Secret Disk Enterprise 2.7

Руководство администратора

Версия	2.0
Статус	Публичный
Дата	19.04.2019
Номер	ID-номер

Аннотация

Secret Disk Enterprise (версия 2.7.0), далее по тексту "SDE" представляет собой корпоративную систему защиты конфиденциальной информации с централизованным управлением защищённых ресурсов.

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

Оглавление

1. Авторские права и торговые знаки 6
2. Список терминов и определений 7
3. Общие сведения 10
3.1 Назначение 10
3.2 Свойства 10
4. Защищаемые ресурсы 11
4.1 Логический раздел 11
4.2 Системный раздел 11
4.3 Виртуальный диск 11
4.4 Съёмные носители 11
4.5 Папки пользователя 11
4.6 Защищённый контейнер 12
5. Роли пользователей 13
6. Системные требования 16
6.1 Требования к программному обеспечению 16
6.2 Требования к аппаратному обеспечению 17
6.2.1. Дисковое пространство 17
6.2.2. Оперативная память 17
6.2.3. Порты и считыватели 17
6.2.4. Поддерживаемые модели JaCarta 17
6.2.5. Поддерживаемые модели eToken 18
6.2.6. Криптопровайдеры алгоритмов шифрования ГОСТ 18
7. Установка Secret Disk Enterprise 19
8. Подготовка инфраструктуры 20
8.1 Предварительные условия 20
8.2 Поддержка токенов и служб криптографии 20
8.3 Сертификаты пользователей на токенах 20
8.4 Создание пользователей и групп Active Directory для ролей SDE 21
8.5 Подготовка СУБД MSSQL 21
8.6 Настройка DNS Service 22
8.7 Настройка Windows Firewall 22
8.8 Настройка службы Web Server IIS 22
9. Установка Secret Disk Management Server 24
9.1 Последовательность установки сервера SDMS 24
10. Мастер первоначальной настройки SDMS 28
10.1 Создание новой Базы данных 28
10.2 Подключение к серверу Базы данных 35
10.3 Завершение установки Secret Disk Management Server 38
10.4 Подключение к существующей Базе данных 39
11. Установка, настройка и удаление Secret Disk Agent 43
11.1 Установка Secret Disk Agent вручную 43
11.2 Установка Secret Disk Agent с помощью групповых политик 44
11.3 Настройка SDA 44

11.3.1. Настройка SDA на рабочей станции ... 44
11.4 Настройка фиксированного подключения к SDMS ... 45
11.5 Удаление Secret Disk Agent ... 46
11.5.1. Удаление Secret Disk Agent вручную ... 46
11.5.2. Удаление Secret Disk Agent через групповые политики ... 46

12. Работа с Веб-порталом SDMS ... 47

13. Управление рабочими станциями SDE ... 48

13.1 Добавление рабочих станций ... 48
13.2 Список зарегистрированных рабочих станций ... 49
13.3 Информация о рабочей станции и действия с ней ... 49
13.4 Блокирование и разблокирование рабочей станции ... 50
13.5 Удаление рабочих станций пользователя ... 51

14. Управление пользователями ... 52

14.1 Управление пользователями SDMS ... 52
14.2 Добавление пользователей в SDMS ... 52
14.3 Регистрация сертификатов пользователей SDE ... 52
14.4 Настройка действительности сертификатов ... 54
14.5 Присвоение ролей и управление ролями ... 54
14.6 Настройка пользовательских политик ... 56
14.6.1. Изменение глобальных (общих) политик для всех пользователей ... 56
14.6.2. Изменение политик для конкретного пользователя ... 57
14.7 Блокирование и разблокирование учетной записи ... 57
14.8 Удаление учетной записи из SDE ... 58

15. Управление защищенными ресурсами ... 59

15.1 Добавление защищенного ресурса пользователю ... 59
15.2 Список защищённых ресурсов рабочих станций ... 60
15.3 Список защищённых ресурсов пользователя ... 60
15.4 Страница управления защищённым ресурсом ... 61
15.5 Операции с логическими разделами ... 63
15.5.1. Операция шифрования ... 63
15.5.2. Операции расшифрования и перешифрования ... 64
15.5.3. Отсоединение, подсоединение и перемещение дисков ... 64
15.5.4. Отсоединение диска ... 65
15.5.5. Подсоединение диска ... 65
15.5.6. Перемещение диска ... 66
15.5.7. Экспорт ключа шифрования логического раздела ... 66
15.6 Операции с виртуальными дисками ... 67
15.6.1. Создание виртуального диска ... 67
15.6.2. Удаление виртуального диска ... 69
15.6.3. Экспорт ключа шифрования виртуального диска ... 69
15.7 Установка и снятие защиты с системного диска ... 69
15.7.1. Установка защиты ... 69
15.7.2. Снятие защиты ... 70
15.8 Групповые операции с рабочими станциями и ресурсами ... 70
15.9 Работа с защищёнными дисками без электронного ключа ... 71
15.10 Мониторинг событий системы ... 72
15.10.1. Журнал аудита ... 72
15.10.2. Журнал предупреждений ... 73
15.10.3. Журнал клиентской активности ... 74
15.10.4. Фильтрация записей ... 74
15.10.5. Журнал планов обслуживания ... 74
15.10.6. Фильтрация записей ... 75

16. Работа с планом обслуживания ... 76

16.1 Конфигурирование Task Scheduler ... 76
16.2 Конфигурирование MaintenancePlanRunner ... 77

17. Функции агента восстановления ... 78

18. Мастер-ключи ... 79

18.1 Пользователи, имеющие доступ к мастер-ключу БД ... 79
18.2 Настройки криптографии ... 79
18.3 Резервное копирование мастер-ключа ... 80
18.4 Восстановление мастер-ключа БД ... 82
18.5 Отзыв мастер-ключа БД ... 85
18.6 Смена мастер-ключа БД ... 86

19. Лицензирование Secret Disk Enterprise ... 87

Приложение А ... 89

20. Авторские права, товарные знаки, ограничения ... 92

20.1 Лицензионное соглашение ... 93

21. Контакты ... 95

21.1 Офис (общие вопросы) ... 95
21.2 Техподдержка ... 95

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 вам права ни на это описание, ни на информацию, содержащуюся в нём или в описываемом Продукте, а лишь предоставляет вам 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

ПО	Программное обеспечение
ОС	Операционная система
ПК	Персональный компьютер
Алгоритм шифрования	Набор логических правил (математических преобразований), определяющих способ преобразования информации из открытого состояния в зашифрованное (процесс зашифрования) и, наоборот, из зашифрованного состояние в открытое (процесс расшифрования).
JaCarta, eToken	Используемые в SDE марки токенов.
Идентификация	Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется идентификацией.
Аутентификация	Аутентификацией (установлением подлинности) называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдаёт.
Двухфакторная аутентификация	Двухфакторная аутентификация (2FA) — расширенная аутентификация, метод контроля доступа к компьютеру или информационной системе, в котором пользователю для получения доступа к информации необходимо предъявить более одного "доказательства механизма аутентификации". К категориям таких доказательств относят: *Знание* — информация, которую знает субъект. В случае с токенами - это PINкод. *Владение* — вещь, которой обладает субъект. В случае SD5 речь идёт о токене.
Виртуальный диск	Логическое устройство, воспринимаемое операционной системой как обычный диск, но отличающееся тем, что все его данные хранятся в файле на одном из доступных физических дисков.
Зашифрованный диск (том)	Логический том или виртуальный диск, предназначенный для безопасного хранения конфиденциальной информации в зашифрованном виде.
CSP	Cryptographic Service Provider, криптопровайдер или поставщик криптографии – программный модуль, реализующий один или несколько алгоритмов шифрования через системную шину операционной системы CryptoAPI.
Secret Disk Crypto Extension Pack (SD CEP)	Пакет расширения, который позволяет использовать алгоритм шифрования ГОСТ 28147-89 (ГОСТ 34.12-2015), предоставляемый сторонними криптопровайдерами.
КриптоПро CSP	Программа для предоставления симметричных и ассиметричных алгоритмов шифрования по ГОСТ. Поставляется компанией КриптоПРО.
ViPNet CSP	Программа для предоставления симметричных и ассиметричных 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 не старше версии 7. Поставляется компанией "Аладдин Р.Д.".
SafeNet Authentication Client (SAC)	Программа для обеспечения работы USB-ключей и смарт-карт eToken на операционных системах семейства Windows с версии 7 и старше. Поставляется компанией SafeNet.

JaCarta Unified Client	Программный комплекс, предназначенный для настройки и работы со всеми моделями USB-токенов и смарт-карт семейства JaCarta. Поставляется компанией "Аладдин Р.Д."
Сертификат открытого ключа	Электронный документ, подтверждающий принадлежность открытого ключа и определенных атрибутов конкретному пользователю.
Криптокопия	Зашифрованное значение параметра.
Крипто-хранилище	Файл или файлы с настройками приложения, содержащие учётные записи пользователей, списки защищаемых ресурсов, параметры доступа к ресурсам, криптокопии ключей доступа и т.д.
Рабочая станция SDE	Компьютер, на котором установлено клиентское программное обеспечение Secret Disk Agent. SDA осуществляет операции с защищёнными ресурсами и предоставляет доступ к ним по заданиям, полученным от сервера управления SDMS. SDA хранит в локальном хранилище рабочей станции сведения о защищённых ресурсах и сообщает эту информацию серверу SDMS. SDA сообщает Серверу Управления данные пользователя, успешно аутентифицировавшегося на рабочей станции. SDA и SDMS совместно поддерживают актуальную информацию о нахождении защищённых ресурсов на рабочих станциях и пользователях.
План обслуживания	Набор действий и проверок, предназначенных для выявления особых ситуаций, возникающих при эксплуатации системы SDE и предупреждения о них.
AD	Active Directory
IIS	Microsoft Internet Information Server
Secret Disk Agent	Клиентская часть системы Secret Disk Enterprise: приложение, позволяющая пользователям получать доступ к защищённым ресурсам, находящимся на их рабочей станции.
Secret Disk Enterprise (SDE)	Корпоративная система защиты конфиденциальной информации путём шифрования с централизованным управлением защищёнными ресурсами.
Secret Disk Management Server (SDMS)	Серверная часть системы Secret Disk Enterprise, объединяющая функции администрирования защищаемых ресурсов, назначения прав доступа пользователям, управления ключами шифрования ресурсов и сертификатами пользователей, а также мониторинга, аудита, хранения и восстановления настроек системы.
UEFI	**Встроенное программное обеспечение, предназначенное для инициализации компьютера** и запуска загрузчика операционной системы. UEFI пришло на замену предыдущей системы инициализации – BIOS – и отличается большим количеством дополнительных возможностей, например, возможность проверку электронной подписи загрузчика.
Веб-портал	Тоже самое, что Веб-портал SDMS и Административный веб-портал: веб-приложение, посредством которого администраторы и другие особые пользователи Secret Disk Enterprise управляют работой системы.
База данных Secret Disk Enterprise (БД)	Объект, представляющий базу данных MS SQL. Используется как хранилище настроек, учётных записей и ключей системы Secret Disk Enterprise.
Лицензия	Файл с данными о передаваемых пользователю правах и возможностях использования Secret Disk Enterprise.
Мастер-ключ базы данных	Ключ шифрования, используемый для создания криптокопий ключей шифровавания ресурсов для безопасного хранения их в базе данных SDE.

Ключ шифрования ресурса	Ключ симметричного шифрования, используемый для зашифрования и расшифрования данных защищённого ресурса, ключ шифрования уникален для каждого ресурса.
Оператор	Одна из ролей в Secret Disk Enterprise. Оператор подключает и отключает криптохранилище, выполняет резервное копирование и экспорт мастер-ключа базы данных и просматривает настройки и журналы событий Secret Disk Enterprise. Оператор должен обладать электронным ключом с сертификатом.
Отключение криптохранилища	Выгрузка из памяти сервера бизнес-логики мастер-ключа базы данных с блокированием доступа к ключам шифрования ресурсов. Операция выполняется операторами SDE через приложение Агент Secret Disk Management Server.
Подключение зашифрованного диска	Действие, в результате которого становятся доступными данные на зашифрованном диске, а также его форматирование и проверка на наличие ошибок. Выполняется приложением Secret Disk Agent по команде пользователя или автоматически.
Подключение криптохранилища	Загрузка в память сервера бизнес-логики мастер-ключа базы данных для получения доступа к ключам шифрования защищённых ресурсов.
Пользователь	Одна из ролей в Secret Disk Enterprise: лицо, имеющее права доступа к защищённым ресурсам рабочих станций. Пользователь должен обладать электронным ключом с выписанным ему сертификатом.
Сервер бизнес-логики	Компонент SDMS, обеспечивающий проведение работ с зашифрованными дисками, сертификатами пользователей, управление учётными записями пользователей, лицензиями, компьютерами, выполнение сервисных функций, и другие операции.
УЦ	Удостоверяющий центр, тоже самое что Служба Сертификации
Шлюз Клиентов	Веб-приложение, отвечающее за аутентификацию и обработку запросов с рабочих станций пользователей, а также перенаправление запросов на сервер бизнес-логики.

3. Общие сведения

3.1 Назначение

Продукт SDE предназначен для защиты конфиденциальной информации в корпоративной системе компании. SDE работает под управлением ОС семейства Windows с централизованным управлением защищенными ресурсами.

3.2 Свойства

1. Защита информации от несанкционированного доступа осуществляется путем шифрования данных на:
   - логических дисках;
   - виртуальных дисках;
   - съемных USB-накопителях;
   - отдельных папках.

Возможность создания шифрованных файл-контейнеров для пересылки конфиденциальной информации по незащищенным каналам связи.

Информация на защищенных ресурсах находится в зашифрованном виде. Расшифрование происходит "на лету" при доступе к ним зарегистрированных пользователей, прошедших процедуру двухфакторной аутентификации.

SDE защищает системные (загрузочные) диски компьютеров. Защита приводит к невозможности запуска ОС без электронного ключа и сертификата. При этом защищаются не только данные пользователя, но и все данные ОС, включая временные файлы, файлы подкачки и файл образа системы в "спящем режиме".

> *Возможность защиты системного диска не гарантируется и требует проверки совместимости на конкретном оборудовании.*

2. Защита ресурсов, управление пользователями и правами доступа осуществляется в SDE централизовано администраторами информационной безопасности системы.
3. Разрешение/запрет сетевого доступа к защищенным ресурсам в корпоративной сети.

4. Защищаемые ресурсы

4.1 Логический раздел

Раздел внутреннего жёсткого диска, не используемый для загрузки ОС. Такому диску должен быть присвоен постоянный буквенный идентификатор ("буква диска").

4.2 Системный раздел

Раздел внутреннего жёсткого диска, на котором находятся файлы ОС, необходимые для её запуска. Для запуска системы с защищённого системного раздела используется специальный загрузчик, который является частью клиентского программного обеспечения Secret Disk Agent.

4.3 Виртуальный диск

Диск (с точки зрения ОС), у которого данные хранятся в файле. Буквенный идентификатор присваивается виртуальному диску динамически, при его подключении. Виртуальные диски, созданные средствами SDE, всегда защищены и их данные зашифрованы.

> *Нельзя создать виртуальный диск на защищенном логическом диске.*

4.4 Съёмные носители

Аппаратные запоминающие устройства, которые могут быть подключены к компьютеру и отключены от него во время работы ОС, без её остановки или изменения настроек.

Если в системе SDE разрешена защита съёмных носителей, то при подключении такого носителя происходит следующее:

- SDE запрещает изменение файлов, уже имеющихся на носителе, но не защищает их и разрешает их чтение;
- вновь созданные папки и файлы защищаются шифрованием;
- пользователь, записавший новые данные, получает разрешение на доступ к ним;
- доступ других пользователей к защищённым данным на съёмном носителе должен быть разрешён Администратором ИБ.

При подключении съёмного носителя с защищёнными данными к незарегистрированному в SDE компьютеру, на нём будут доступны все имевшиеся ранее обычные файлы и папки. Защищённые данные будут выглядеть как новые файлы и папки с бессмысленными именами и нераспознаваемыми данными (при этом их можно будет скопировать, например, для создания резервной копии защищённых данных).

> *Снять защиту со съёмного носителя нельзя по соображениям безопасности, зашифрованные данные можно только удалить.*

4.5 Папки пользователя

Администратор системы управляет установкой и снятием защиты логических разделов, системных разделов и виртуальных дисков.

Пользователь не может включить защиту разделов или создать виртуальный диск. При необходимости создания защищённого ресурса, пользователь может установить защиту для папки и хранить там свои конфиденциальные данные.

Доступ других пользователей к содержимому защищённой папки может быть разрешён Администратором ИБ. При обращении к защищённой папке без разрешения на доступ, содержимое папки будет представлено в нераспознаваемом виде.

4.6 Защищённый контейнер

Защищённый контейнер предназначен для обмена конфиденциальной информации с получателями вне системы SDE по незащищённым каналам связи (почта, мессенджеры и прочее). Защищенный контейнер представляет собой защищённый виртуальный диск, который можно открыть как в системе SDE, так и на другом компьютере.

Типовой сценарий использования контейнера:

- пользователь SDE, создаёт контейнер и работает с ним как с виртуальным диском, куда помещается передаваемая информация;
- перед отправкой контейнера SDE генерирует пароль, без которого получатель не сможет открыть контейнер;
- контейнер и пароль к нему отправляются получателю по разным каналам доставки. Например, контейнер отправляется по электронной почте, а пароль сообщается по телефону;
- получатель открывает контейнер с помощью специального программного обеспечения – Secret Disk Reader (скачать дистрибутив можно с официального сайта Алладин Р. Д.;
- получатель может изменить информацию в контейнере и отправить его обратно;
- пользователь SDE, получивший изменённый контейнер, открывает его без ввода пароля;
- при повторной подготовке контейнера к отправке генерируется новый пароль для получателя.

Работа с защищённым контейнером похожа на обмен данными с использования файлового архива, защищённым паролем, но имеет следующие преимущества:

- пользователь SDE работает с контейнером без ввода пароля;
- SDE создаёт сложные пароли, которые меняются при каждой подготовке контейнера к отправке;
- для защиты используется стойкий алгоритм шифрования (AES с длиной ключа 256 бит).

5. Роли пользователей

В SDE используется ролевая модель управления полномочиями пользователей: права доступа в системе назначаются присвоением каждой учётной записи одной или нескольких ролей, обладающих определённым набором прав.

> *В SDE имеются семь встроенных ролей, набор прав которых не может быть изменён. Дополнительно к ним можно создать новые роли с произвольным набором прав.*

Встроенные роли SDE:

1. Администратор ИБ.
2. Оператор.
3. Пользователь.
4. Аудитор.
5. Агент восстановления.
6. Запуск плана обслуживания.
7. Агент управления криптографией.

Правом назначения ролей обладают пользователи с ролью *Администратор ИБ*.

> *Первым пользователем с этой ролью становится пользователь, осуществивший установку программного обеспечения сервера управления SDMS.*

Также, три роли SDE могут присваиваться пользователям, входящим в выбранные группы домена Active Directory. К группам Active Directory можно привязать следующие роли SDE:

1. Администратор ИБ.
2. Аудитор.
3. Запуск плана обслуживания.

> *Связывание групп Active Directory с ролями SDE делается Мастером первоначальной конфигурации при установке SDMS, в дальнейшем эту настройку изменить* ***нельзя****.*

Доступ к *Административному Веб-Порталу* предоставляется всем ролям SDE, кроме ролей *Пользователь*, *Запуск плана обслуживания* и *Агент управления криптографией*.

Полная информация о наборах прав, связанных с каждой ролью, содержится на вкладке *Безопасность* Веб-портала.

> *Один пользователь может иметь несколько ролей SDMS.*

Таблица 1 – Описание ролей SDMS

Роль	Описание
Администратор ИБ	Выполняет все действия, связанные с созданием защищённых ресурсов и предоставлением прав доступа к ним. Управляет настройками самой системы SDE, её политиками и ролями пользователей. Действия, осуществляемые через **Веб-портал:** • управление пользователями SDE: добавление, удаление, блокирование, назначение ролей; • регистрация и удаление сертификатов учётных записей с ролями Пользователь и Оператор; • управление рабочими станциями; • действия с защищаемыми ресурсами: зашифрование, расшифрование, присоединение, отсоединение и т.д.; • изменение политик SDE.

	Действия, осуществляемые через **Агента Secret Disk Management Server** • изменение настроек управляющего сервера SDMS; • запуск и остановка службы SDMS; • операции с мастер-ключом базы данных (копирование, восстановление, отзыв, смена ключа); • изменение настроек поставщиков криптографии.
Оператор[1]	Включает или отключает доступ ко всем защищённым ресурсам, находящимся под управлением SDE. Эти операции выполняются через приложение Агент SDMS и называются *Монтированием криптохранилища* и *Демонтированием криптохранилища* соответственно. Кроме операций с криптохранилищем, Оператор может делать резервное копирование и восстановление Мастер-ключа БД. Операции смены и отзыва Мастер-ключа БД оператору недоступны. У Оператора нет прав на изменение настроек пользователей и рабочих станций через Веб-портал и на действия с защищёнными ресурсами, но он может просматривать настройки системы и журналы операций. Также Оператор может запустить план обслуживания.
Пользователь[2]	Единственная роль, позволяющая получить доступ к данным, защищёнными средствами SDE. Для этого используется приложение Secret Disk Agent (SDA), установленное на рабочей станции пользователя. С помощью Secret Disk Agent пользователь может создавать защищённые папки и контейнеры, если это разрешено пользовательской или глобальной политикой. Учётные записи с ролью Пользователь не имеют доступа к Веб-порталу.
Аудитор	Не является активным пользователем SDE, имеющим возможность вносить изменения или использовать защищённые ресурсы. Возможно просматривать настройки, выполненные Администратором ИБ и просматривать журналы событий в системе. Доступная информация: • конфигурация сервера (настройки, хранящиеся в реестре сервера бизнес-логики); • списки компьютеров, дисков, ролей, пользователей и их сертификатов, входящих в план обслуживания процедур; • информация о лицензиях; • информация о мастер-ключе БД; • журнал событий.
Агент восстановления	Предоставление доступа к защищённым ресурсам в особых ситуациях, когда это невозможно сделать обычным образом. Например, токен

[1] Для монтирования криптохранилища к управляющему серверу подключается токен с сертификатом Оператора и оператор вводит свой пароль к нему. Сервер бизнес-логики читает из базы данных зашифрованный Мастер-ключ и расшифровывает его с помощью электронного ключа оператора. Расшифрованный Мастер-ключ помещается в память сервера бизнес-логики, после чего сервер бизнес-логики может получать ключи к защищённым ресурсам и отправлять их в зашифрованном виде на рабочие станции для доступа к ресурсам.

При демонтировании криптохранилища, Мастер-ключ и все загруженные ключи шифрованания стираются из памяти сервера бизнес-логики и предоставление ключей клиентам рабочих станций прекращается.

[2] Для доступа к защищённым ресурсам Пользователь подключает к компьютеру свой токен и вводит пароль. При успешной авторизации SDA обращается к управляющему серверу и получает от него ключи шифрования для защищённых ресурсов. (Ключи шифрования ресурсов пересылаются зашифрованными так, что расшифровать их может только конкретный пользователь, которому они отправлены). После получения и расшифрования ключей, SDA присоединяет защищённые ресурсы своей рабочей станции, и Пользователь получает к ним доступ.

	недоступен (утерян, поврежден). Или требуется открыть защищённый ресурс в условиях, когда компьютер пользователя не может соединиться с сетью предприятия и подключиться к системе SDE. Пользователю может быть передан ключ защищённого ресурса напрямую *Агентом восстановления*, для чего он должен быть экспортирован из криптохранилища. Список действий: • экспорт ключей шифрования для логических, виртуальных и системных дисков; • выполнение плана обслуживания; • просмотр настроек SDE; • просмотр журнала аудита. *После восстановления нормального функционирования рабочей станции, ресурс, ключ которого был экспортирован, должен быть перешифрован. Использование экспортированного ключа для доступа приводит к его компрометации.*
Запуск плана обслуживания	Роль назначается учётным записям, от имени которых производится выполнение Плана обслуживания, осуществляемое с помощью Планировщика задач. Все прочие операции, включая доступ к веб-порталу, для этой роли недоступны.
Агент управления криптографией	Роль даёт право изменять настройки параметров алгоритмов шифрования для защищённых ресурсов, которые доступны в приложении SDMS.

6. Системные требования

6.1 Требования к программному обеспечению

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

Программное обеспечение	Сервер SDMS	Сервер СУБД	Рабочая станция	Примечание
Операционная система	Windows Server 2008 SP2 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	Windows Server 2008 SP2 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	Windows 7 Windows 8 Windows 8.1 Windows 10	32-битные и 64-битные
Microsoft .NET Framework	Microsoft .NET Framework 4.5.x	—	—	
Microsoft IIS	IIS 6 и выше	—	—	В настройках Microsoft IIS должен быть включён режим IIS 6 Management Compatibility
SQL Server	—	MS SQL Server 2008 SP1 и выше MS SQL Server 2008 R2 MS SQL Server 2012 Windows Server 2016	—	
Драйверы и приложение для ключей eToken	eToken PKI Client 5.1 SP1 или SafeNet Authentication Client 8.3 SP2 и выше	—	eToken PKI Client 5.1 SP1 или SafeNet Authentication Client 8.3 SP2 и выше	
Драйверы и приложение для ключей JaCarta	JaCarta Unified Client 2.12		JaCarta Unified Client 2.12	Перед установкой JaCarta Unified Client необходимо установить eToken PKI Client 5.1 SP1

Программное обеспечение	Сервер SDMS	Сервер СУБД	Рабочая станция	Примечание
Пакет поддержки дополнительной криптографии	Crypto Extension Pack 4.13.7	–	Crypto Extension Pack 4.13.7	Необходим для поддержки дополнительных алгоритмов шифрования и сторонних криптографических решений CryptoPro CSP и Infotecs Vipnet CSP
Поставщик шифрования ГОСТ	CryptoPro CSP 4.0 R3, R4 или Infotecs VIPNet CSP 4.2 и выше	–	CryptoPro CSP 4.0 R3, R4 или Infotecs VIPNet CSP 4.2 и выше	

Для обращения к Веб-порталу необходимо использовать браузер Internet Explorer 8.0 или более поздней версии. При использовании серверной ОС необходимо отключить компонент Конфигурация усиленной безопасности Internet Explorer (IE CSP).

Поддержка токенов, поставщик шифрования ГОСТ и пакет поддержки дополнительной криптографии должны быть установлены на компьютере с ролью Служба сертификации.

6.2 Требования к аппаратному обеспечению

6.2.1. Дисковое пространство

SDMS	SDA
Не менее 250 МБ	Не менее 15 МБ

6.2.2. Оперативная память

SDMS	SDA
Не менее 2 ГБ	Не менее 512 МБ

6.2.3. Порты и считыватели

Для работы с токеном в форм-факторе USB-ключа требуется один и более свободных портов USB 2.0 (3.0).

Для работы с токеном в форм-факторе смарт-карты требуется считыватель для смарт-карт, например, Athena ASEDrive IIIe.

На рабочих станциях рекомендуется применять USB-считыватели.

COM-считыватели не используются на рабочих станциях, так как загрузчик Secret Disk Agent их не поддерживает, что делает недоступным функцию защиты системного раздела.

6.2.4. Поддерживаемые модели JaCarta

- JaCarta PKI в форм-факторе USB-ключа или смарт-карты;
- JaCarta PKI с обратной совместимостью с продуктами компании Aladdin в форм-факторе USB-ключа или смарт-карты.

6.2.5. Поддерживаемые модели eToken

- eToken PRO 32K/64K — электронный ключ eToken PRO с объёмом памяти 32 КБ/64 КБ в форм-факторе USB-ключа;
- eToken PRO Smartcard — электронный ключ eToken PRO с объёмом памяти 32 КБ/64 КБ в форм-факторе смарт-карты;
- eToken PRO (Java) – электронный ключ eToken PRO с объёмом памяти 72 КБ с возможностью расширения функционала за счёт загрузки дополнительных приложений (Java-апплетов) в форм-факторе USB-ключа или смарт-карты.

6.2.6. Криптопровайдеры алгоритмов шифрования ГОСТ

SDE может использовать внешние криптопровайдеры, реализующие алгоритмы шифрования, определенные стандартами ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012, ГОСТ 28147-89.

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

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

> *Алгоритмы шифрования ГОСТ могут быть использованы только после загрузки ядра ОС и неприменимы для защиты системного диска.*

Таблица 2 – Совместимое ПО

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

7. Установка Secret Disk Enterprise

Перед установкой программного комплекса SDE необходимо подготовить следующие службы:

1. Установить поддержку токенов и служб криптографии.
2. Выпустить сертификаты пользователей на токенах.
3. Создать пользователей и группы Active Directory для назначения ролей SDE.
4. Настроить службы:
   - СУБД MSSQL Server;
   - DNS Service;
   - Windows Firewall;
   - Web Server IIS.

После подготовки инфраструктуры, развёртывание Secret Disk Enterprise происходит следующим образом:

1. Установка управляющего сервера SDMS.
2. Первоначальная настройка сервера SDMS:
   - добавление пользователей;
   - регистрация сертификатов;
   - сохранение настроек и резервное копирование.
3. Установка клиентского программного обеспечения Secret Disk Agent на рабочие станции.

8. Подготовка инфраструктуры

В разделе приводятся требования и рекомендации по настройке общесистемных компонент и служб, которые необходимо выполнить для успешной установки и работы SDE.

Для настройки рекомендуется пользоваться документацией производителя программного обеспечения и разделами приложений настоящего документа.

8.1 Предварительные условия

1. Вычислительная инфраструктура организации работает под управлением службы Active Directory Domain Service.
2. Установлен сервер СУБД Microsoft SQL Server.
3. Известны реквизиты учётной записи, обладающей административными полномочиями для доступа к базе данных.
4. На компьютер, предназначенный для установки сервера управления SDMS, установлена ОС семейства Windows Server, и он является членом домена Active Directory.
5. Рабочие станции находятся под управлением клиентских ОС семейства Windows, и они являются членами домена Active Directory.
6. Установлена Службы сертификации (доменная или сторонняя), способная выпускать сертификаты пользователей с необходимыми свойствами.

8.2 Поддержка токенов и служб криптографии

1. Требования.
   - токены должны подключаться к управляющему серверу SDMS и рабочим станциям, поэтому на этих компьютерах должно быть установлено программное обеспечения для работы с ними;
   - при использовании сторонних поставщиков криптографии ГОСТ (CryptoPRO CSP, ViPNet CSP), соответствующее программное обеспечение должно быть установлено на рабочих станциях, управляющем сервере SDMS и на сервере с ролью *Certificate Authority Domain Service*, если он имеется в инфраструктуре Active Directory.
   - при использовании поставщика криптографии ГОСТ необходима установка Aladdin Crypto Extension Pack.
2. Рекомендации.
   - установите ПО для имеющихся токенов, проверьте их работоспособность;
   - установите ПО сторонних поставщиков криптографии ГОСТ.

