SECRET DISK AGENT

Руководство Пользователя

Версия	2.0
Статус	Публичный
Дата	19.04.2019
Номер	ID-номер

Аннотация

Настоящий документ представляет собой руководство пользователя по работе с приложением SDA версии 2.7, которое является клиентской частью системы Secret Disk (SD). Приложение предназначено для защиты данных на запоминающих устройствах компьютеров от несанкционированного доступа.

Оглавление

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 Secret Disk 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 Secret Disk 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 Secret Disk	Компьютер, на котором установлено клиентское программное обеспечение SDA. 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 Secret Disk и предупреждения о них.
AD	Active Directory

IIS	Microsoft Internet Information Server
SDA	Клиентская часть системы Secret Disk: приложение, позволяющая пользователям получать доступ к защищённым ресурсам, находящимся на их рабочей станции.
Secret Disk Management Server (SDMS)	Серверная часть системы Secret Disk, 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 управляют работой системы.
База данных Secret Disk (БД)	Объект, представляющий базу данных MS SQL. Используется как хранилище настроек, учётных записей и ключей системы Secret Disk.
Лицензия	Файл с данными о передаваемых пользователю правах и возможностях использования Secret Disk.
Мастер-ключ базы данных	Ключ шифрования, используемый для создания криптокопий ключей шифровавания ресурсов для безопасного хранения их в базе данных Secret Disk.
Ключ шифрования ресурса	Ключ симметричного шифрования, используемый для зашифрования и расшифрования данных защищённого ресурса, ключ шифрования уникален для каждого ресурса.
Отключение криптохранилища	Выгрузка из памяти сервера бизнес-логики мастер-ключа базы данных с блокированием доступа к ключам шифрования ресурсов. Операция выполняется операторами Secret Disk 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 SDA 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: 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

Приложение SDA предназначено для защиты конфиденциальной информации в корпоративной системе компании. SDA работает под управлением ОС семейства Windows с централизованным управлением защищенными ресурсами. Оно является компонентом корпоративной системы защиты конфиденциальной информации Secret Disk.

Защита осуществляется путём шифрования ресурсов, которое делает невозможным извлечение информации посторонними лицами из запоминающих устройств компьютера.

SDA позволяет:

- защищать информацию на внутренних дисках компьютеров;
- защищать информацию на внешних запоминающих устройствах, таких как флэш-накопители, внешние диски с USB-интерфейсом и карты памяти;
- защищать системные диски компьютеров, разрешая загрузку ОС и доступ к системным данным только зарегистрированным пользователям с электронным ключом;
- создавать защищённые папки на обычных дисках;
- удалять информацию с дисков без возможности её восстановления;

Для доступа к защищённым данным зарегистрированному пользователю необходимо иметь специальный электронный ключ (USB-токен или смарт-карту) и знать PIN-код.

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.

SD 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 SD централизовано администраторами информационной безопасности.
3. Разрешение/запрет сетевого доступа к защищенным ресурсам в корпоративной сети.

3.3 Администратор Информационной Безопасности Secret Disk

Система Secret Disk управляется централизовано специально уполномоченным лицом – Администратором ИБ. Он определяет общие настройки системы, устанавливает и снимает защиту для обычных и виртуальных дисков и предоставляет пользователям разрешения на их использование.

3.4 Сервер управления Secret Disk

После запуска приложение устанавливает соединение с сервером управления системы Secret Disk, чтобы получить необходимые настройки и ключи для подключения защищённых дисков и других ресурсов пользователя.

> *Если соединение с управляющим сервером установить не удалось, подключение всех или части защищённых ресурсов будет невозможно.*

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 SDA.

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 SD, 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 SD разрешена защита съёмных носителей, то при подключении такого носителя происходит следующее:

- SD 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 SD 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, 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 информацией с получателями вне системы SD по незащищённым каналам связи (почта, мессенджеры и прочее). Защищенный контейнер представляет собой защищённый виртуальный диск, который можно открыть как в системе SD, так и на другом компьютере.

Типовой сценарий использования контейнера:

- пользователь SD, создаёт контейнер и работает с ним как с виртуальным диском, куда помещается передаваемая информация;
- перед отправкой контейнера SD 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 SD, 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 SD работает с контейнером без ввода пароля;
- SD создаёт сложные пароли, которые меняются при каждой подготовке контейнера к отправке;
- для защиты используется стойкий алгоритм шифрования (AES с длиной ключа 256 бит).

