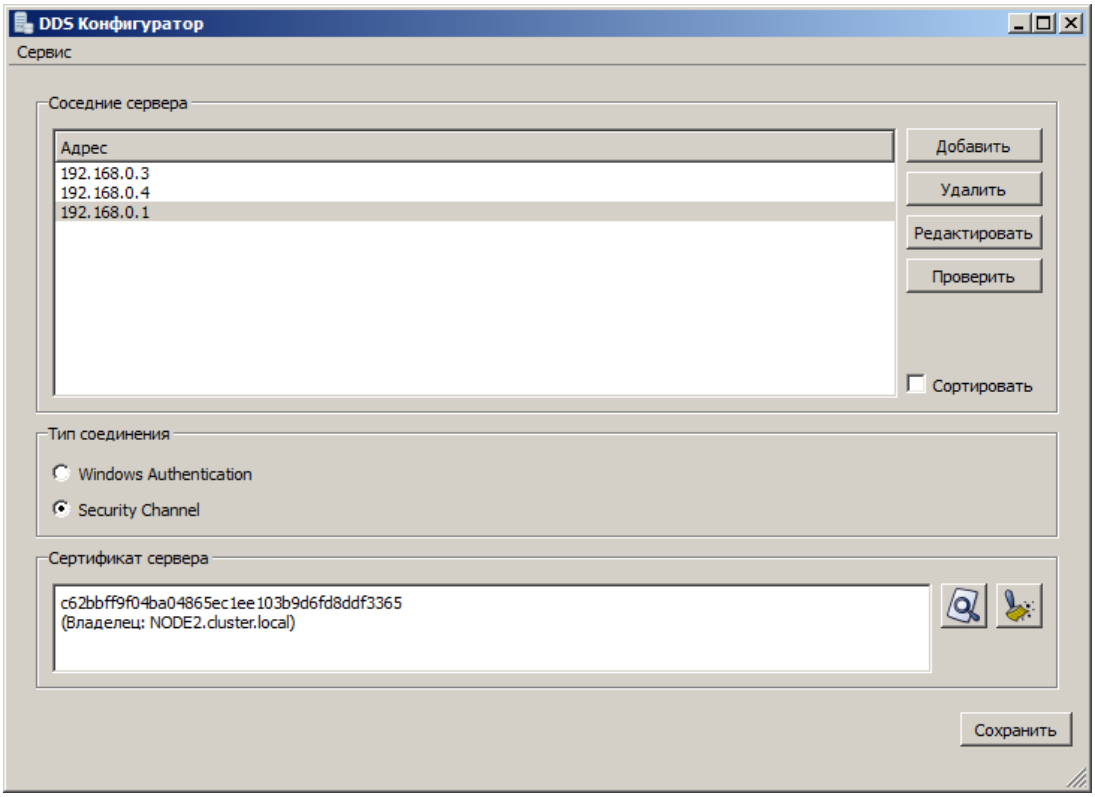


Рисунок 22 – DDS Конфигуратор

3. Введите адрес сервера (рабочей станции). Нажмите **Сохранить**.

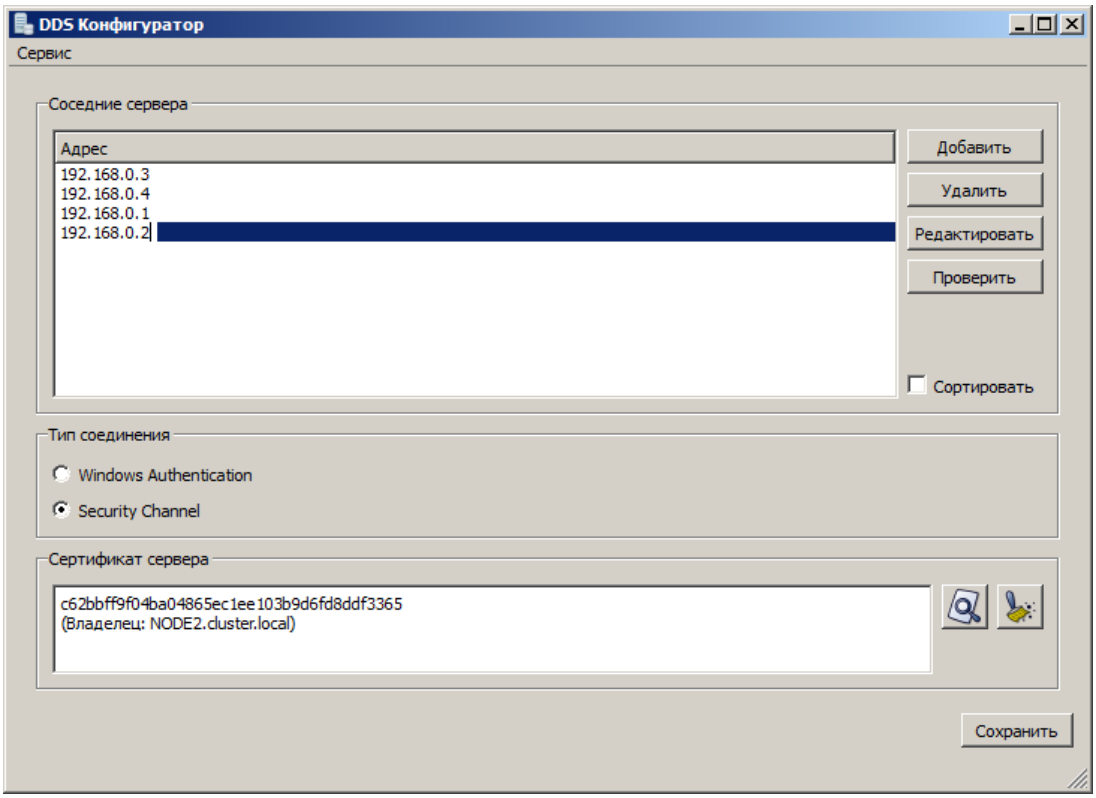


Рисунок 23 – DDS Конфигуратор

4. Перезапустите **Сервис**.

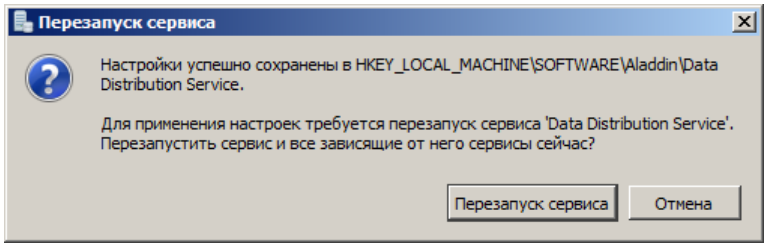


Рисунок 24 – Окно перезапуска сервиса

5. Для проверки работоспособности подключенного сервера (компьютера) выберите добавленный адрес сервера и нажмите **Проверить**.

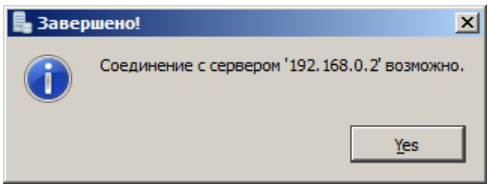


Рисунок 25 – Окно уведомления об успешном соединении с сервером

10. Сигнал "тревога" и отключение сервера

10.1 Описание и особенности

В качестве рабочей станции для подачи сигнала "тревога" может выступать любой компьютер с сетевым доступом к SDS NG. На этот компьютер устанавливается дополнительная утилита для систем контроля и управления доступом (СКУД), а сам компьютер не включается в состав домена Windows (чтобы исключить доступ с него к ресурсам сети организации).

10.2 Установка

Для установки "тревожной кнопки" выполните следующие действия:

1. Запустите программу Alarm-4.x.y.z.msi.
2. Нажмите **Установить**.

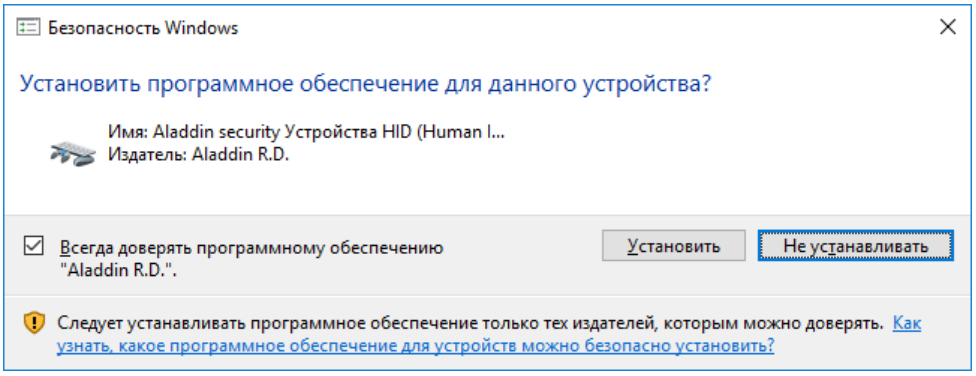


Рисунок 26 – Окно установки программы

3. Нажмите **Далее**.

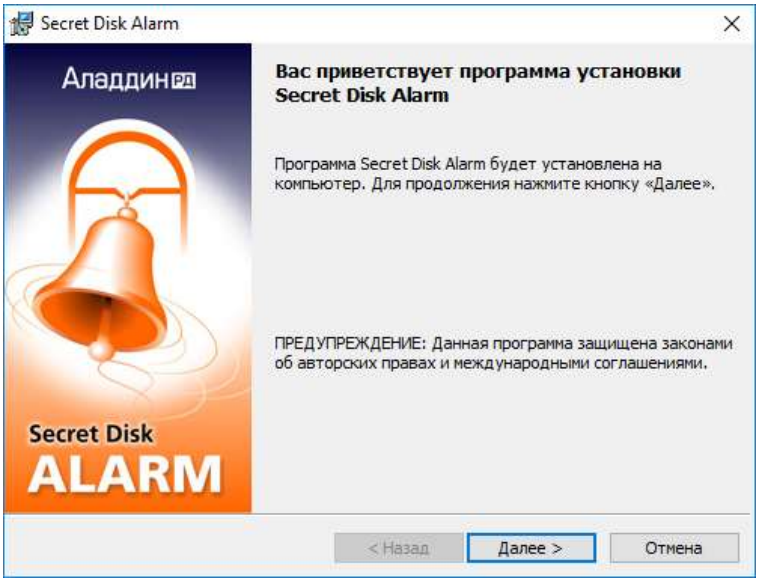


Рисунок 27 – Окно приветствия программы установки

4. Прочитайте условия лицензионного соглашения. Выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.

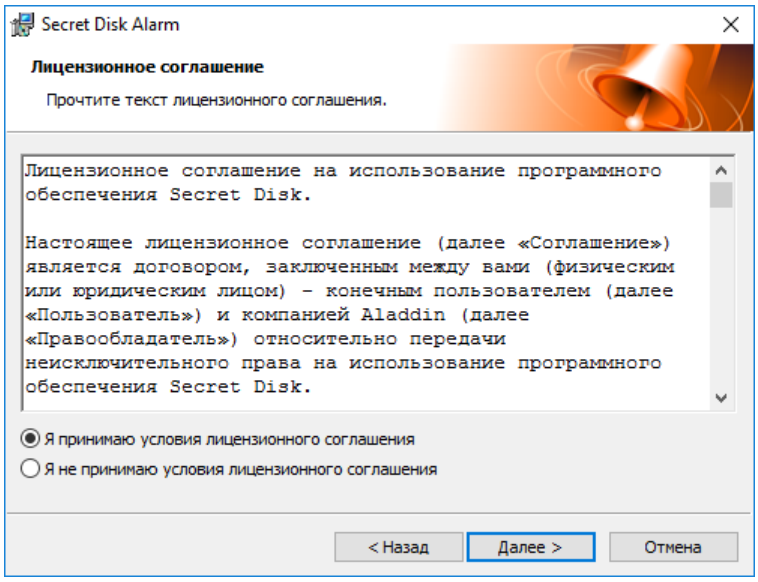


Рисунок 28 – Окно лицензионного соглашения

5. Выберите папку для установки программы. Нажмите **Далее**.

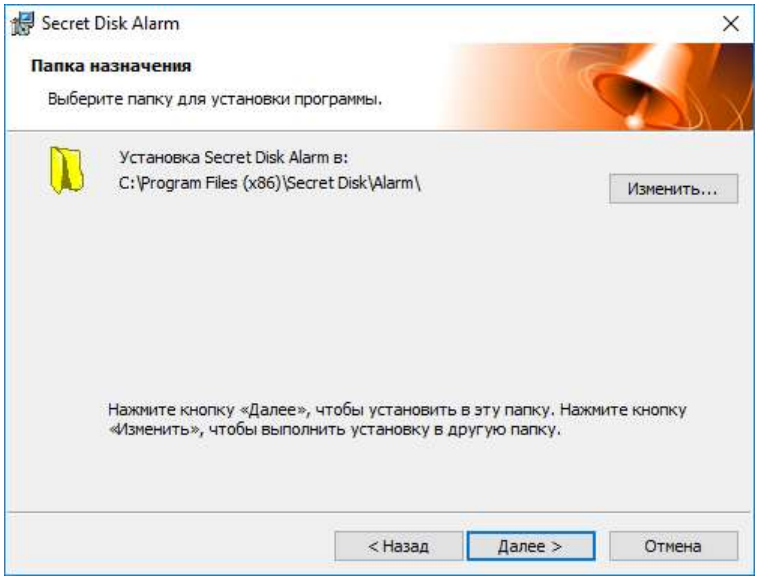


Рисунок 29 – Окно выбора папки установки программы

6. Нажмите **Установить**.

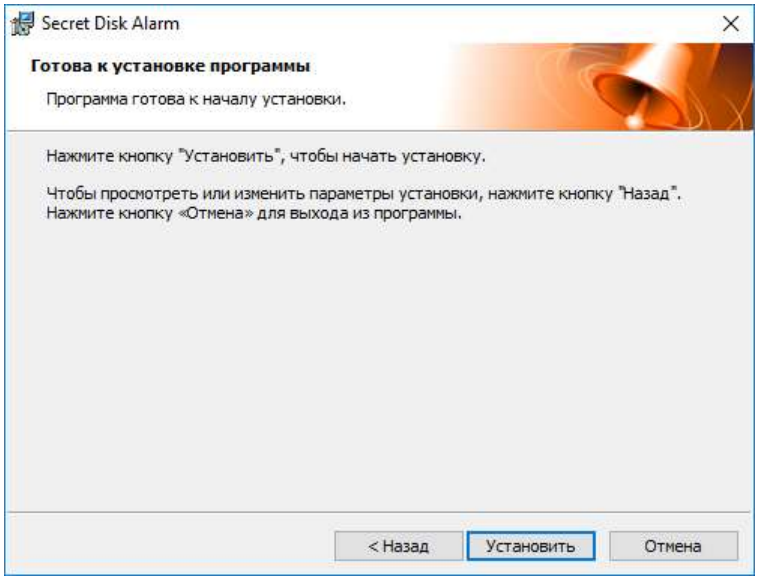


Рисунок 30 – Окно готовности программы к установке

7. Дождитесь окончания установки программы.

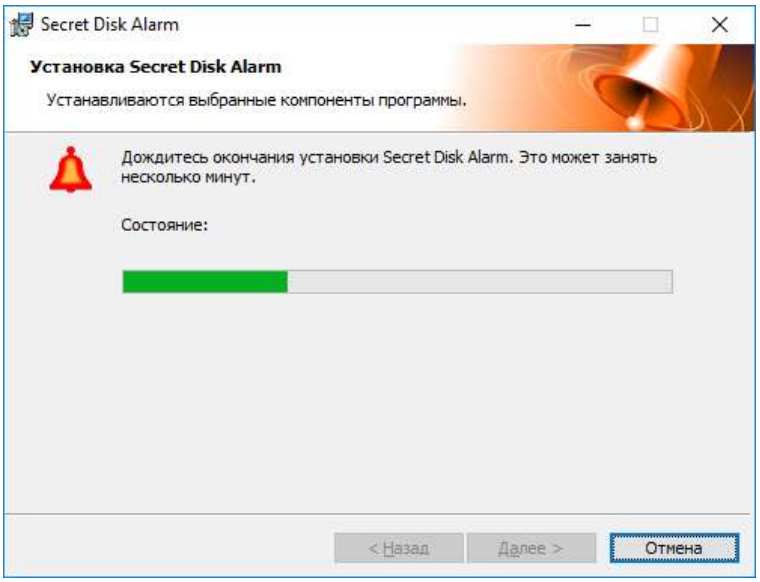


Рисунок 31 – Процесс установки программы

8. Нажмите **Готово**.