> *Устанавливайте только одного дополнительного поставщика криптографии ГОСТ.*

8.3 Сертификаты пользователей на токенах

1. Требования.
   - сертификаты и закрытые ключи должны находиться на токенах;
   - поле *Key Usage* сертификатов должно содержать значение *Key Encipherment*;
   - в поле *Public Key* сертификатов длина ключа не менее 1024 бит для RSA-сертификатов;
   - сертификат удостоверяющего центра должен быть импортирован в хранилище сертификатов *Local Computer/Trusted Root Certification* сервера SDMS и контроллера домена Active Directory.
2. Рекомендации.
   - разверните службу *Active Directory Certification Service*, входящую в состав ОС Windows Server;

Если в инфраструктуре предприятия нет установленной Службы сертификации.

- используйте шаблон "*Smart Card User*" или "*Smart Card Logon*" для выпуска сертификатов службой *Active Directory Certification Service*.
- разрешите публикацию сертификатов в Active. Если сертификаты не будут опубликованы, для регистрации потребуются файлы с экспортированными сертификатами пользователей.

8.4 Создание пользователей и групп Active Directory для ролей SDE

1. Требования.
   - необходимо подготовить *Учётные записи* для групп и пользователей, которые потребуются в ходе начальной настройки SDE. Список создаваемых записей приведён в Таблица 3 (имена групп даны для примера и могут быть любыми):

Таблица 3 – Список создаваемых записей в Active Directory

Имя	Тип	Примечание
SDE_Admins	**Group**	Для назначения роли *Администратор ИБ*
SDE_Audit	**Group**	Для назначения роли *Аудит*
SDE_Maintenance	**Group**	Для назначения роли *Запуск плана обслуживания*
SDE-op	**User**	Пользователь с SDE-ролью *Оператор*

2. Рекомендации.
   - группы Active Directory, соответствующие встроенным ролям SDE, при развёртывании системы могут быть пустыми, то есть не содержать учётных записей;
   - в качестве учётной записи для роли *Оператор* может быть использована любая учётная запись.

8.5 Подготовка СУБД MSSQL

1. Требования.
   - предоставить серверу SDMS доступ к базе данных Microsoft SQL Server с подключением по протоколу TCP/IP и авторизацией по учётной записи домена или по учётной записи сервера MSSQL;
   - учётная запись для сервера SDMS должна обладать правом создания и администрирования базы данных MSSQL.
2. Рекомендации.
   - для работы SDMS рекомендуется *SQL Database Engine* редакции Standard или Enterprise;
   - использование редакции Express допустимо, но не рекомендуется из-за ограниченных возможностей обеспечения высокой доступности и производительности, необходимой для SDE;

Создайте учётную запись на сервере MSSQL с правом создания базы данных, или дайте право на создание новой базы данных учётной записи AD, которая будет использоваться для установки управляющего сервера.

- мастер настройки SDMS использует сервис *SQL Service Browser* для обнаружения доступных серверов MSSQL, наличие этого сервиса упрощает конфигурирование SDMS.

8.6 Настройка DNS Service

1. Рекомендации.
   - рекомендуется иметь в DNS Service запись типа SRV для сервиса sdms. Это позволит приложениям Secret Disk Agent обращаться к серверу SDMS без явного указания имени сервера;
   - запись о сервисе должна размещаться в ветке Forward Lookup Zones/_tcp и иметь следующие значения полей (внимание: доменное имя должно заканчиваться точкой!):
     - Service: **_sdms;**
     - Protocol: **_tcp;**
     - Port Number: **8888;**
     - Host offering this service: <полное доменное имя сервера SDMS с точкой на конце>.

Если сервисную запись создать невозможно, то имя сервера SDMS нужно будет задать записью в реестре при настройке Secret Disk Agent на каждой рабочей станции.

8.7 Настройка Windows Firewall

1. Рекомендации.
   - на сервере SDMS разрешите все входящие соединения со стороны компьютеров, входящих в домен. По умолчанию они запрещены и подключение рабочих станций к SDMS будет невозможно;
   - создайте правила, разрешающие входящие подключения к порту клиентского шлюза SDMS – порт 8888/TCP по умолчанию;
   - на сервере СУБД MSSQL разрешите входящие соединения со стороны домена к портам 1433/TCP и 1434/UDP (если используется служба SQL Server Browser), либо разрешите все входящие соединения.

8.8 Настройка службы Web Server IIS

1. Требования.
   - На сервере SDMS должен быть установлен пакет Microsoft .NET Framework версии не ниже 4.5;
   - на сервере SDMS активируйте роль Web Server (IIS) и установите следующие дополнительные компоненты для неё:
     - Application Development → ASP.NET;
     - Application Development → ASP;
     - Security → Windows Authentication;
     - Management Tools → IIS 6 Management Compatibility;
   - служба Web Server IIS должна быть настроена на работу с библиотеками .NET Framework установленной версии, вместо используемых по умолчанию. Для этого настройки ISAPI and CGI Restriction в приложении IIS Manager должны выглядеть так, как показано на рисунке:

Active Server Pages	Allowed	%windir%\system32\inetsrv\asp.dll
ASP.NET v2.0.50727	Not Allowed	%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll
ASP.NET v2.0.50727	Not Allowed	%windir%\Microsoft.NET\Framework64\v2.0.50727\aspnet_isapi.dll
ASP.NET v4.0	Allowed	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
ASP.NET v4.0	Allowed	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll

Первые три записи присутствуют в таблице после установки IIS, четвертую и пятую записи необходимо добавить вручную.

   - на сервере SDMS отключите конфигурацию усиленной безопасности браузера Internet Explorer (IE ESC). Это препятствует работе с Веб-Порталом SDMS на компьютере.

2. Рекомендации.

- для отключения IE ESC откройте Server Manager на сервере SDMS и выполнить следующее:
  - на главной странице Server Manager перейдите по ссылке Configure IE ESC;
  - установите Administrators: Off;
  - установите Users: Off;
  - нажмите OK.

9. Установка Secret Disk Management Server

> *Перед началом установки сервера SDMS проверьте готовность инфраструктуры и выполнение требований и рекомендаций раздела 8.*
>
> *Подготовьте токены с сертификатами для учётных записей с ролями Администратор ИБ, Оператор и Пользователь.*

9.1 Последовательность установки сервера SDMS

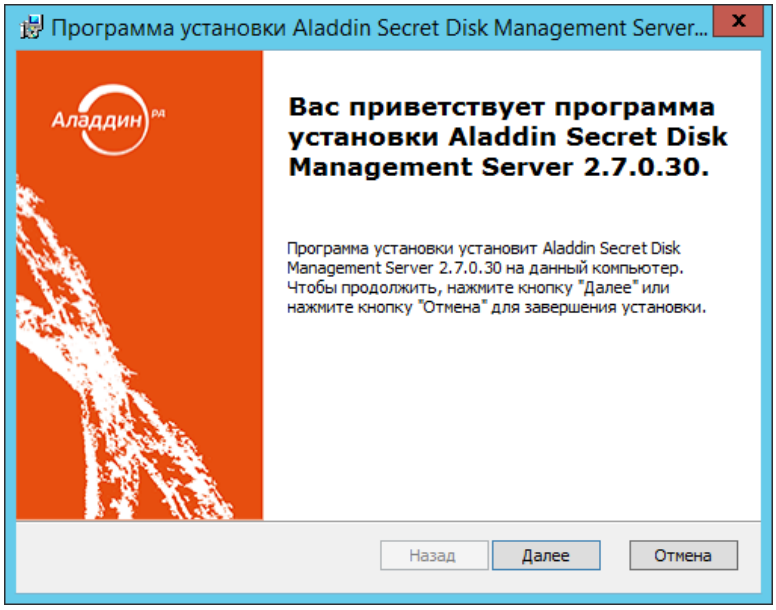
Установка SDMS проходит под управлением *Программы установки SDMS*.

> *Учётная запись, от имени которой была запущена установка, станет первым зарегистрированным пользователем SDE и приобретёт роли Администратора ИБ и Оператора.*

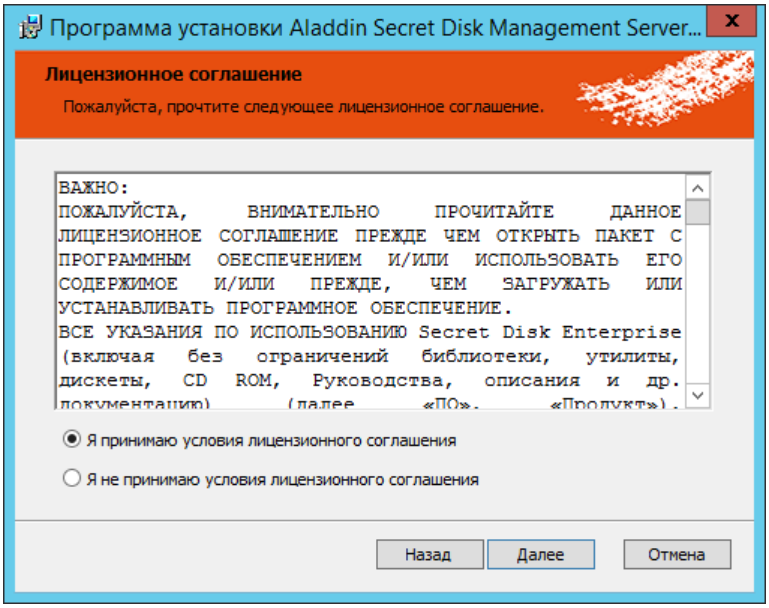
Эта же учётная запись будет использована для доступа к базе данных MSSQL, если при настройке не будет указана учётная запись сервера MSSQL.

> *Убедитесь, что запуск Программы установки происходит от нужной учётной записи.*

1. Запустите мастер установки из файла sdMS-2.7.x.xx-ru-x86.msi (для 32-битных редакций Windows) или sdMS-2.7.x.xx-ru-x64.msi (для 64-битных редакций), где xx – номер сборки. На экране появится окно приветствия мастера установки SDMS. Для продолжения *Далее*.

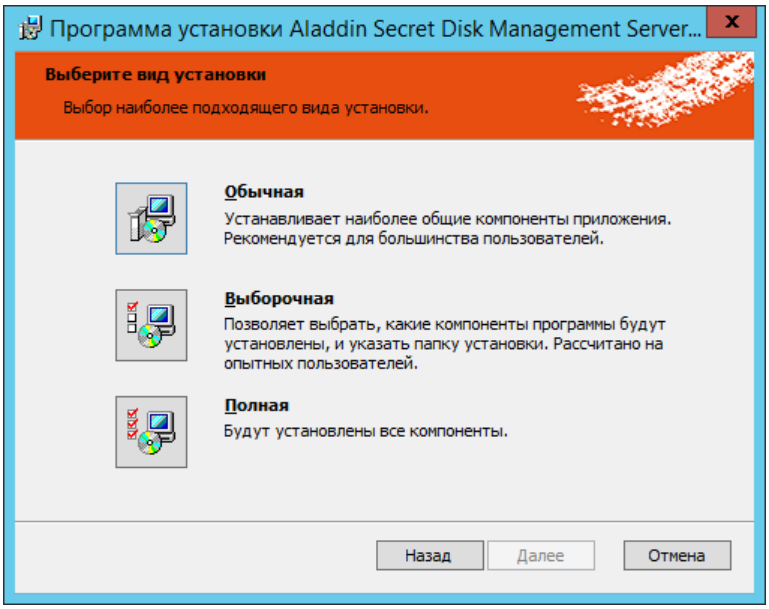


2. Ознакомьтесь с лицензионным соглашением. Выберите *Я принимаю условия лицензионного соглашения и нажмите Далее*.



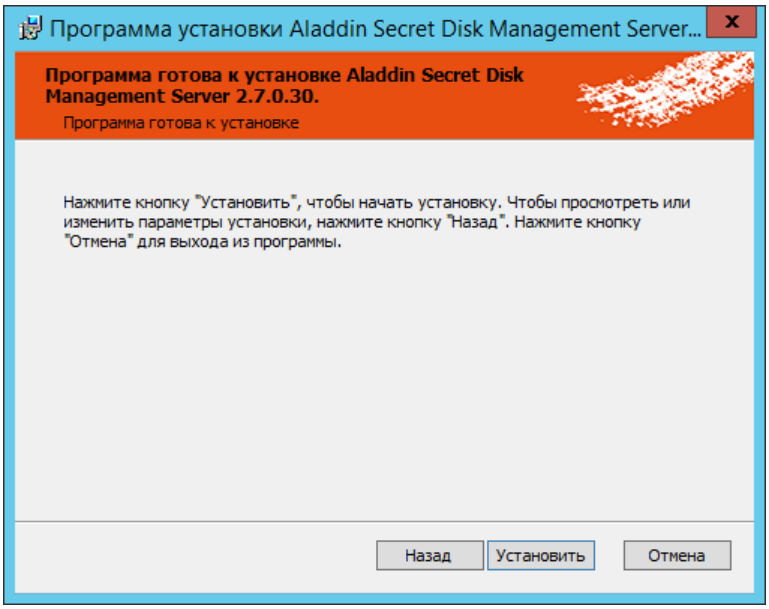
3. Выберите нужный вид установки и нажмите *Далее*.

Рекомендуется Полная установка.

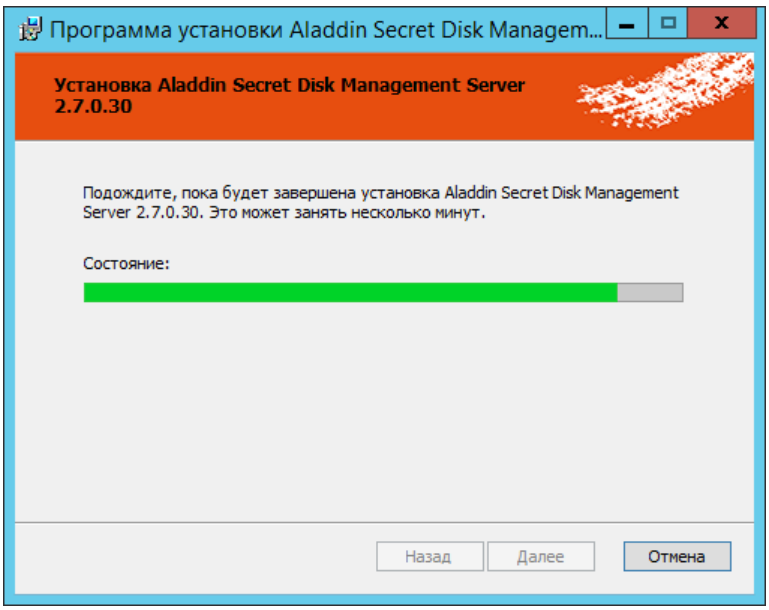


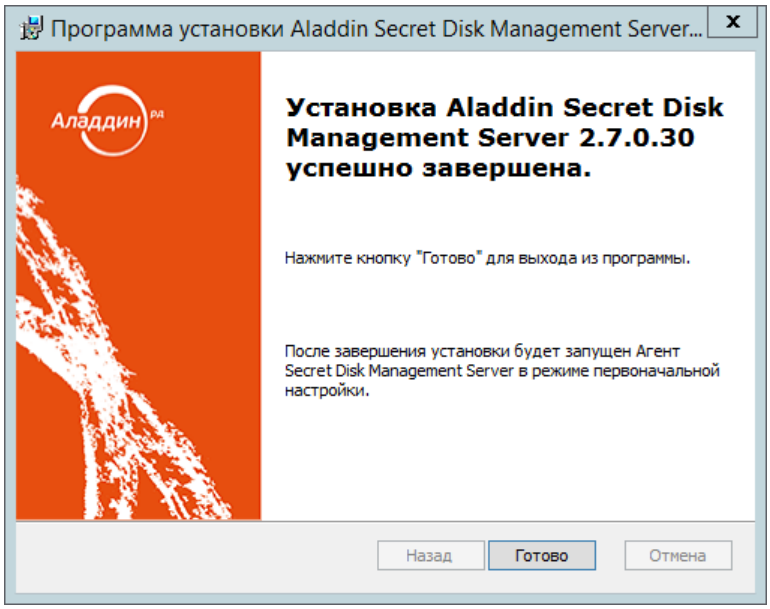
4. При необходимости измените путь установки программы. Нажмите *Далее*.

5. Нажмите *Установить*.



6. Дождитесь уведомления об успешной установке и нажмите *Готово*.





После установки SDMS на компьютер запустится Мастер первоначальной настройки SDMS.

10. Мастер первоначальной настройки SDMS

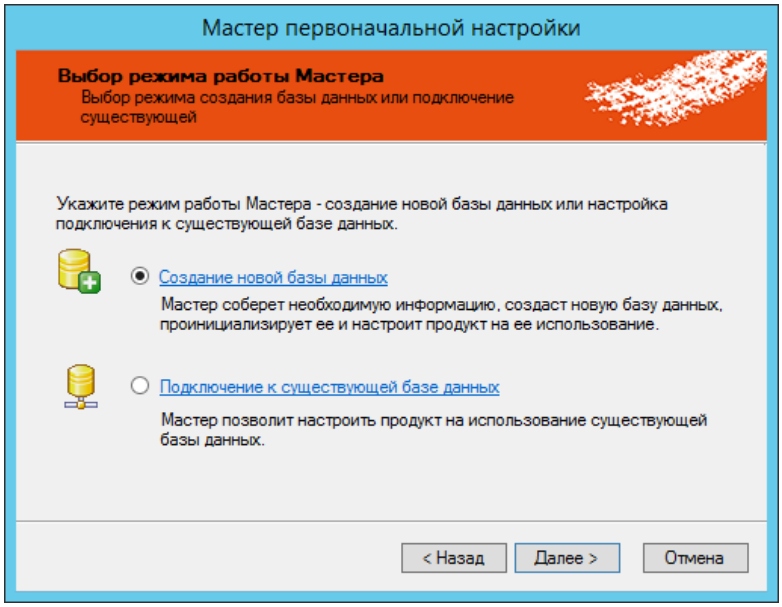
Настройка SDMS с помощью *Мастера первоначальной настройки SDMS* происходит 2 способами:

1. При создании новой база данных SDE.
2. При использовании уже существующей базы данных.

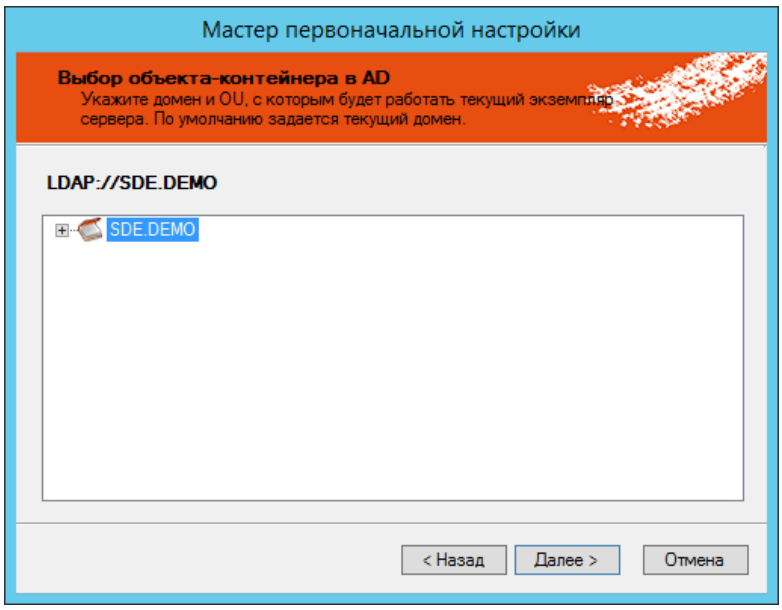
10.1 Создание новой Базы данных

Заканчивается установка параметров для создания новой базы данных настроек SDMS и Мастер переходит к установке соединения с сервером базы данных.

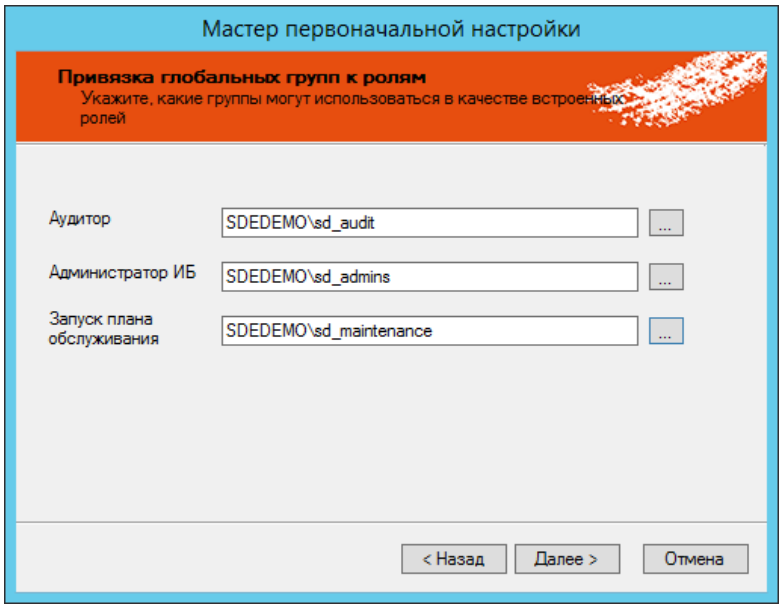
1. Выберите режим работы Мастера настройки – *Создание новой базы данных*. Нажмите *Далее*.



2. Выберите домен Active Directory, который будет обслуживать устанавливаемый сервер. Нажмите *Далее*.



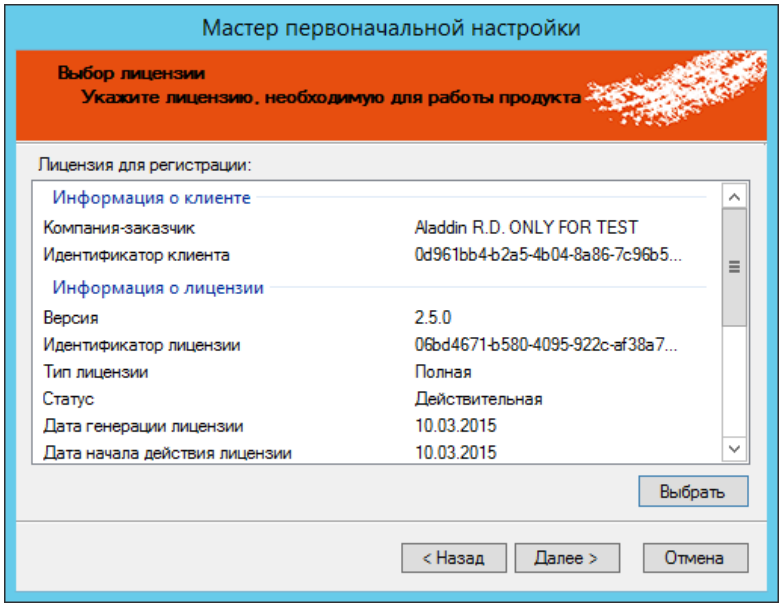
3. Укажите группы, пользователи которых приобретут права трех встроенных ролей SDE:
   - аудитор;
   - администратор ИБ;
   - запуск плана обслуживания.



Если групп нет или привязка не требуется – оставьте поля пустыми.

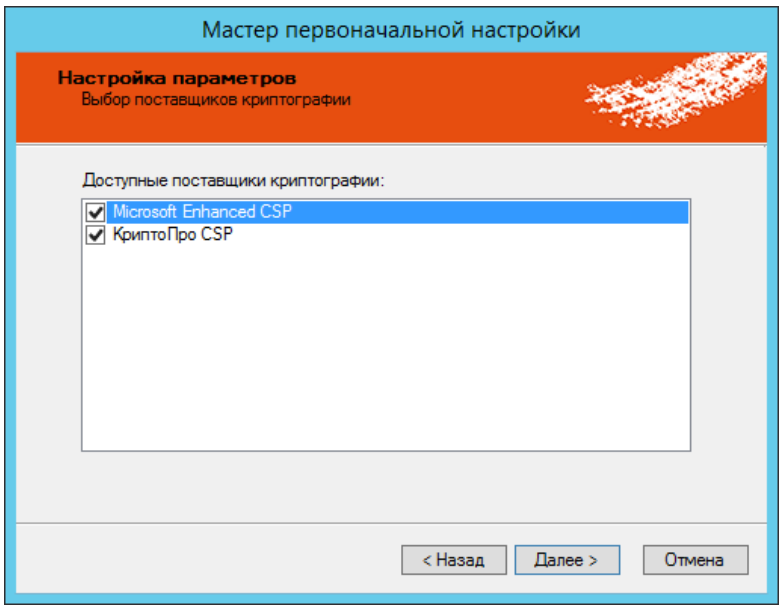
Нажмите *Далее*.

4. Для выбора лицензии нажмите *Выбрать*. Выберите файл, полученный при приобретении продукта.
5. Нажмите *Далее*.

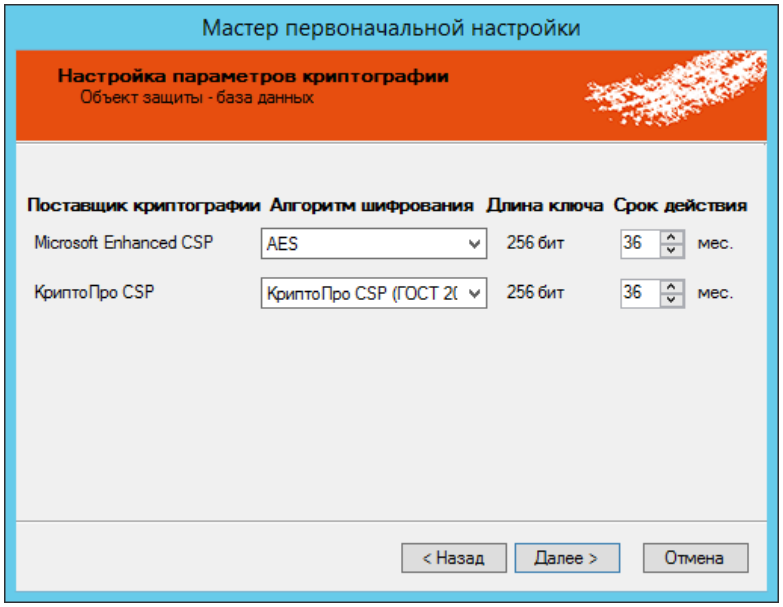


6. Выберите поставщиков криптографии и нажмите *Далее*.

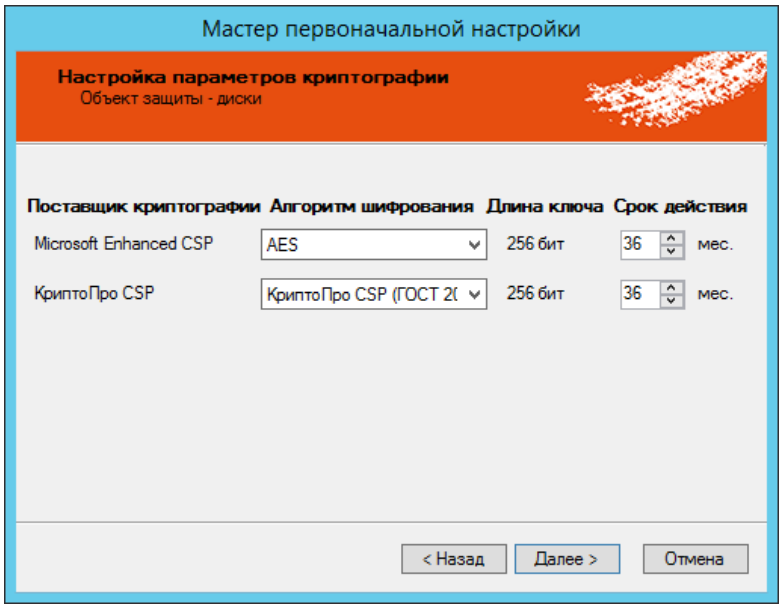
Поставщик Microsoft Enhanced CSP требуется для защиты системных разделов. Устанавливается при необходимости защиты системных разделов.



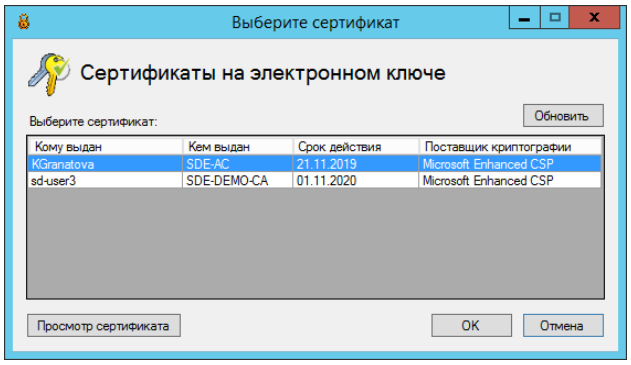
7. Укажите алгоритм и срок действия ключей для шифрования базы данных. Нажмите *Далее*.



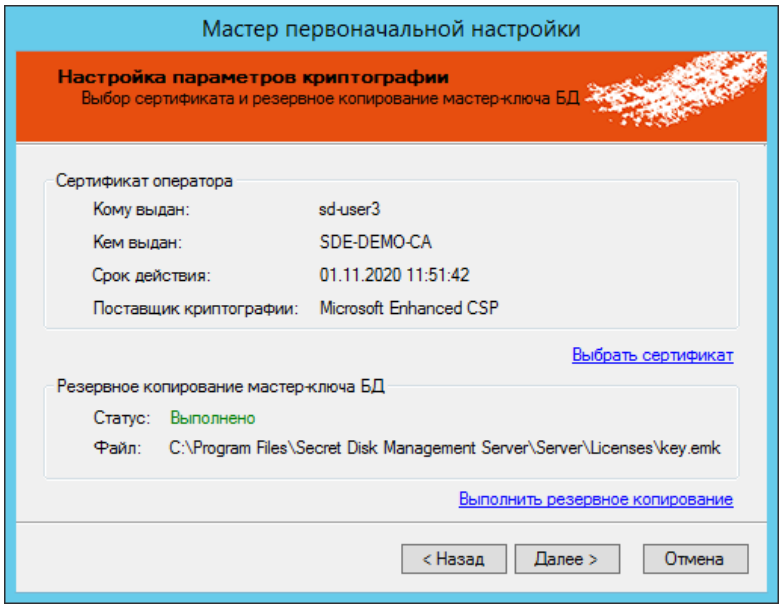
8. Укажите алгоритм и срок действия ключей для разделов (дисков) данных. Нажмите *Далее*.



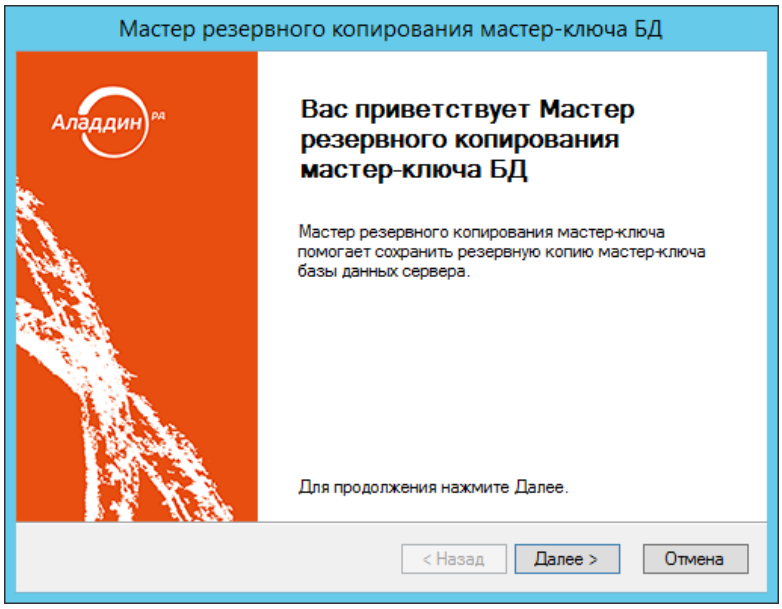
9. Укажите алгоритм и срок действия ключей для шифрования системных разделов. Нажмите *Далее*.
10. Зарегистрируйте сертификат оператора и сохраните копию мастер-ключа:
    - подключите токен пользователя, которому будет назначена роль *Оператор*;
    - нажмите *Выбрать сертификат*. Выберите сертификат, созданный ранее для учетной записи с ролью *Оператора*.