5. Работа с SDA

5.1 Электронный ключ пользователя

Электронный ключ (токен) требуется в следующих случаях:

1. Для загрузки ОС с защищённого системного диска. В этом случае токен запрашивается Загрузчиком Secret Disk до начала загрузки ОС.
2. Для запуска SDA после успешной авторизации пользователя в ОС. В этом случае токен можно подключить только тогда, когда требуется начать работу с защищёнными ресурсами.

При отключении токена SDA продолжает предоставлять доступ к уже открытым защищённым ресурсам, но может и прекратить доступ к ним.

> *Поведение приложения в ситуации, когда токен отключен от компьютера настраивается Администратором.*

В случае недоступности токена в Загрузчике Secret Disk предусмотрена возможность запуска ОС по специальному коду. Все защищённые ресурсы, кроме системного диска, без токена будут недоступны. Для восстановления доступа нужно получить новый токен или использовать токен другого пользователя системы, имеющего разрешение на доступ к ресурсам на выбранном компьютере.

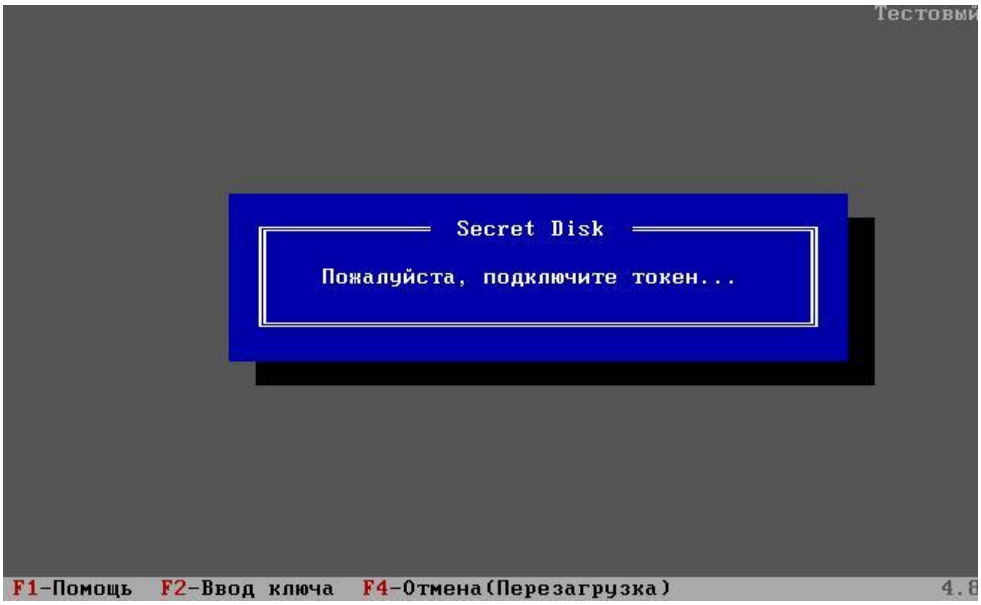
5.2 Старт ПК с защищенным системным диском

Программа-загрузчик SDA запускается сразу после включения компьютера и выводит запрос на подключение токена, если обнаруживает защищённый системный диск.

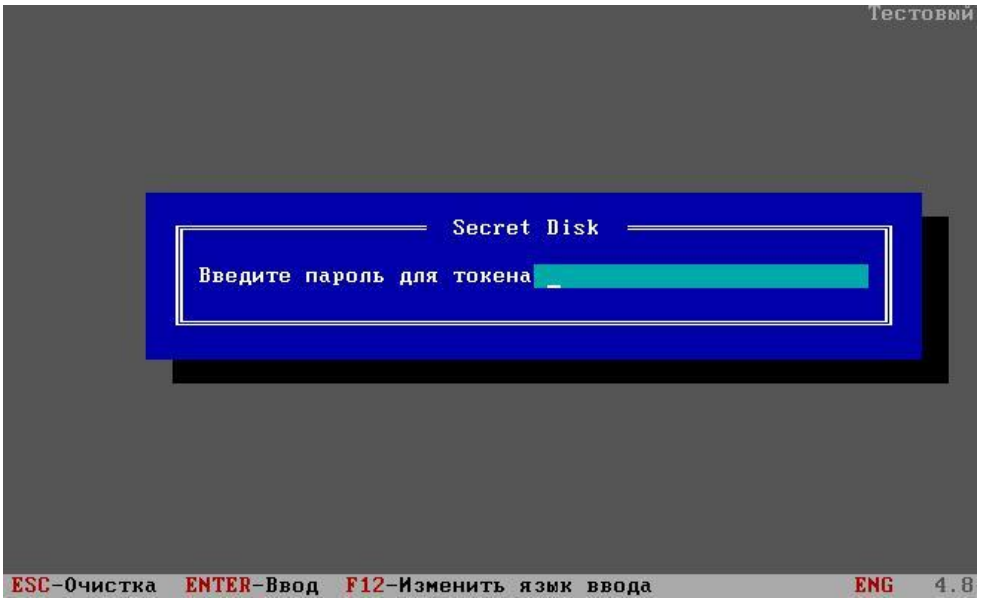
> *Если защита не установлена, то ОС запускается в обычном режиме без дополнительных запросов.*