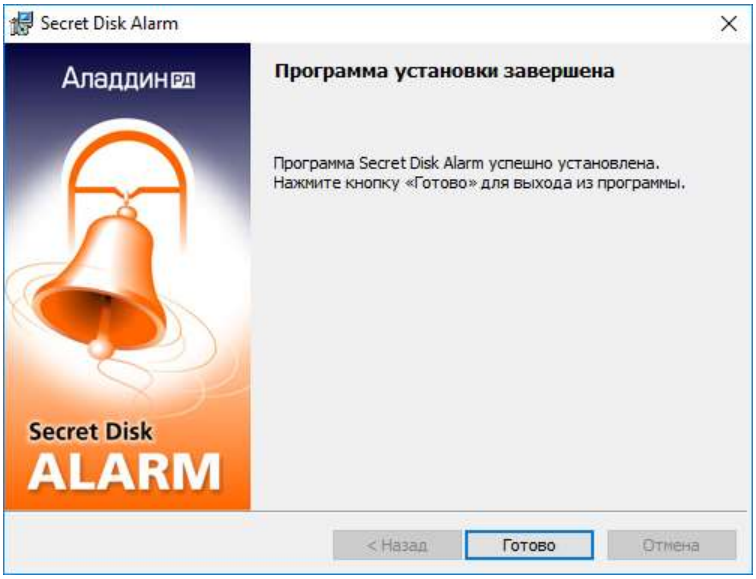


Рисунок 32 – Окно уведомления об успешной установке программы

10.3 Настройка

1. Запустите **Консоль администратора → Серверы**.
2. Нажмите по нужному серверу **правой кнопкой мыши → Настройка сигнала "тревога".**

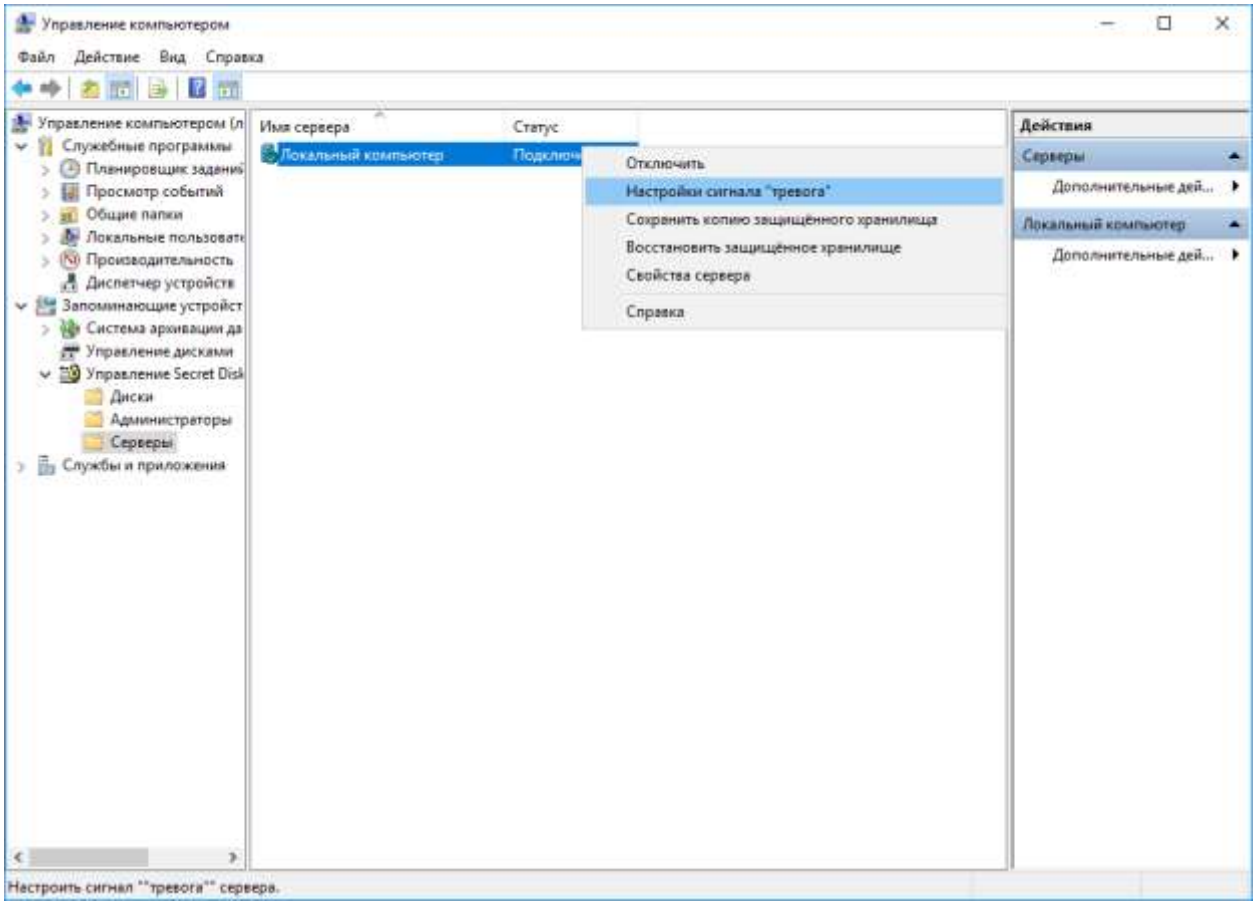


Рисунок 33 – Консоль администрирования

3. Задайте пароль, выберите тип соединения. Нажмите **OK**.

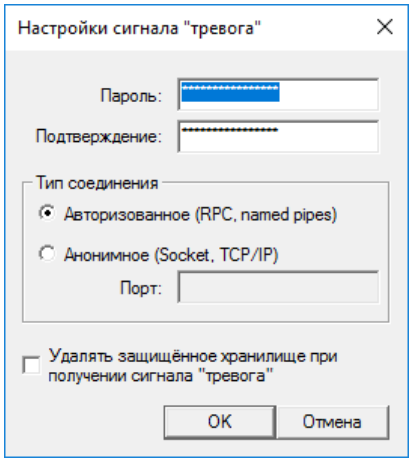


Рисунок 34 – Настройка сигнала "тревога"

> *Авторизованное соединение (RPC, named pipes) гарантирует доставку сигнала "тревога" и обеспечивает защиту при передачи пароля. Работа авторизованного соединения возможна только при наличии домена.*
>
> *Анонимное соединение (Socket, TCP/IP) не требует развернутой инфраструктуры домена, однако не обеспечивает защиту пароля при передачи.*
>
> *Флаг **Удалять защищенное хранилище при получении сигнала "тревога"** необходимо поставить если это требуется.*

10.3.1 Настройка приемника

1. В панели задач нажмите правой кнопкой мыши по значку утилиты **"Тревога"** и выберите **Настройки приемников**.

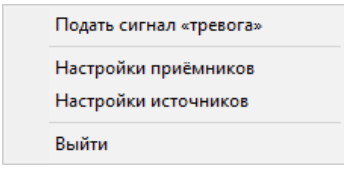


Рисунок 35 – Настройки сигнала "тревога"

2. Нажмите **Добавить**...

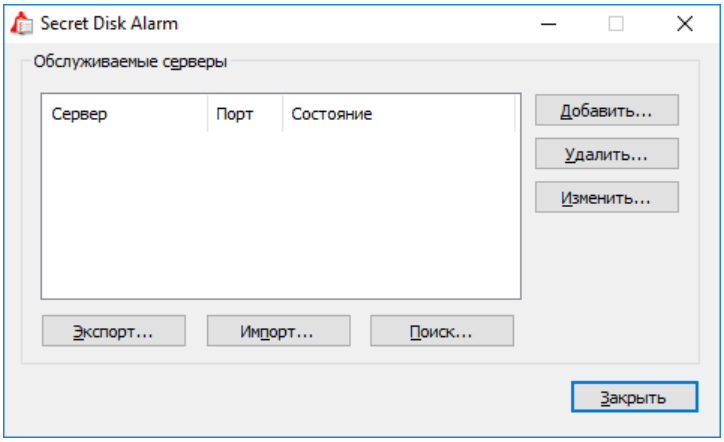


Рисунок 36 – Окно настройки приемника

3. Введите адрес сервера и пароль, заданный ранее. Выберите тип соединения. Нажмите **Сохранить**.

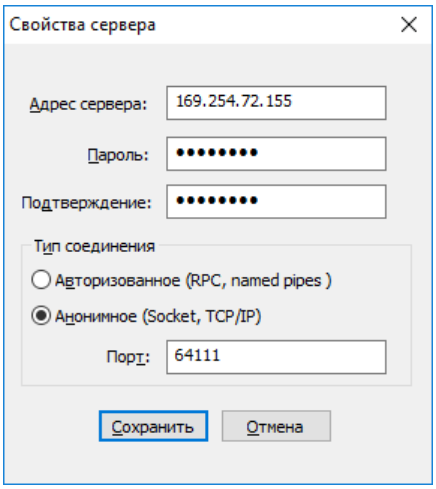


Рисунок 37 – Окно свойств сервера

4. Нажмите **Закрыть**.

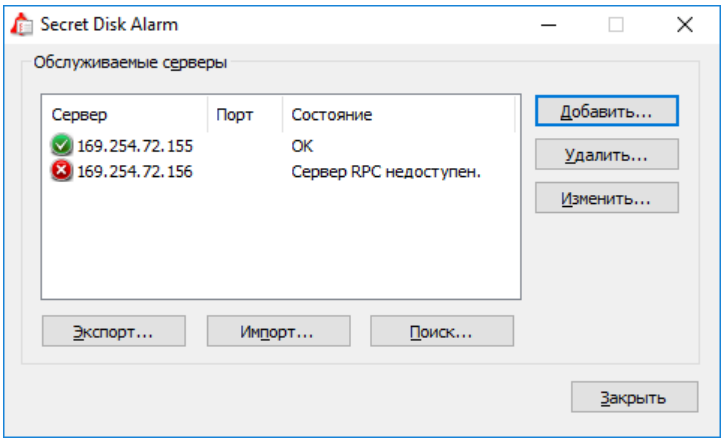


Рисунок 38 – Окно настройки приемника

10.3.2 Настройка источников

Подключите все устройства, входящие в комплект.

1. В панели задач нажмите правой кнопкой мыши по значку утилиты "Тревога" и выберите **Настройки источников**.

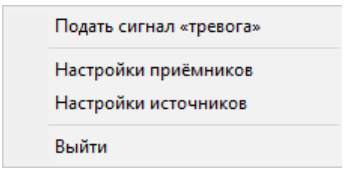


Рисунок 39 – Настройка сигнала "тревога"

2. Нажмите **Добавить**.

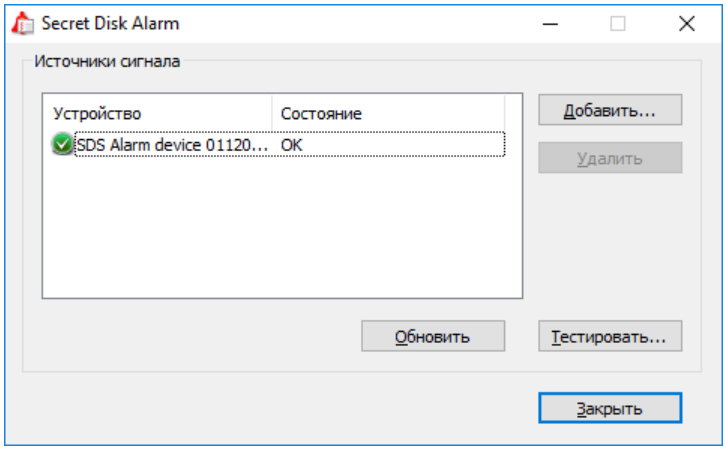


Рисунок 40 – Окно настройки источника

3. Выберите устройство.

Если устройство не подключено, то появится ошибка с уведомлением.

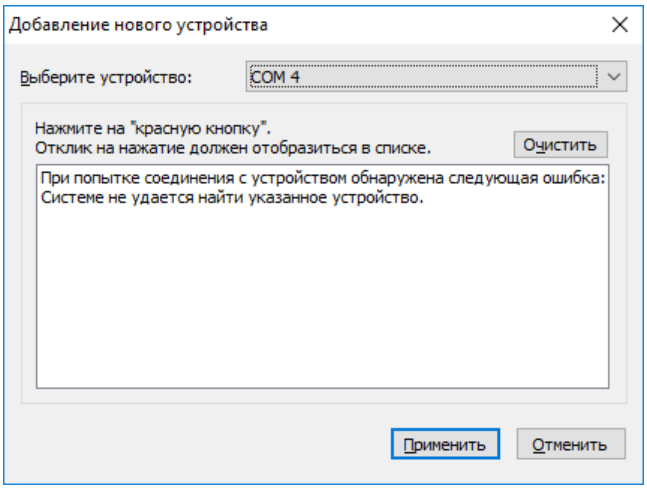


Рисунок 41 – Добавление нового устройства

Если устройство подключено и доступно, то появится уведомление об успешном добавлении.

4. Нажмите **Применить**.

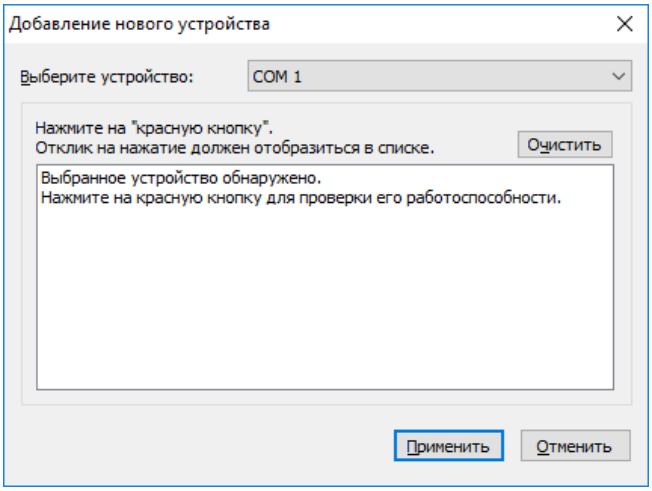


Рисунок 42 – Добавление нового устройства

5. Для проверки работоспособности "красной кнопки" нажмите **Тестировать**.

11. Управление SDS

11.1 Работа сервера

Сервер запускается автоматически, как служба с именем Secret Disk.

После запуска сервера все защищённые диски отключены и их необходимо подключить. Подключение дисков возможно с помощью консоли администратора. Каждый работающий экземпляр SDS должен быть подключен к своему серверному токену с лицензией сервера.

Серверный токен с лицензией сервера может быть подключен прямо к серверу или с другого компьютера с помощью Сервиса Лицензирования.

При подключении и отключении дисков в SDS можно настроить выполнение сценариев, назначенных администратором сценариев.

Защищенные диски SDS отключаются при получении сигнала "тревога". Повторное подключение защищенных дисков может сделать только администратор.

11.2 Удаленное подключение к серверу

SDS NG позволяет в одной оснастке одновременно управлять подключениями к другим серверам, а также выполнять прочие административные операции с дисками.

11.3 Установка подключения к локальному серверу

1. Откройте оснастку **Управление Secret Disk Server.**
2. Правой кнопкой мыши нажмите на ветвь **Серверы → Панель управления серверами**.