Загруженный сертификат появится в окне *Настройки параметров криптографии*.



11. Выполните резервное копирование мастер-ключа БД. Нажмите *Выполнить резервное копирование*.
12. В окне приветствия *Мастера резервного копирования мастер-ключа БД* нажмите *Далее.*



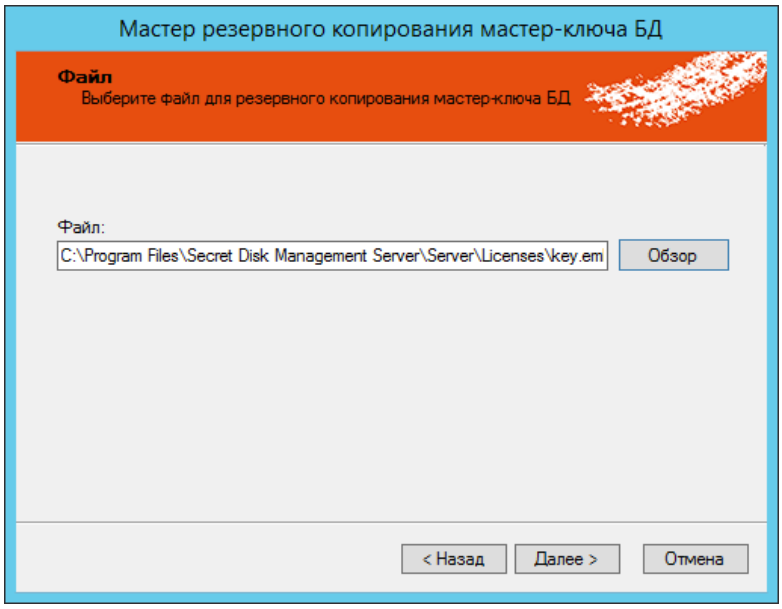
13. Выберите файл для сохранения мастер-ключа БД. Нажмите *Обзор* и укажите расположение и имя файла для сохранения копии мастер-ключа БД. Нажмите *Далее*.

Резервные копии мастер-ключей необходимы для восстановления доступа к защищённым ресурсам.

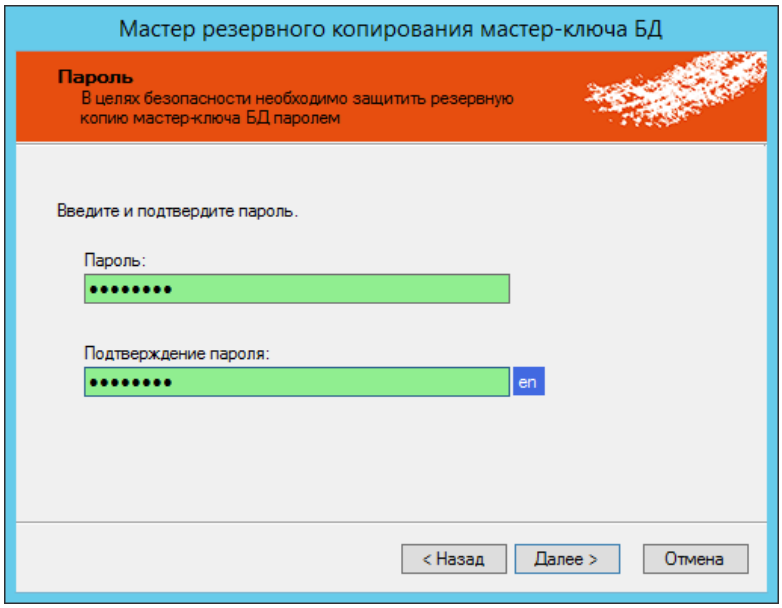
При потере или не сохранении резервной копии мастер-ключа защищённого ресурса – доступ к этому ресурсу будет невозможен.

Рекомендуется сохранять копии мастер-ключей в файле и распечатывать на принтере.

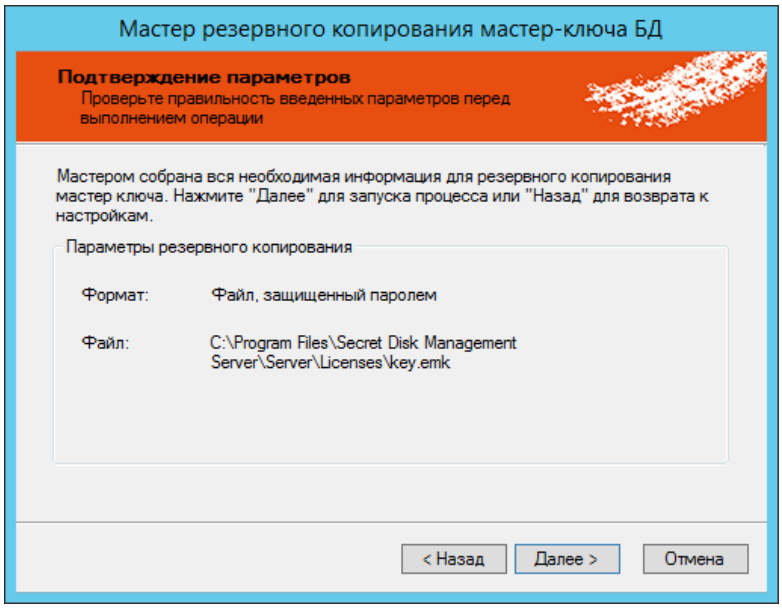
При распечатывании на принтере необходимо хранить ключ в защищённом месте, например в сейфе.



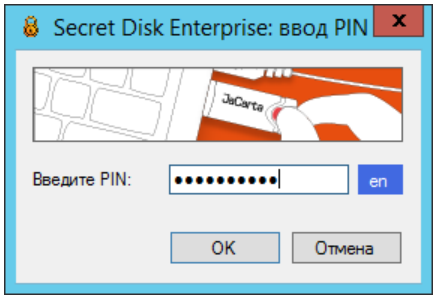
14. Введите пароль резервной копии мастер-ключа. Нажмите *Далее*.



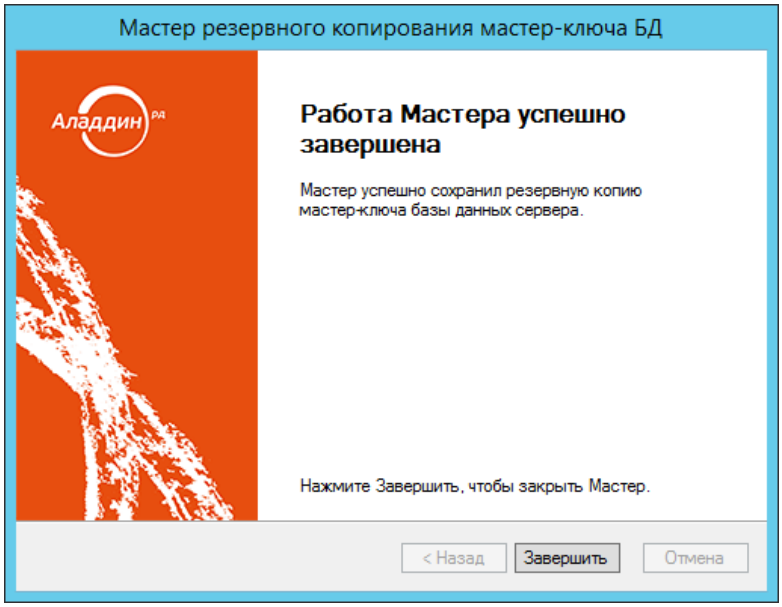
15. Проверьте правильность введенных параметров. Нажмите *Далее*.



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



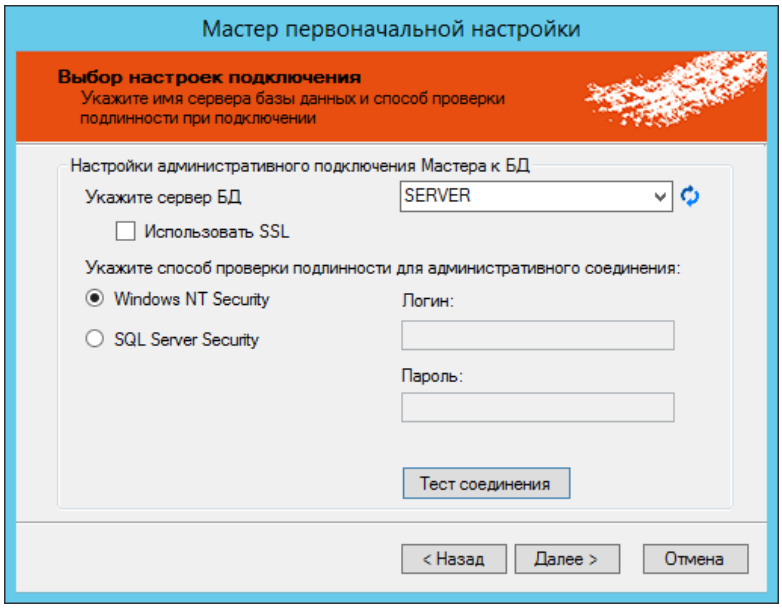
17. Нажмите *Завершить*.



На этом этапе установка параметров для создания новой базы данных настроек SDMS заканчивается. Мастер переходит к установке соединения с сервером базы данных.

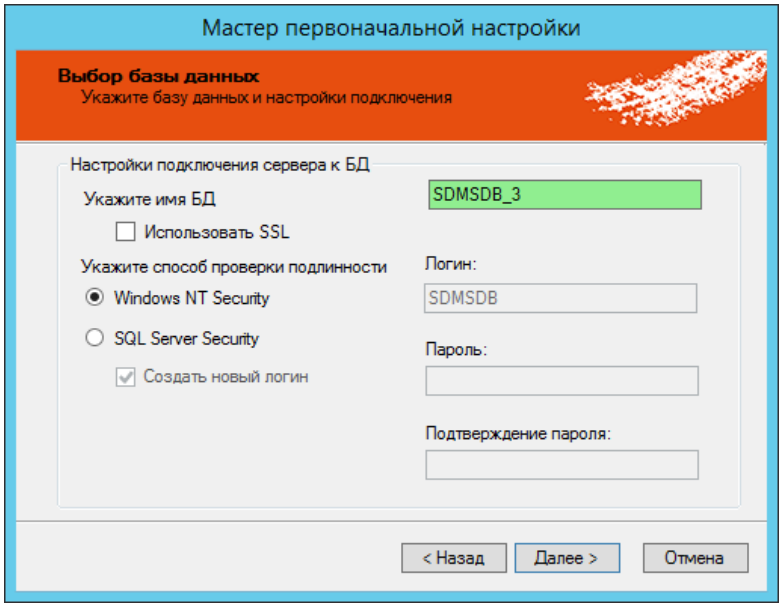
10.2 Подключение к серверу Базы данных

1. Введите имя сервера MS SQL Server.
2. Отметьте пункт SQL Server Security для ввода реквизитов учетной записи сервера MSSQL.

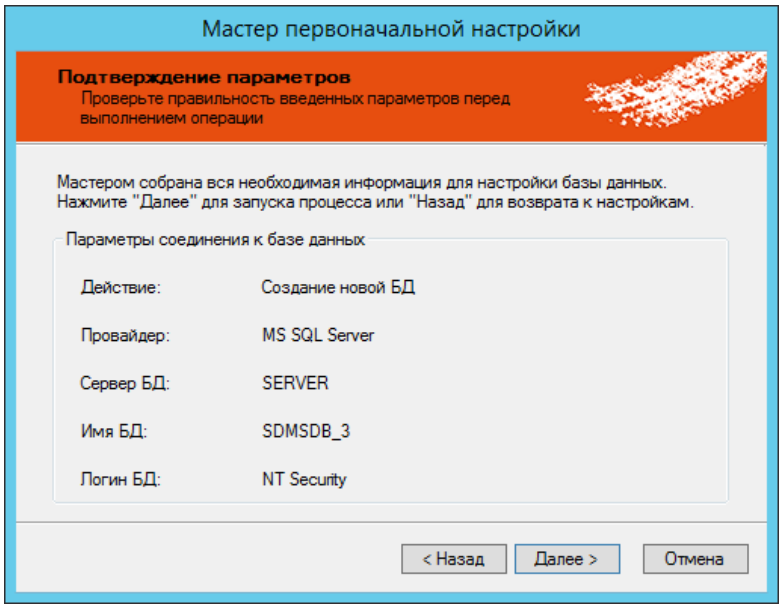


Пункт Windows NT Security необходимо выбрать при использовании доменной учетной записи из под которой происходит установка SDMS.

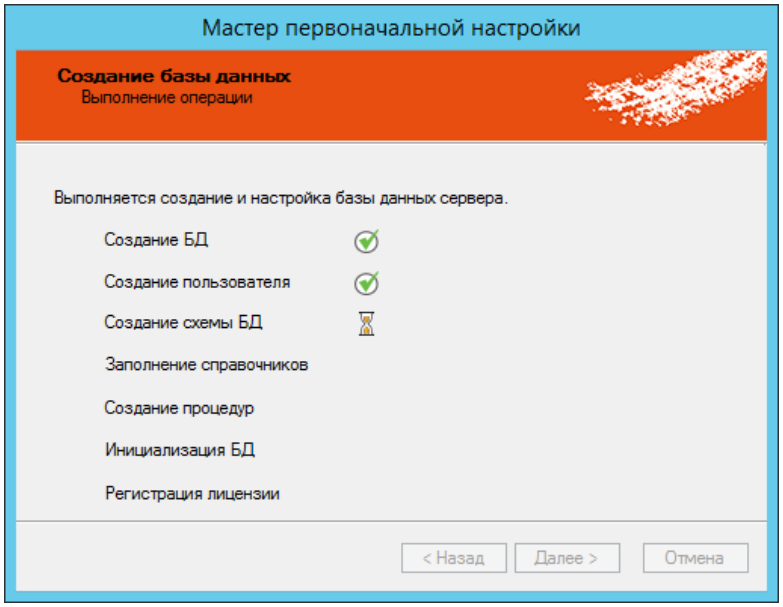
3. Нажмите *Тест соединения* для проверки доступа к серверу. При неудачном тесте проверьте имя сервера, учетную запись и права доступа.
4. Нажмите *Далее*.
5. Введите Базы данных или оставьте предлагаемое по умолчанию имя *SDMSDB*.
6. Отметьте пункт *SQL Server Security* для ввода реквизитов учетной записи сервера или создания новой учетной записи для владельца базы SDE.
7. Нажмите *Далее*.



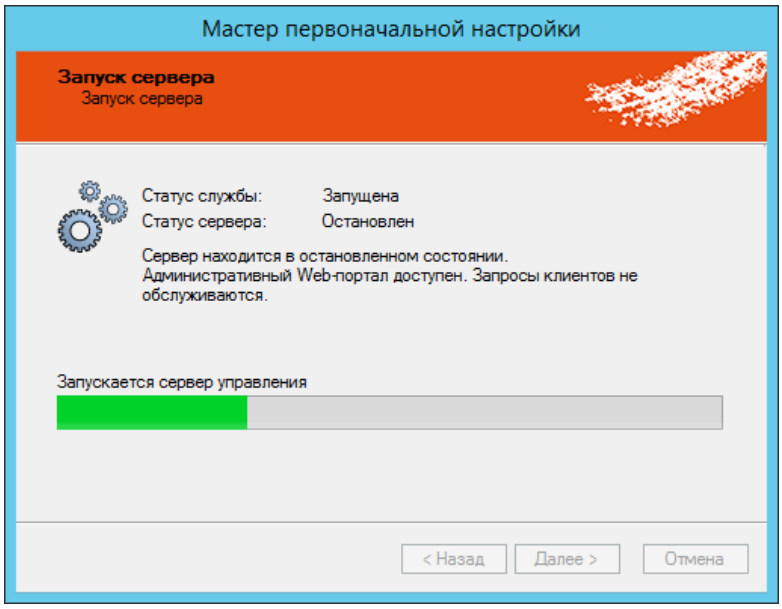
8. Проверьте правильность введенных параметров. Нажмите *Далее*.



9. После успешного создания Базы данных настроек нажмите *Далее*.



10. После успешного старта сервера нажмите *Далее*.

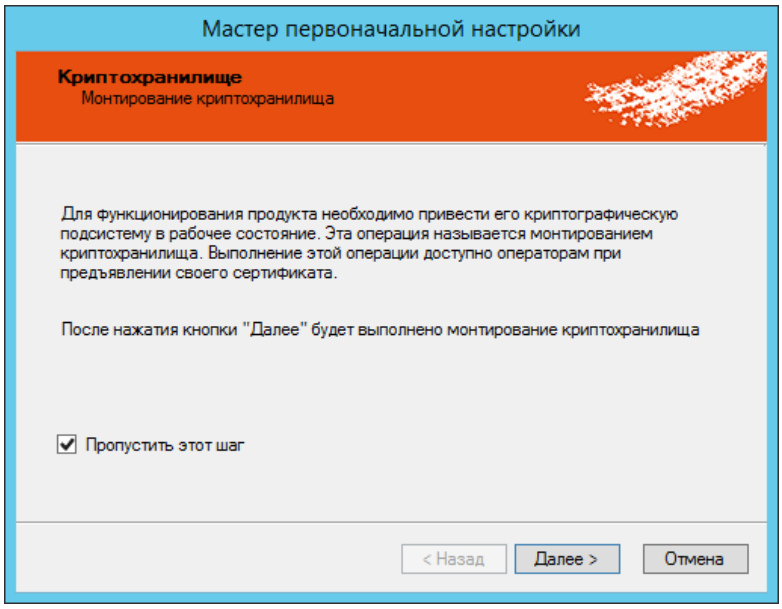


Запуск управляющего сервера SDMS.

11. Мастер первоначальной настройки предложит произвести подключение криптохранилища.

> *Если инсталляция производилась в учетной записи пользователя, для которой был зарегистрирован сертификат оператора, нажмите Далее.*

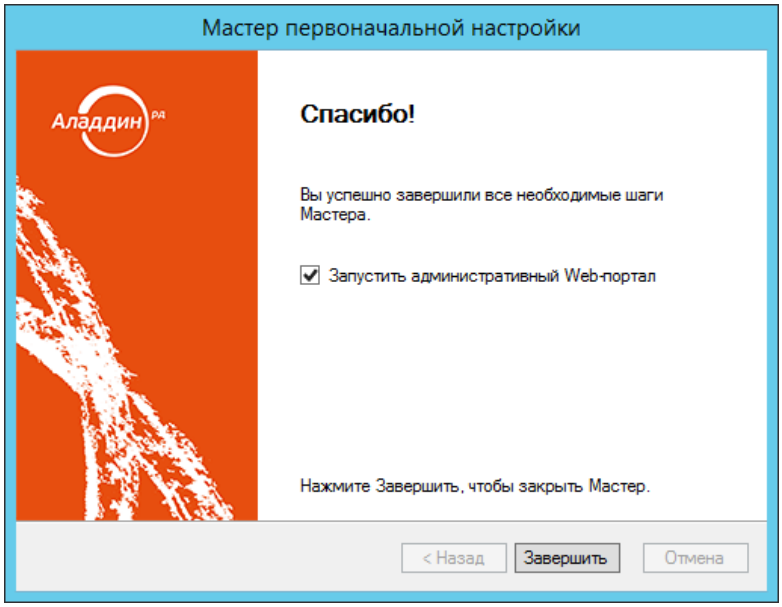
12. При необходимости сменить пользователя, выберите *Пропустить этот шаг* и нажмите *Далее*.
13. Монтирование криптохранилища можно сделать позже с помощью *Агента управления SDMS*.



14. Нажмите *Завершить*.

> *При активном флаге Запустить административный Web-портал откроется браузер Internet Explorer после завершения установки.*

*Административный Web-портал работает **только** в браузере Internet Explorer.*



10.3 Завершение установки Secret Disk Management Server

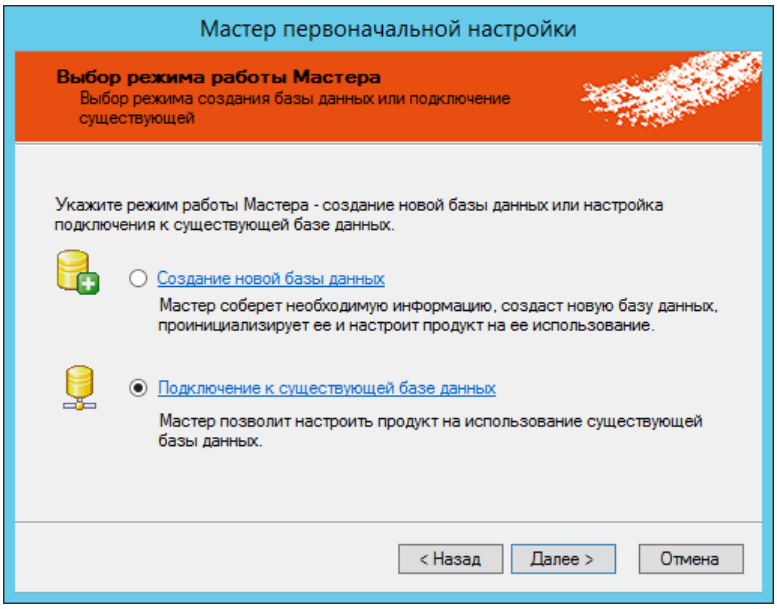
После установки управляющего сервера SDMS Администратор может приступить к добавлению пользователей, рабочих станций и защищаемых ресурсов, используя Административный веб-портал.

Рекомендуется сделать следующие действия и проверки:

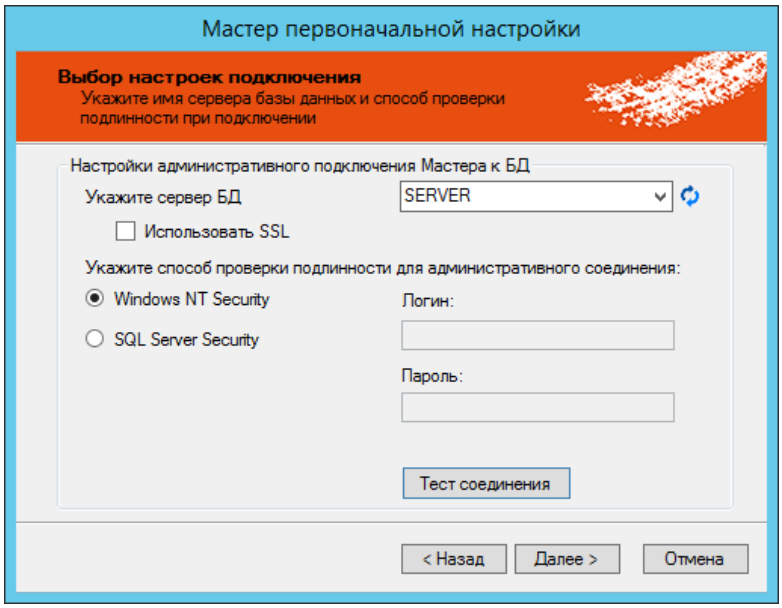
1. Назначить дополнительных пользователей на роль *Оператор* и зарегистрировать их сертификаты.
2. Проверить, что *Операторы* могут выполнять операции в Агенте Secret Disk Management Server (запускать и останавливать сервис SDMS, подключать криптохранилище и т.д.).
3. После успешной проверки, пользователь-*Администратор*, может снять с себя роль *Оператора*, которую он приобрёл в процессе инсталляции системы.
4. Настроить резервное копирование базы данных SDE средствами MS SQL Server или с помощью других средств.

10.4 Подключение к существующей Базе данных

Порядок действий при подключении управляющего сервера к существующей базе данные SDE:



1. Укажите сервер БД, под управлением которого находится существующая БД.

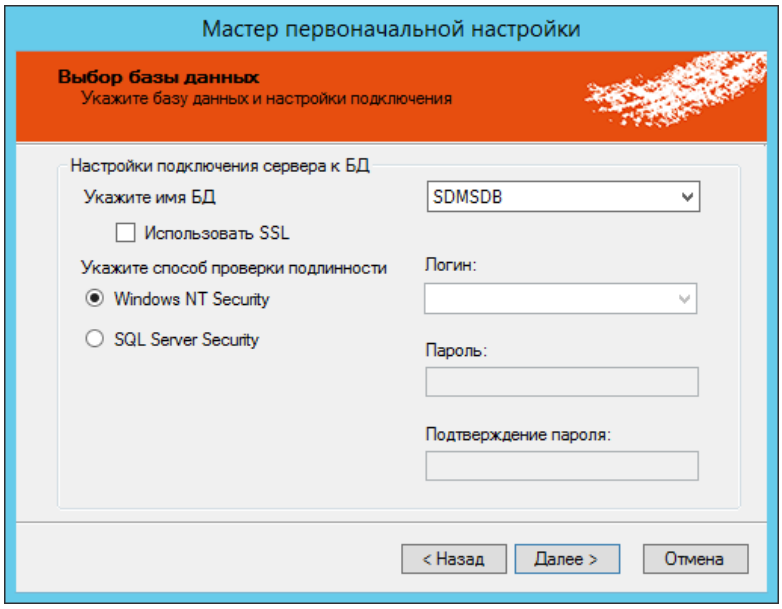


В списке серверов могут отображаться не все имеющиеся экземпляры Microsoft SQL Server, т.к. определение серверов БД в сети не является гарантированным. Если нужный экземпляр SQL Server не отображается в списке, следует ввести его полное имя вручную.

2. Если вы хотите использовать соединение по протоколу SSL, отметьте пункт *Использовать SSL*.
3. Укажите способ проверки подлинности для административного соединения:
   - *Windows NT Security*: используется текущая доменная учётная запись;
   - *SQL Server Security*: для авторизации в полях *Логин* и *Пароль* необходимо указать имя и пароль учётной записи пользователя Microsoft SQL Server.
4. Для проверки соединения с сервером БД нажмите кнопку *Тест соединения*. При успешном соединении появится окно с сообщением *Соединение с сервером успешно установлено*.
5. Нажмите *Далее*.
6. Введите имя базы данных в поле *Укажите имя БД* и выберите способ логина:

- *Windows NT Security*: используется учётная запись пользователя Windows;
- *SQL Server Security*: здесь можно указать существующую учётную запись (поле *Логин*) или создать новую, отметив пункт *Создать новый логин* и указав новый пароль в полях *Пароль* и *Подтверждение пароля* (пароль должен иметь длину не менее 8 символов и включать символы следующих типов: цифры, спецсимволы и буквы в верхнем и нижнем регистре).

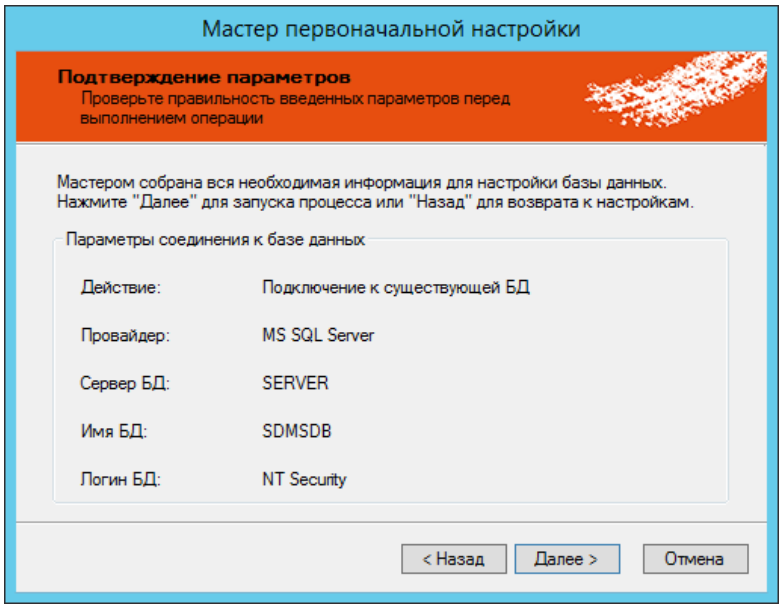
7. Нажмите *Далее*.



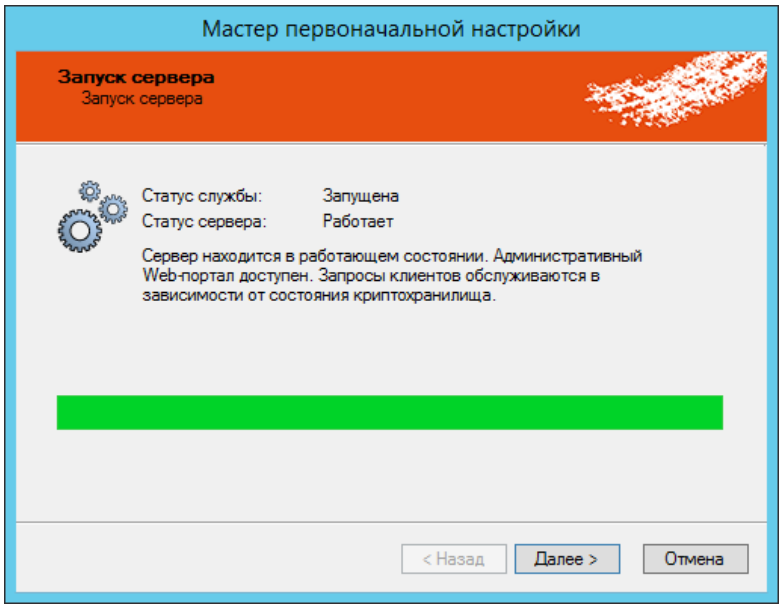
8. Если на этапе подключения к существующей базе данных будет обнаружено, что её версия ниже минимально поддерживаемой сервером, то будет предложено выполнить обновление БД. Дождитесь завершения операции обновления базы данных. Этот процесс может занять несколько минут — в зависимости от объёма данных.