Порядок действий при загрузке с защищённого системного диска представлен ниже.

1. Включите компьютер.
2. Подключите токен к ПК при появлении запроса.



3. Введите PIN-код токена и нажмите Enter.



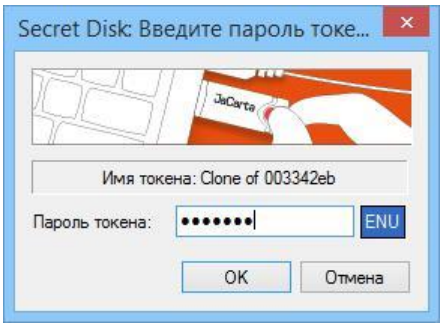
После начала загрузки ОС токен можно отключить, если в дальнейшем не предполагается работа с другими защищёнными ресурсами кроме системного диска.

5.3 Вход пользователя в систему Windows

Процедура входа в систему с установленным SDA не отличается от обычной, но может различаться в разных организациях. Инструкцию по входу в систему пользователю должен сообщить системный администратор. Обычно для входа в систему после загрузки, нужно выбрать учётную запись на экране входа и ввести пароль этой учётной записи. Если для входа используется токен, следует ввести его PIN-код.

5.4 Запуск SDA

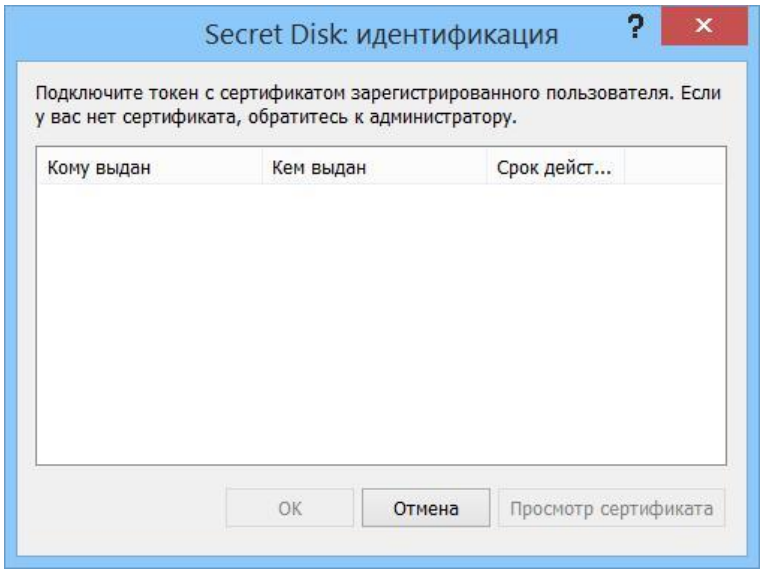
После входа в систему следует подключить токен, если он не был подключён раньше. Если в системе настроен автоматический запуск SDA при подключении токена, то появится окно ввода пароля Secret Disk.



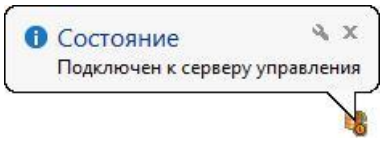
Если автоматический запуск не произошёл, необходимо запустить приложение SDA вручную.

Если на токене отсутствует сертификат пользователя, то приложение покажет соответствующее предупреждение.