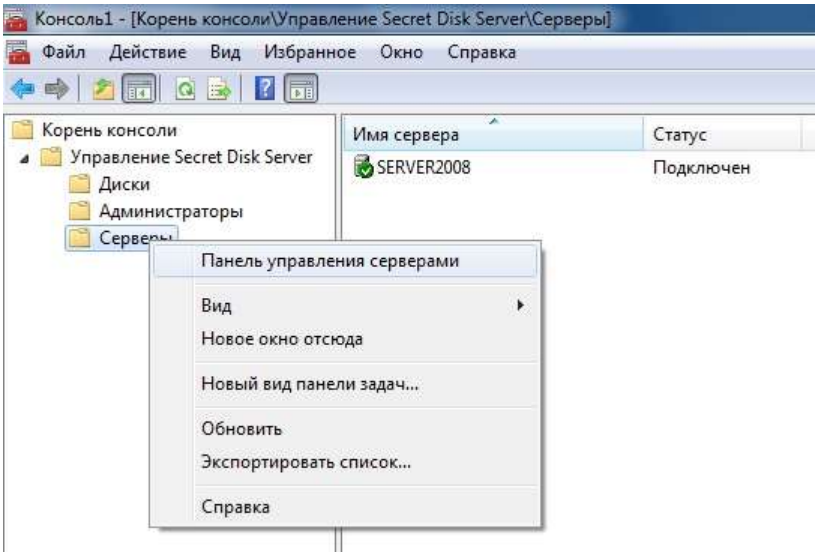


Рисунок 43 – консоль администрирования

3. В Панели управления серверами добавьте нужный сервер из списка слева (>).

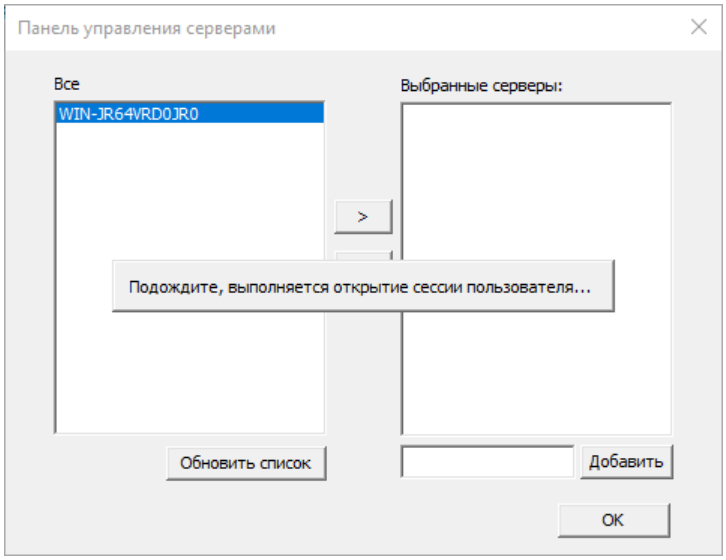
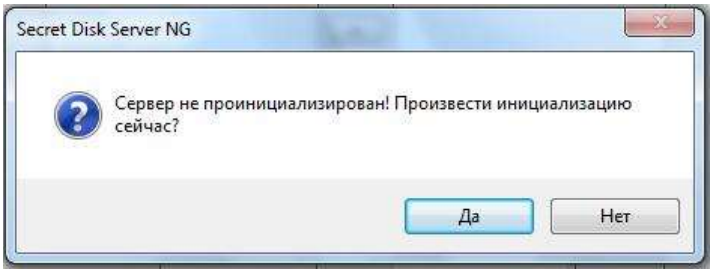


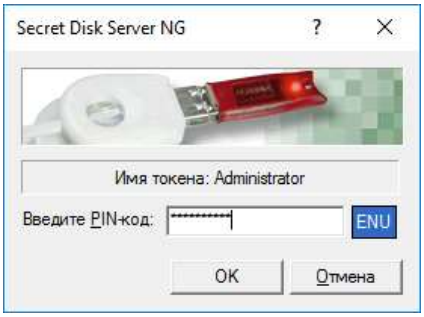
Рисунок 44 – Панель управления серверами

Если контроллер домена недоступен (основной и резервный), то будут недоступны так же все сервера, находящиеся в этом домене.

Если установлен сервис депонирования данных, то приложение предложит проинициализировать сервер.



4. Введите ПИН-код токена администратора и выберите сертификат для аутентификации.



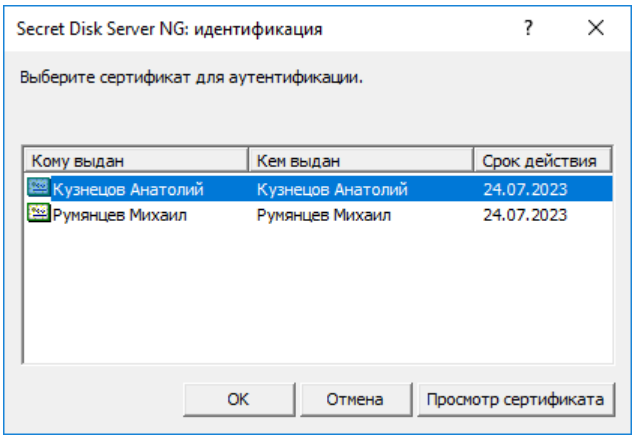


Рисунок 45 – Выбор сертификата администратора

5. Режим работы сервера настроен.
   Доступна функция **Сбросить текущее состояние**.

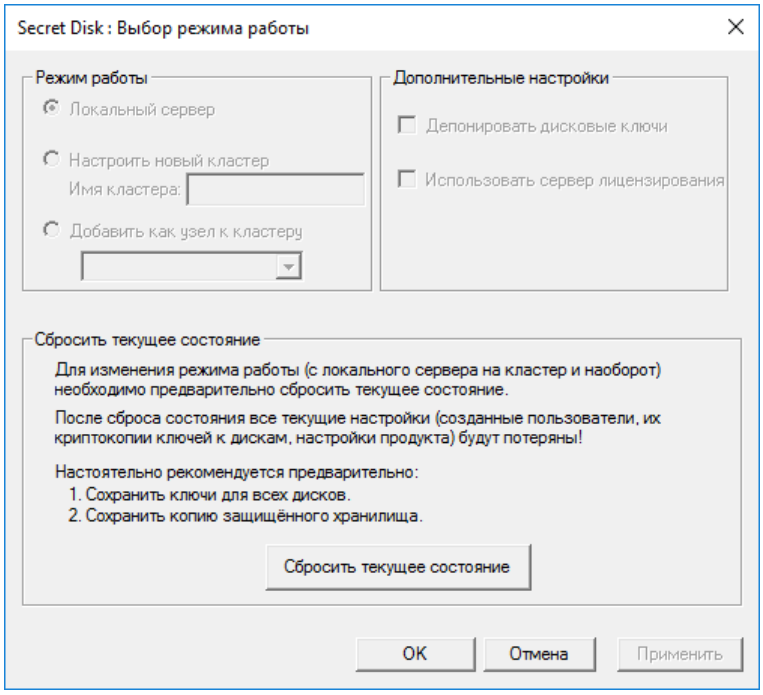
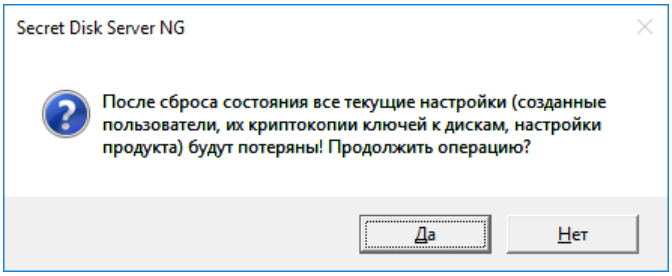


Рисунок 46 – Выбор режима работы

После сброса текущего состояния сервера все настройки будут потеряны (созданные пользователи, криптокопии ключей с дисками, настройки продукта)!!!



11.4 Автоматическое подключение ко всем серверам

После настройки оснастки **Управление Secret Disk Server** при повторном ее запуске будет выполнено автоматическое подключение ко всем добавленным серверам.

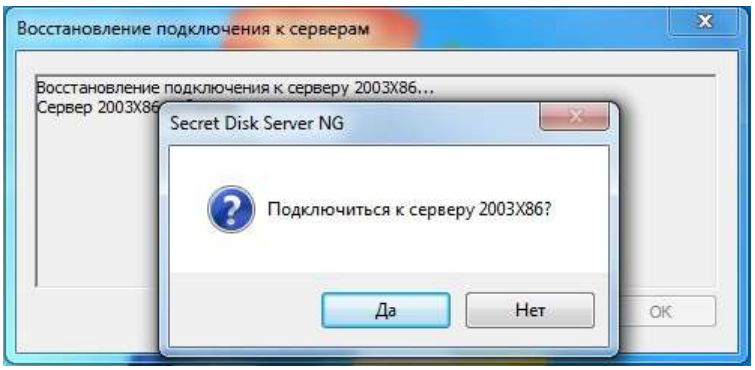


Рисунок 47 – Восстановление подключения к серверам

> *Для подключения к серверу выберите из списка сертификатов сертификат для нужного сервера, хранящихся в памяти токена администратора. Запрос о выборе сертификата будет появляться повторно для каждого сервера, к которому будет выполняться подключение.*

По окончании окно **Восстановление подключения к серверам** будет иметь следующий вид.

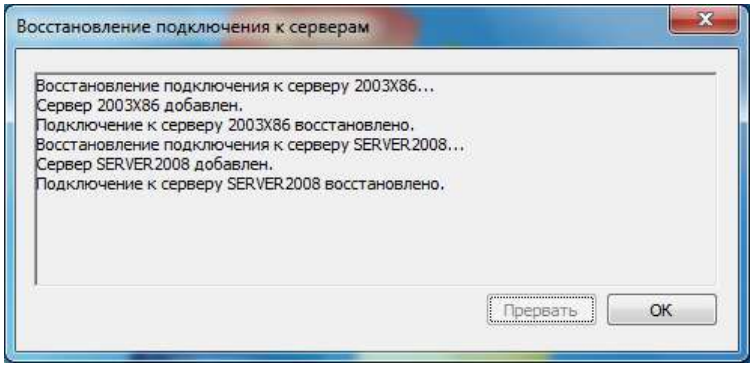


Рисунок 48 – Восстановление подключения к серверам

В списке серверов в оснастке **Управление SDS** появятся выбранные сервера.

11.5 Установка соединения с сервером вручную

Если автоматически установить соединение с сервером не удалось, это можно сделать вручную. Необходимо проверить, чтобы к серверу был подсоединен токен сервера. При использовании сервиса лицензирования проверьте корректность его настройки.

> *К серверу, с которого выполняется подключение, должен быть подсоединен токен администратора.*

Далее необходимо выполнить следующие действия:

1. В оснастке Управление Secret Disk Server раскройте ветвь **Серверы**.
2. Нажмите правой кнопкой мыши на нужный сервер и в контекстном меню выберите пункт **Подключить**.

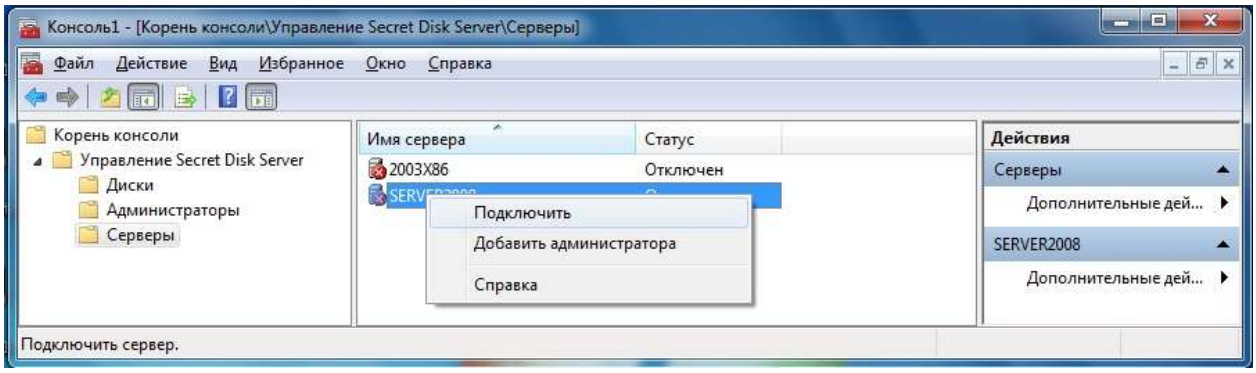


Рисунок 49 – Консоль администрирования

Если для выбранного сервера еще нет ни одной зарегистрированной учетной записи администратора, то будет автоматически предложено создать такую запись.

3. Укажите сертификат администратора, зарегистрированного на сервере, и нажмите **OK**.

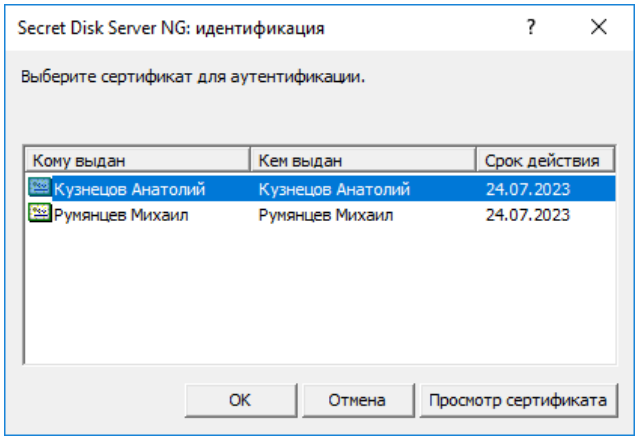


Рисунок 50 – Окно аутентификации

6. Проверьте, чтобы токен администратора, на котором хранится сертификат, был подсоединен, и введите пароль.

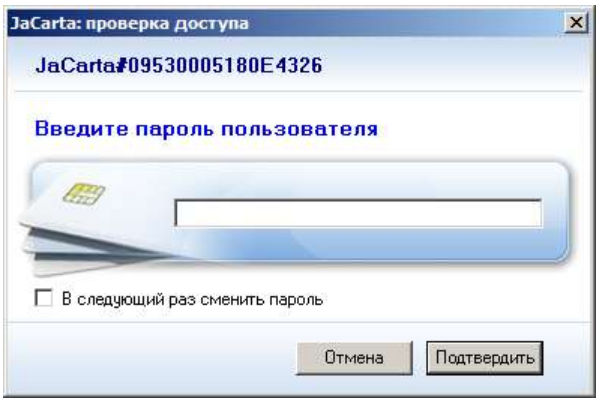


Рисунок 51 – Окно ввода ПИН-кода токена

4. Нажмите кнопку **OK**. После успешной авторизации значок сервера в списке будет иметь следующий вид:

Рисунок 52 – Статус сервера

11.6 Добавление и удаление серверов

Чтобы добавить или удалить сервер из списка серверов в оснастке Управление Secret Disk Server, выполните следующее:

1. Откройте оснастку Управление Secret Disk Server.
2. Раскройте ветвь **Серверы**.
3. Нажмите в свободной области под списком серверов правой кнопкой мыши и в открывшемся контекстном меню выберите пункт **Панель управления серверами**.

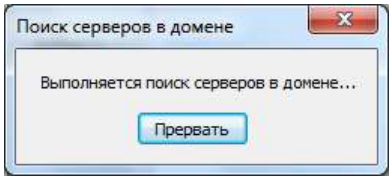


Рисунок 53 – Поиск сервера в домене

4. В панели управления серверами выберите в правом поле сервер, который вы хотите удалить из списка и нажмите кнопку <, чтобы переместить его в список слева.
   Чтобы добавить сервер под управление Secret Disk Server NG, выберите сервер слева и нажмите >.

При добавлении серверов необходимо пройти аутентификацию – выбрать сертификат администратора, убедиться, что токен администратора подключен, и ввести пароль.