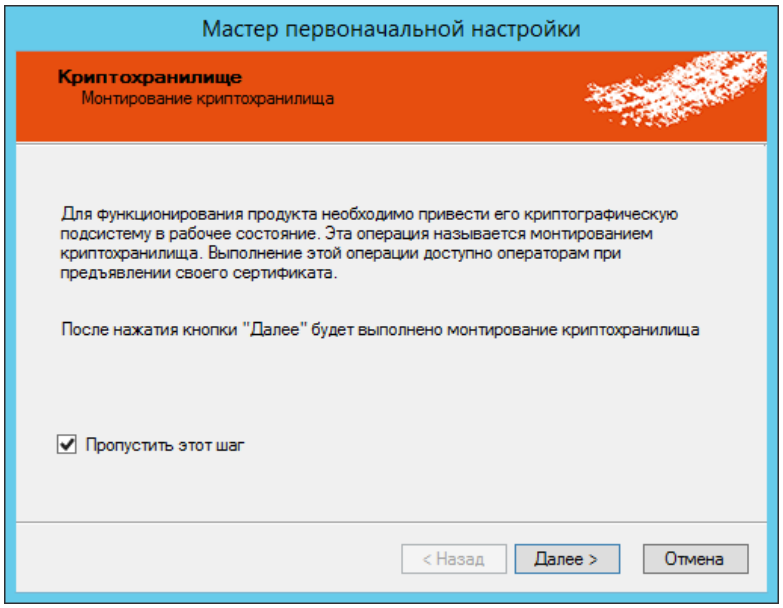
Перед началом обновления базы данных настоятельно рекомендуется выполнить резервное копирование существующей версии базы данных. Кроме того, по возможности, следует завершить все ранее начатые операции с дисками.

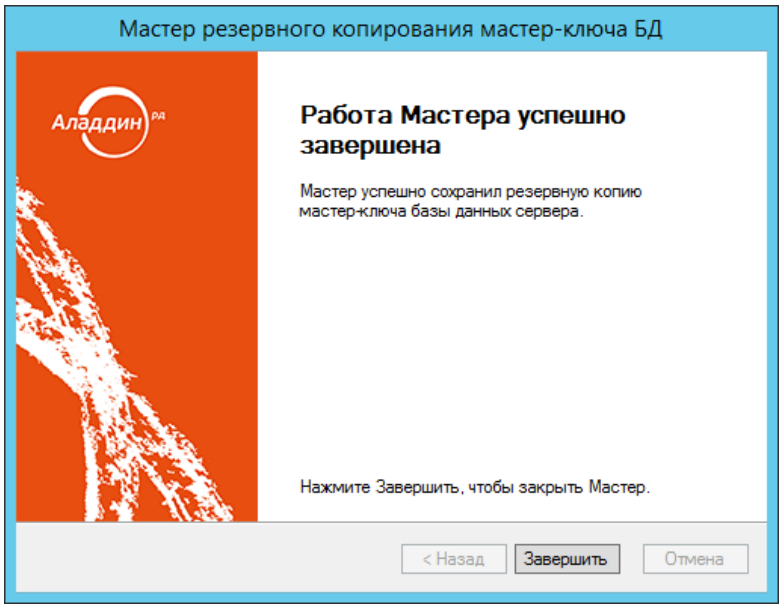
9. После завершения обновления мастер укажет актуальную версию базы данных. Нажмите *Далее*.



10. После подключения к базе данных мастер переходит к запуску сервера SDMS.







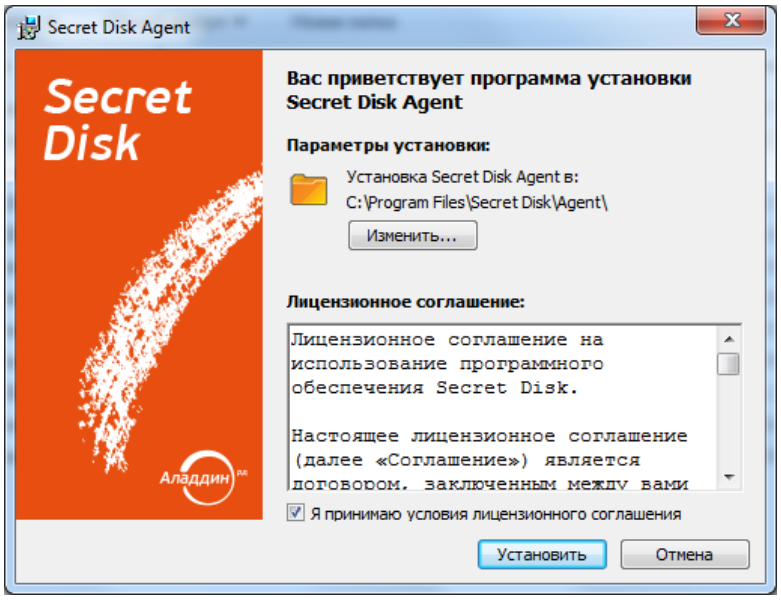
11. Нажмите *Завершить*.

11. Установка, настройка и удаление Secret Disk Agent

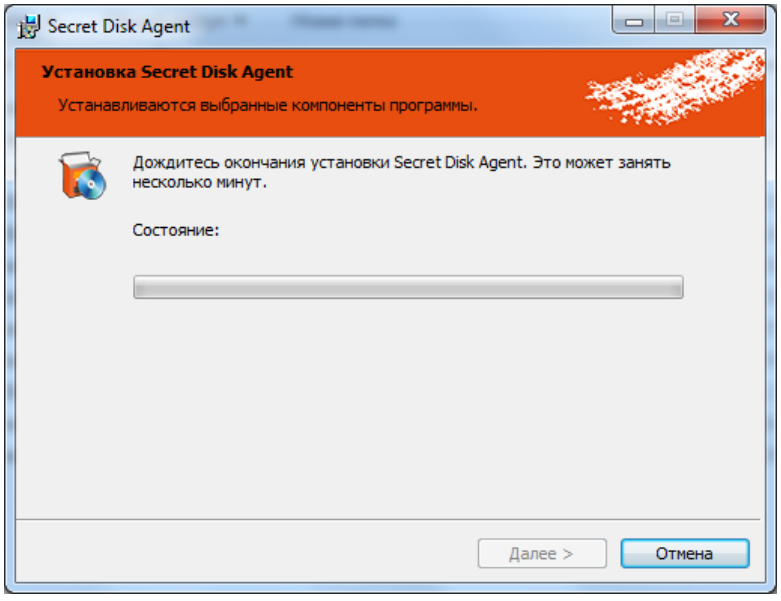
11.1 Установка Secret Disk Agent вручную

Для установка SDA на рабочую станцию необходимы права локального администратора.

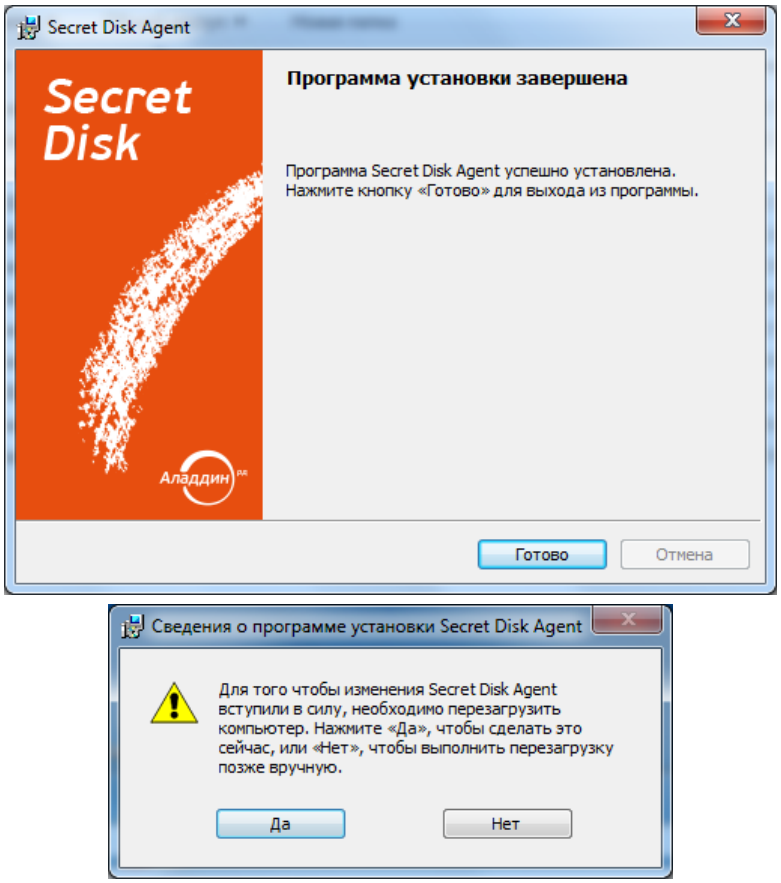
1. Запустите файл sdA-2.7.x.xx-ru-x32.msi (или sdA-2.7.x.xx-ru-x64.msi для 64-битной платформы), где xx — номер сборки.
2. Выберите папку установки программы, нажав *Изменить...*.
3. Ознакомьтесь с лицензионным соглашением и примите его условия.
4. Нажмите *Установить*.



5. Дождитесь окончания установки программы. Нажмите *Далее*.



6. Нажмите *Готово*. Перезагрузите компьютер.



11.2 Установка Secret Disk Agent с помощью групповых политик

Secret Disk Agent поддерживает установку с помощью объектов групповых политик. Для этого используются политики компьютеров (Computer Configuration), а не пользователей (User Configuration).

Для получения подробной информации о процессе установки программного обеспечения через групповые политики обратитесь к официальной документации Microsoft по ОС, используемой на контроллере домена.

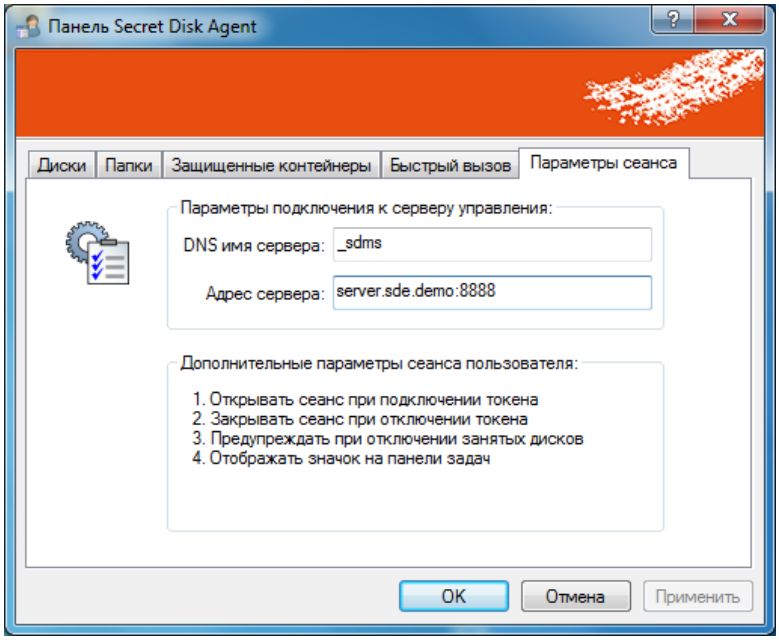
11.3 Настройка SDA

11.3.1. Настройка SDA на рабочей станции

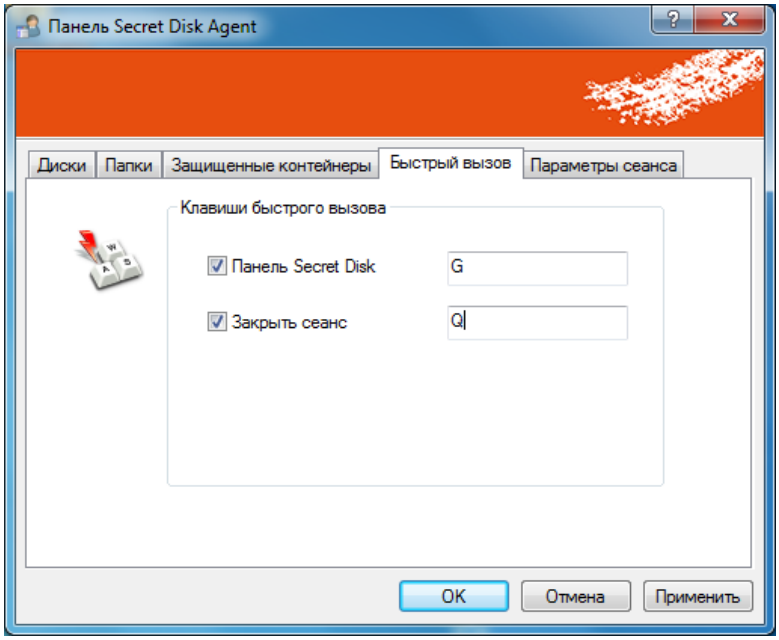
Большая часть настроек и операций с зашифрованными дисками на пользовательских компьютерах выполняется администратором на стороне сервера управления.

Пользователь может только просмотреть часть пользовательских настроек, относящихся к сеансу.

Информация о настройках находится на вкладке *Параметры сеанса*.



Настройка клавиш быстрого реагирования находится на вкладке *Быстрый вызов*.



11.4 Настройка фиксированного подключения к SDMS

В Secret Disk Agent предусмотрена возможность настройки адреса и порта шлюза клиентов. Если эти настройки выполнены, подключение по этим параметрам имеют приоритет по сравнению с поиском сервера управления по имени сервиса _sdms.

Чтобы настроить фиксированные параметры подключения к шлюзу клиентов, на рабочей станции в разделе реестра *\HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Secret Disk NG* задайте параметры, указанные в следующей таблице:

Имя параметра	Тип данных	Описание
SDMSServiceHostName	STRING	IP-адрес или имя сервера

Имя параметра	Тип данных	Описание
SDMSServicePort	DWORD	Порт сервера (значение должно быть представлено в десятичном формате)

11.5 Удаление Secret Disk Agent

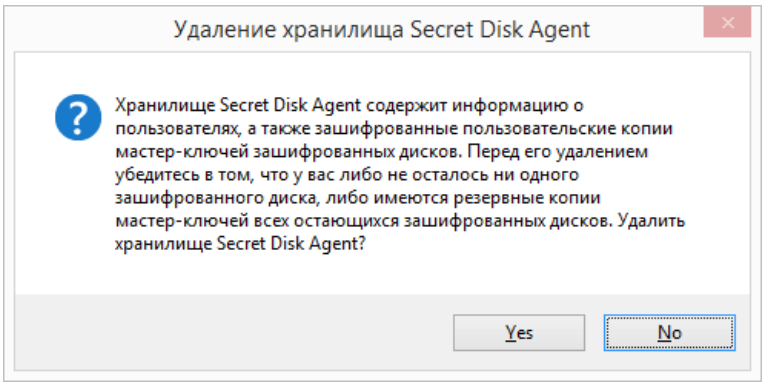
11.5.1. Удаление Secret Disk Agent вручную

Для удаления Secret Disk Agent на рабочей станции, необходимо выполнить следующие действия с правами администратора:

1. В *Панели управления* откройте список установленных программ.
2. Выберите в списке *Secret Disk Agent*.
3. Нажмите *Удалить*, в окне подтверждения нажмите кнопку *Да*.
4. Подтвердите или отклоните удаление локального хранилища настроек *Secret Disk Agent*.

Если на компьютере не осталось зашифрованных ресурсов или для них имеются ключи в базе данных SDE, нажмите кнопку Да для удаления локального хранилища на рабочей станции.

Если Secret Disk Agent на компьютере может быть установлен вновь и зашифрованные ресурсы требуется сохранить, нажмите Нет, чтобы сохранить хранилище Secret Disk Agent на этом компьютере.



5. Перезагрузите компьютер.

11.5.2. Удаление Secret Disk Agent через групповые политики

Secret Disk Agent, установленный с помощью групповой политики, можно удалить с её же помощью. Для получения подробной информации об удалении программного обеспечения, установленного с помощью групповых политик, обратитесь к официальной документации Microsoft для ОС, используемой на контроллере домена.

12. Работа с Веб-порталом SDMS

Чтобы войти на административный Веб-портал Secret Disk Enterprise, откройте в браузере **Internet Explorer** следующую ссылку: http://<имя сервера SDMS>:8888/AdminWebClient/Default.aspx/.

> *Открыть Веб-портал можно через стартовое меню системы: Start > All Programs > Aladdin > Административный Веб-портал. Ссылка для обращения к Веб-порталу создаётся при установке SDMS.*

На Рисунок 1 представлена главная страница Веб-портала. Основную область окна занимают ссылки на разделы, в которых сгруппированы ключевые функции Secret Disk Management Server.

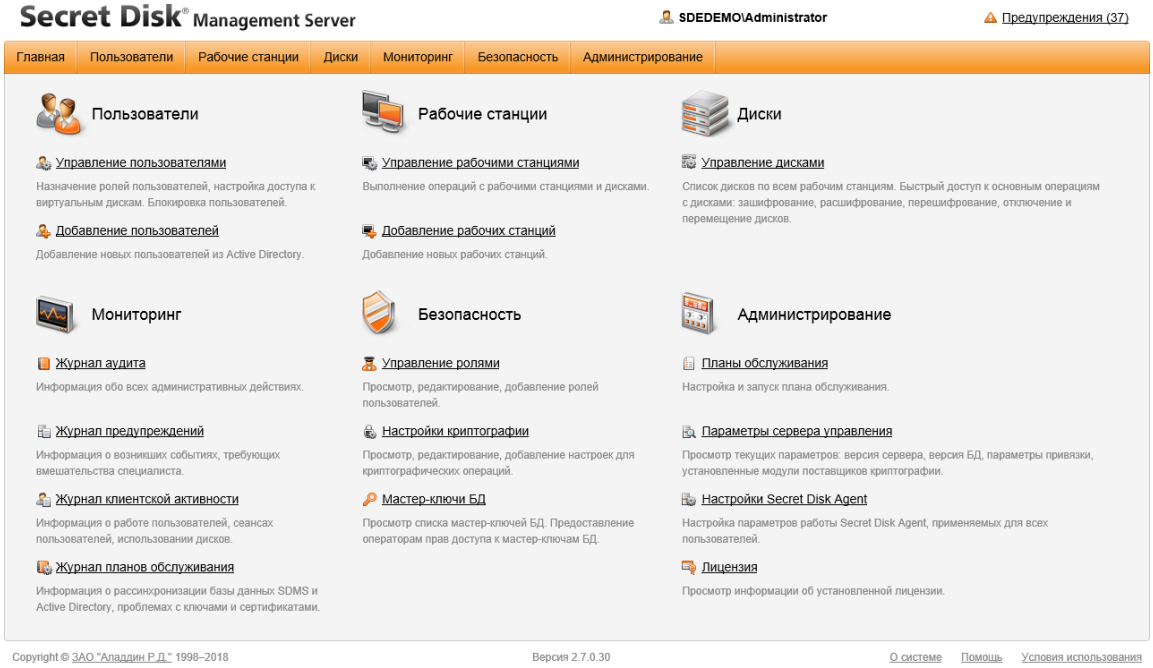


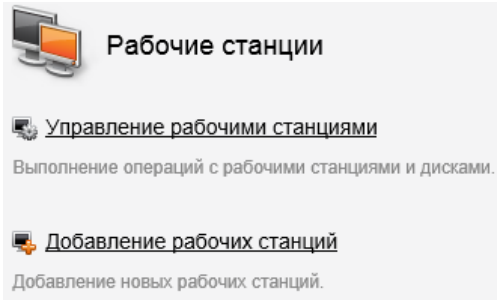
Рисунок 1 – Главная страница административного Веб-портала

13. Управление рабочими станциями SDE

Для управления рабочими станциями, через Веб-портал поддерживаются следующие операции и настройки:

1. Добавление рабочих станций.
2. Просмотр списков рабочих станций, их конфигурации и перечня защищённых ресурсов.
3. Запрос конфигурации рабочих станций.
4. Блокирование доступа к защищённым ресурсам на рабочих станциях.
5. Включение или отключение кеширования ключей на рабочих станциях.
6. Удаление рабочих станций.

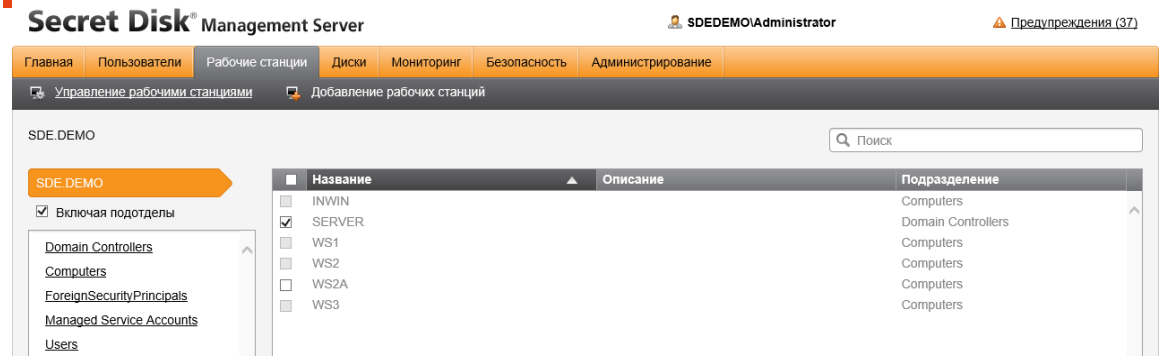
Все функции, связанные с управлением рабочими станциями, представлены в отдельном разделе *Рабочие станции* Веб-портала SDMS.



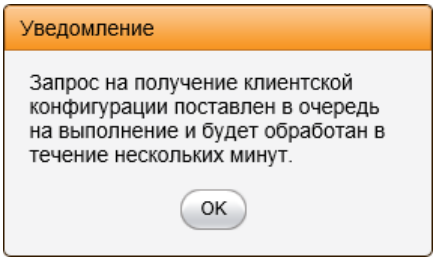
13.1 Добавление рабочих станций

Перейдите к списку рабочих станций по ссылке *Добавление рабочих станций*.

Компьютеры, уже зарегистрированные как рабочие станции SDE будут помечены серым флагом и недоступны для выбора. Флаг незарегистрированных компьютеров будет белым.

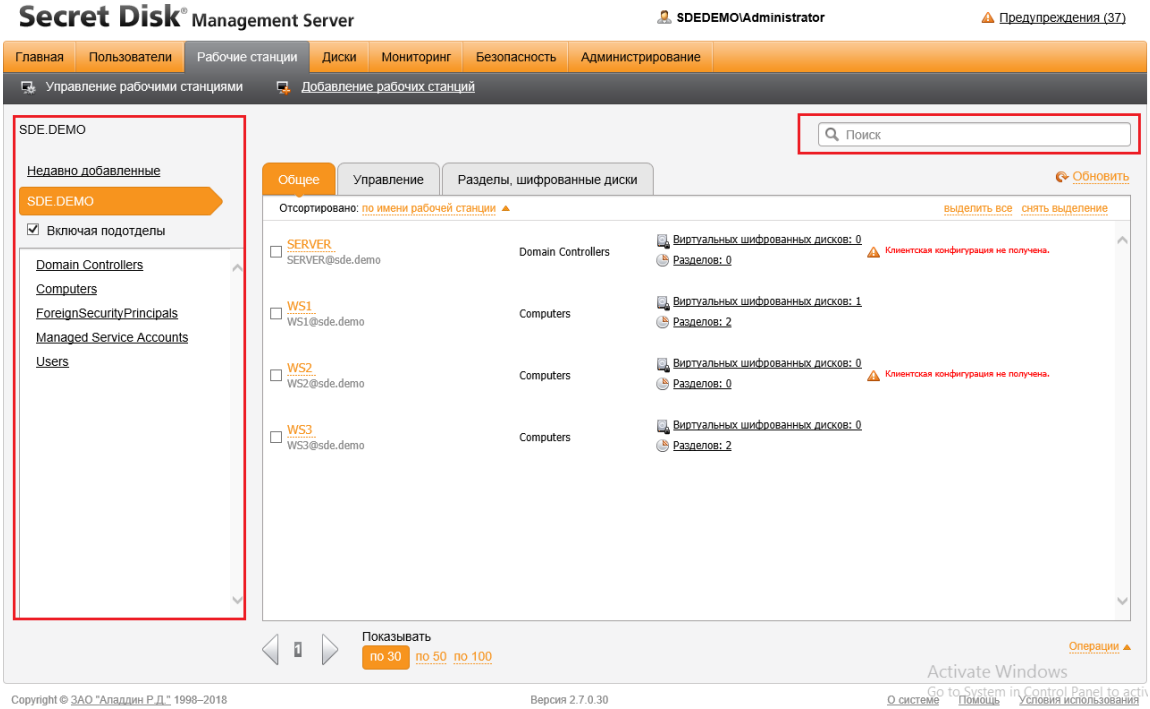


1. Отметьте компьютеры, которые необходимо зарегистрировать как рабочие станции SDE, и нажмите *Зарегистрировать выбранные*.
2. Откроется вкладка *Общее* в разделе *Управление рабочими станциями*. Вновь добавленные рабочие станции будут сопровождаться предупреждением "Клиентская конфигурация не получена", которое исчезнет после того, как SDA на рабочей станции сообщит её конфигурацию серверу управления, на что может потребоваться несколько минут.



13.2 Список зарегистрированных рабочих станций

Доступ к списку зарегистрированных рабочих станций выполняется в разделе *Управление рабочими станциями* на главной странице.



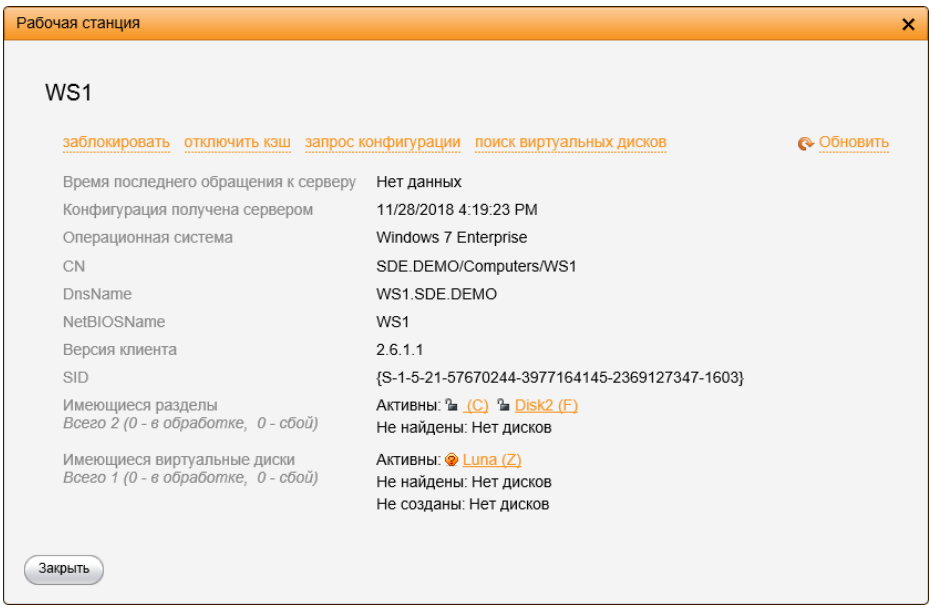
> *Если количество записей выходит за рамки одной страницы, следует воспользоваться строкой навигации в нижней части страницы.*

Для ограничения длины выводимого списка выберите организационное подразделение нужной рабочей станции в списке слева.

Для перехода к конкретной записи пользуйтесь строкой поиска справа над списком рабочих станций.

13.3 Информация о рабочей станции и действия с ней

Информацию о рабочей станции можно получить, перейдя по ссылке с её именем в любом месте портала.



В меню представлены ссылки на диски, которые расположены на выбранной рабочей станции. Доступны подробные данные по соответствующему диску (те же данные доступны на странице *Рабочие станции*, на вкладке *Управление*).

Действия с рабочей станцией:

1. Заблокировать.
   Блокирование рабочей станции делает невозможным для всех пользователей на ней подключение зашифрованных дисков. После блокирования эта ссылка меняется на ссылку *Разблокировать*.
2. Отключить кэш.
   При отключенном кэше работа с дисками в автономном режиме (без доступа к серверу SDMS) блокируется. После отключения кэша ссылка сменяется на ссылку *Включить кэш*.

> *Кэш нельзя отключить у защищённых системных дисков, у которых он всегда включён.*

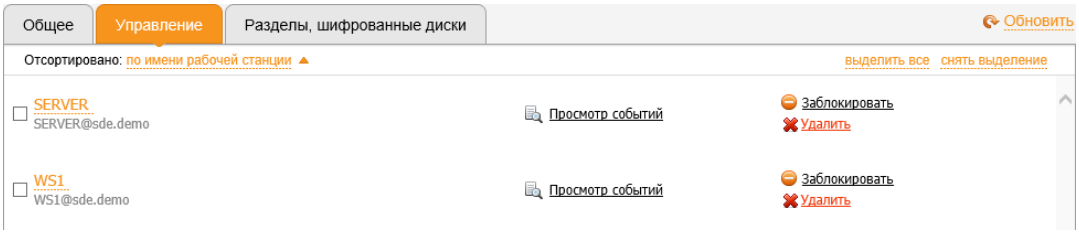
3. Запрос конфигурации.
   Операция предназначена для принудительной актуализации сведений о рабочей станции пользователя. Обновление данных может занять несколько минут. Чтобы увидеть обновлённые данные нажмите в правом верхнем углу на ссылке *Обновить*.
4. Поиск виртуальных дисков.
   Операция предназначена для поиска виртуальных дисков выбранной рабочей станции пользователя.

13.4 Блокирование и разблокирование рабочей станции

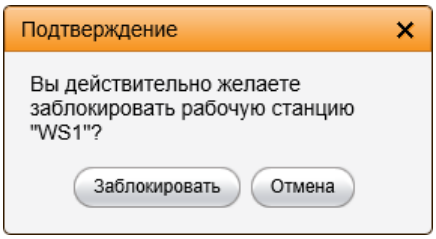
Блокирование рабочей станции позволяет Администратору отключить использование на ней любых защищённых ресурсов для всех пользователей.

Для блокирования рабочей станции выполните следующие действия:

1. Перейдите по ссылке *Управление рабочими станциями* на главной странице Веб-портала или в разделе Рабочие станции.
2. Перейдите на вкладку *Управление*.
3. Выберите нужную рабочую станцию, нажмите *Заблокировать*.



4. Подтвердите действие, нажмите *Заблокировать*.



5. Информация о заблокированной станции отобразится как указано на рисунке ниже:

> *Для разблокирования рабочей станции пользователя выполните те же действия, нажав кнопку Разблокировать.*

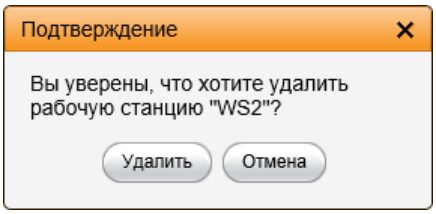
13.5 Удаление рабочих станций пользователя

> *Удаление рабочей стации из списка зарегистрированных не приводит к уничтожению защищённых ресурсов, находящихся на ней, но блокирует к ним доступ.*
>
> *При возобновлении регистрации управление ресурсами будет восстановлено, если информация о них сохранится в локальном хранилище Secret Disk Agent.*

Для удаления рабочей станции выполните следующие действия:

1. На главной странице перейдите по ссылке *Управление рабочими станциями* → вкладка *Управление*.
2. Выберите рабочую станцию, которую необходимо удалить, нажмите *Удалить*.

3. В запросе на подтверждение нажмите *Удалить*.



14. Управление пользователями

14.1 Управление пользователями SDMS

> *Перед использованием защищенных ресурсов под управлением SDE и приобретением других ролей – необходимо зарегистрировать учетные записи пользователей SDE. Список имеющихся учетных записей сервер управления получает из Active Directory.*

Для учётных записей с ролями *Пользователь* и *Оператор* должны быть зарегистрированы сертификаты, которые будут использоваться для аутентификации этих пользователей.

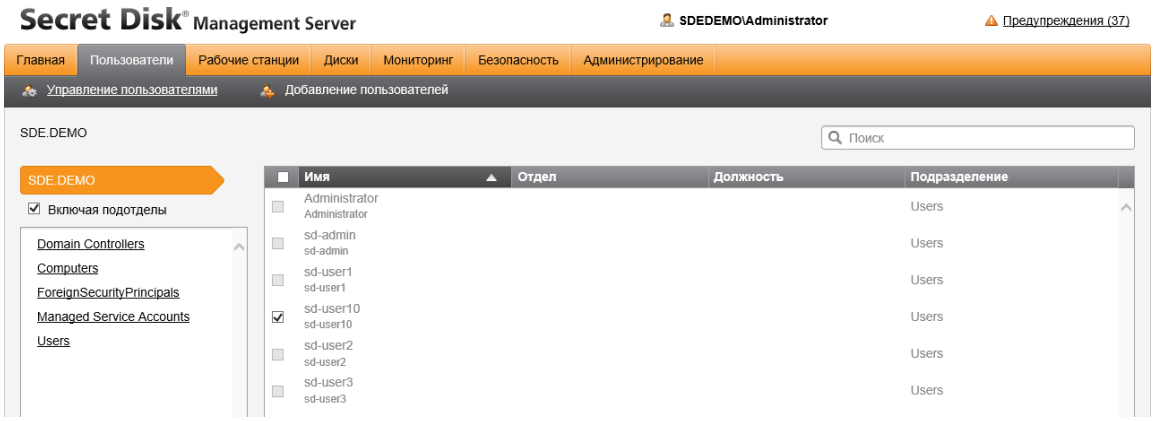
> *Регистрация учётных записей и сертификатов – функция операторов SDE.*

Возможные действия Администратора в отношении пользователей SDE:

1. Добавление учётной записи пользователя в SDE.
2. Регистрация сертификата для роли *Пользователя* или для роли *Оператор*.
3. Присвоение ролей и управление ролями.
4. Настройка пользовательских политик.
5. Блокирование и разблокирование учётной записи.
6. Удаление учётной записи из SDE.
7. Просмотр журнала событий, связанного с пользователями (*Администраторы ИБ*, *Операторы* и *Аудиторы)*.

14.2 Добавление пользователей в SDMS

1. Откройте административный Веб-портал → *Пользователи* → *Добавление пользователей*.
2. Отметьте тех пользователей Active Directory, которых необходимо добавить в качестве пользователей SDE.



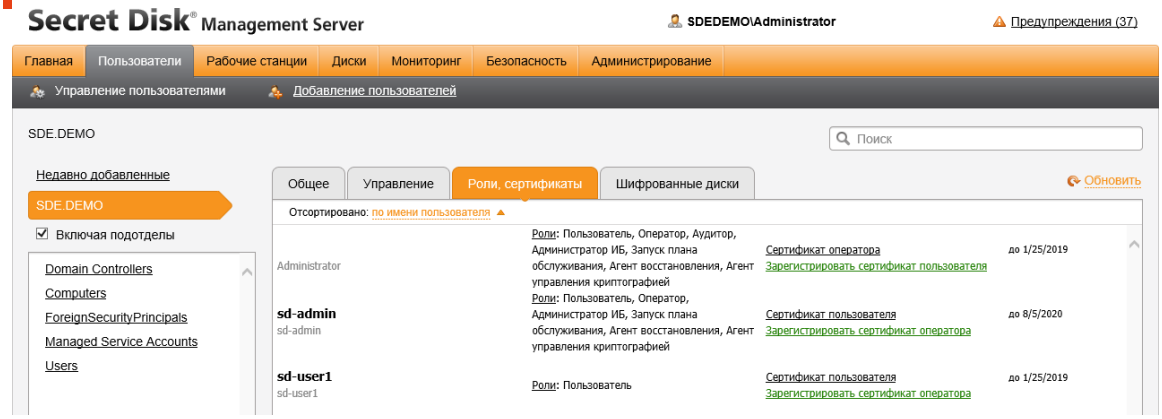
3. Нажмите *Добавить выбранных*.

> *В списке всех пользователей, которых необходимо добавить, может не быть пользователей AD, созданных относительно недавно. Чтобы заставить сервер SDMS обновить список пользователей AD, его следует перезапустить.*
>
> 1. *Откройте панель Сервер управления Secret Disk Enterprise → Статус.*
> 2. *Активируйте действие Перезапустить.*
> 3. *После перезапуска сервера SDMS обновите список пользователей в Веб-портале с помощью ссылки Обновить.*

14.3 Регистрация сертификатов пользователей SDE

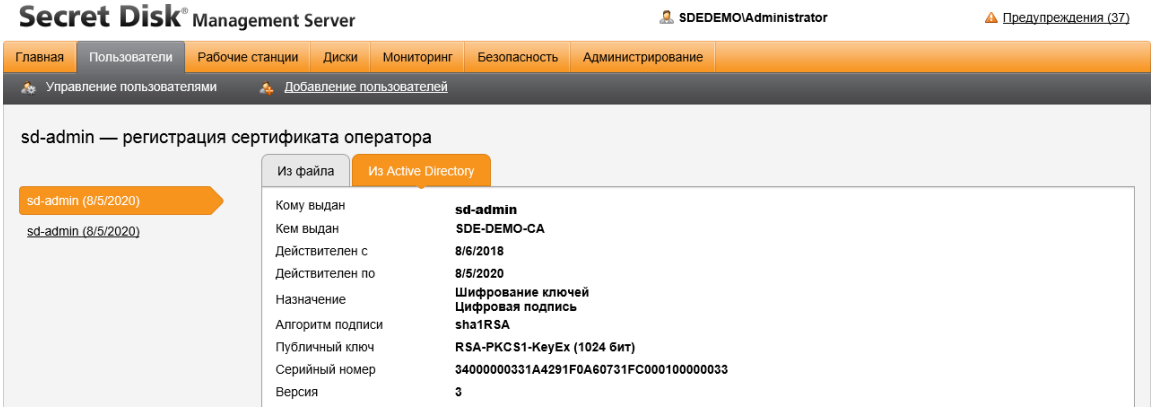
1. Откройте административный Веб-портал → *Пользователи* → вкладка *Роли, сертификаты*.

В строке каждой учётной записи SDE будут присутствовать ссылки, позволяющие зарегистрировать сертификат пользователя или сертификат оператора для этой учётной записи, либо просмотреть ранее зарегистрированный сертификат.



2. Нажмите ссылку *Зарегистрировать сертификат пользователя* или *Зарегистрировать сертификат оператора* в зависимости от того, какая роль будет присвоена учётной записи в дальнейшем.
3. Далее последовательность действий будет зависеть от расположения сертификата, который может быть экспортирован и сохранен в файле, либо опубликован в Active Directory:

Регистрация сертификата из файла:	**Регистрация сертификата из Active Directory:**
Выберите **Из файла**, если сертификат содержится в файле. Нажмите кнопку **Обзор** и выберите файл сертификата. После выбора файла он будет прочитан и сведения о нём будут представлены на экране. Нажмите кнопку *Зарегистрировать сертификат*.	Выберите **Из Active Directory**, если сертификат опубликован в Active Directory. Сведения о сертификатах, имеющихся у учётной записи в Active Directory, будут представлены на экране. Выберите нужный сертификат и нажмите кнопку *Зарегистрировать сертификат*.



У одного пользователя могут быть одновременно две роли – пользователь SDA и оператор SDMS. Для совмещения ролей его сертификат нужно зарегистрировать и как сертификат пользователя и как сертификат оператора. Регистрация сертификата оператора для учётной записи SD5 NET не приводит к автоматическому присвоению этой учётной записи роли Оператора.

Роль оператора должна быть явно назначена учётной записи Администратором ИБ.

14.4 Настройка действительности сертификатов

Настройка проверки действительности сертификатов проводится на рабочих станциях пользователей.

Для проверки действительности сертификатов в Secret Disk используются следующие разделы и параметры реестра:

- для пользовательских приложений — параметр "ValidateCertEnableFlags" (REG_DWORD) ветки HKLM\SOFTWARE\Aladdin\Secret Disk NG\Admin;
- для сервисов — параметр "ValidateCertEnableFlags" (REG_DWORD) ветки HKLM\SOFTWARE\Aladdin\Secret Disk NG\Admin.

> *Если параметр "ValidateCertEnableFlags" (REG_DWORD) отсутствует, его следует создать.*

Возможные значения параметра *ValidateCertEnableFlags*:

- 0 — проверка сертификатов полностью отключена;
- 1 — проверяется действительность времени начала и конца действия сертификата;
- 2 — проверяется только действительность цепочки сертификатов;
- 3 — осуществляется полная проверка.

> *Проверка действительности сертификата в соответствии с настроенными параметрами осуществляется при каждом открытии сеанса пользователя.*

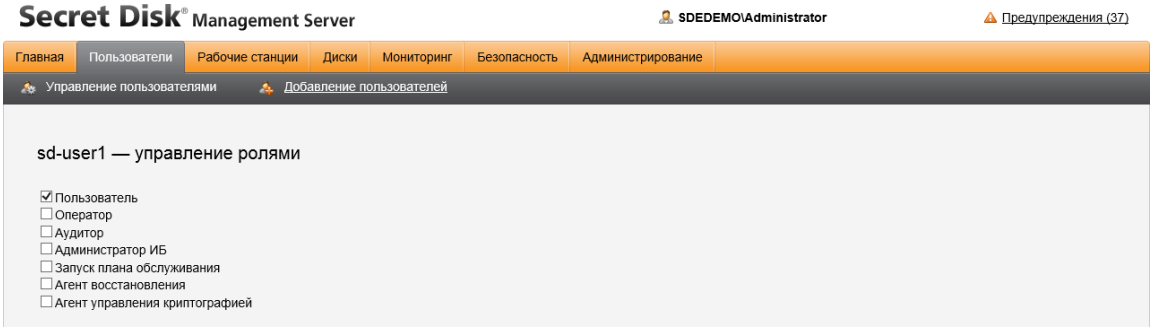
14.5 Присвоение ролей и управление ролями

При добавлении пользователя в SDE учётная запись по умолчанию приобретает роль *Пользователь SDE*.

Присвоение других ролей можно осуществить двумя способами:

1-й способ. Назначение роли(-ей) конкретному пользователю.

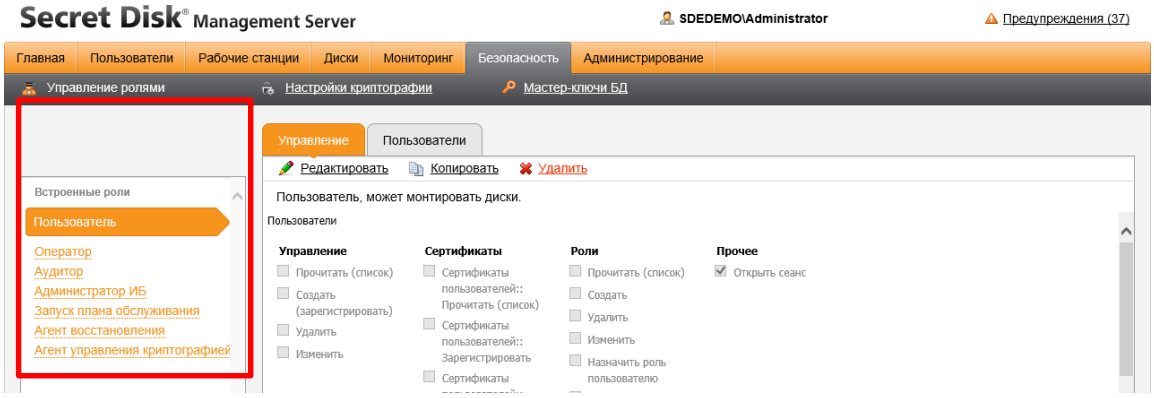
1. Откройте *Пользователи* → *Роли, сертификаты*.
2. Нажмите *Роли*.
3. Отметьте роли, которые необходимо назначить учётной записи.



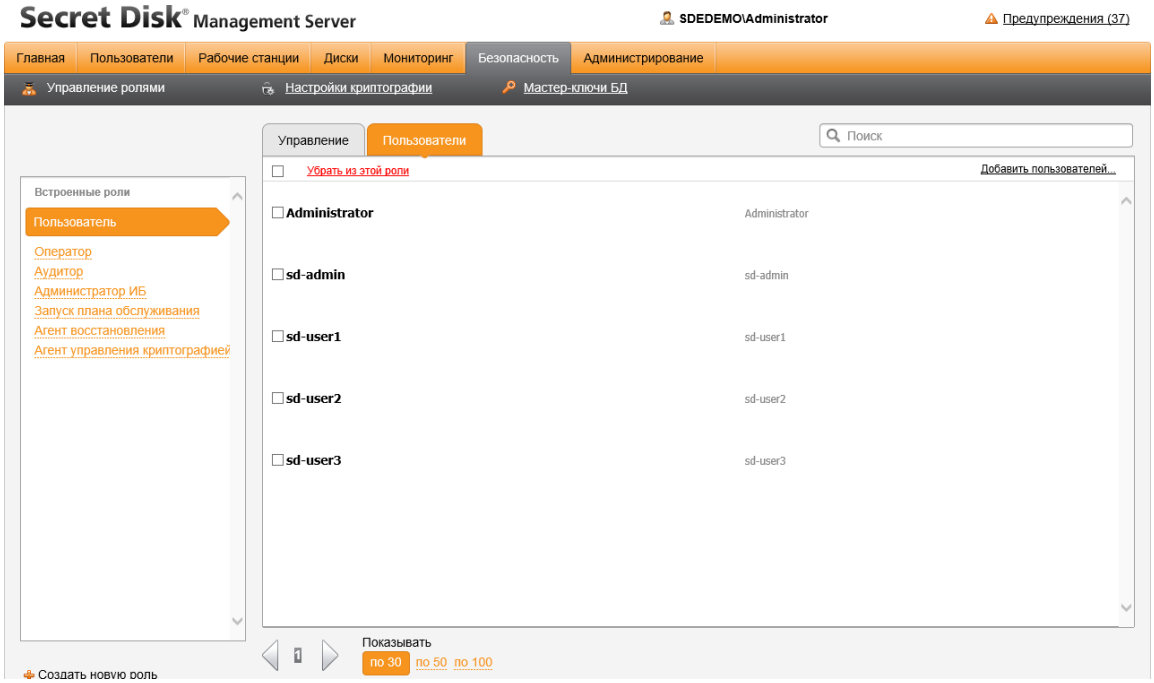
4. Нажмите *Сохранить изменения*.

2-й способ. Управление списком пользователей для конкретной роли.

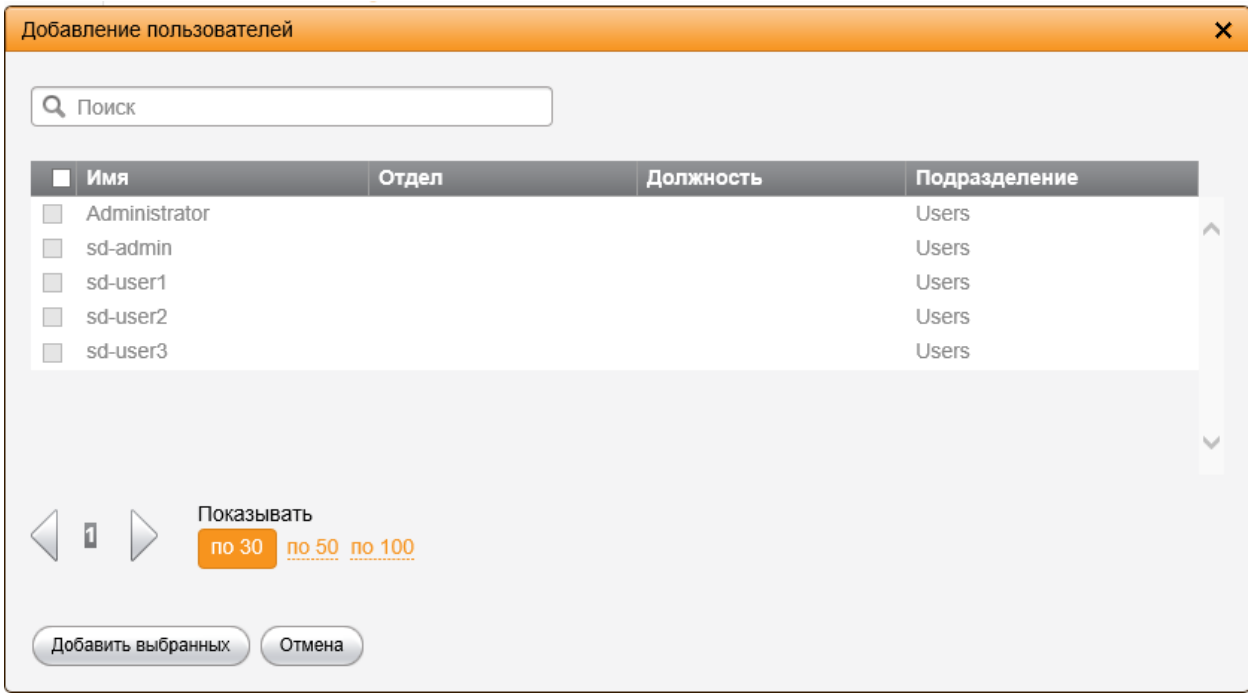
1. Откройте раздел *Безопасность* и выберите слева нужную роль.



2. В правой панели перейдите на вкладку *Пользователи*. В окне будет выведен список пользователей, имеющих выбранную роль.



3. Нажмите ссылку *Добавить пользователей* → отметьте пользователей, которым необходимо назначить роль → *Добавить выбранных.*



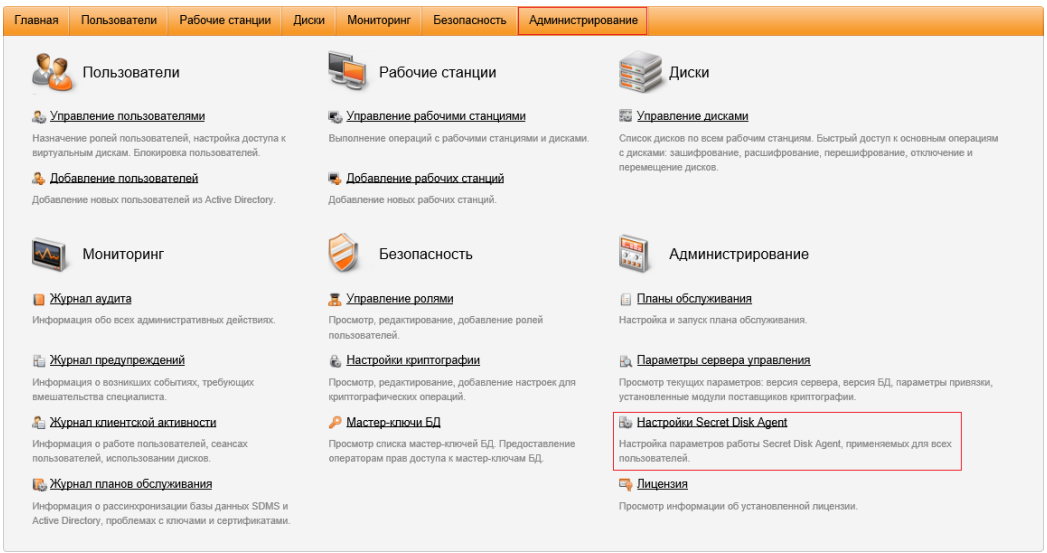
Пользователей можно удалить из роли, отметив их в списке и нажав ссылку Убрать из этой роли.

14.6 Настройка пользовательских политик

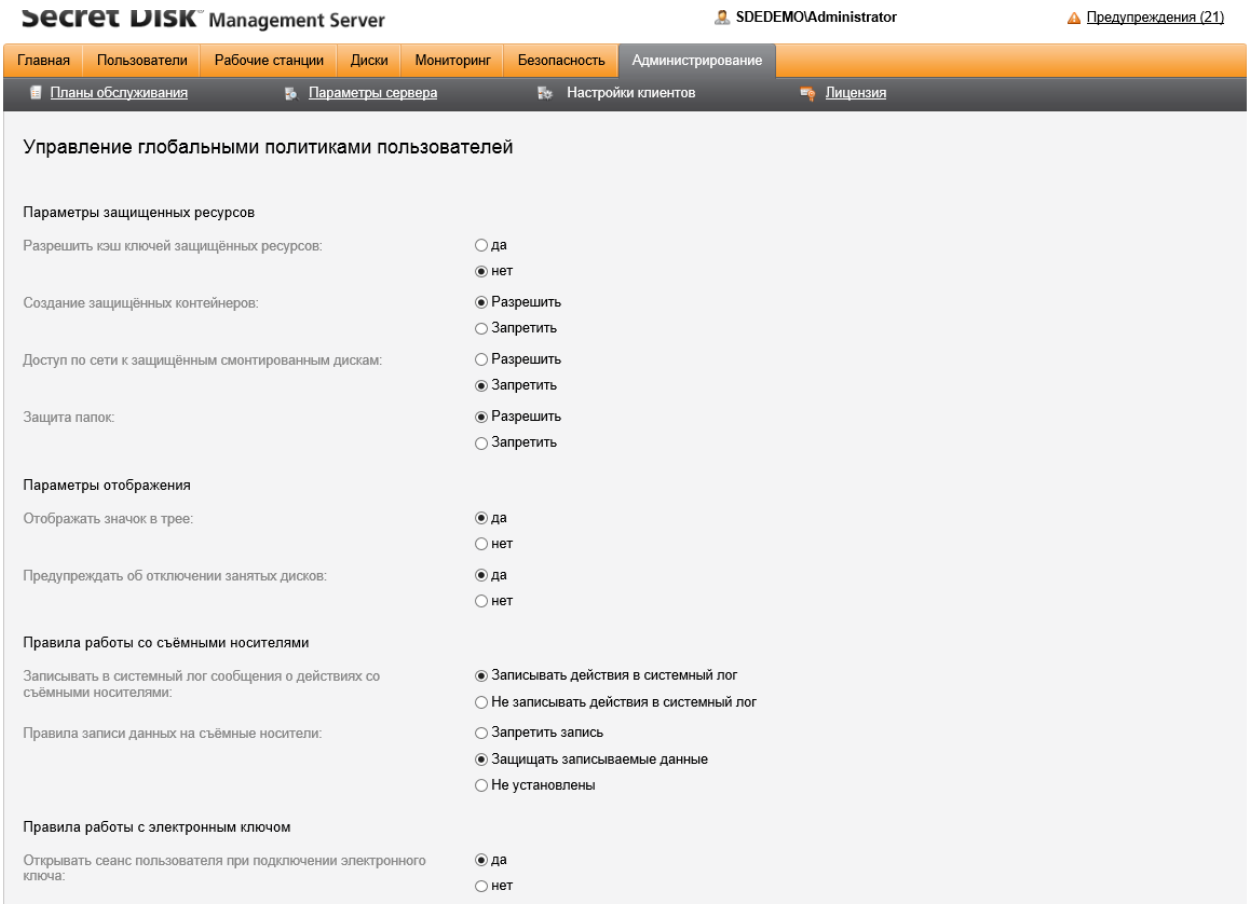
14.6.1. Изменение глобальных (общих) политик для всех пользователей

Основные настройки Secret Disk Agent делаются централизовано в Веб-портале SDMS путём изменения общей политики для всех пользователей и изменения настроек для конкретного пользователя.

1. На главной странице Веб-портала активируйте ссылку *Настройки Secret Disk Agent* или перейдите по ссылке *Администрирование / Настройки клиентов.*



2. Установите необходимые настройки глобальных политик, применяемых для всех пользователей, для которых не установлены индивидуальные настройки.



3. Все настройки можно вернуть к исходным значениям, нажав кнопку *Установить по умолчанию*.
4. Нажмите *Сохранить изменения*.

14.6.2. Изменение политик для конкретного пользователя

1. На главной странице Веб-портала активируйте ссылку *Управление пользователями* или перейти в раздел *Пользователи* из основного меню Веб-портала → *Управление* → *Настройка политик*.
2. Выберите использование общей политики, нажав *Использовать пользовательскую политику*, если для этого пользователя индивидуальные настройки ещё не применялись.
3. Самостоятельно выполните настройку политики и нажмите *Сохранить изменения*.

> *Изменившиеся настройки вступят в силу после открытия нового сеанса Secret Disk Agent.*

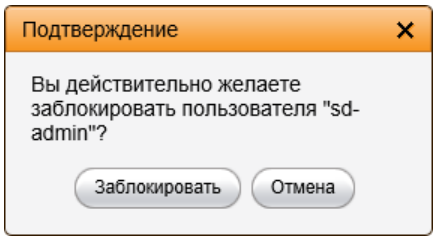
14.7 Блокирование и разблокирование учетной записи

Блокирование рабочей станции позволяет Администратору отключить использование на ней любых защищённых ресурсов для всех пользователей.

Чтобы заблокировать рабочую станцию выполните следующие действия:

1. Перейдите по ссылке *Управление рабочими станциями* на главной странице Веб-портала или в разделе *Рабочие станции*.
2. Перейдите на вкладку *Управление* → *Заблокировать*.

3. Подтвердите действие, нажав *Заблокировать*.



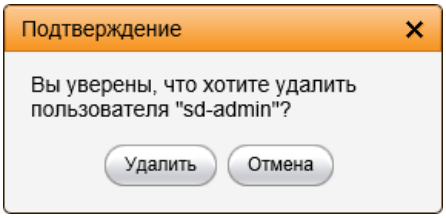
Для разблокировки учетной записи необходимо выполнить ту же последовательность действий, нажав ссылку Разблокировать.

14.8 Удаление учетной записи из SDE

При удалении учётной записи пользователя происходит стирание зарегистрированных сертификатов и удаление учётной записи из списков ролей. Защищённые ресурсы рабочих станций, связанные с учётной записью, не удаляются. Администратор может предоставить доступ к ним другим пользователям.

Для удаления учётной записи необходимо:

1. Открыть вкладку *Управление* в разделе *Пользователи*.
2. Найти в списке нужную учётную запись и нажать ссылку *Удалить*.
3. Подтвердить или отменить удаление учётной записи.

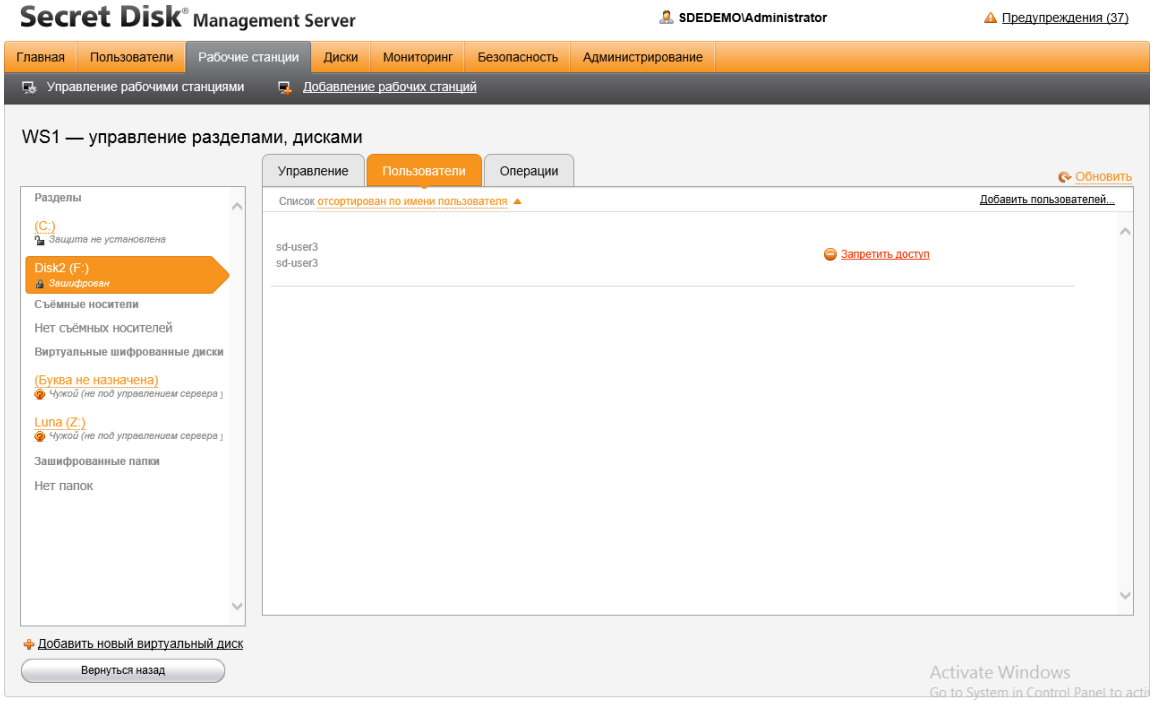


15. Управление защищенными ресурсами

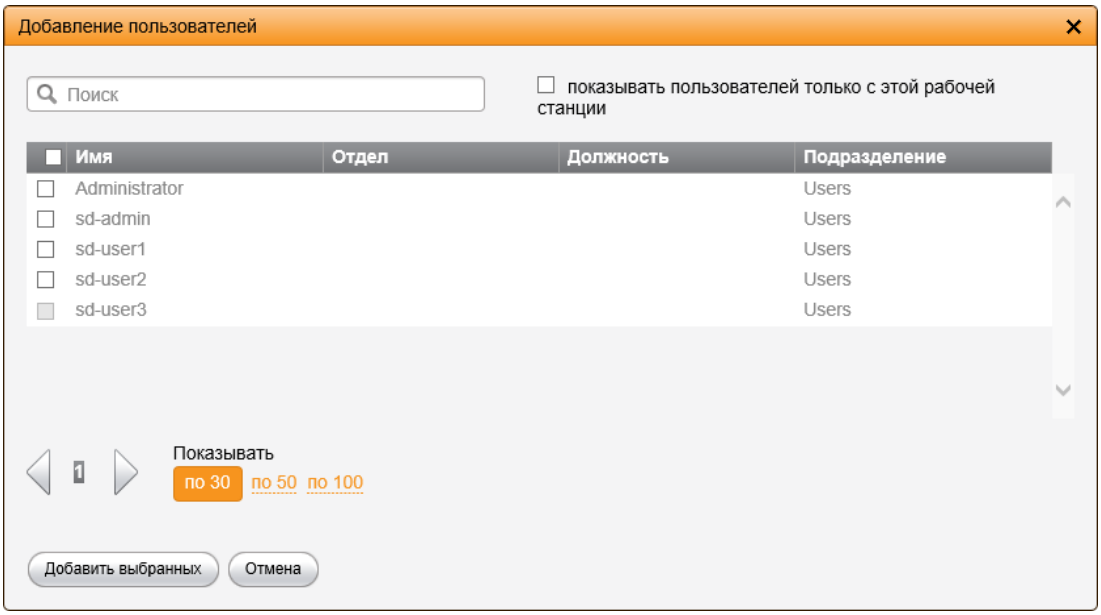
15.1 Добавление защищенного ресурса пользователю

Для добавления защищённого ресурса конкретному пользователю выполните следующие действия:

1. Перейдите во вкладку *Управление дисками*.
2. Выберите нужный диск и нажмите на него.
3. В окне *Управления разделами, дисками* зайдите во вкладку *Пользователи*.
4. Нажмите *Добавить пользователей*.