5. Нажмите **Готово**.

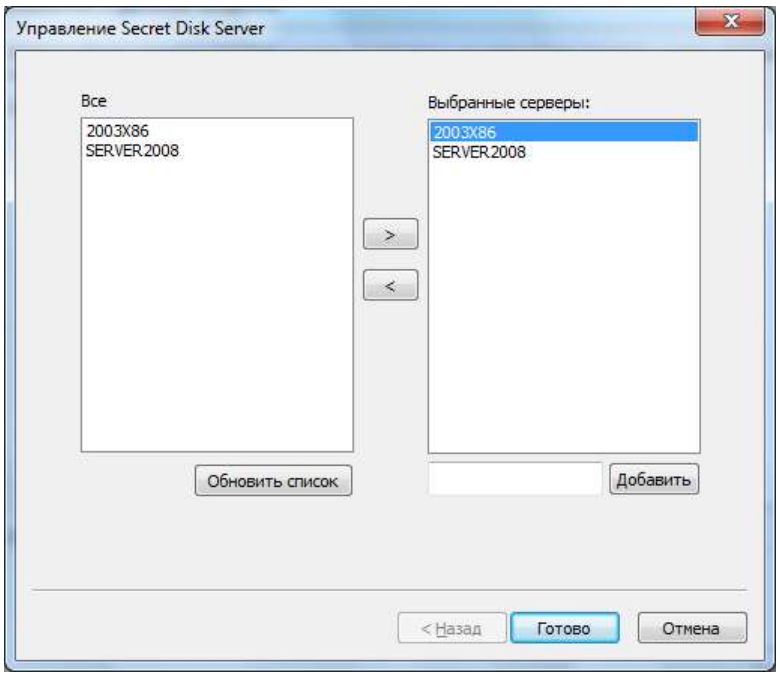
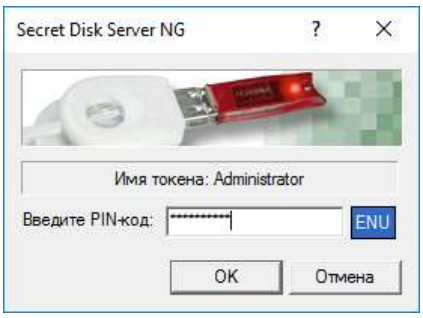


Рисунок 54 – Окно управления серверами SDS

11.7 Консоль администратора SecretDisk

Консоль администратора SDS NG является специальным приложением – оснасткой, запускаемой в системном приложении "Консоль управления компьютером" (MMC).

1. Для начала работы необходимо подключить токены сервера и администратора к компьютеру и ввести их ПИН-коды.



2. Если у администратора сервера несколько сертификатов или несколько администраторов администрируют сервер с одним токеном, то необходимо выбрать нужный сертификат и нажать **OK**.

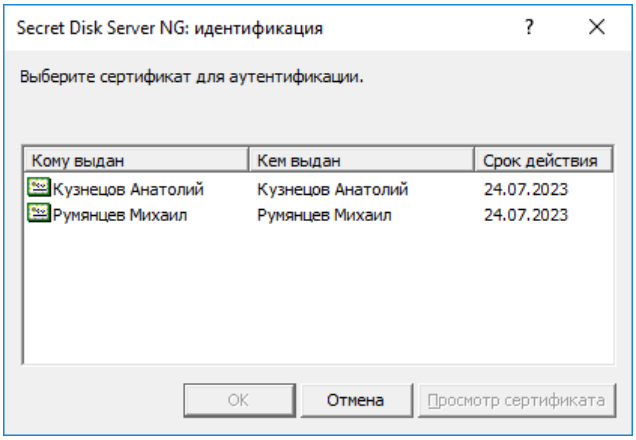


Рисунок 55 – Окно аутентификации

3. Введите повторно ПИН-код токена администратора.

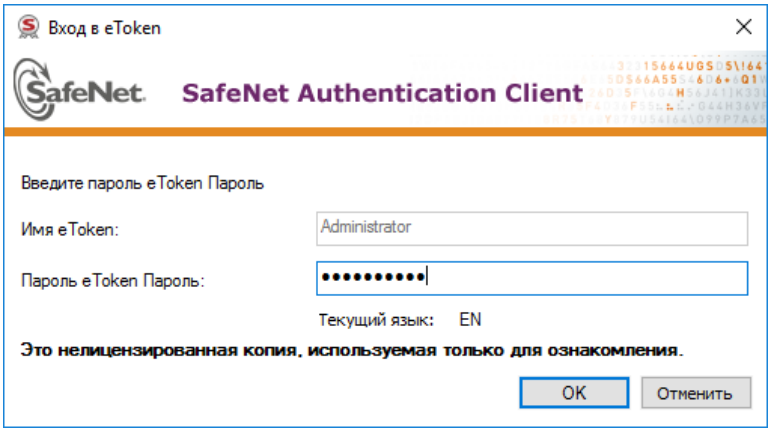


Рисунок 56 – Окно ввода ПИН-кода токена администратора

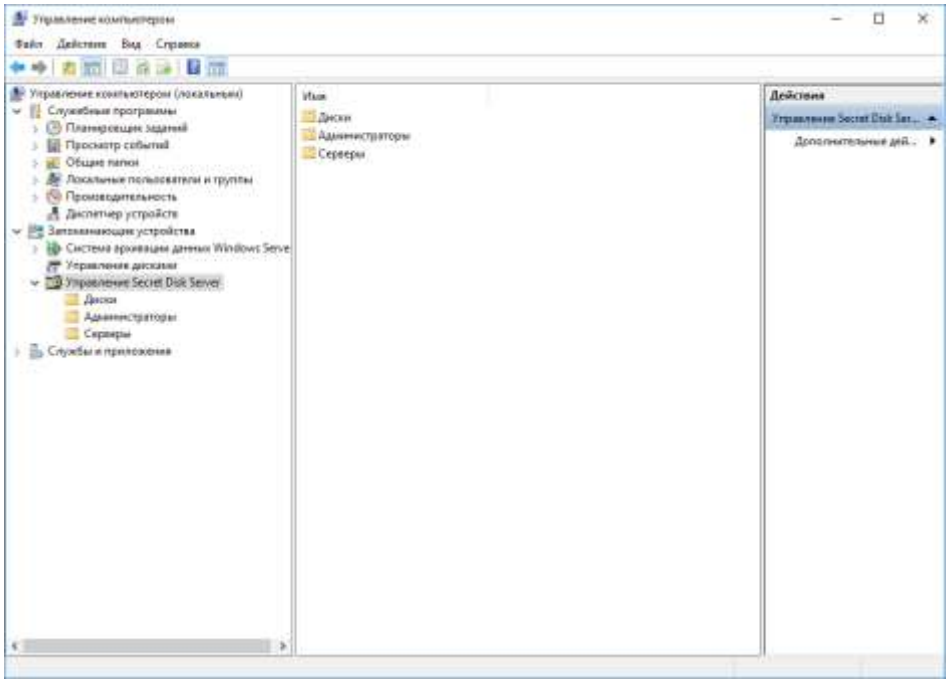


Рисунок 57 – Консоль администрирования

11.8 Регистрация новых администраторов

Администратор сервера может добавлять (регистрировать) новых администраторов и давать другим администраторам право управления защищенными ресурсами. При регистрации нового администратора требуется его токен.

Для регистрации нового администратора сервера выполните следующие действия:

1. В Консоле управления MMC откройте **список администраторов Secret Disk (Управление Secret Disk Server → Администраторы)**.
2. Выберете действие **"Добавить администратора"** в контекстном меню списка администраторов, или в списке доступных действий.

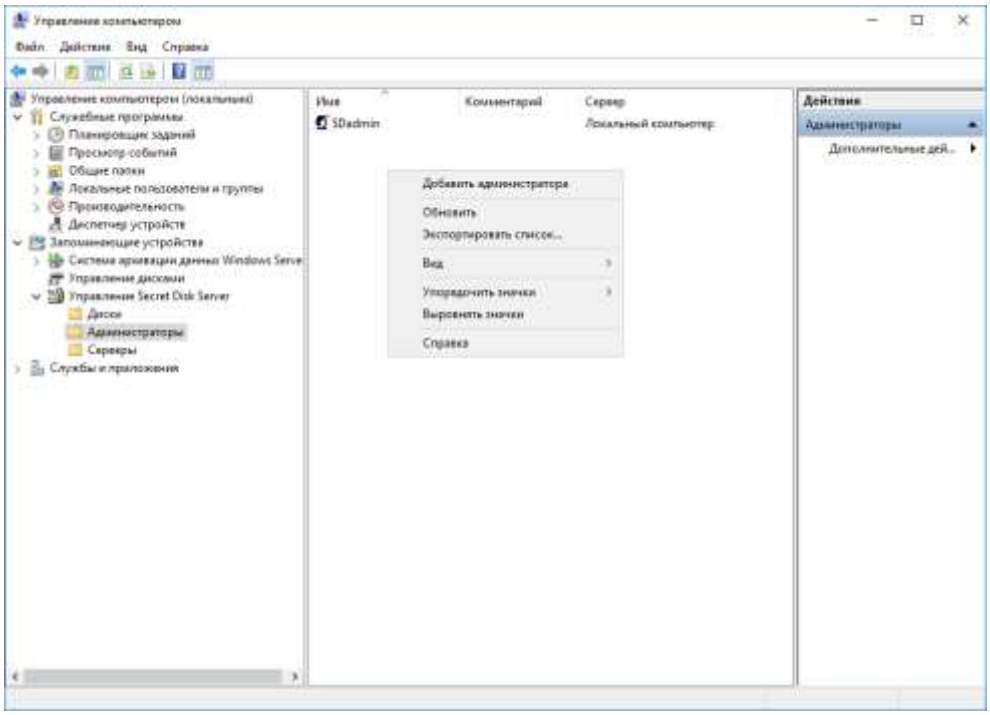


Рисунок 58 – Консоль администрирования

3. В открывшемся окне заполните поля "**Имя администратора**" и "**Комментарий**".

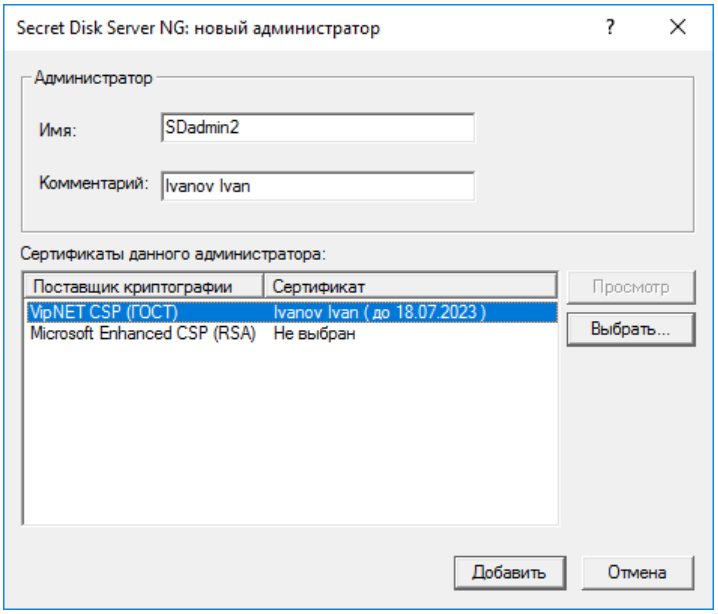


Рисунок 59 – Регистрация нового администратора

4. Подключите токен нового администратора, если он не был подключен раньше, и выберите сертификат для нового администратора из его токена.

У администратора должен быть хотя бы один сертификат.

Нельзя выбрать уже используемый сертификат другим администратором.

Создание сертификата описано в главе Создание сертификата.

5. После выбора сертификата нажмите кнопку "Добавить" для завершения регистрации нового администратора.

6. Если необходимо, добавьте нового администратора в список администраторов защищённых дисков, которыми он будет управлять.

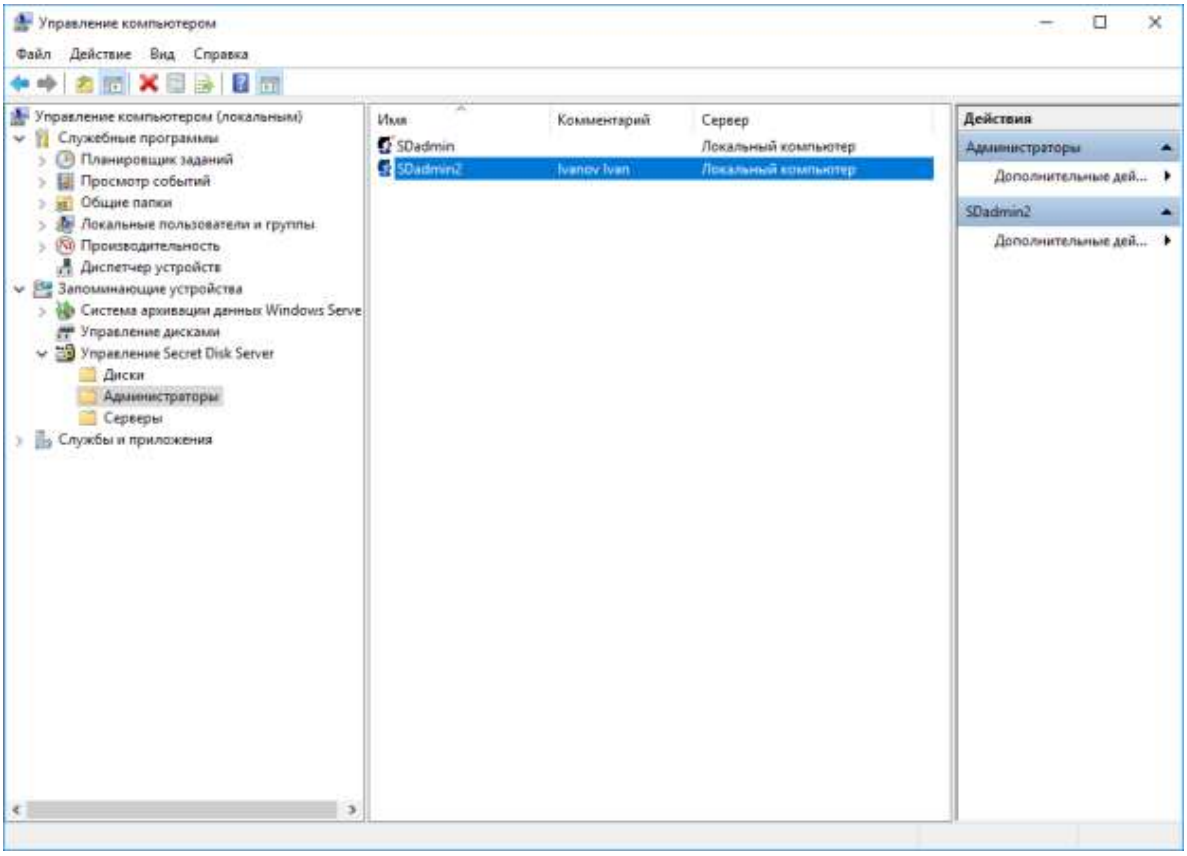


Рисунок 60 – Консоль администрирования

11.9 Сохранение и восстановление копии защищенного хранилища

11.9.1 Сохранение

Защищенное хранилище содержит ключи дисков, регистрационные данные администраторов и настройки защищенных дисков.

Когда защищенное хранилище удаляется в результате нажатия кнопки "тревога", то все настройки стираются и доступ к дискам становится невозможным. При восстановлении защищенного хранилища из резервной копии, все настройки восстанавливаются, кроме настроек сигнала "тревога".

Для сохранения защищенного хранилища выполните следующие действия:

1. Откройте консоль управления сервером (MMC), вкладку Серверы.
2. Выберите нужный сервер → **Сохранить копию защищенного хранилища**.