5. Выберите из списка пользователей, которым необходимо предоставить доступ к выбранному диску. Нажмите *Добавить выбранных*.



15.2 Список защищённых ресурсов рабочих станций

Список защищённых ресурсов всех типов, находящихся под управлением системы SDE, представлен в разделе *Диски* Веб-Портала.

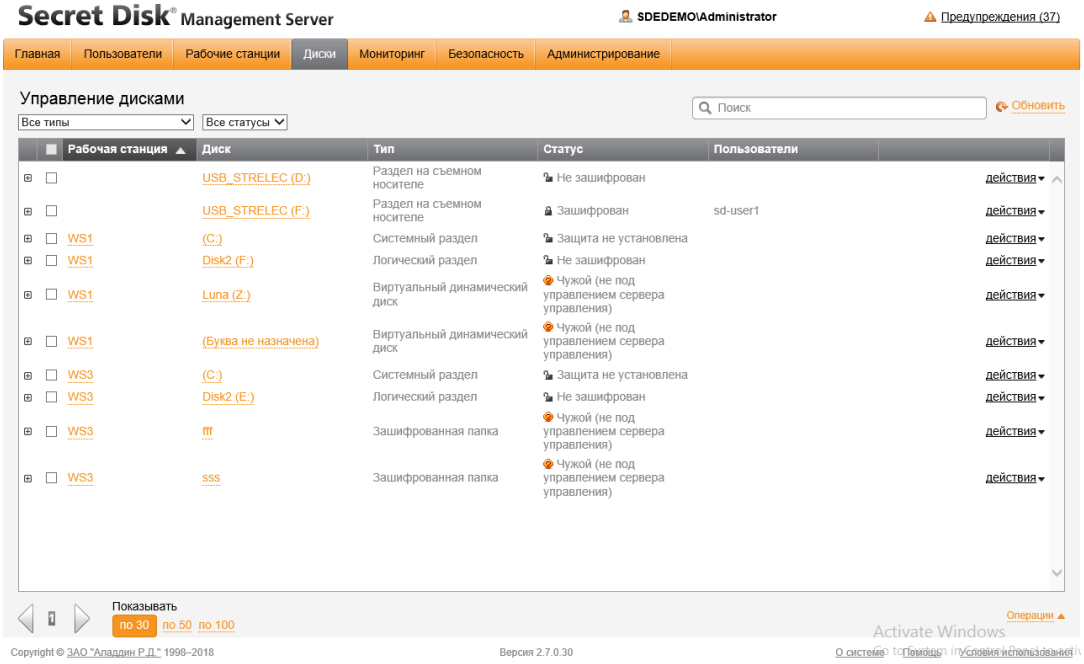


Таблица представляет наиболее полную информацию о защищаемых ресурсах, их состоянии, местонахождении и их пользователях.

Ресурсы можно отфильтровать по типу и статусу, а также сделать текстовый поиск по имени рабочей станции и имени диска.

Из списка управляемых ресурсов можно выполнить следующие переходы и действия:

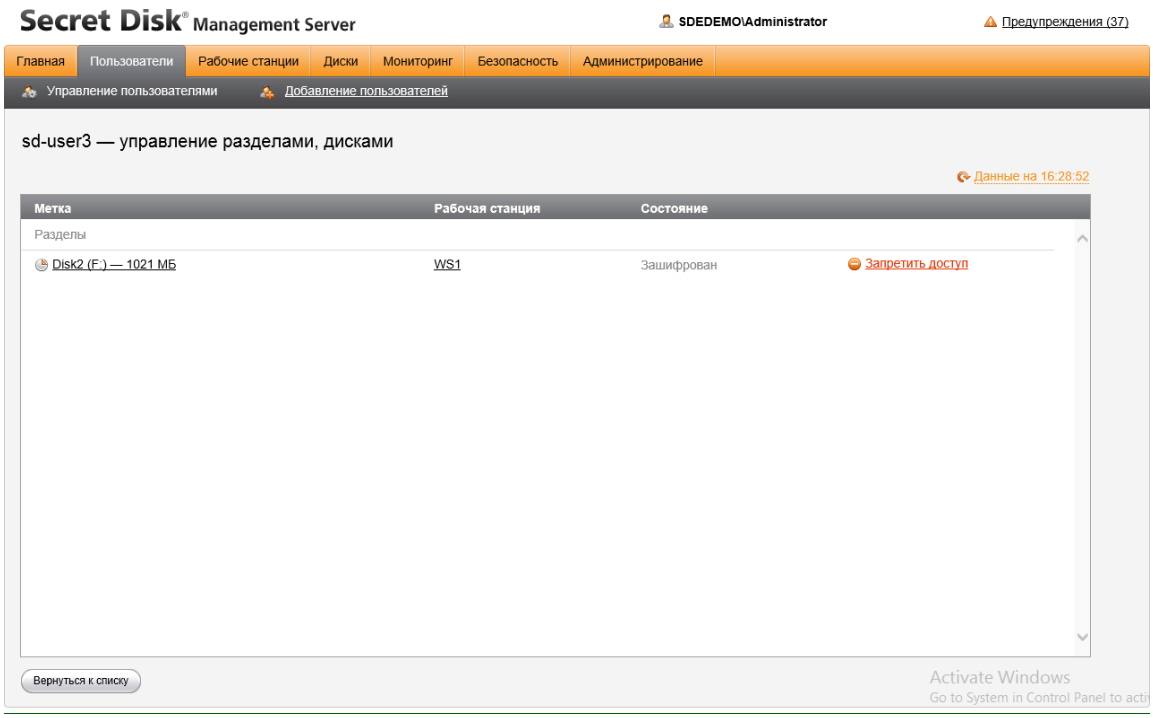
1. Перейти к конфигурации и управлению рабочей станцией, нажав на имя рабочей станции в колонке *Рабочая станция*.
2. Перейти к конфигурации и управлению дисковым разделом или виртуальным диском, нажав на имя ресурса в колонке *Диск*.
3. Выполнить действие над выбранным ресурсом, нажав на список действий в строке ресурса. В меню перечислены действия, которые можно выполнить в отношении ресурса (доступные действия будут такими же, что и на странице управления ресурсом).

15.3 Список защищённых ресурсов пользователя

Для отображения списка ресурсов, к которым имеет доступ конкретный пользователь SDE выполните следующее:

1. Откройте вкладку *Общее* в разделе *Пользователи.*
2. Нажмите на ссылку *Дисков: XX* в строке пользователя, после чего откроется список ресурсов, к которому имеет доступ выбранный пользователь.

> *В разделе можно запретить доступ к диску. Для этого нажмите Запретить доступ и подтвердите действие, нажав Да.*

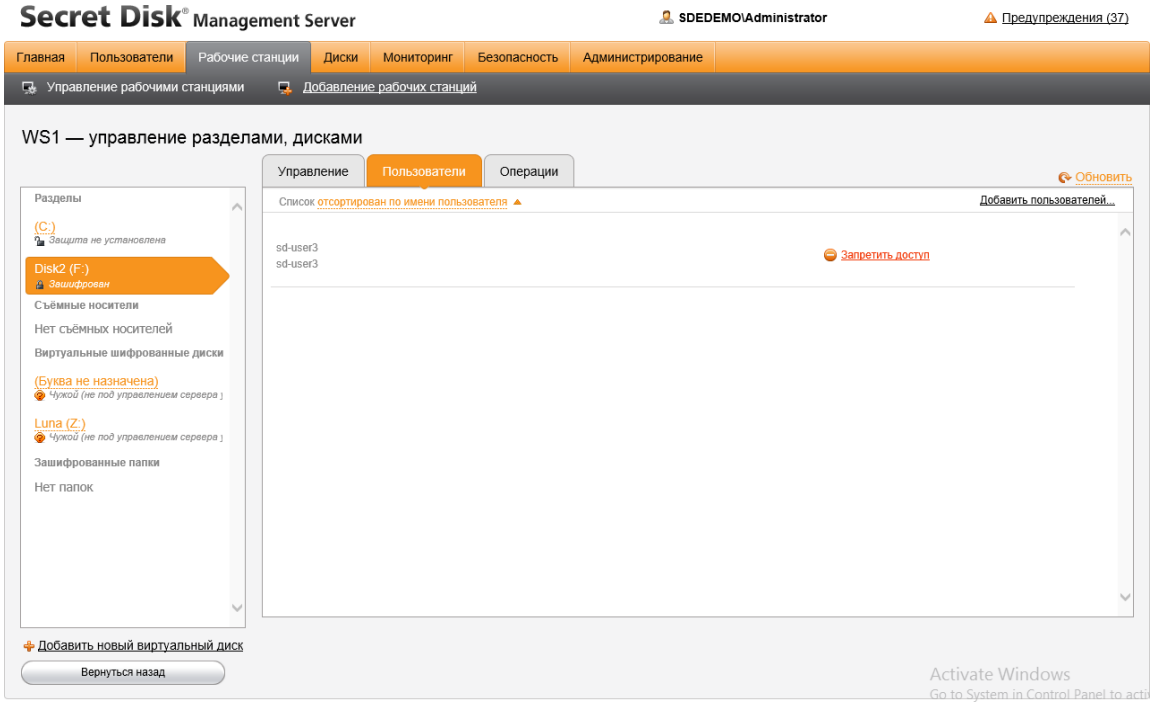


15.4 Страница управления защищённым ресурсом

Так как каждый защищённый ресурс размещён на рабочих станциях, страница управления защищённым ресурсом отображается как находящаяся в разделе рабочих станций.

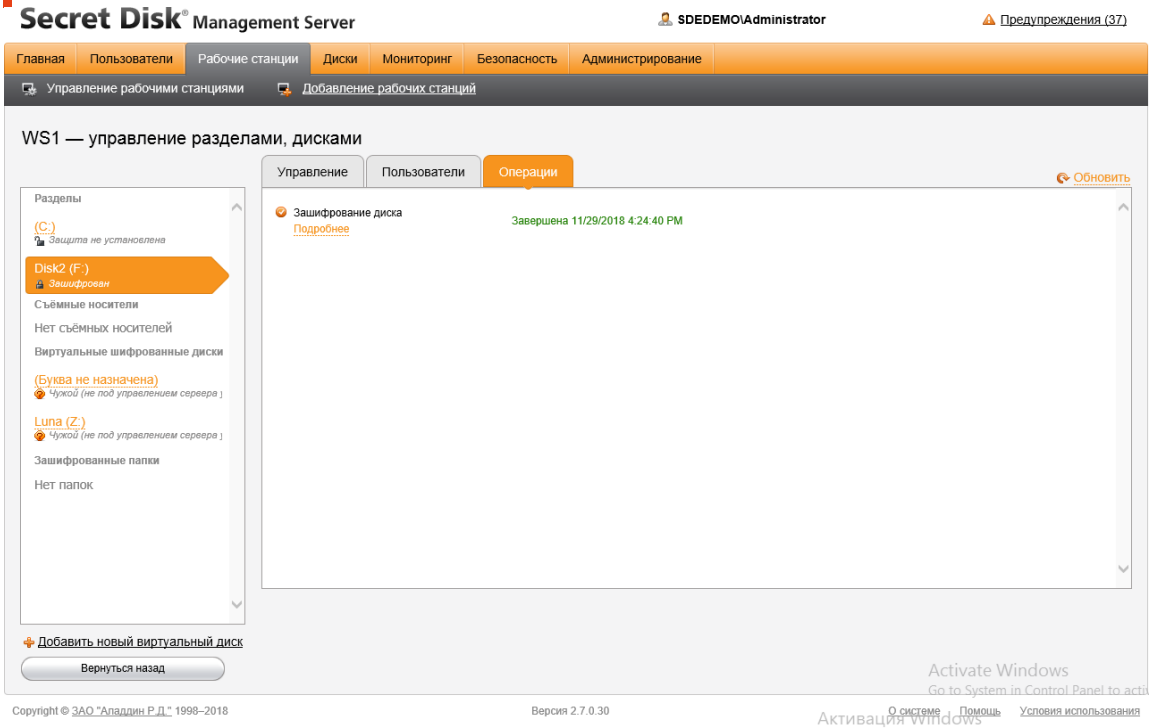
В правой части экрана выводится список других ресурсов той же рабочей станции, где находится управляемый ресурс.

Вкладка *Пользователи* позволяет видеть список пользователей, имеющих доступ к защищённому ресурсу.



Вкладка *Операции* содержит историю операций с выбранным ресурсом. Те операции, которые ещё не начались или находятся в процессе исполнения можно отменить.

Отменить шифрование диска возможно в случае, пока рабочая станция пользователя не приняла запрос на шифрование.



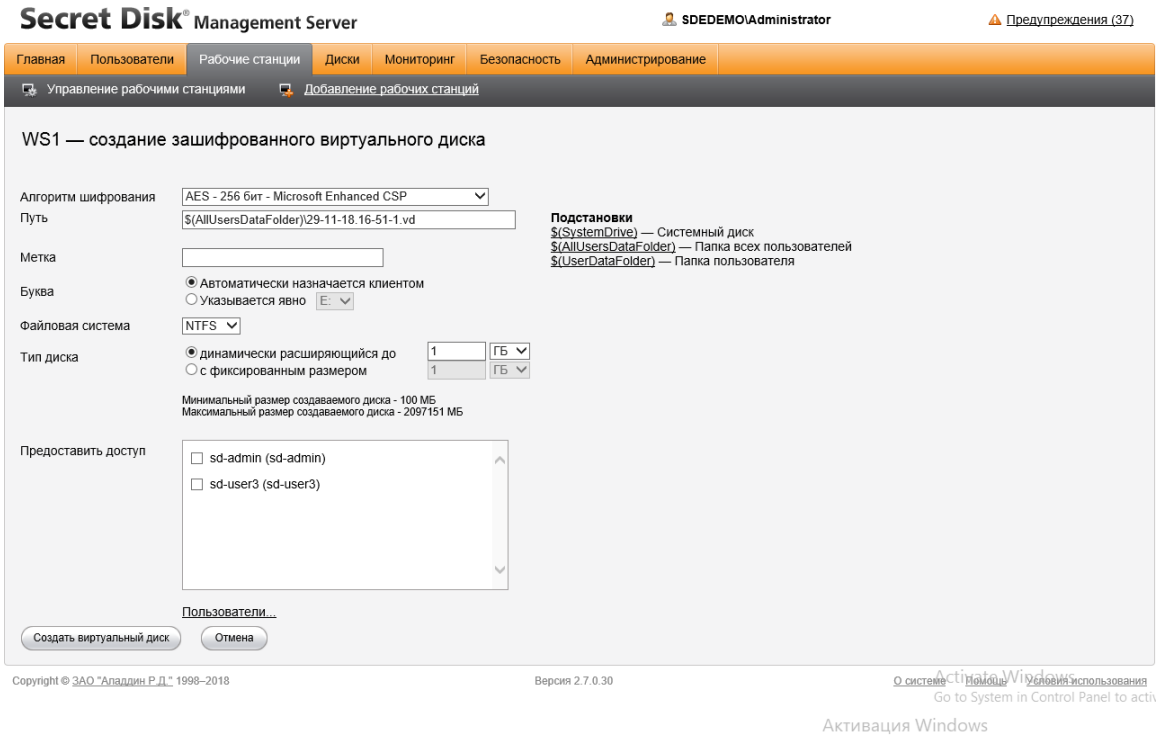
Ссылка *Добавить новый виртуальных диск* предназначена для создания нового защищённого ресурса – виртуального диска, так как только этот тип ресурса может быть создан Администратором непосредственно из Веб-портала.

Для создания виртуального диска на выбранной рабочей станции выполните следующие действия:

1. Перейдите по ссылке *Добавить новый виртуальный диск*.
2. Заполните форму создания виртуального диска.

Не забудьте предоставить доступ к виртуальному диску пользователям!

3. Нажмите *Создать виртуальный диск*.
4. Дождитесь окончания создания диска.



15.5 Операции с логическими разделами

Раздел запоминающего устройства, перед началом использования его в качестве защищённого ресурса под управлением SDE, должен быть создан и отформатирован средствами ОС.

Если логический раздел ещё не зашифрован или был зашифрован и расшифрован средствами SDE, такой раздел не является защищённым и единственная операция, которая может быть с ним сделана средствами SDE – это операция зашифрования.

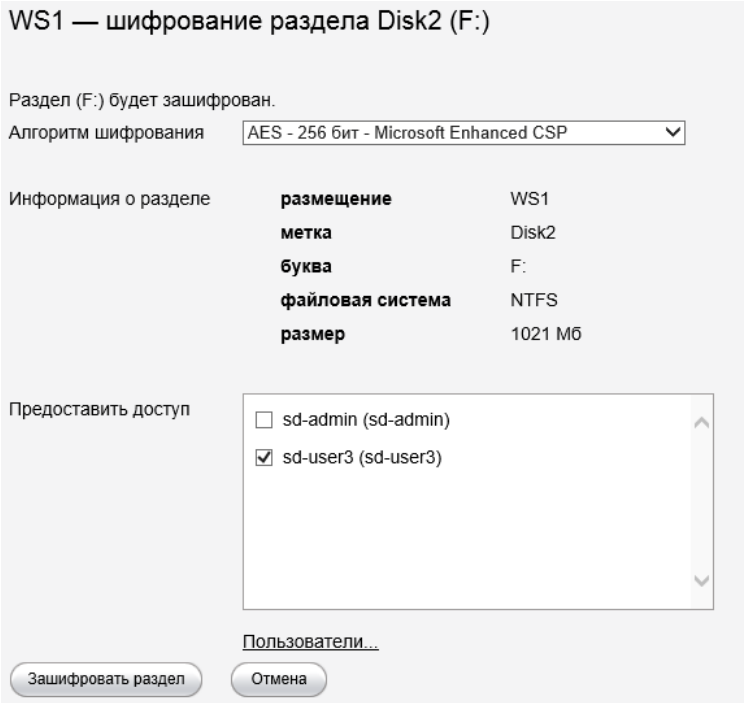
С зашифрованными логическими разделами возможны следующие действия:

1. Управление правами доступа пользователей.
2. Расшифрование.
3. Перешифрование.
4. Отсоединение и подсоединение.
5. Перемещение.
6. Экспорт ключа.

15.5.1. Операция шифрования

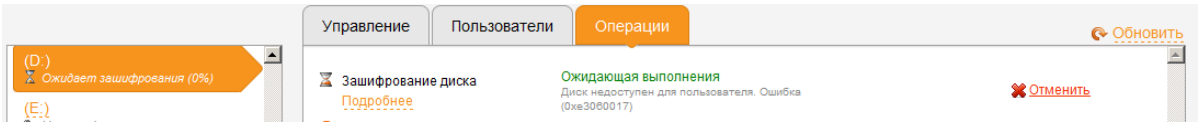
1. Операция зашифрования дискового раздела запускается командой *Зашифровать* из экрана управления ресурсами рабочей станции или из меню действий раздела *Диски*.

2. На открывшемся экране зашифрования раздела необходимо выбрать пользователей, которым будет предоставлен доступ к зашифрованному ресурсу.



После начала зашифрования сервер управления SDMS создаст задачу зашифрования раздела, которая будет выполнена агентом SDA на рабочей станции во время сессии, запущенной одним из пользователей, которому предоставлен доступ к ресурсу.

До этого шифруемый раздел будет находиться в статусе *Ожидает зашифрования* и на вкладке *Операции* будет отображаться сообщение о недоступности диска.



15.5.2. Операции расшифрования и перешифрования

Операции расшифрования и перешифрования (замена ключа шифрования) дискового раздела запускаются командами *Расшифровать* и *Перешифровать* из экрана управления ресурсами рабочей станции или из меню действий раздела *Диски*.

Для исполнения этих операций на рабочей станции, где находится защищённый ресурс, должна быть активна клиентская сессия SDA, запущенная пользователем, имеющим доступ к ресурсу.

15.5.3. Отсоединение, подсоединение и перемещение дисков

Система SDE позволяет управлять зашифрованными дисками, местоположение которых относительно клиентских компьютеров изменилось.

Запоминающее устройство, содержащее зашифрованный раздел, можно отсоединить от рабочей станции, отменив привязку к ней, перенести на другой компьютер, и подсоединить снова, восстановив управление его защитой со стороны SDE.

> *Положение касается только логических дисков и не относится к съёмным носителям, подключаемым к интерфейсу USB.*

Без выполнения процедуры переноса логический диск на другом компьютере использовать нельзя, так как ключ шифрования для него не будет передан из криптохранилища.

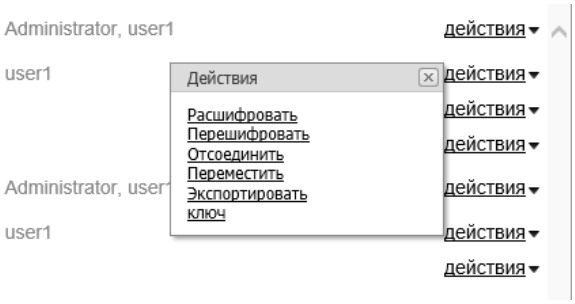
> *Такое поведение позволяет предотвратить несанкционированный доступ к зашифрованным данным при хищении физического диска вместе с электронным ключом пользователя.*

15.5.4. Отсоединение диска

Операция отсоединения приводит к отмене связи между зашифрованным разделом и рабочей станцией, на которой диск находится. Отсоединённый диск можно перенести на другой компьютер и, подключив снова, передать его под управление SDMS.

Перед тем как отключить физический диск, необходимо выполнить соответствующую операцию в панели управления сервером.

1. На странице *Диски* откройте меню *Действия*:



2. Выберите пункт *Отсоединить*.
   Поля *Пользователи и Рабочая станция* этого диска станут пустыми.

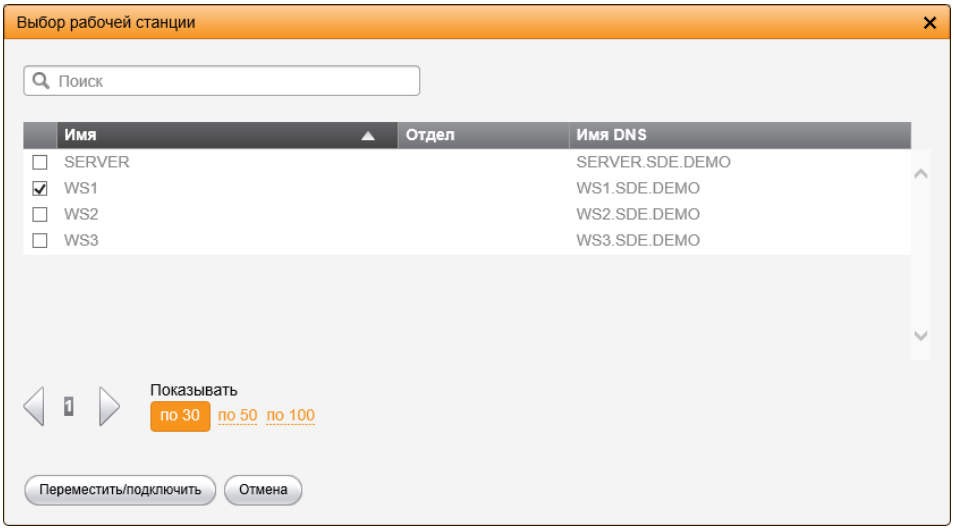
> *После этого диск можно только подключить заново, удалить или экспортировать ключ шифрования. Все прочие действия, включая предоставление прав и криптографические операции, для отключённых дисков недоступны.*

15.5.5. Подсоединение диска

После установки отсоединенного диска, необходимо выполнить операцию его подсоединения к SDE, чтобы передать контроль над ним серверу SDMS.

Для подсоединения диска выполните следующие действия:

1. На странице *Диски* откройте меню *Действия* для отсоединённого диска и выберите пункт *Подсоединить*.
2. Отметьте рабочую станцию, к которой теперь подключён диск и нажмите *Переместить/подключить*.



3. Перезапустите SDA на рабочей станции, на которой находится подключённый диск.

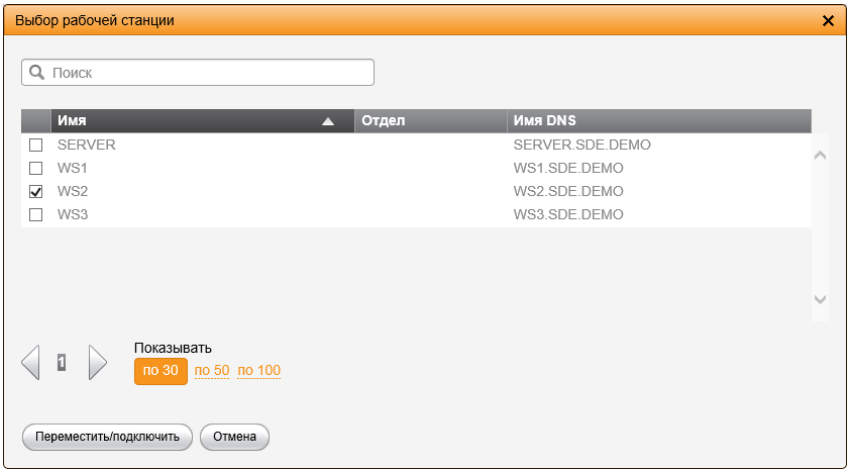
> *После отключения зашифрованного логического диска происходит сброс всех прав доступа, поэтому после подключения этого диска необходимо заново предоставить пользователям права доступа.*

15.5.6. Перемещение диска

Перемещение дисков – это операция по одновременному отсоединению и подсоединению зашифрованного логического (не виртуального) диска с сохранением прав доступа к нему.

Для перемещения диска необходимо выполните следующие действия:

1. На странице *Диски* откройте меню *Действия* для перемещаемого диска и выберите пункт *Переместить*.
2. Выберите рабочую станцию, к которой будет подключён диск и нажмите *Переместить/подключить*.



15.5.7. Экспорт ключа шифрования логического раздела

Экспортированная копия ключа шифрования диска может потребоваться для восстановления доступа в особых ситуациях (при повреждении электронного ключа или необходимости получить доступ к защищённым данным вне инфраструктуры SDE).

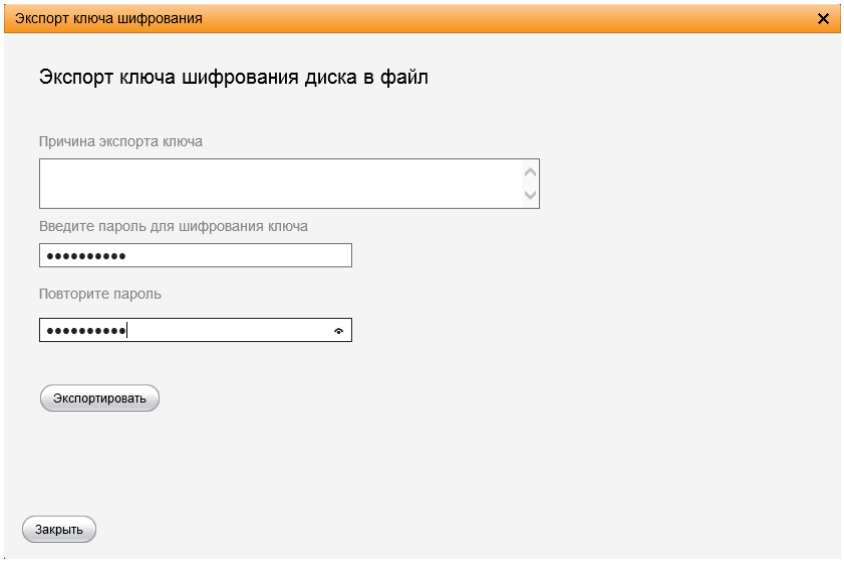
> *Экспортированный ключ шифрования ресурса считается скомпрометированным и должен быть заменён.*

Процедура экспорта ключей шифрования выполняется пользователями с ролью *Агент Восстановления*.

Последовательность действий при экспорте:

1. На странице *Диски* откройте меню *Действия* для нужного диска и выбрать пункт *Экспортировать ключ*.
2. Укажите причину экспорта ключа (она будет записана в журнале мониторинга) и введите пароль для шифрования ключа.
3. Нажмите *Экспортировать*.

Файл типа .emk необходимо сохранить.



15.6 Операции с виртуальными дисками

Виртуальный диск на рабочей станции создаётся Администратором удалённо средствами Веб-портала, без использования системных утилит ОС.

Операция Расшифрование не применима к виртуальным дискам, так как данные виртуальных дисков всегда зашифрованы.

15.6.1. Создание виртуального диска

Для создания виртуального диска выполните следующие действия:

1. Откройте раздел *Управление рабочими станциями*.
2. На вкладке Общее нажмите по ссылке *Разделов: <кол-во разделов>* → *Добавить новый виртуальный диск.*

Ссылка Разделов: <кол-во разделов> активна после того получения данных о конфигурации выбранного компьютера пользователя.

3. Введите необходимые данные в поля формы *Создание зашифрованного виртуального диска*, руководствуясь Таблица 4.

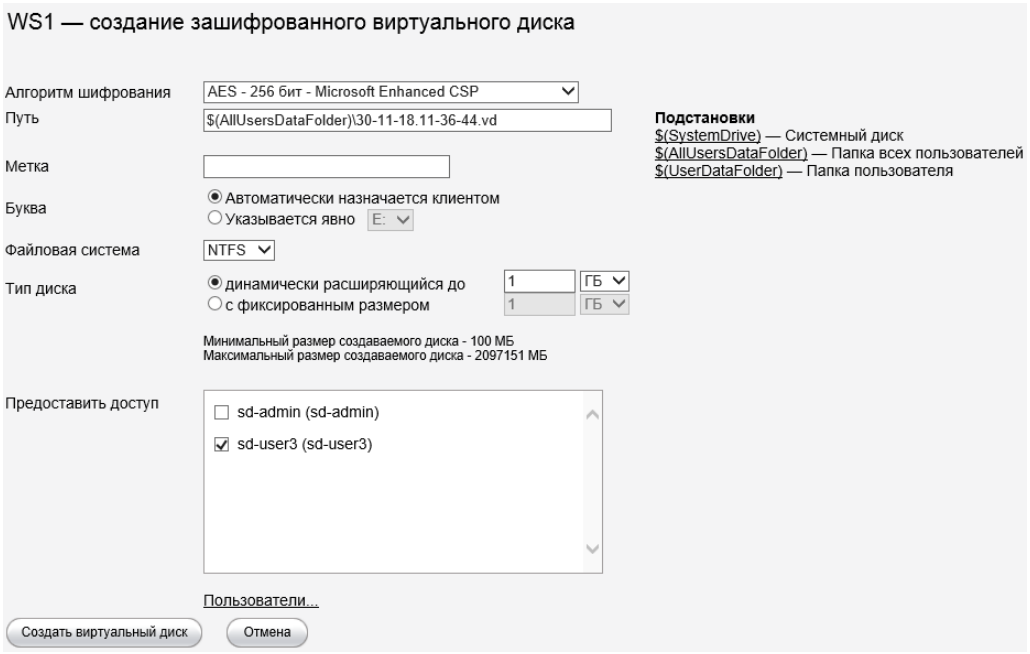


Таблица 4 – Значение полей формы для создания зашифрованного виртуального диска

Поле	Значение
Путь	Папка, в которую на клиентском компьютере будет сохранен файл виртуального диска (файл-контейнер). Для подстановки переменных на позицию курсора пользуйтесь ссылками в правой части окна. Создаваемый файл по умолчанию будет иметь расширение *.vd. В значении допускается использование следующих переменных: • $(SystemDrive) – системный диск; • $(AllUsersDataFolder) – общая папка для всех пользователей (например, c:\Documents and Settings\All Users\); • $(UserDataFolder) – папка конкретного пользователя (например, C:\Documents and Settings\User\). Пример: $(AllUsersDataFolder)\14-12-09 35-19-14.vd
Метка	Метка диска
Буква	*Автоматически назначается клиентом*: при создании зашифрованного диска диску присваивается следующая доступная буква диска. *Указывается явно*: буква диска определяется явно из поля со списком.
Файловая система	FAT, FAT32, NTFS.
Тип диска	*Динамически расширяющийся* (по умолчанию). В поле со списком указывается максимальный объем файла виртуального диска, который варьируется в зависимости от объёма данных. *С фиксированным размером*. Объем диска задается явно.

Поле	Значение
Предоставить доступ	Отметьте пользователей, которые будут иметь доступ к создаваемому виртуальному диску. По умолчанию в списке перечислены пользователи, зарегистрированные на компьютере клиента. Чтобы выбрать других пользователей, перейдите на ссылке *Пользователи* и отметьте пользователей в общем списке. *По умолчанию в списке не отмечен ни один пользователь. Важно установить разрешение на доступ минимум для одного пользователя, иначе SDA не сможет создать виртуальный диск.*

4. Нажмите *Создать виртуальный диск*.

В окне *Управление дисками* для созданного диска будет отображаться статус: *Ожидает создания*.

После запуска Secret Disk Agent на клиентском компьютере будет создан виртуальный зашифрованный диск.

В строке информации виртуальный диск имеет статус: Зашифрован.

15.6.2. Удаление виртуального диска

При выполнении действия *Удалить*, информация о виртуальном диске удаляется из базы данных SDE и доступ к нему через Secret Disk Agent не предоставляется.

Ключ шифрования сохраняется в базе данных SDE, а также может быть сохранён в виде резервной копии.

Для полного удаления данных виртуального диска, необходимо удалить файл его образа с рабочей станции пользователя.

15.6.3. Экспорт ключа шифрования виртуального диска

Экспорт ключа шифрования виртуального диска аналогичен экспорту ключа логического раздела.

15.7 Установка и снятие защиты с системного диска

В Secret Disk Enterprise существует возможность установить защиту на системный раздел.

Ограничения на защиту системного раздела:

1. Если на рабочей станции пользователя имеется несколько жёстких дисков, то защищённый системный раздел должен находиться на жёстком диске, который BIOS или UEFI определяет как первый.
2. Secret Disk Agent совместим только со стандартным загрузчиком ОС семейства Windows.

   Другие загрузчики не могут использоваться вместе с защищённым системным разделом.
3. После установки защиты системного раздела на рабочей станции не должны запускаться утилиты, изменяющие Главную загрузочную запись диска (Master Boot Record).
4. Системный раздел, находящийся на динамическом томе, не может быть защищён средствами Secret Disk Enterprise.

При необходимости восстановления загрузки защищённого системного раздела, воспользуйтесь аварийным загрузочным диском Secret Disk.

Внимание! На компьютерах использующих UEFI необходимо отключить режим SECURE BOOT.

15.7.1. Установка защиты

Чтобы установить защиту на системный раздел выполните следующие действия:

1. В разделе *Диски* Административного Веб-портала выберите нужный системный диск пользователя → *Установить защиту*.
2. Выберите **по крайней мере одного пользователя**, который будет иметь доступ к системному диску.
3. Нажмите *Защитить раздел*.

> *После выполнения задачи диск получит статус Защита установлена.*

15.7.2. Снятие защиты

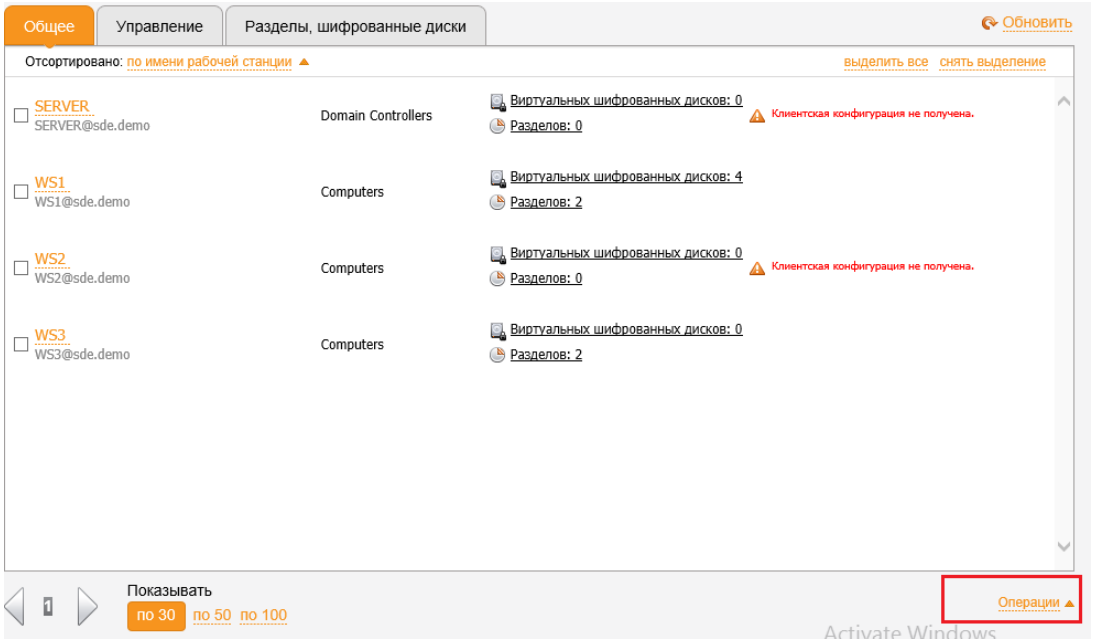
Чтобы снять защиту с системного раздела, выполните действия, описанные в пункте *Установка защиты*, но на втором шаге активируйте действие *Снять защиту*.

Задача на расшифрование системного раздела будет поставлена в очередь, и после её выполнения диск получит статус *Защита не установлена*.

15.8 Групповые операции с рабочими станциями и ресурсами

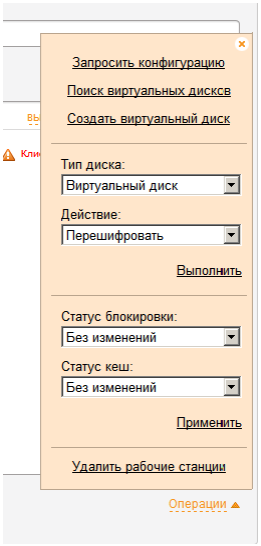
В Веб-портале имеется возможность выполнения однотипных операций одновременно с несколькими рабочими станциями или разделами дисков.

Доступные групповые операции перечислены в меню (*Рабочие станции* → *Общее* → *Операции*).



Предусмотрены следующие групповые операции:

1. Для системных разделов: Установить защиту, Обновить защиту, Снять защиту.
2. Для логических дисков: Зашифровать, Перешифровать, Расшифровать.
3. Для виртуальных дисков: Перешифровать, Удалить.
4. Для рабочих станций: Запрос конфигурации, Создание виртуальных дисков, Блокировка рабочих станций, Включения/отключения кэша, Удаление нескольких рабочих станций.



Для выполнения групповой операции выполните:

1. Перейдите в раздел *Рабочие станции* → *Управление рабочими станциями* → *Общее*.
2. Отметьте рабочие станции, с которыми требуется выполнить одинаковые операции и активируйте ссылку *Операции* под списком рабочих станций.
3. Задайте необходимые настройки и запустите их на выполнение, нажав *Применить*.

15.9 Работа с защищёнными дисками без электронного ключа

SDE поддерживает возможность подключения зашифрованных дисков (включая системные разделы дисков) снятых с других компьютеров, в режиме "только для чтения" без токена пользователя при наличии резервных копий ключей шифрования дисков.

> *Для этого используйте утилиту командной строки SDEmergencyMounter, по умолчанию устанавливаемая в папку C:\Program Files\Secret Disk\Platform.*

Утилита позволяет выполнять следующие действия:

- вывод справочной информации об использовании утилиты;
- подключение защищённого диска;
- отключение всех защищённых дисков.

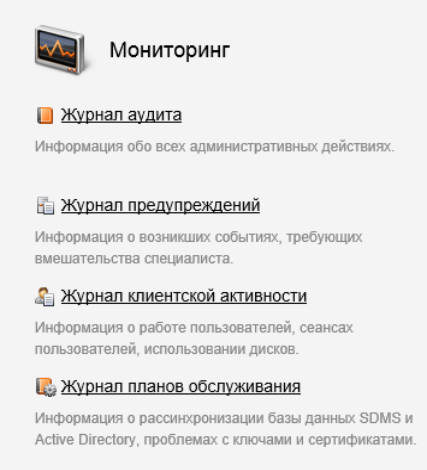
Запуск утилиты выполняется из командной строки со следующими возможными параметрами:

- **-h** (или **--help**) — отображение информации об использовании утилиты. Необязательный параметр;
- **-f** (или **--file**) — путь к файлу с ключом шифрования (типа *.emk). Обязательный параметр в случае восстановления доступа к диску по emk-файлу;
- **-p** (или **--password**) — пароль к ключу шифрования. Обязательный параметр в случае восстановления доступа к диску по emk-файлу;
- **-k** (или **--key**) — ключ в виде последовательности символов. Обязательный параметр в случае восстановления доступа к диску по напечатанной копии ключа;
- **-v** (или **--virtualdiskfile**) — путь к файлу виртуального диска. Обязательный параметр в случае подключения виртуального диска, информация о котором отсутствует в базе данных SDE;
- **-l** (или **--diskletter**) — буква диска. Необязательный параметр. В отсутствие этого параметра буква может быть назначена автоматически. Если выполняется подключение диска, информация о котором (включая букву диска) имеется в базе данных SDE, то значение параметра будет проигнорировано;

- **-s** (или --**systemdiskkey**) — обязательный параметр в случае восстановления доступа к защищённому системному разделу, подключённому как обычный диск для восстановления доступа;
- **-u** (или **--unmountall**) — отключение всех ранее подключённых/временно добавленных дисков. Завершение работы с утилитой.

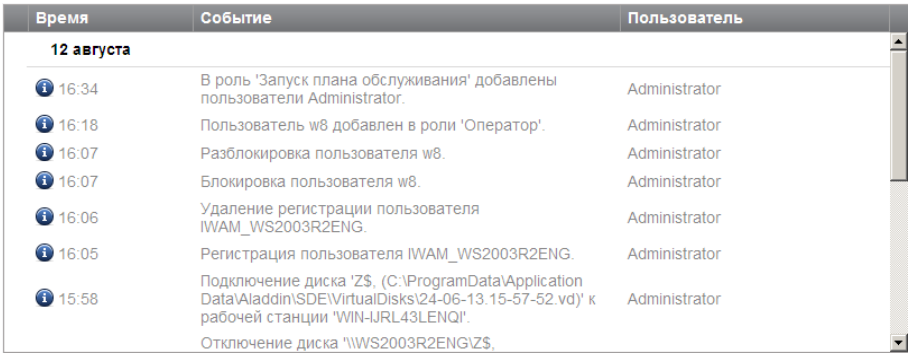
15.10 Мониторинг событий системы

Информация системных журналов о событиях и действиях, происходящих в системе Secret Disk Enterprise, организована в четыре журнала раздела *Мониторинг*.



15.10.1. Журнал аудита

Журнал аудита содержит информацию о выполненных административных операциях, переход в него осуществляется по ссылке *Журнал аудита* на главной странице Веб-портала или на странице раздела *Мониторинг*.



При выборе конкретной записи в журнале, в нижней части экрана отображается подробная информация о событии.

15.10.1.1 Фильтрация записей

Отображаемые записи журнала можно отфильтровать с помощью фильтра в правой части страницы:

1. Выбор календарного диапазона.
2. Группировка записей по дате.
3. Группировка записей по пользователю.
4. Выбор категории записей: Все, Информация, Предупреждение, Ошибка, Критическая ошибка.

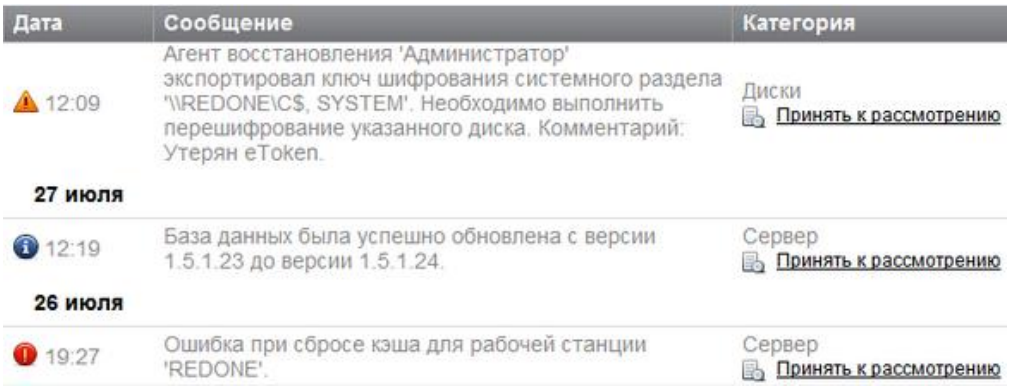
15.10.2. Журнал предупреждений

Журнал предупреждений содержит информацию о событиях, которые требуют внимания со стороны аудитора, но не являются ошибками.

В их число входят такие ситуации, как автоматическое блокирование учётной записи пользователя:

- при длительной неактивности;
- при истечении срока действия ключей и сертификатов;
- при завершении исполнения заданий и т.д.

Чтобы открыть журнал предупреждений, откройте соответствующую ссылку на главной странице.



Для каждого события в журнале предупреждений указано время, описание и категория (т.е. к чему относится событие).

> *Отличительная особенность журнала предупреждений – наличие действия "Принять к рассмотрению" для событий журнала.*
>
> *Активация этой ссылки помечает запись как рассмотренную и с помощью фильтра этого журнала можно скрывать рассмотренные предупреждения.*

15.10.1.2 Фильтрация записей

Отображаемые записи журнала предупреждений можно отфильтровать с помощью фильтра в правой части страницы.

Возможности фильтра:

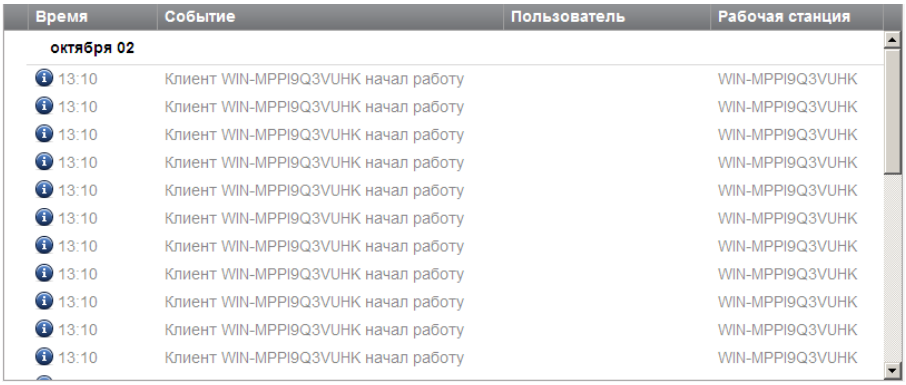
1. Выбор календарного диапазона.
2. Сокрытие записей, помеченных как просмотренные.
3. Выбор категории записи из следующего списка:
   - пользователи;
   - рабочие станции;
   - диски;
   - ключи шифрования дисков;
   - мастер-ключи БД;
   - сертификаты;
   - лицензии;
   - планы обслуживания;
   - сервер;
   - роли;
   - операции.

15.10.3. Журнал клиентской активности

Журнал клиентской активности содержит информацию о подключении пользователей к системе управления и операциях с защищёнными ресурсами.

> *Информация предназначена для просмотра.*

Чтобы открыть журнал клиентской активности, пройдите по соответствующей ссылке на главной странице.



Для каждого события в журнале клиентской активности указаны дата, описание, пользователь и рабочая станция.

15.10.4. Фильтрация записей

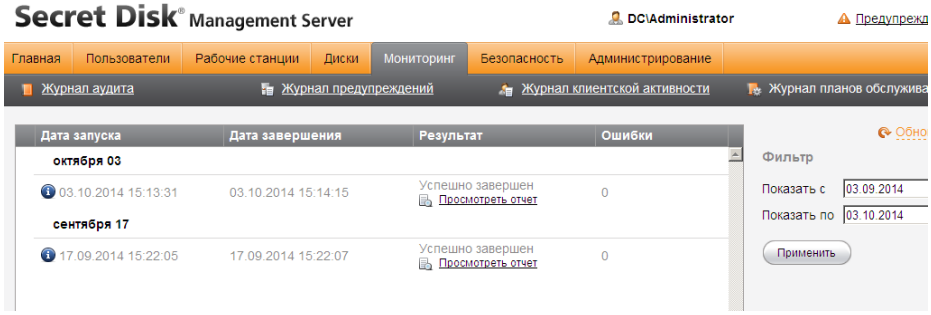
Записи журнала клиентской активности можно отфильтровать по следующим критериям:

1. По календарному диапазону.
2. По типу активности:
   - активность рабочих станций;
   - активность пользователей;
   - по использованию защищённых ресурсов.

15.10.5. Журнал планов обслуживания

Журнал содержит результат выполнения планов обслуживания системы.

Чтобы открыть журнал планов обслуживания, нажмите на соответствующей ссылке на главной странице.



Записи журнала содержат следующую информацию:

1. Дату и время запуска плана обслуживания.
2. Дату и время завершения плана обслуживания.
3. Результат: успешно завершён или отменен.
4. Ошибки: ошибки, требующие рассмотрения.

> *В каждой записи журнала имеется ссылка Просмотреть отчёт, позволяющая перейти на страницу с подробным отчётом выполнения плана обслуживания.*

15.10.6. Фильтрация записей

Для журнала планов обслуживания предусмотрен только фильтр по календарному диапазону записей.

16. Работа с планом обслуживания

План обслуживания запускается периодически как задача *Планировщика ОС* (Task Scheduler).

План обслуживания может быть запущен через Веб-Портал SDMS.

> *Это могут сделать пользователи с ролями Оператор или Запуск плана обслуживания.*

План обслуживания может включать в себя следующие задачи:

1. Выявление рассинхронизации учётных записей в базе данных SDE и учётных записей Active Directory.
2. Выявление сертификатов пользователей и операторов, срок действия которых истёк или истекает.
3. Выявление ключей шифрования дисков, срок действия которых истёк или истекает.
4. Выявление истечения срока действия мастер-ключа БД.
5. Выявление неактивных пользователей.
6. Выявление неактивных рабочих станций.
7. Проверка лицензионного состояния сервера.
8. Выполнение ротации логов в базе данных.

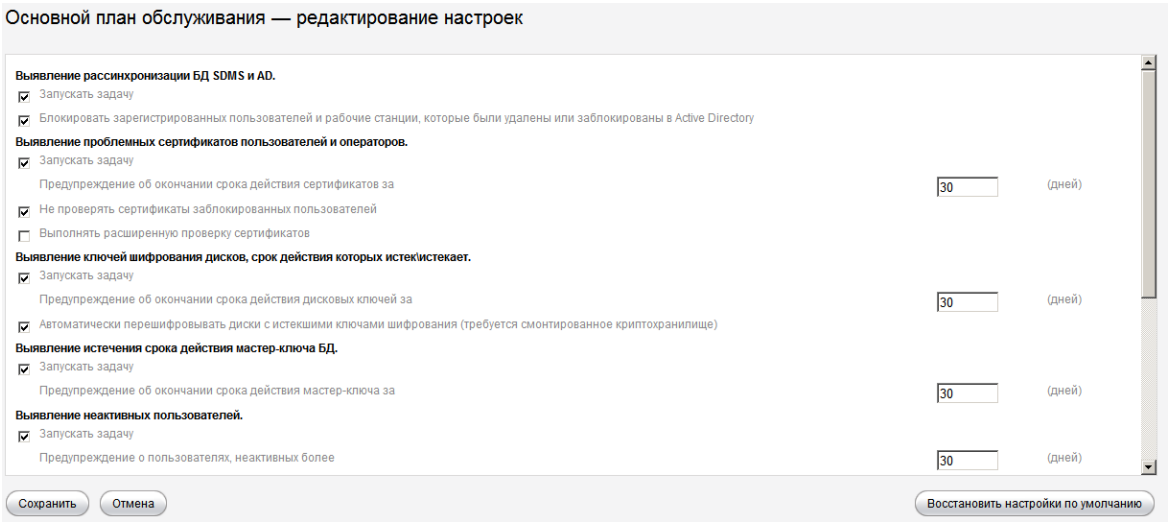
Список задач плана обслуживания может быть отредактирован в разделе *Администрирование/Планы обслуживания* Веб-портала SDMS/

Для этого необходимо:

1. Перейти в раздел *Администрирование/Планы обслуживания* → *Редактировать* (окно Состав плана).
2. Отметить флагом необходимые задачи или снять флаги у тех задач, которые необходимо исключить из плана.
3. В полях условий установить срок (количество дней или месяцев) для формирования соответствующего предупреждения.
4. Сохранить изменения в плане обслуживания.

Кнопка *Восстановить настройки по умолчанию* восстанавливает первоначальные настройки по умолчанию.

Изменённые настройки будут использованы при следующем запуске Плана обслуживания.



16.1 Конфигурирование Task Scheduler

Для автоматизированного запуска плана обслуживания по расписанию необходимо настроить задачу в Планировщике задач ОС. При этом должны выполняться следующие требования:

1. Системный сервис планировщика (Schedule) должен быть включён.

2. Конфигурирование планировщика должно производиться от учётной записи с правами Администратора.

Чтобы настроить задачу в планировщике в командной строке введите следующую команду:

```
Aladdin.SDMS.TaskScheduleTest.exe –c
```

После запуска сценария будет создана задача в системном Планировщике, для которой следует установить расписание исполнения. При этом задачи планировщика запускаются от имени локальной учётной записи SYSTEM.

По умолчанию вызов задачи по плану обслуживания Aladdin.SDMS.MaintenancePlanRunner.exe производится ежедневно в 03:30.

При ручном конфигурировании запуска плана обслуживания в планировщике задач важно, чтобы рабочий процесс запускался от имени SYSTEM, LOCAL SERVICE, NETWORK_SERVICE, либо учётной записи оператора.

Удалить задачу из планировщика можно командой:

```
Aladdin.SDMS.TaskScheduleTest.exe  -d
```

16.2 Конфигурирование MaintenancePlanRunner

Программа MaintenancePlanRunner используется для управления процессом запуска плана обслуживания. Предполагается, что запуск Aladdin.SDMS.MaintenancePlanRunner.exe будет происходить при помощи задания планировщика задач, сформированного программой Aladdin.SDMS.TaskScheduleTest.exe.

Однако, для управления планом обслуживания можно непосредственно использовать Aladdin.SDMS.MaintenancePlanRunner.exe в ручном режиме. По умолчанию она расположена по пути: *C:\Program Files\Secret Disk Management Server\Server*. Запустить программу можно со следующими параметрами:

- `–run` - немедленный запуск плана обслуживания;
- `–cancel` - остановка выполнения плана обслуживания;
- `–state` - получение текущего состояния плана обслуживания.

17. Функции агента восстановления

В функции агента восстановления входит экспорт ключей шифрования виртуальных дисков, логических и системных разделов, для восстановления доступа к ним в случаях, когда электронный ключ пользователя недоступен.

Для экспорта ключа шифрования действуют следующие ограничения:

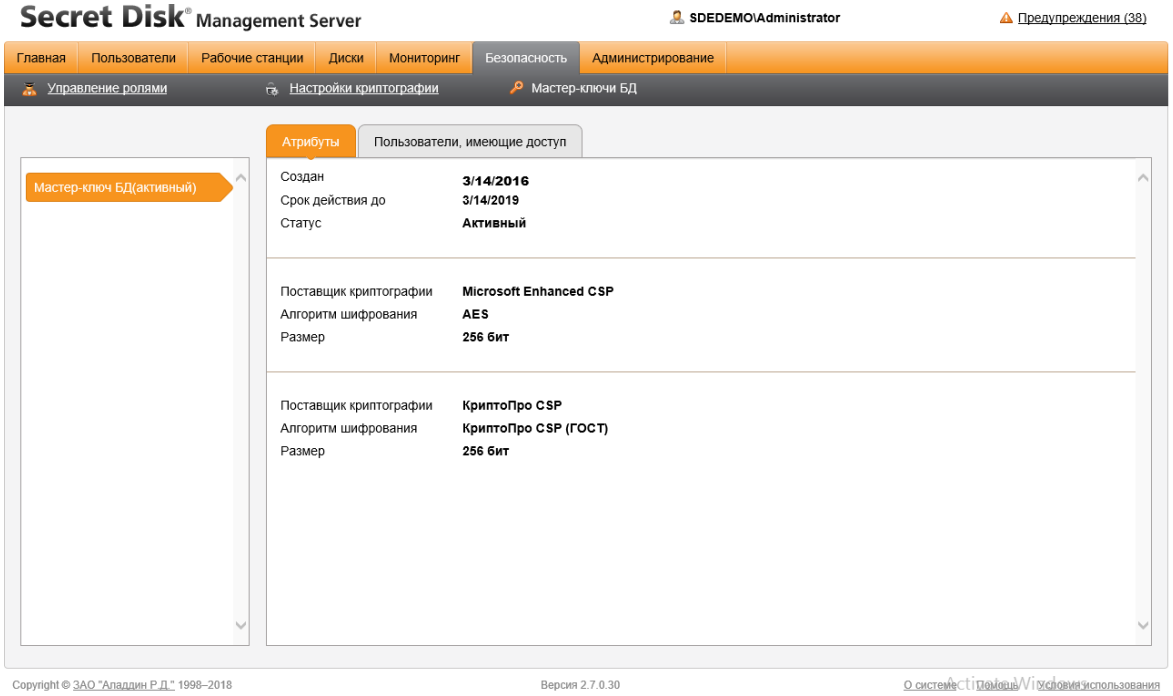
1. Экспорт ключа может выполнять только пользователь с ролью Агент восстановления.
2. Диск на компьютере пользователя может находиться в любом состоянии, кроме "расшифрован".

Порядок экспорта ключей описан в разделах, посвящённых работе с логическими и системным разделом.

18. Мастер-ключи

Информация о Мастер-ключе БД и операторах, имеющих к нему доступ, указана на странице *Мастер-ключи БД* и доступна для всех ролей, кроме роли *Запуск плана обслуживания*.

На главной странице в разделе *Безопасность* нажмите на ссылку *Мастер-ключи БД*.



Во вкладке представлены параметры Мастер-ключа БД:

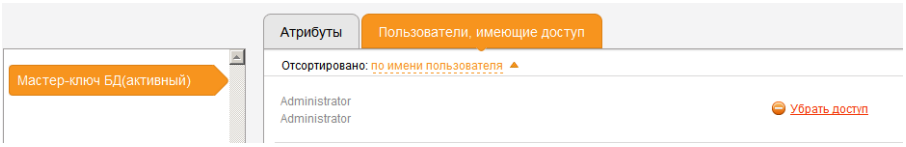
- срок действия;
- поставщик криптографии;
- алгоритм шифрования;
- длина ключа.

> *Все данные предназначены исключительно для справки и не подлежат изменению.*

18.1 Пользователи, имеющие доступ к мастер-ключу БД

Представлена таблица, в которой перечислены все операторы, обладающие доступом к мастер-ключу БД и имеющие полномочия для подключения и отключения криптохранилища.

Администратор или другой пользователь, обладающий правом *Сертификаты операторов* может удалить любого из перечисленных пользователей, активировав ссылку *Убрать доступ*.

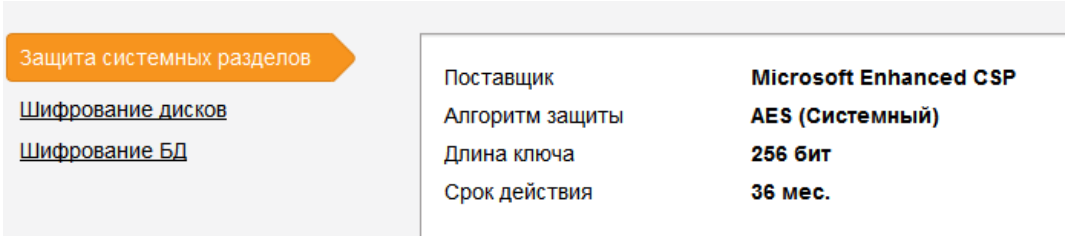


> *В системе всегда должен оставаться, по крайней мере, один оператор, обладающий доступом к мастер-ключу. Таким образом, убрать доступ к мастер-ключу для единственного оператора невозможно.*

18.2 Настройки криптографии

Раздел Веб-портала предназначен только для ознакомления.

Для доступа к нему используйте ссылку *Настройки криптографии* на главной странице.



В разделе представлена следующая информацию о настройках поставщиков криптографии, используемых для трех задач:

1. Защита системных разделов.
2. Шифрование дисков.
3. Шифрование БД.

> *Изменить настройки криптографии можно в приложении Агент Secret Management Server. Для этого пользователь должен обладать ролью Агент управления криптографией.*

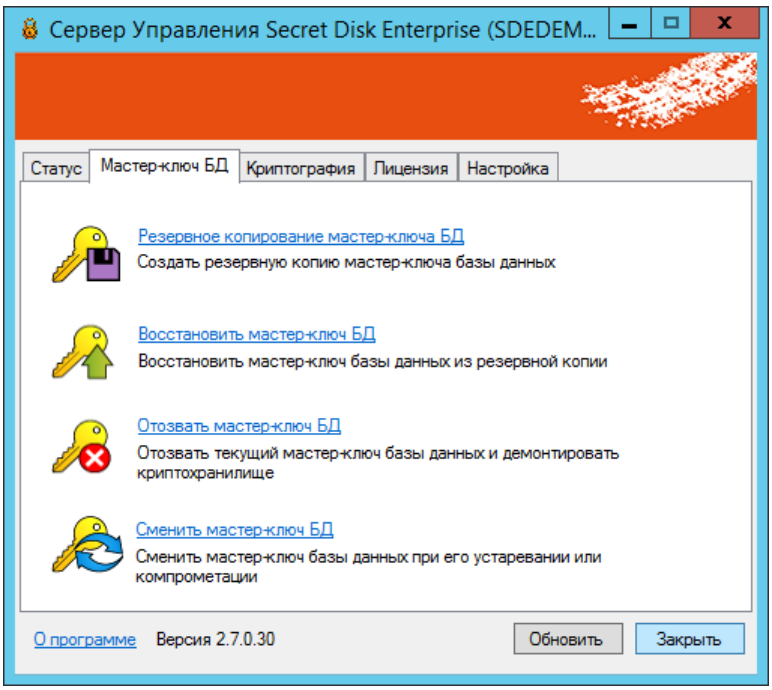
18.3 Резервное копирование мастер-ключа

Резервное копирование мастер-ключа БД предполагает возможность его хранения и последующего восстановления оператором. При экспорте мастер-ключа БД зашифровывается с использованием пароля.