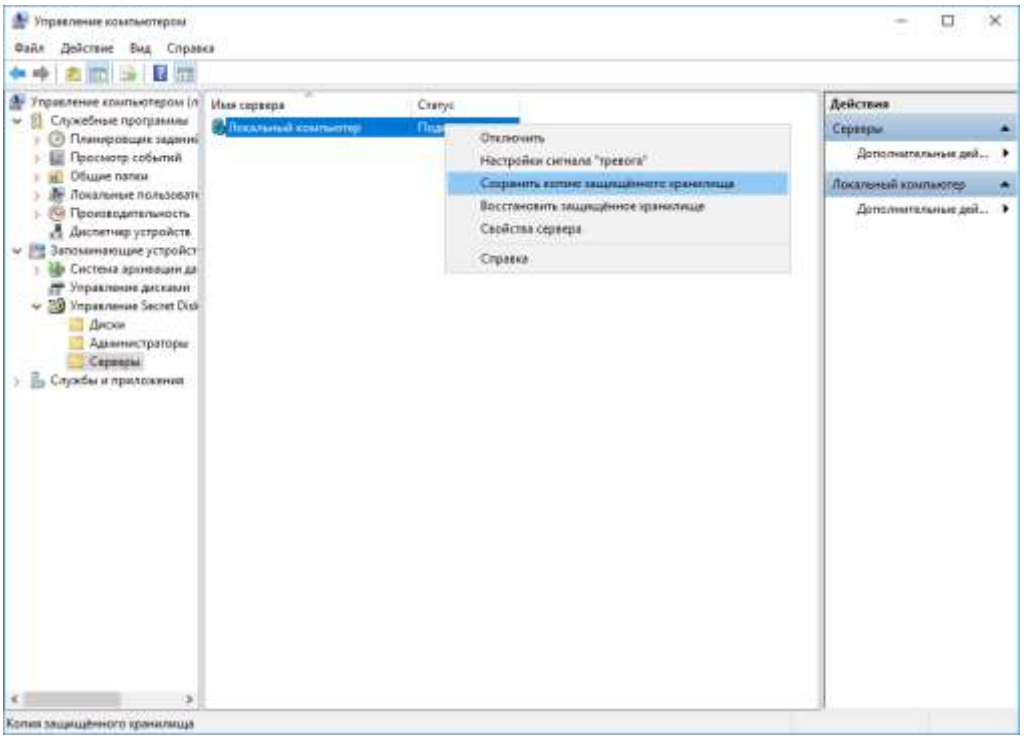


Рисунок 61 – Консоль администрирования

> *Рекомендуется хранить файл с копией защищенного хранилища в выделенном отдельном месте.*

3. Нажмите Сохранить.

11.9.2 Восстановление

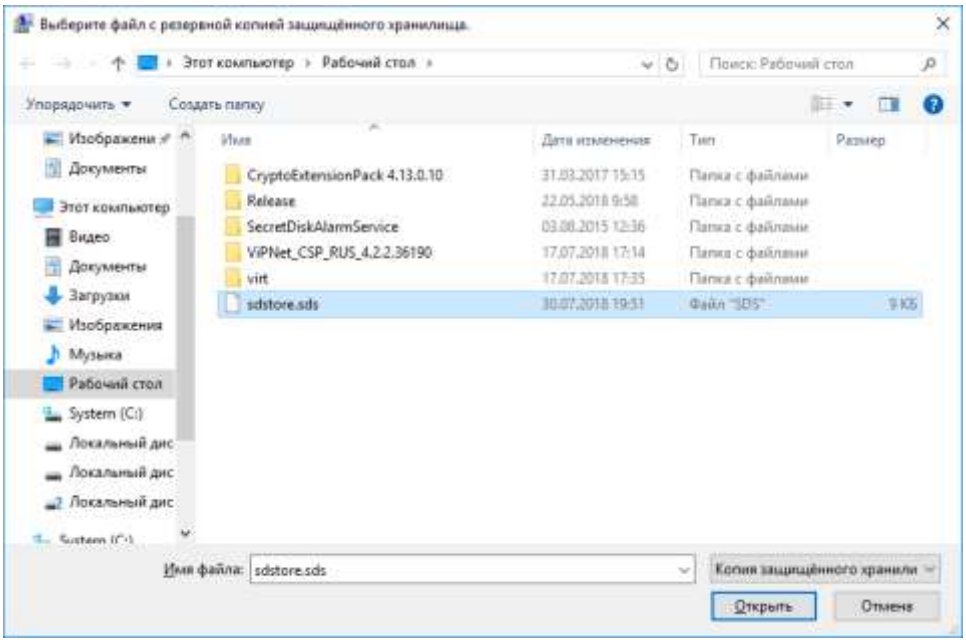
> *Для надежного восстановления необходимо иметь копии закрытого ключа и сертификата администратора в формате .pfx. В этом случае полное восстановление возможно из копии защищённого хранилища и без токенов администраторов.*

Возможны 2 варианта восстановления доступа к защищенным дискам.

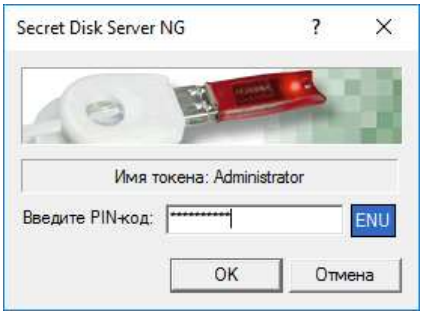
1 вариант (с помощью копии защищенного хранилища).

Для восстановления защищенного хранилища выполните следующие действия:

1. Зарегистрируйте временного администратора в SDS.
2. Откройте консоль управления сервером (MMC), вкладку **Серверы**.
3. Выберите нужный сервер → **Восстановить копию защищённого хранилища.**
4. Выберите нужный файл и нажмите **Открыть**.



5. Подключите сервер.
6. Введите ПИН-код администратора.



2 вариант (без копии защищенного хранилища).

Восстановить доступ к защищенным ресурсам с помощью сохраненный копий мастер-ключей дисков. При таком способе доступ к дискам будет восстановлен, но все настройки сервера и данные администраторов будут не доступны.

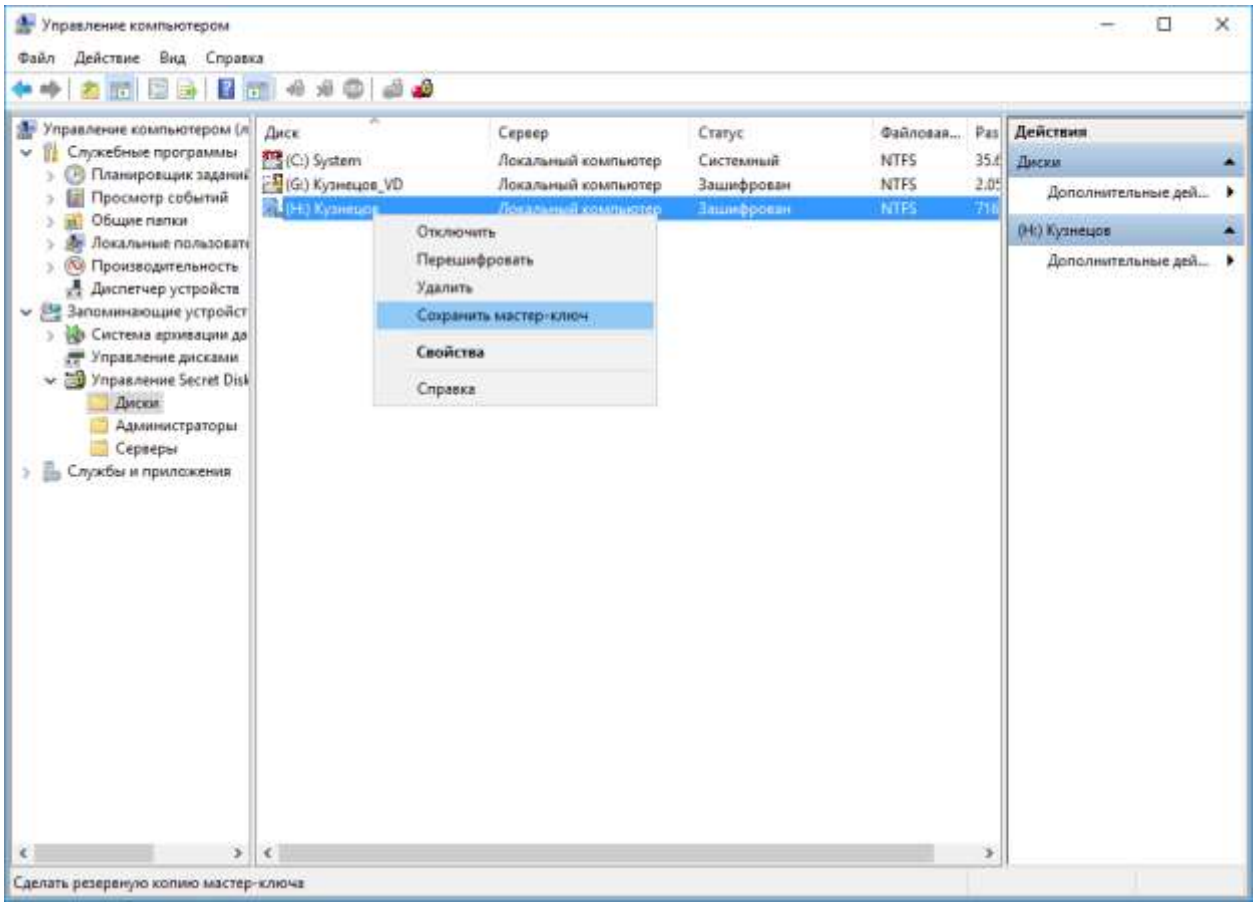
Подробнее о восстановлении доступа с помощью копий мастер-ключей дисков смотрите в главе Добавление/восстановление защищенного ресурса.

11.10 Сохранение резервных копий мастер-ключей логических и виртуальных томов

> *Восстановление доступа к защищённым ресурсам без копии мастер-ключа не возможно!*
>
> *Сохранение резервной копии мастер-ключа для логических и виртуальных томов идентично.*
>
> *В процессе зашифрования или перешифрования ресурсов приложение всегда предлагает сохранить резервную копию мастер-ключей. Если процесс сохранения мастер-ключа был пропущен, то рекомендуется это сделать позже.*

Для сохранения резервной копии мастер-ключа защищённого ресурса выполните следующие действия:

1. Выберите нужный защищённый ресурс.
2. В контекстном меню выберите **Сохранить мастер-ключ**.



3. Выберите место сохранения копии мастер-ключа.

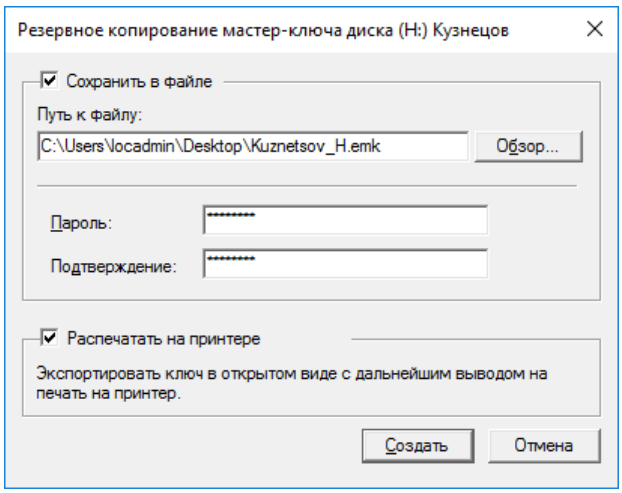


Рисунок 62 – Окно резервного сохранения копии мастер-ключей

> *При выборе "Сохранить в файле" убедитесь, что файл будет находится в защищённом месте.*
>
> *Рекомендуется сохранять копию мастер-ключа в файле на съёмном носителе. Съёмный носитель необходимо хранить в защищённом месте, например сейфе.*
>
> *При выборе "Распечатать на принтере" убедитесь, что принтер находится не в общедоступном месте.*
>
> *Распечатанный ключ необходимо хранить в защищённом месте, например сейфе.*

При выборе "Распечатать на принтере" приложение выведет ключ к диску на экран. Нажмите распечатать.

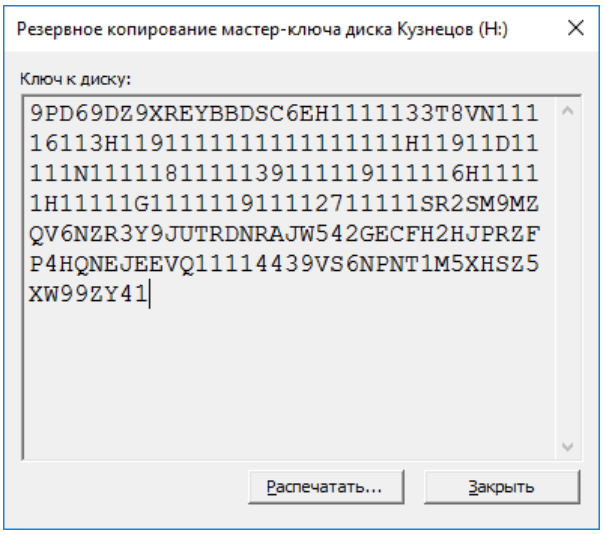
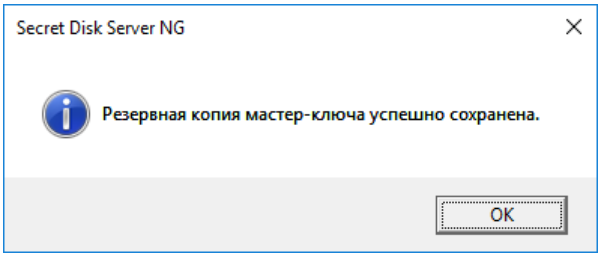


Рисунок 63 – Окно ключа к защищенному диску

4. Нажмите **OK**.



11.11 Настройка действий по сигналу «тревога»

Для каждого защищённого ресурса действия при нажатии кнопки "Тревога" могут отличаться.

Для настройки тревожной кнопки необходимо:

1. Установить на сервер дополнительную утилиту Alarm-4.x.y.z.msi (описание, процесс установки и настройки описаны в главе Сигнал "тревога" и отключение сервера).
2. В контекстном меню нужного защищенного ресурса выбрать **Свойства** → вкладка **Сигнал "Тревога".**
5. Выбрать реакцию сервера на сигнал "**Тревога**".

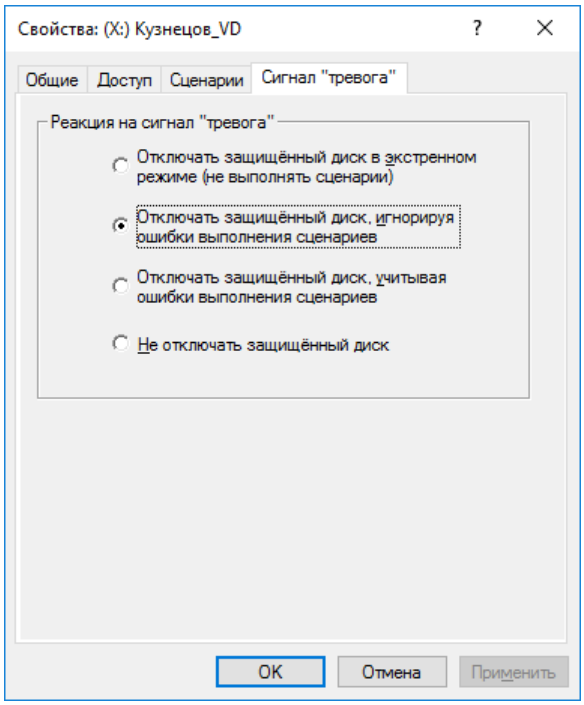


Рисунок 64 – Окно настройки реакции защищенных дисков на сигнал "тревога"

В зависимости от требований организации разные зашифрованные диски могут по-разному реагировать на сигнал "тревога".

Реакции зашифрованного диска на подачу сигнала "Тревога":

Реакция	Описание
Отключать защищенный диск в экстренном режиме (не выполнять сценарии)	Сценарии, указанные во вкладке Сценарии окна свойств зашифрованного диска выполнятся не будут
Отключать защищенный диск, игнорируя ошибки выполнения сценариев	Сценарии, указанные во вкладке Сценарии окна свойств зашифрованного диска будут выполнятся, но при этом ресурс будет отключен независимо от результата выполнения сценария
Отключать защищенный диск, учитывая ошибки выполнения сценариев	Сценарии, указанные во вкладке Сценарии окна свойств зашифрованного диска будут выполнятся с учетом настроек, сделанных в этой вкладке
Не отключать защищенный диск	Отключения зашифрованного диска происходить не будет

11.12 Настройка сценариев

11.12.1 Отключение защищенных дисков

Отключение дисков происходит без удаления защищенного хранилища. Для повторного подключения дисков необходимо авторизованному администратору подключить диски.

11.12.2 Отключение дисков с удалением защищённого хранилища

Отключение дисков происходит с полным удалением защищённого хранилища. При этом полностью удаляются все настройки SDS (список администраторов, ключи дисков, настройки дисков). Доступ к защищённым дискам невозможен.

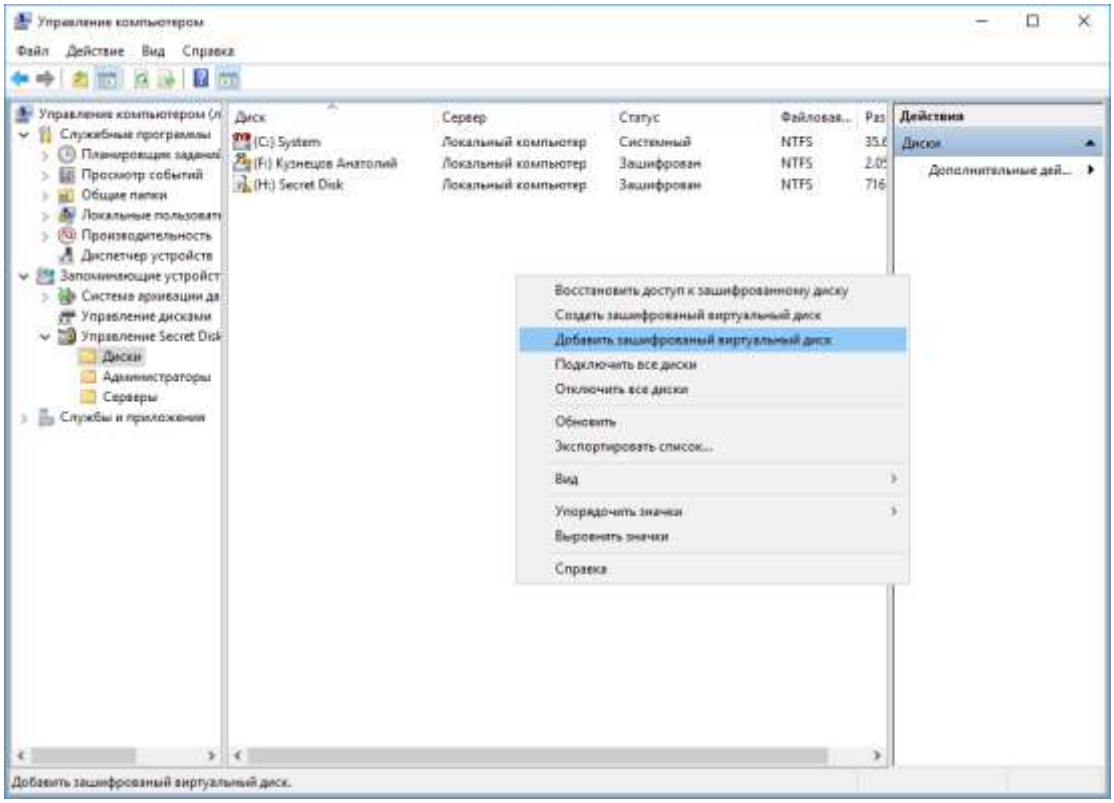
12. Управление защищёнными дисками

12.1 Добавление/восстановление защищённого ресурса

> *Добавление возможно только при наличии сохраненного файла виртуального диска и копии мастер-ключа диска. Если хотя бы один файл отсутствует, то добавление невозможно.*

Для добавления виртуального тома выполните следующие действия:

1. В консоли администратора во вкладке Диски в контекстном меню выберите **Добавить зашифрованный виртуальный диск**.



2. Выберите файл виртуального диска.
3. По желанию измените метку диска и букву диска.
4. Нажмите **Добавить**.

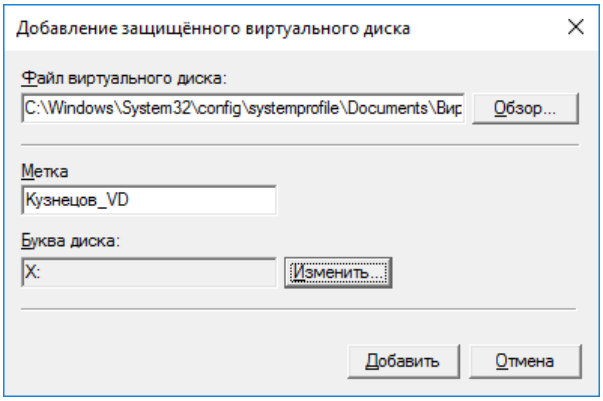
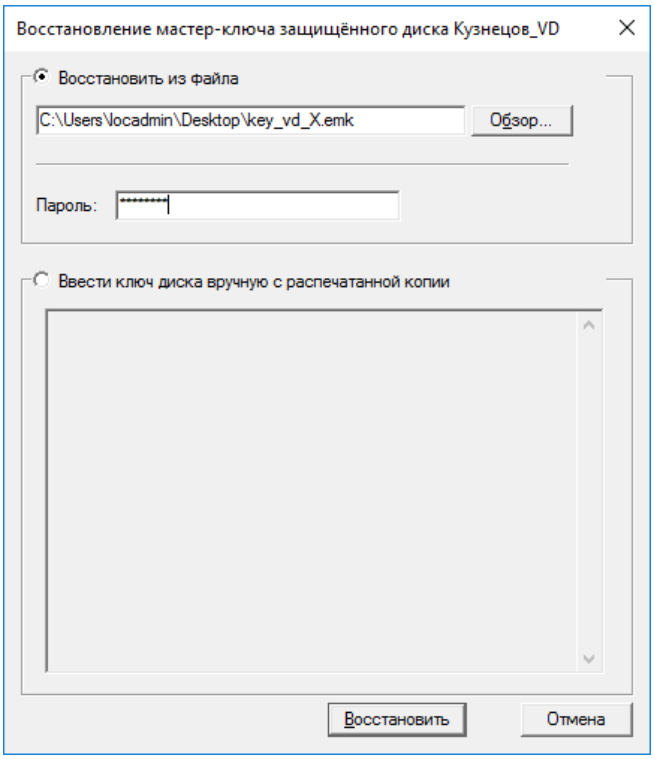
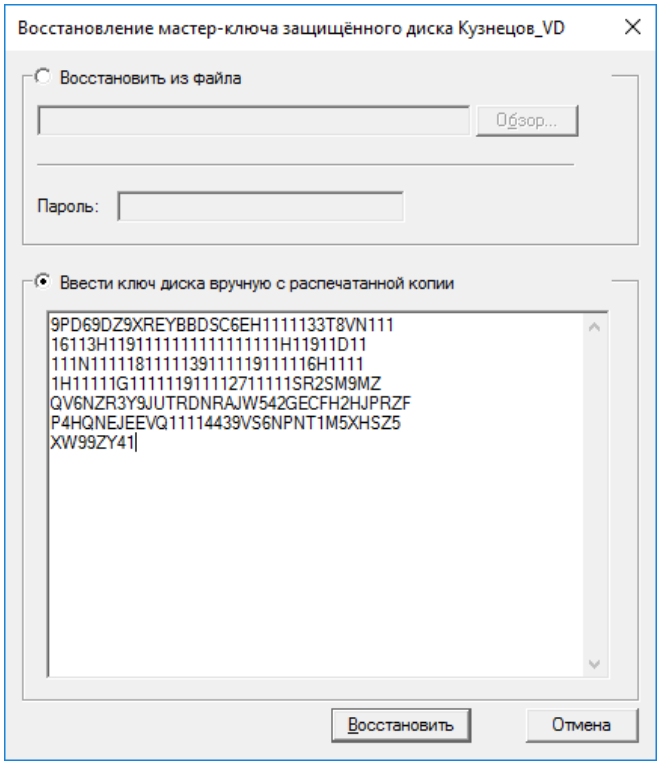


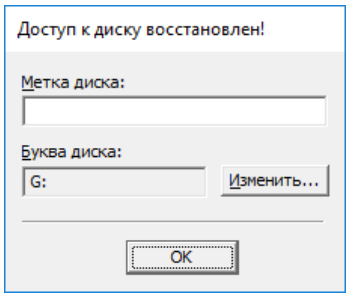
Рисунок 65 – Добавление виртуального диска

5. Для восстановления мастер-ключа диска выберите файл с копией мастер-ключа и введите пароль. Либо введите ключ диска вручную с распечатанной копии.
6. Нажмите **Восстановить**.





7. При успешном восстановлении виртуального диска из файла появится уведомление о восстановлении доступа к диску. Заполните метку диска и нажмите OK.



12.2 Работа с виртуальными томами

Возможности работы с виртуальным томом:

1. Подключить/отключить.
2. Перешифровать.
3. Удалить.
4. Сохранить копию мастер-ключа.
5. Изменить метку диска (свойства).
6. Настроить доступ других администраторов сервера к диску(свойства).
7. Настроить сценарии поведения диска при подключении/отключении (свойства).
8. Настроить реакцию на сигнал "Тревога" (свойства).

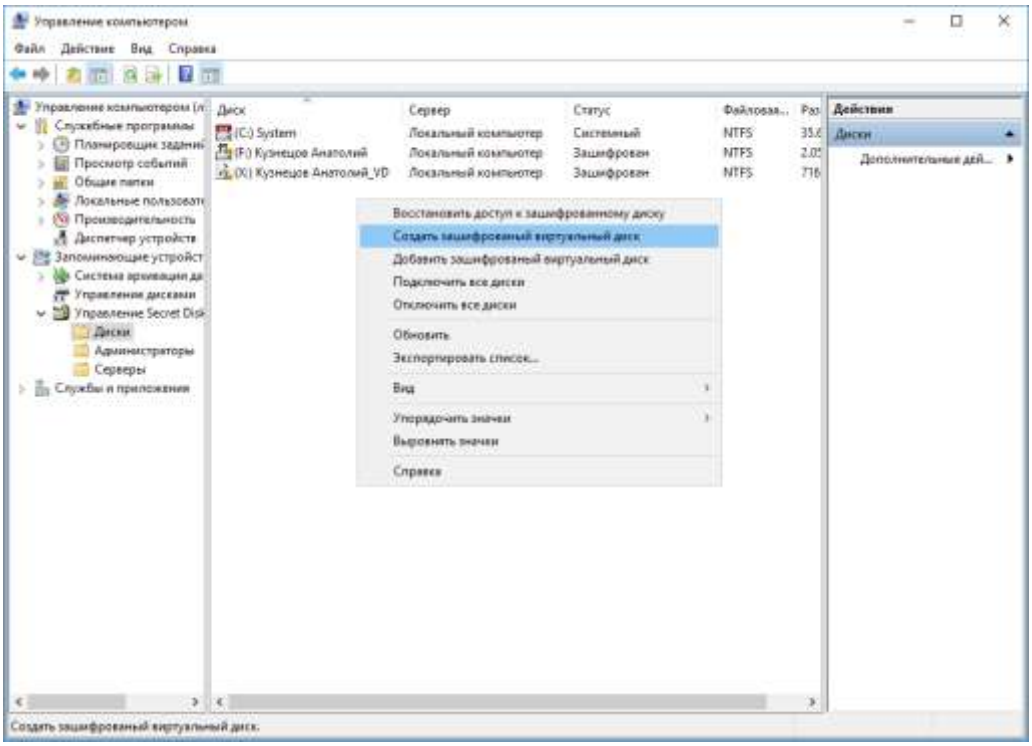
> *Виртуальный том создается сразу зашифрованным!*
>
> *Расшифрование виртуального тома недоступно!*

12.2.1 Создание виртуального тома

> *Создание виртуального тома на кластере не рекомендуется.*

Для создания виртуального тома выполните следующие действия:

1. В контекстом меню панели управления SDS во вкладке Диски выберите **Создать зашифрованный виртуальный диск**.

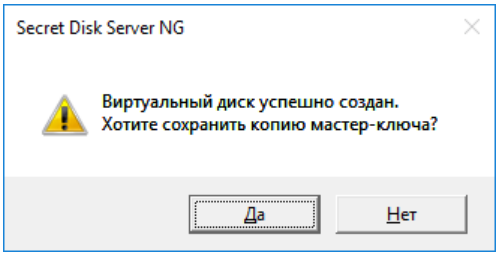


2. Заполните поля, необходимые для создания виртуального тома:
   - место хранения файла виртуального тома;
   - алгоритм шифрования;
   - метка диска;
   - буква диска;
   - файловая система;
   - максимальный размер;
   - тип диска (расширяемый или фиксированный).
3. Нажмите **Создать**.

> *Рекомендуется всегда сохранять резервные копии мастер-ключей при создании или перешифровании дисков. Без них восстановить доступ к данным невозможно!*
>
> *Восстановление доступа к защищенным ресурсам без копии мастер-ключа не возможо!*
>
> *Все данные будут безвозвратно утеряны!*

Более подробное описание сохранения резервных копий мастер-ключей дисков находится в главе Сохранение резервных копий мастер-ключей логических и виртуальных томов

4. Для создания резервной копии мастер-ключа диска нажмите **Да**. Для отмены создания резервной копии мастер-ключа нажмите **Нет**.



12.2.2 Перешифрование виртуального тома

Для перешифрования виртуального тома необходимо выполнить следующие действия:

1. Выберите **Перешифровать** в контекстном меню нужного виртуального тома.
2. Выберите нужный алгоритм шифрования. Нажмите **ОК**.
3. Дождитесь процесса перешифрования.

12.3 Работа с логическими томами

Администратор может управлять теми томами, для которых он включил защиту, либо если право управления ему дал другой администратор. В списке доступных дисков администратор видит только те диски, которыми он может управлять.