> *Сертификаты и электронные ключи не используются для шифрования резервной копии мастер-ключа БД.*

Чтобы экспортировать мастер-ключ, необходимо выполнить следующие действия:

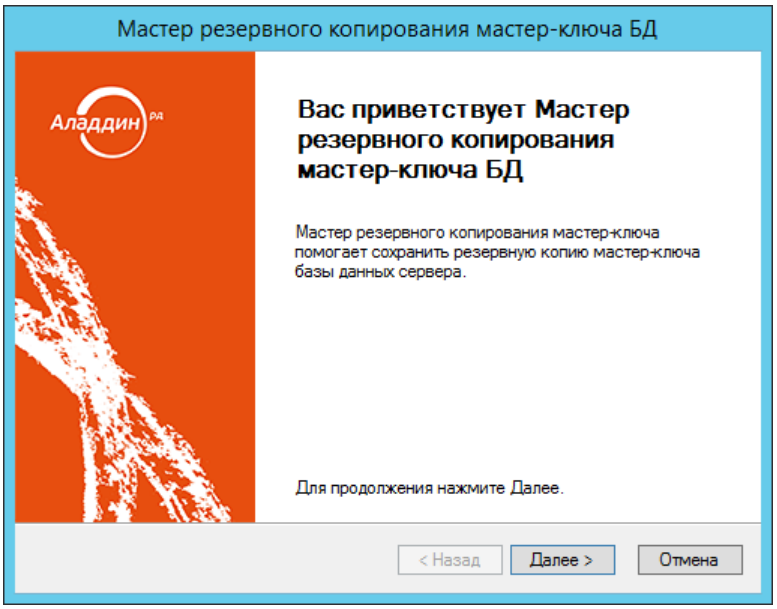
1. Откройте *Агент Secret Disk Management Server* через системное меню или двойным щелчком по иконке приложения в области уведомлений и перейдите на вкладку *Мастер-ключ БД*.



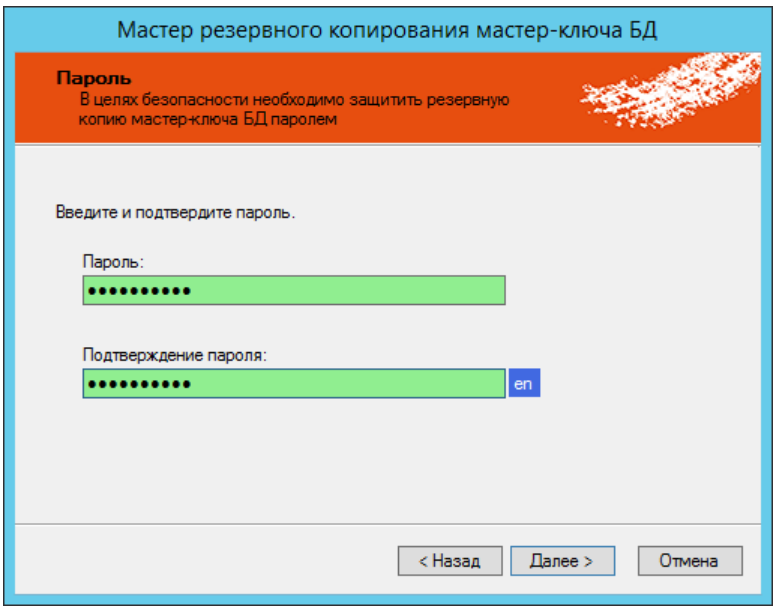
2. Активируйте ссылку *Резервное копирование мастер-ключа БД*.
3. Нажмите Далее.
4. Введите путь и имя файла с расширением *.emk, в котором будет сохранена резервная копия мастер-ключа БД.

> *Для выбора пути нажмите Обзор.*

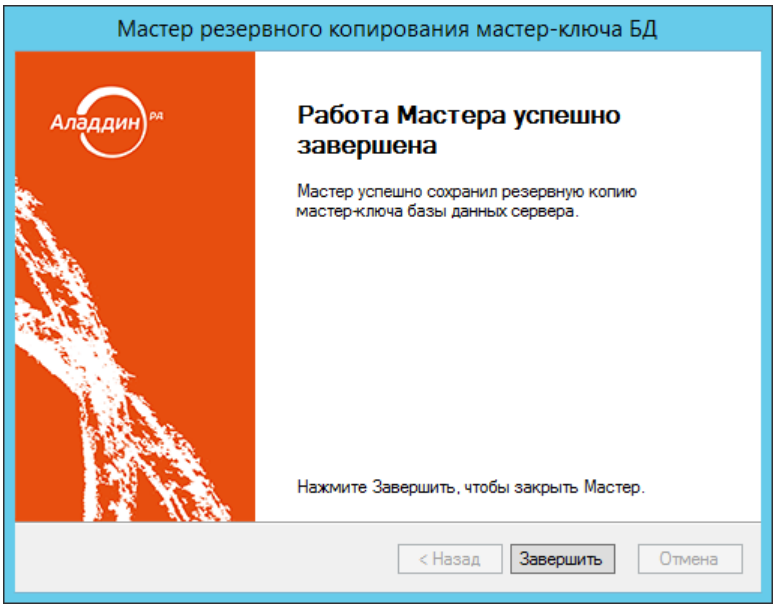
5. Нажмите *Далее*.



6. Введите пароль, следуя рекомендациям на экране и нажмите *Далее*.



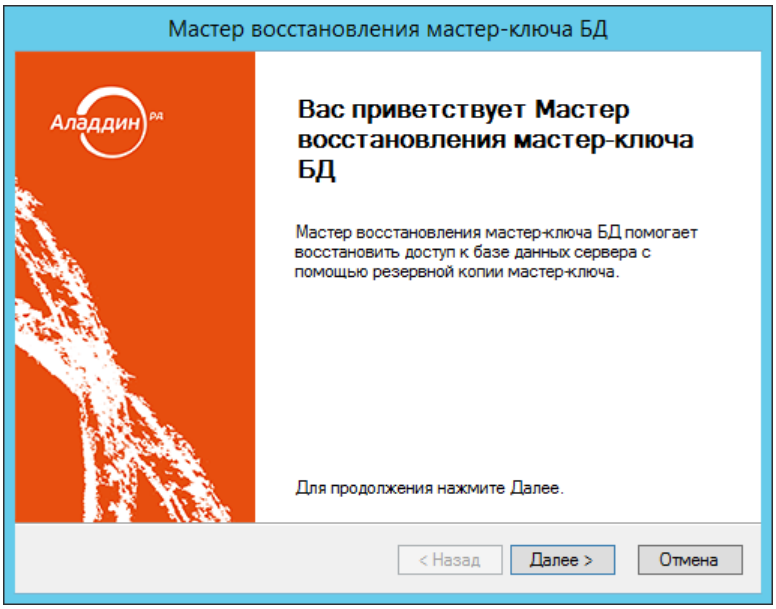
7. Подтвердите введённые на предыдущем шаге данные и нажмите *Далее*.
8. Нажмите *Далее*.
9. Нажмите *Завершить*.



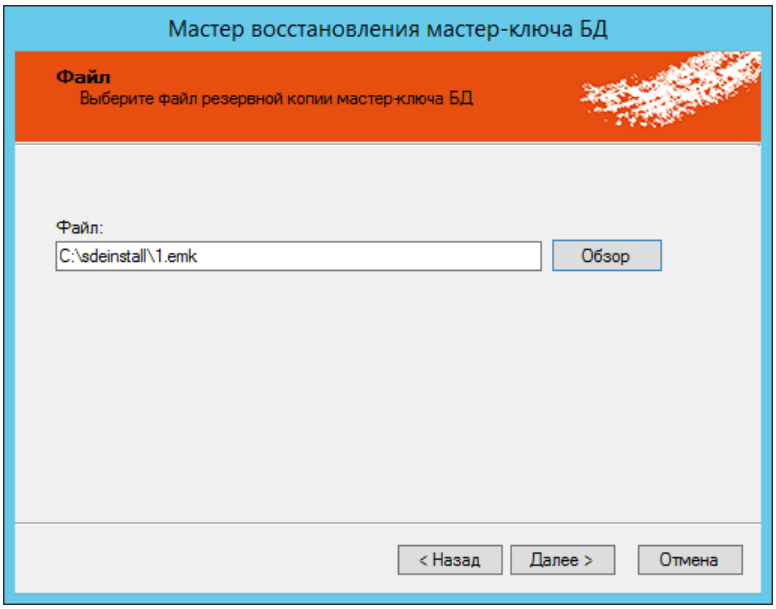
18.4 Восстановление мастер-ключа БД

В случаях, когда электронный ключ Оператора недоступен, есть возможность восстановить мастер-ключ из резервной копии. Для этого необходимо выполнить следующие действия:

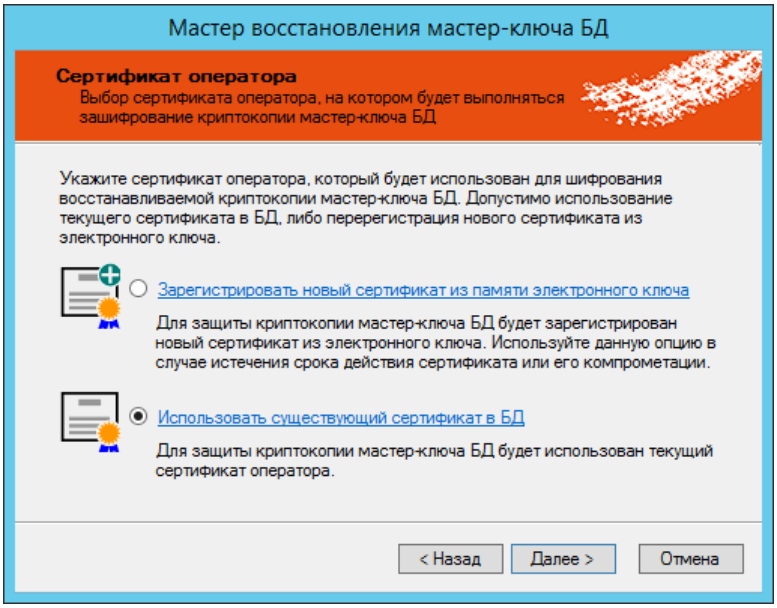
1. Откройте *Агент Secret Disk Management Server* и перейдите на вкладку *Мастер-ключ БД*.
2. Активируйте ссылку *Восстановить мастер-ключ БД*. Нажмите *Далее*.



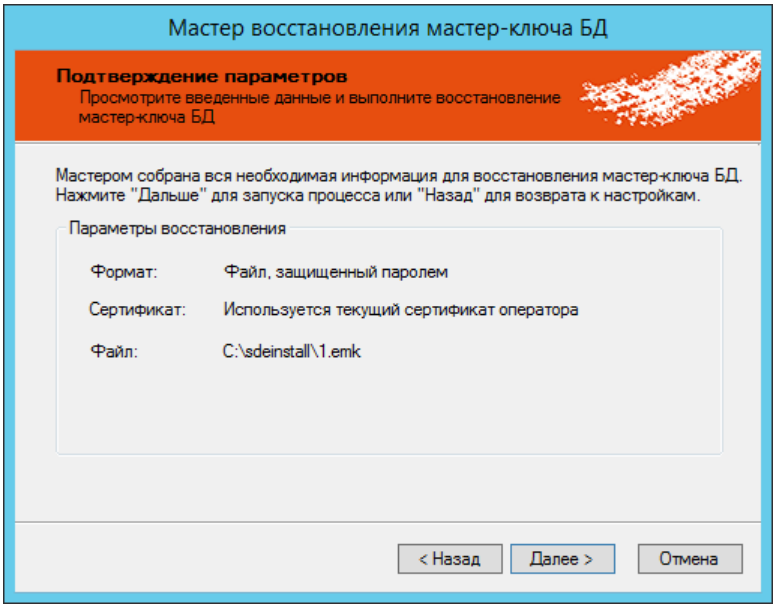
3. Укажите путь к файлу типа *.emk с резервной копией мастер-ключа БД и нажмите *Далее*.



4. Введите пароль, заданный при экспорте ключа. Нажмите *Далее*. Откроется окно с запросом сертификата оператора, который сможет использовать восстановленный ключ.

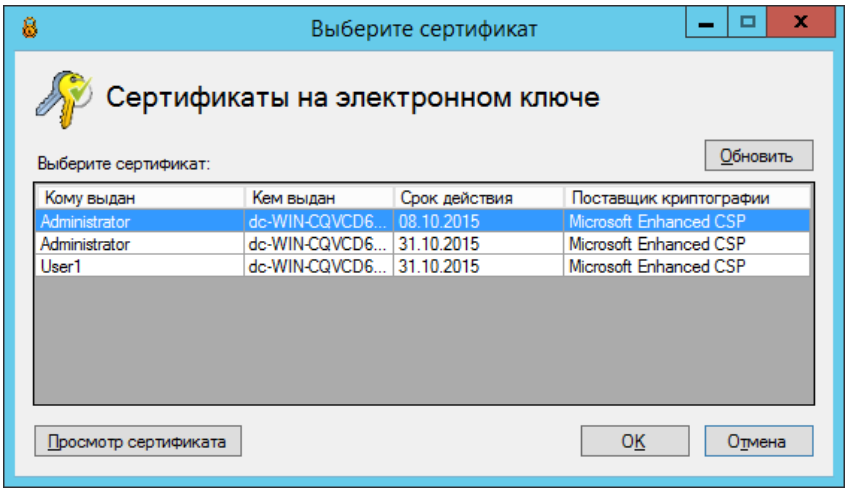


5. Для использования сертификата оператора, который выполняет процедуру восстановления, выберете пункт *Использовать существующий сертификат в БД* и нажмите *Далее.*



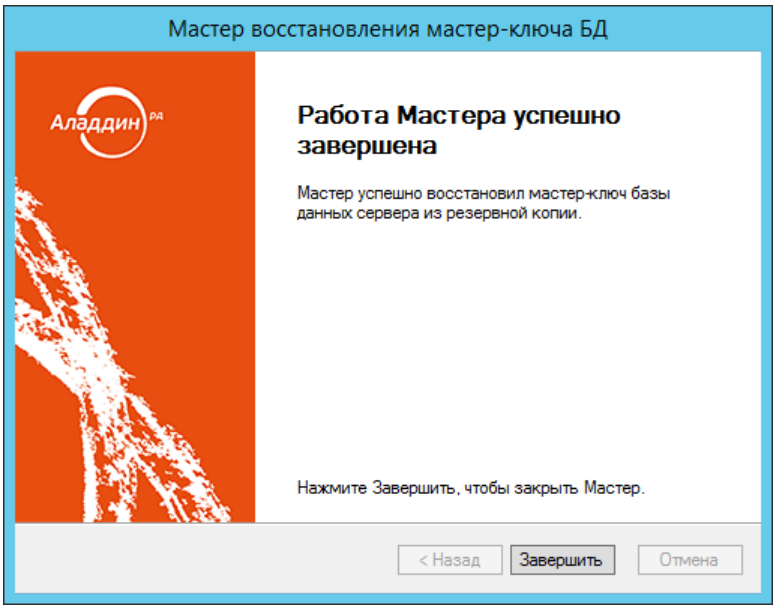
6. Для ввода нового сертификата оператора, находящегося на электронном ключе, выберите пункт *Зарегистрировать новый сертификат из памяти электронного ключа*.

В этом случае появится окно со списком доступных сертификатов на электронном ключе, один из которых следует выбрать и подтвердить выбор нажатием кнопки OK.



7. Подтвердите выбранный способ восстановления ключа и нажмите *Далее*.

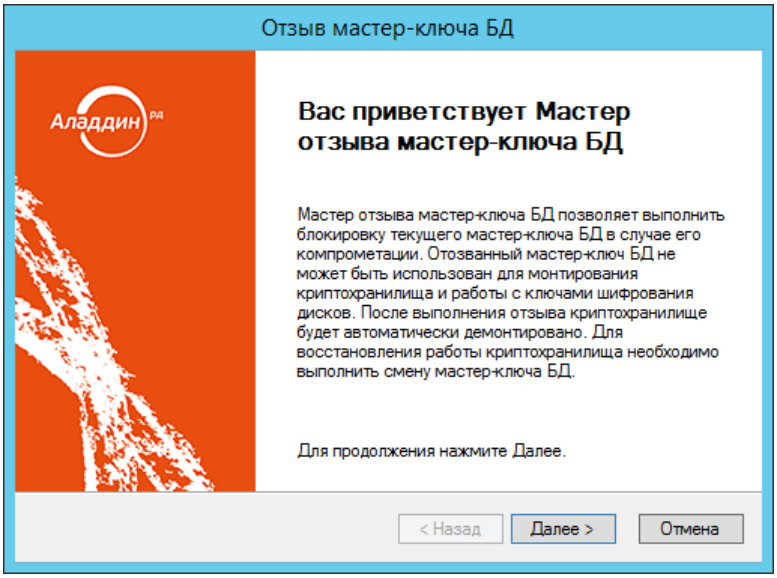
8. Нажмите *Завершить*.



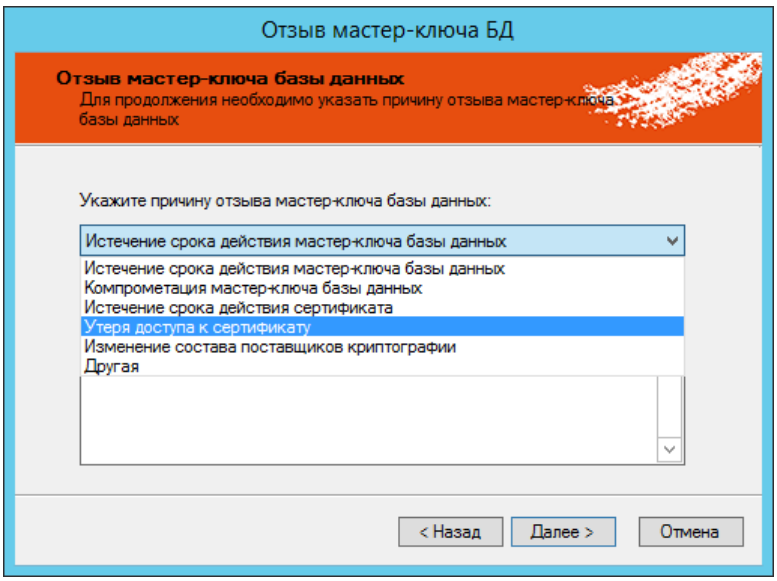
18.5 Отзыв мастер-ключа БД

Отзыв мастер-ключа БД используется в случае его компрометации и невозможности дальнейшего использования для подключения криптохранилища. Для отзыва мастер-ключа необходимо выполнить следующие действия:

1. Откройте *Агент Secret Disk Management Server* перейдите на вкладку *Мастер-ключ БД*.
2. Нажмите *Отозвать мастер-ключ БД*. Нажмите кнопку *Далее*.



3. Укажите причину отзыва мастер-ключа БД. По желанию введите дополнительный комментарий, который появится в журнале. Нажмите кнопку *Далее.*



4. Нажмите *Далее*.
5. Нажмите *Завершить.*

> *Если перед завершением Мастера был выбран пункт Запустить Мастер смены мастер-ключа БД, то после закрытия окна откроется Мастер смены мастер-ключа БД.*

18.6 Смена мастер-ключа БД

В случае утери или компрометации мастер-ключа, его необходимо сменить. Процедура смены мастер-ключа включает в себя отзыв действующего мастер-ключа и создание нового ключа. Чтобы сменить мастер-ключ БД, выполните следующие действия:

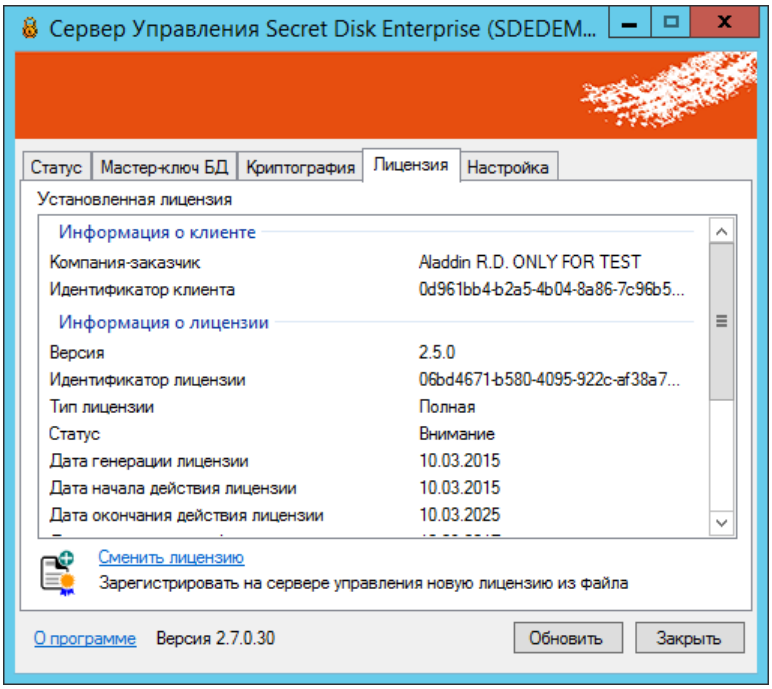
1. Откройте *Агент Secret Disk Management Server* и перейдите на вкладку *Мастер-ключ БД*.
2. Нажмите *Сменить мастер-ключ БД*. Нажмите *Далее*.
3. Укажите причину смены мастер-ключа БД, выбрав соответствующий пункт в поле со списком. Также можно добавить комментарий, который появится в журнале. Нажмите *Далее*.
4. Мастеру потребуется проверить электронный ключ с действующим сертификатом оператора. Подключите ключ и нажмите *Далее*.
5. Укажите нужный сертификат в окне выбора сертификата оператора. Нажмите *Далее.*
6. Для шифрования нового мастер-ключа БД можно использовать сертификат оператора, который уже зарегистрирован в базе данных, для этого выберите пункт *Использовать существующий сертификат в БД*.
7. В качестве нового сертификата оператора можно зарегистрировать сертификат, находящийся на токене. Для этого отметьте пункт *Зарегистрировать новый сертификат из памяти электронного ключа*.
8. Нажмите *Далее*.
9. Если был выбран пункт *Зарегистрировать новый сертификат из памяти электронного ключа*, появится окно со списком доступных сертификатов на электронном ключе, один из которых следует выбрать и подтвердить выбор, нажав *OK*.
10. Подтвердите выполнение операции, нажав *Далее.*
11. Введите пароль токена и нажмите кнопку *OK*.
12. Дождитесь окончания процесса смены мастер-ключа БД.
13. После того в поле *Состояние* появится сообщение *Успешно завершён*, нажмите *Далее*.
14. Смонтируйте криптохранилище и выполните резервное копирование нового мастер-ключа БД.
15. Нажмите *Завершить*.

19. Лицензирование Secret Disk Enterprise

Лицензия на использование Secret Disk Enterprise распространяется в виде файла, который загружается в процессе установки системы. Лицензия определяет доступные для использования функциональные возможности Secret Disk Enterprise:

1. Количество рабочих мест.
2. Возможность работы в кластерной конфигурации.
3. Доступ по сети к защищённым дискам.
4. Защита съёмных носителей.
5. Создание защищённых контейнеров.

> *При необходимости файл лицензии может быть замен посредством операции Сменить лицензию.*



Информация о лицензии также доступна на странице Веб-Портала SDMS *Администрирование/Лицензия*.

> *Изменить лицензию через Веб-Портал нельзя.*

Статус лицензирования определяет набор операций, которые позволяет осуществлять управляющий сервер SDMS. Список операций для различных статусов лицензирования приведён в следующей таблице:

Статус лицензирования	Операции				
	Запуск сервиса SDMS и доступ к панели	Запуск Веб-портала SDMS	Регистрация новой рабочей станции	Административные операции	Доступ к защищённым ресурсам
Лицензия действительная	разрешено	разрешено	разрешено	разрешено	разрешено
Лицензия отсутствует или повреждена	разрешено	запрещено	запрещено	запрещено	запрещено

Закончился период действия	разрешено	разрешено	запрещено	разрешено	запрещено
Достигнут лимит количества рабочих станций	разрешено	разрешено	запрещено	разрешено	разрешено

Приложение А

Система Secret Disk Enterprise состоит из нескольких взаимодействующих частей (Рисунок 2):

- управляющего сервера Secret Disk Management Server в составе:
  - сервер бизнес-логики;
  - шлюз клиентов;
  - административный веб-портал.
- база данных SDE под управлением СУБД MS SQL Server;
- рабочие станции пользователей с клиентским программным обеспечением Secret Disk Agent;
- рабочие станции пользователей с ролями Администраторов, Операторов, Аудиторов.

Также при работе SDE используется две общие службы инфраструктуры предприятия, которые показаны на рисунке:

- служба Active Directory;
- служба Сертификации.

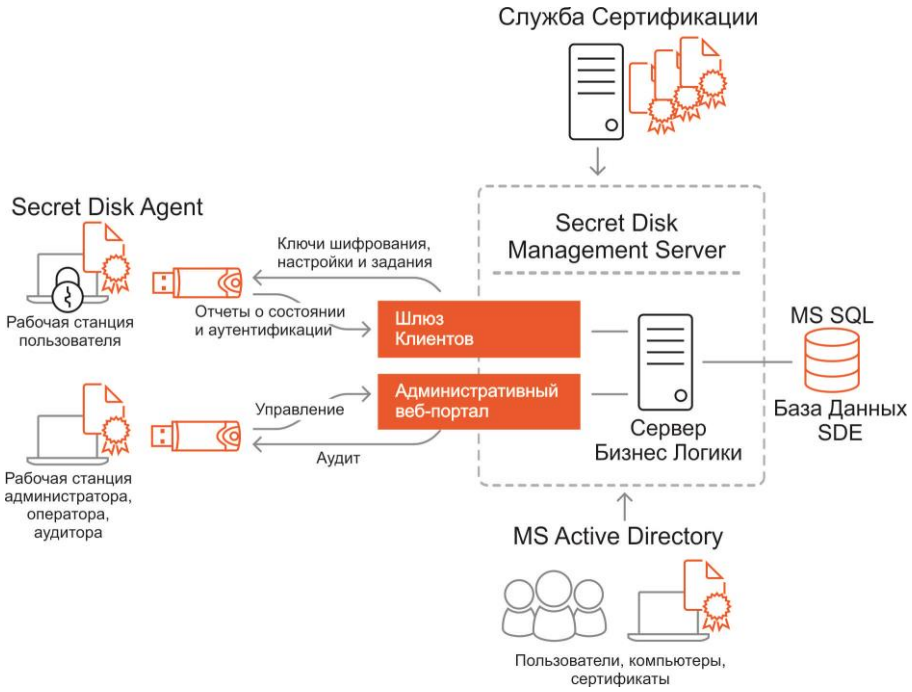


Рисунок 2 – Состав системы Secret Disk Enterprise

Сервер бизнес-логики

Назначение центрального компонента Сервера Управления SDE:

- обеспечение взаимодействия компонентов и процессов SDE;
- управление созданием, хранением и использованием ключей шифрования данных;
- отправление на рабочие станции команд на создание защищённых ресурсов и операции с ними;
- хранение учётных записей пользователей, рабочих станций и защищаемых ресурсов и связях между ними;
- предоставление уполномоченному пользователю доступ к защищённому ресурсу, предоставляя ключ шифрования ресурса.

Сервер работает как служба ОС. Приложение SDMS, позволяет запускать и останавливать службу, монтировать (приводить в рабочее состояние) Криптохранилище, устанавливать мастер-ключ Базы Данных SDE и настраивать основные параметры системы.

Шлюз клиентов

Поддерживает сетевое подключение Агентов рабочих станций к серверу Бизнес-логики и их взаимодействие в рамках сессий. Обладает возможностью масштабирования за счёт кластеризации.

Клиенты работают по протоколу HTTP, номер порта по умолчанию 8888 (при необходимости можно изменить). Порт используется совместно с Административным веб-порталом. Для работы шлюза необходим Веб-сервер IIS с поддержкой приложений ASP.NET.

Административный веб-портал

Веб-приложение, при помощи которого пользователи с ролями Администратор ИБ, Оператор и Аудитор управляют системой Secret Disk Enterprise. Другие пользователи SDE не имеют доступа к этому приложению.

> *Для работы приложения необходим Веб-сервер IIS с поддержкой ASP.NET.*

База данных SDE

Хранится полная конфигурация работающей системы SDE, журналы операций и событий в системе, сертификаты пользователей и ключи шифрования защищаемых ресурсов, зашифрованные с использованием Мастер-ключа. Также в базе данных хранятся криптокопии Мастер-ключа, зашифрованные открытыми ключами сертификатов операторов.

Рабочую конфигурацию SDE и доступ к защищённым ресурсам можно полностью восстановить, имея базу данных SDE (или её резервную копию), а также копию мастер-ключа БД.

> *Используется СУБД MS SQL Server. Необходимо выполнять регулярное резервное копирование базы данных SDE и принять меры по обеспечению высокой доступности СУБД.*

Secret Disk Agent

Клиентское программное обеспечение, устанавливаемое на рабочих станциях пользователей.

Функции:

- осуществление двухфакторной аутентификации пользователей по электронным ключам;
- получение от управляющего сервера ключей шифрования защищённых ресурсов;
- подключение и отключение защищённых ресурсов и обеспечение доступа пользователя к ним;
- исполнение команды управляющего сервера на действия с защищаемыми ресурсами;
- передача управляющему серверу информации о конфигурации рабочих станций и действий пользователя;
- обеспечение работы с защищёнными папками и контейнерами;
- включает в себя загрузочный драйвер для защищённого системного диска.

Служба Active Directory

Используется управляющим сервером для получения информации о пользователях и компьютерах домена Active Directory корпоративной сети, которые могут быть добавлены в качестве пользователей и рабочих станций системы Secret Disk Enterprise.

Получает из Active Directory сертификаты новых пользователей для занесения их в базу данных SDE, если они там имеются.

Система SDE не хранит собственных данных в Active Directory и не модифицирует имеющиеся там данные. После регистрации пользователей и рабочих станций в SDE вся необходимая информация находится в базе данных SDE.

Служба Сертификации

Используется для выпуска сертификатов стандарта X.509 на электронных ключах и удостоверения выпущенных сертификатов при операциях с ними. Вместе с SDE можно использовать различные Службы сертификации, если обеспечивается выполнение следующих требований:

- сертификаты выпускаются на электронных криптографических ключах;
- сертификаты предназначены для шифрования ключей (поле Key Usage сертификата содержит значение "Key Encipherment");
- длина открытого ключа шифрования RSA сертификата не менее 1024 бит (поле Public Key).

> *Сертификаты пользователей SDE на электронных ключах могут использоваться и для других целей, например, для аутентификации пользователей корпоративной сети, но это не является обязательным.*

20. 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.

20.1 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.

21. Контакты

21.1 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.

21.2 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.
2.0	

Коротко о компании

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

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

Основные направления

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

Лицензии

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

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании соответствует требованиям ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15

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