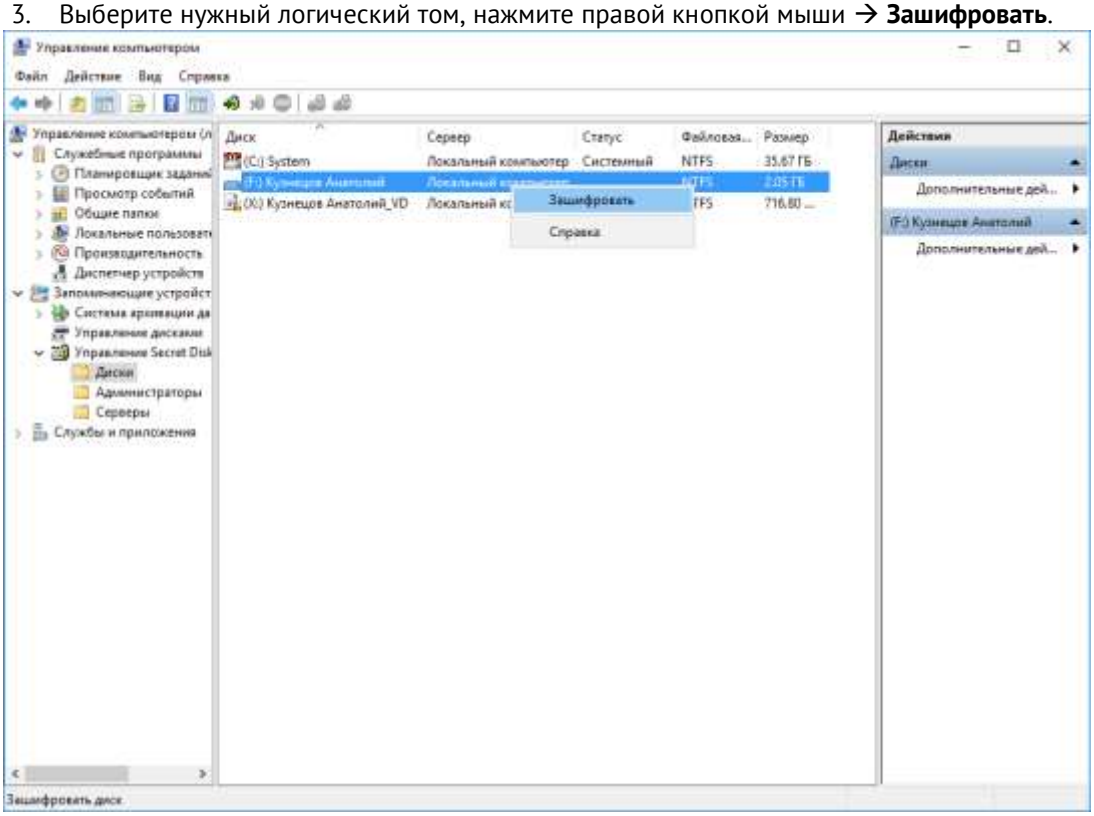
Возможности работы с логическим томом:

1. Подключить/отключить.
2. Создать.
3. Зашифровать.
4. Расшифровать.
5. Перешифровать.
6. Удалить.
7. Сохранить копию мастер-ключа.
8. Изменить метку диска (свойства).
9. Настроить доступ других администраторов сервера к диску(свойства).
10. Настроить сценарии поведения диска при подключении/отключении (свойства).
11. Настроить реакцию на сигнал "Тревога" (свойства).

12.3.1 Зашифрование логического тома

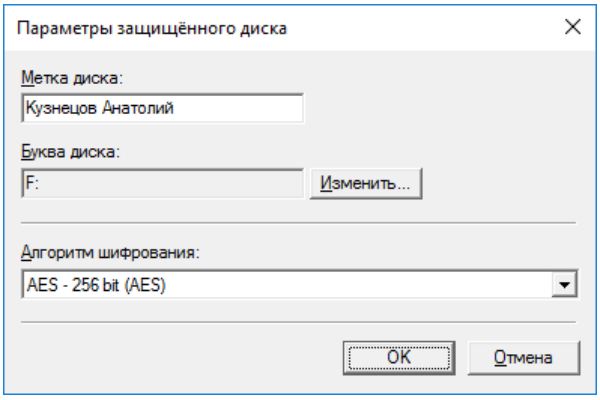
Для зашифрования логического тома выполните следующие действия:

1. Запустите консоль администратора.
2. Выберите вкладку **Диски**.
3. Выберите нужный логический том, нажмите правой кнопкой мыши → **Зашифровать**.



4. Назначьте параметры защищённого диска:
   - выберите метку диска;
   - букву диска;
   - алгоритм шифрования;

   Нажмите OK.



Рекомендуется сохранить резервную копию мастер-ключа для восстановления!

Восстановление доступа к защищенным ресурсам без копии мастер-ключа не возможо!

Все данные будут безвозвратно утеряны!

Более подробное описание сохранения резервных копий мастер-ключей дисков находится в главе Сохранение резервных копий мастер-ключей логических и виртуальных томов.

Для сохранения резервной копии мастер-ключа заполните поля окна и нажмите **Создать**. Для отмены операции сохранения резервной копии нажмите **Пропустить**.

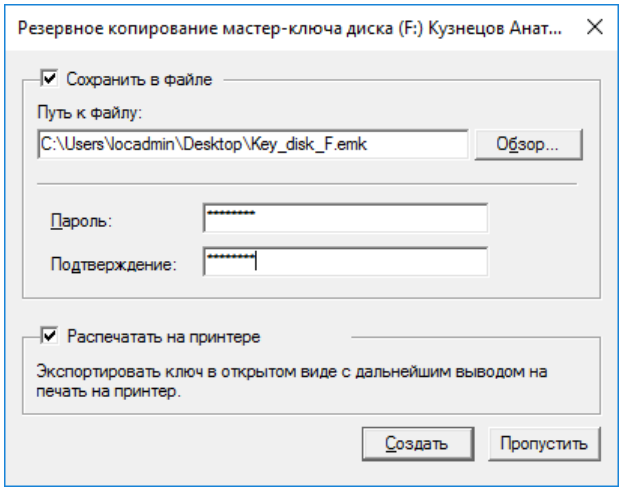


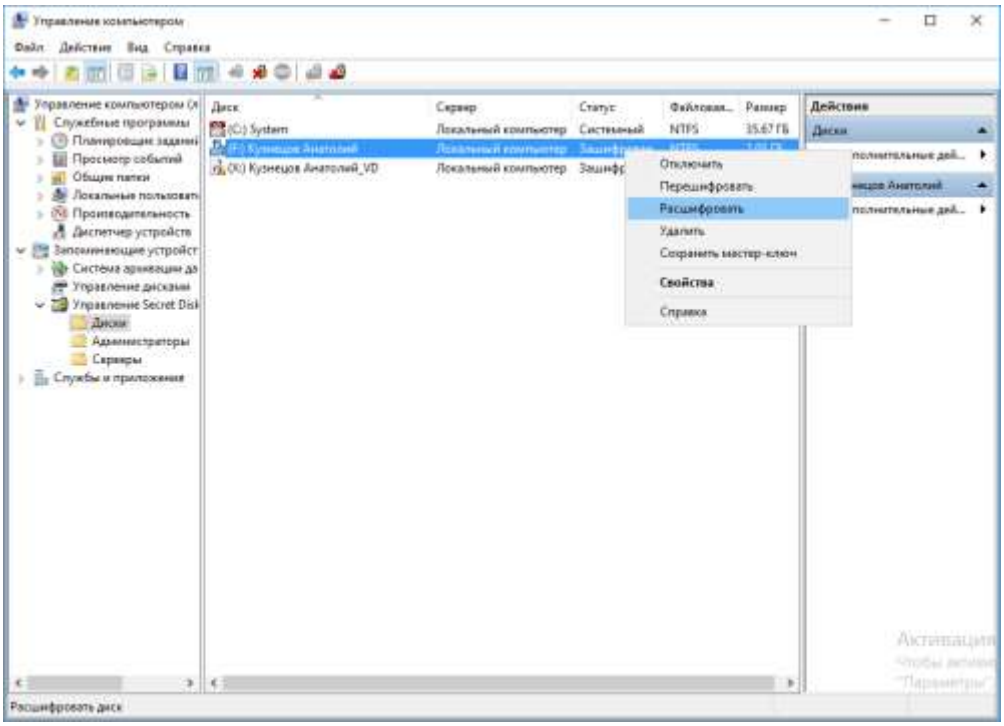
Рисунок 66 – Окно резервного копирования мастер-ключа диска

5. Дождитесь окончания процесса зашифрования.

12.3.2 Расшифрование логического тома

Для расшифрования логического тома выполните следующие действия:

1. Выберите нужный защищённый логический том, нажмите правой кнопкой мыши → **Расшифровать**.

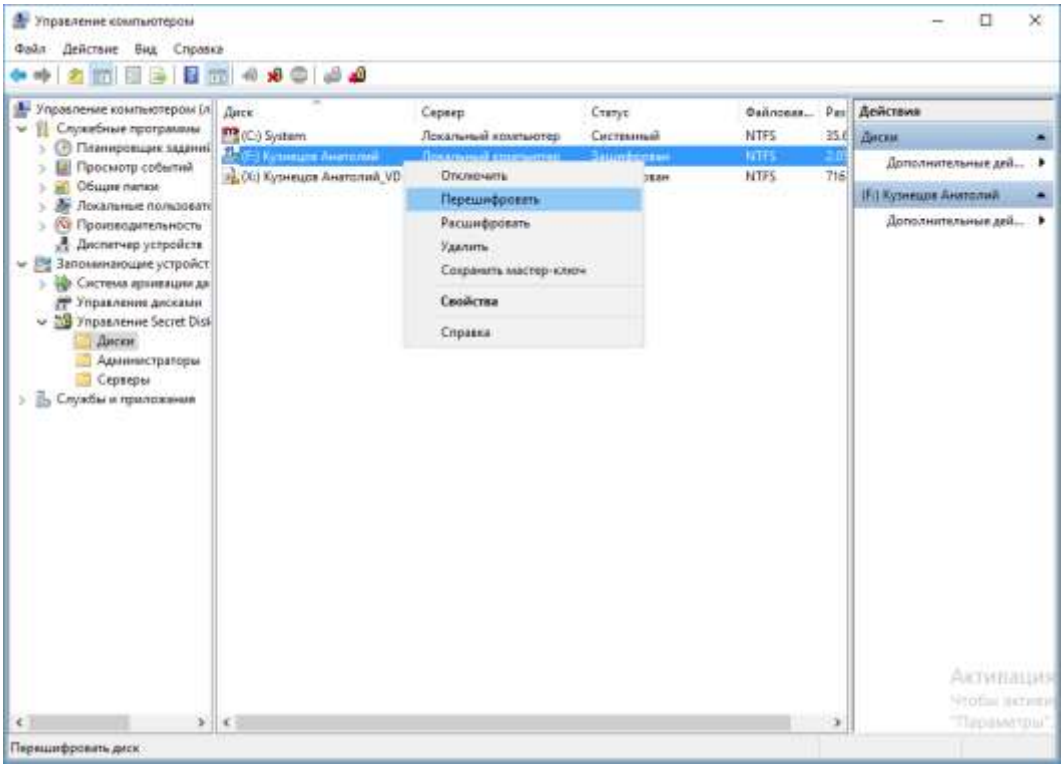


2. Дождитесь окончания процесса расшифрования.

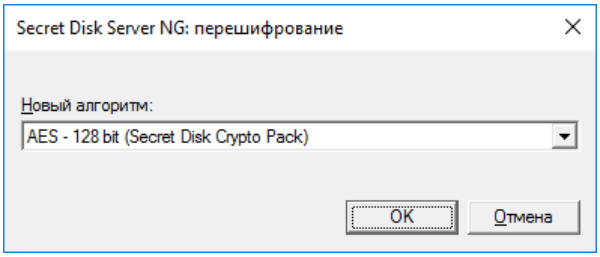
12.3.3 Перешифрование логического тома

Для перешифрования выполните следующие действия:

1. Выберите логический том и нажмите **Перешифровать** в контекстном меню.



2. Выберите новый алгоритм шифрования. Нажмите **OK**



Рекомендуется сохранить резервную копию мастер-ключа для восстановления!

Восстановление доступа к защищенным ресурсам без копии мастер-ключа не возможо!

Все данные будут безвозвратно утеряны!

Более подробное описание сохранения резервных копий мастер-ключей дисков находится в главе Сохранение резервных копий мастер-ключей логических и виртуальных томов

3. Дождитесь окончания процесса перешифрования.

12.3.4 Отключение и подключение логического тома

Если том не подключен, то работа с ним не возможна. Для совершения каких-либо действий с томом (зашифрования, перешифрования, расшифрования и работы) необходимо подключить том. Для подключения выберите **Подключить** в контекстном меню логического тома.

12.4 Доступ к защищенному диску по сети

Для повышения безопасности можно полностью запретить доступ к защищённому диску по сети.

Для запрета доступа к защищённому диску необходимо использовать лицензию сервера приложений. Для разрешения доступа к защищенному диску по сети необходимо использовать лицензию файл-сервера.

Настройка доступа к защищённому ресурсу не доступна при отсутствии хотя бы одной из лицензий на токене сервера.

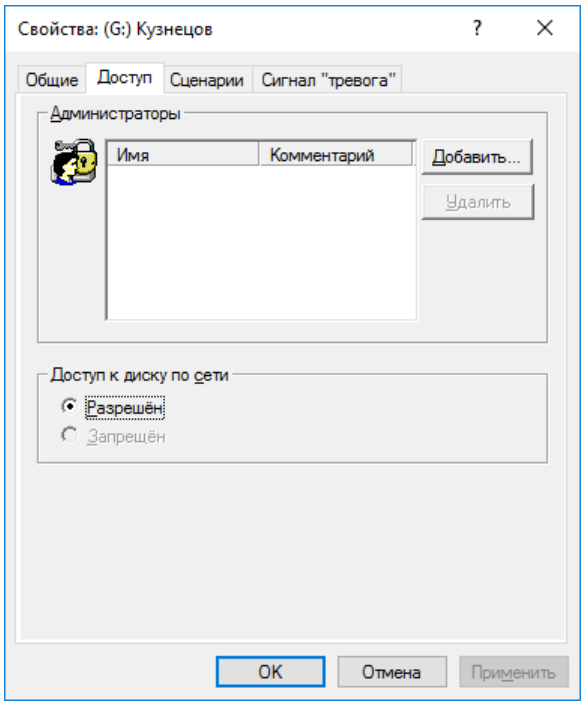
Доступ к диску по сети:

1. *Опция "Разрешён" активна, опция "Запрещён" не активна – на токене сервера установлена лицензия типа "файл-сервер".*
2. *Опция " Разрешён" не активна, опция "Запрещён" активна – на токене сервера установлена лицензия типа "сервер приложений".*
3. *Комбинированная (опции "Разрешён" и "Запрещён" доступны на выбор) – на токене сервера установлены лицензии "файл-сервера" и "сервера приложений". Администратор может выбрать одну из них.*

Для установки или отмены запрета на доступ к защищённому ресурсу по сети выполните следующие действия:

1. Откройте окно Свойства защищенного диска → Вкладка **Доступ**.

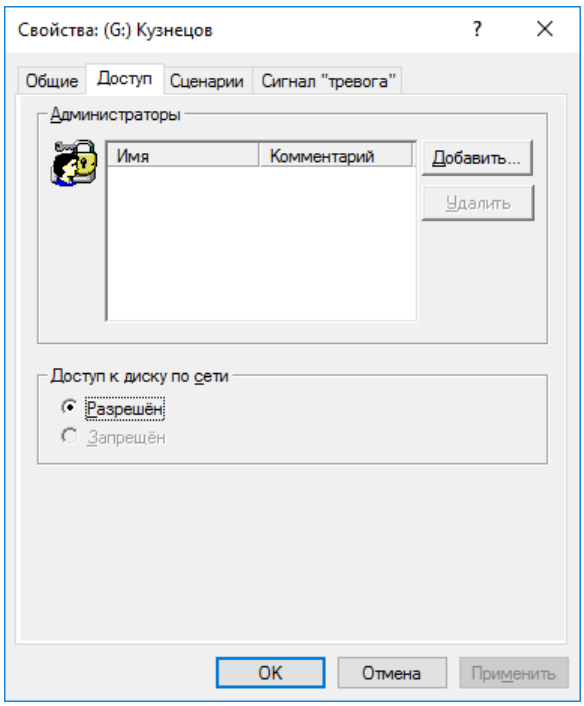
2. В области **Доступ** выберите:
   - запрещен – для запрета доступа к этому ресурсу;
   - разрешен – для отмены запрета доступа к этому ресурсу.



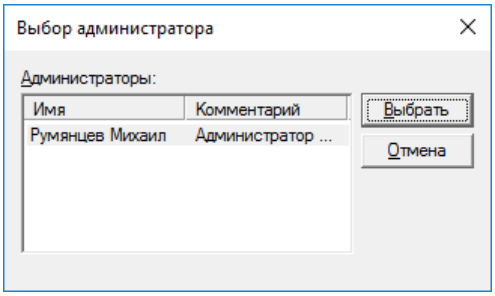
3. Нажмите **OK**.

12.5 Доступ администраторов к защищенным ресурсам

1. Для разграничения доступа администраторов к защищенным ресурсам откройте вкладку **Доступ** меню **Свойства диска**.
2. Для добавления администратора нажмите Добавить.



3. Выберите нужного администратора и нажмите **Выбрать**.



13. Работа с сертификатами

13.1 Сертификат администратора сервера

Зарегистрированный пользователь (администратор сервера) должен обладать сертификатом и соответствующей ключевой парой, находящейся на токене администратора.

Сертификат может быть выдан центром сертификации ОС Windows или домена, либо может быть создан в SDS NG при регистрации администратора сервера.

Рекомендуется использовать сертификаты, выданные центром сертификации.

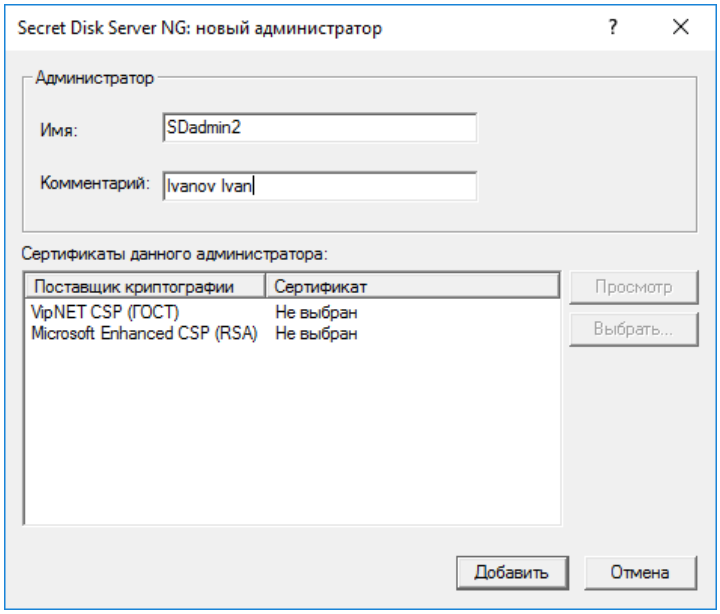
Приложение SDS NG поддерживает 2 вида сертификатов:

1. RSA (встроен в ОС Windows).
2. ГОСТ (устанавливается с помощью дополнительного ПО).

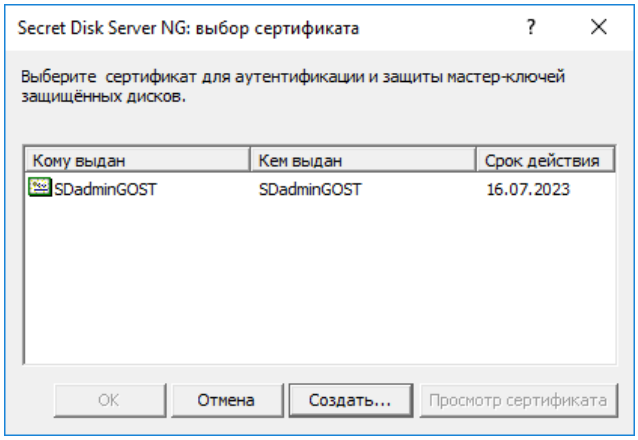
13.1.1 Создание сертификата

Для создания сертификата выполните следующие действия:

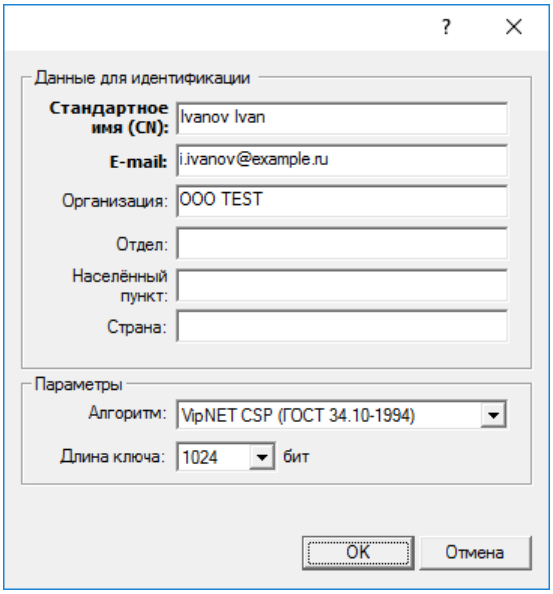
1. Зайдите в средство создания нового администратора. Заполните поля Имя и Комментарий.
2. Выберите поставщика криптографии (ViPNet CSP или КриптоPRO CSP– если он установлен, Microsoft Enhanced CSP (RSA) – встроен в ОС). Нажмите **Выбрать**.



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

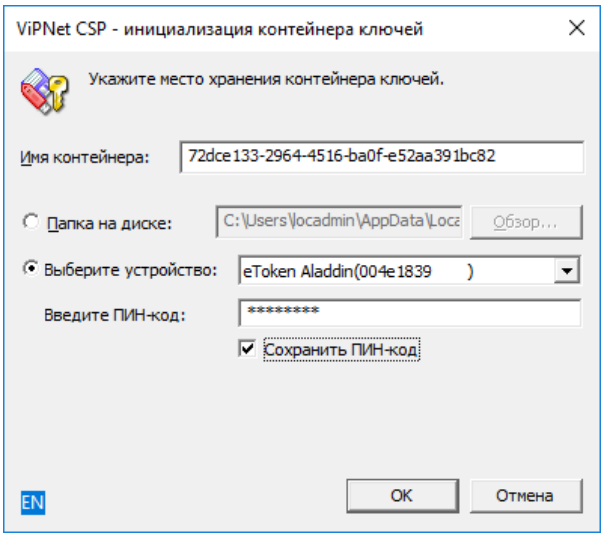


4. Заполните обязательные поля для идентификации и, по желанию, не обязательные поля.
5. Выберите параметры шифрования (алгоритм и длину ключа).

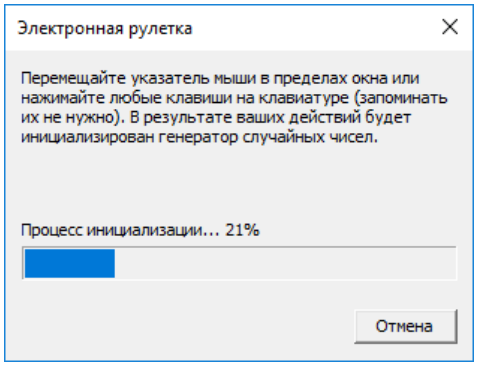


6. Укажите место хранения контейнера ключей. Введите ПИН-код.

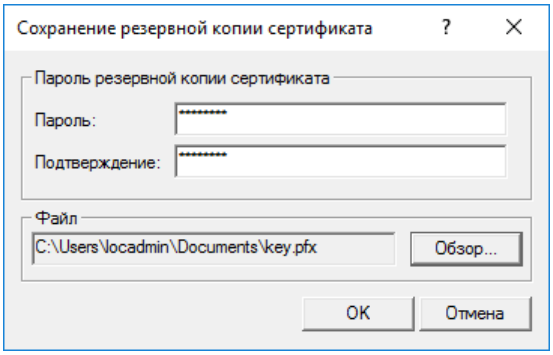
Рекомендуется хранить контейнер ключей на токене.



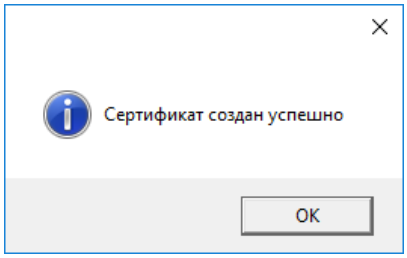
7. Следуйте дальнейшей инструкции по генерации случайных чисел.



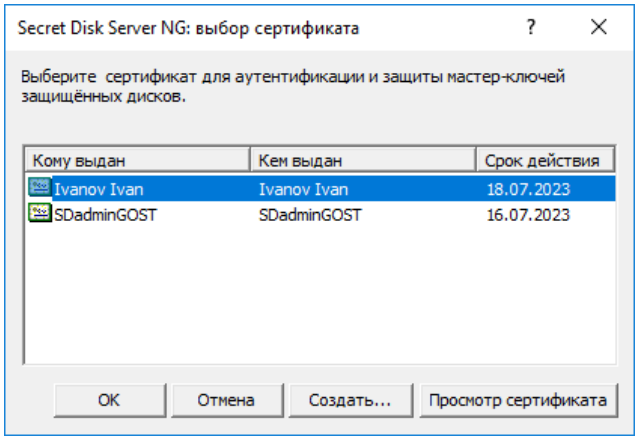
8. Рекомендуется сохранить резервную копию сертификата.



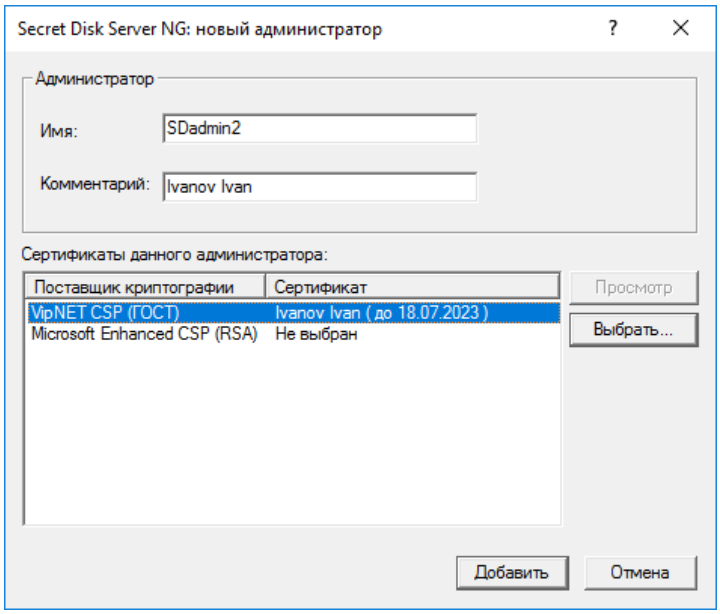
9. Нажмите **OK**.



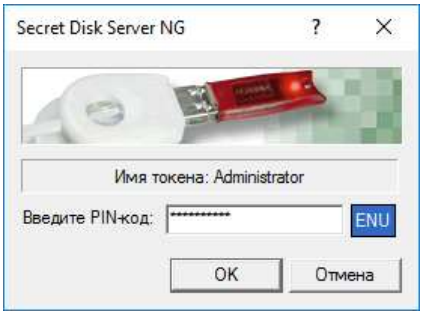
10. Созданный сертификат появится в списке доступных сертификатов. Выберите его и нажмите **OK**.



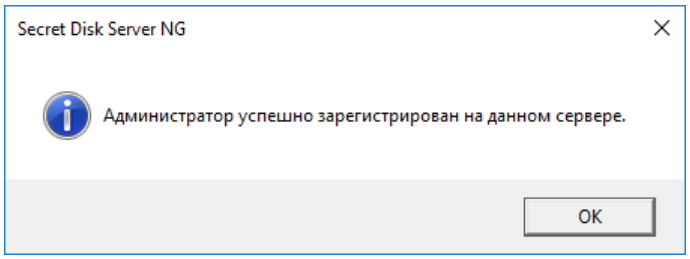
11. Нажмите **Добавить**. При необходимости можно добавить второй сертификат типа RSA.



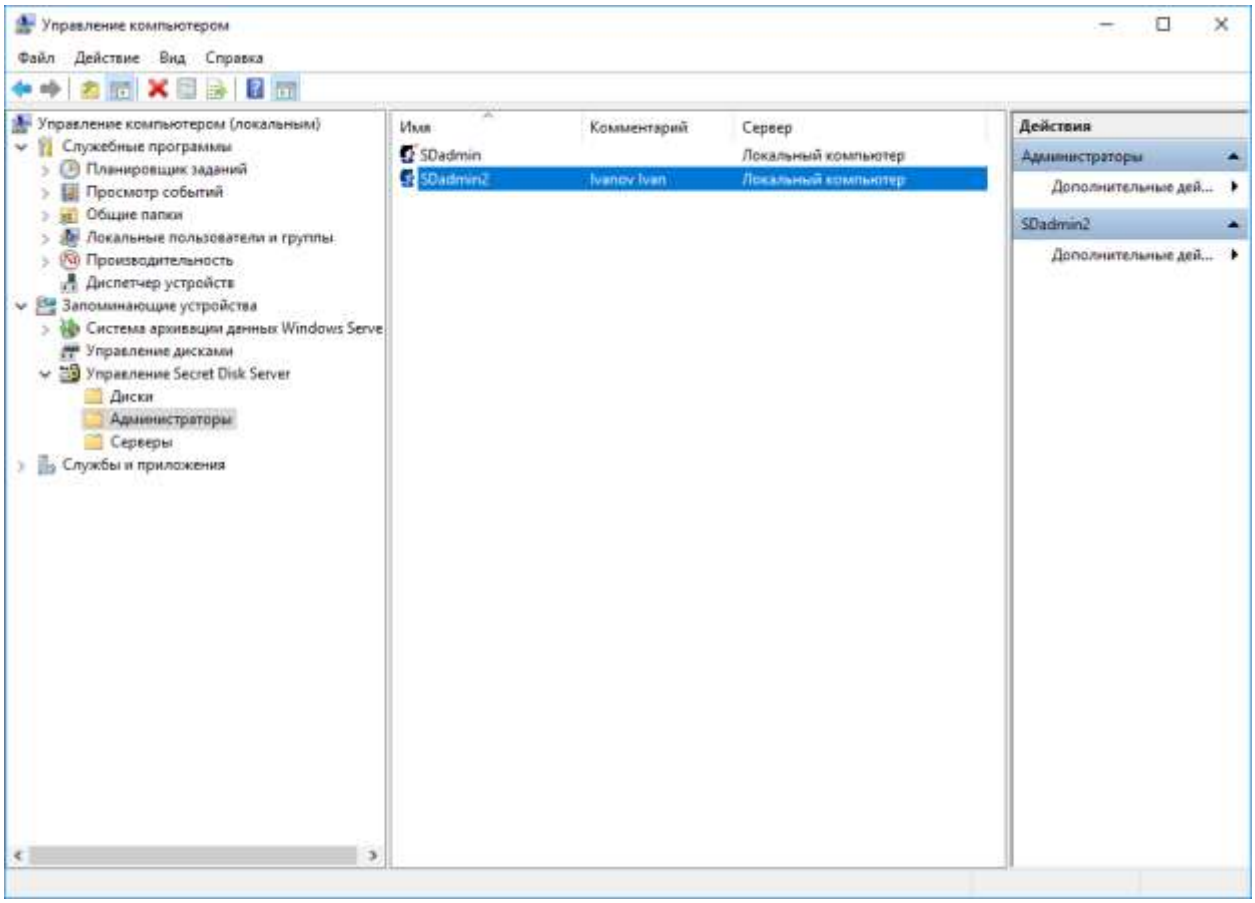
12. Введите ПИН-код токена администратора и нажмите **OK**.



13. Нажмите **OK**.



14. Новый администратор появится в панели управления компьютером.


Управление компьютером
Файл Действие Вид Справка
Управление компьютером (локальным)
Служебные программы
Планировщик заданий
Просмотр событий
Общие папки
Локальные пользователи и группы
Производительность
Диспетчер устройств
Запоминающие устройства
Система архивации данных Windows Serve
Управление дисками
Управление Secret Disk Server
Диски
Администраторы
Серверы
Службы и приложения
Имя
Комментарий
Сервер
SDadmin
Локальный компьютер
SDadmin2
Ivanov Ivan
Локальный компьютер
Действия
Администраторы
Дополнительные дей...
SDadmin2
Дополнительные дей...

14. Авторские права, товарные знаки, ограничения

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.

14.1 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.

15. Контакты

15.1 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.

15.2 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.

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, Web-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 России, ФСБ России 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