Для записи сертификата пользователя на токен обратитесь к системному администратору компании.



Если токен и пароль действительны, то приложение начнёт работу. В области уведомлений появится значок SDA и будет выведены сообщения о состоянии подключения к серверу управления, и о подключении дисков, если настроено их автоматическое подключение.



Значок SDA в области уведомлений о подключении дисков

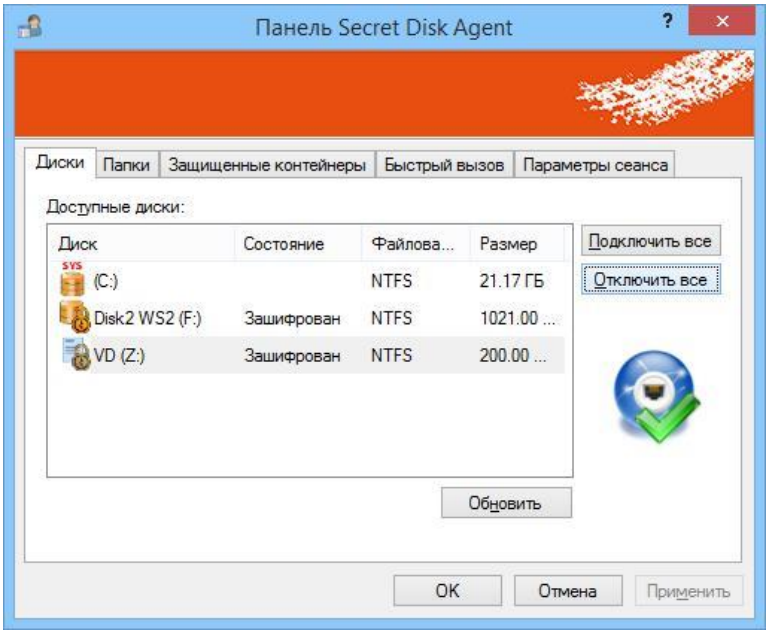
Значок SDA в области уведомлений

Сообщение

5.5 Панель управления SDA

Панель SDA – это главное окно приложения. Его можно вызвать несколькими способами:

1. Запуском приложения SDA с помощью значка в меню (экране) Пуск.
2. Двойным щелчком левой кнопкой мыши по значку SDA.
3. Выбором пункта Панель Secret Disk в контекстном меню значка SDA.
4. Нажатием комбинации клавиш быстрого вызова (настраивается на вкладке Быстрый вызов).



Закрыть панель можно кнопками *OK*, *Отмена* или системной кнопкой закрытия окна ("крестиком").

> *Закрытие панели не прекращает работу SDA и не закрывает сессию работы с Secret Disk.*

Значок состояния сервера в правой части окна показывает состояние взаимодействия Агента и управляющего сервера SDMS:

SDA подключён к серверу управления

SDA не подключён к серверу управления

> *При отсутствии подключения к серверу управления SDA продолжает предоставлять доступ подключённым дискам, но не может подключить отключённые диски и выполнять операции, поступающие в виде команд от сервера управления.*

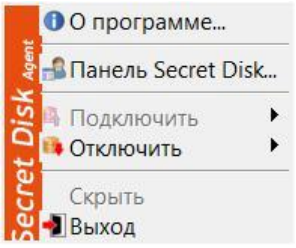
Использование панели для работы с защищёнными ресурсами, описано в разделах, посвящённых работе с ними.

5.6 Выход из приложения и перезапуск SDA

При выходе пользователя из системы Windows, работа приложения SDA завершается автоматически, при этом все диски и другие защищённые ресурсы отключаются.

Выход из SDA без выхода из системы может потребоваться при изменениях в настройках, сделанных Администратором. Например, если пользователю был предоставлен доступ к зашифрованному диску, то, чтобы начать работать с ним, нужно перезапустить SDA на рабочем месте пользователя. Выход из SDA делается следующим образом:

1. Сохраните все открытые документы и файлы, находящиеся на защищённых дисках, в контейнерах и папках.
2. Откройте меню значка SDA правой кнопкой мыши и нажмите Выход.



3. SDA выведет уведомление об отключении дисков и завершит сеанс.

> *Для закрытия сеанса и выхода из SDA может быть использована комбинация горячих клавиш, если она была настроена в Панели.*

5.7 Подключение и отключение защищённых дисков

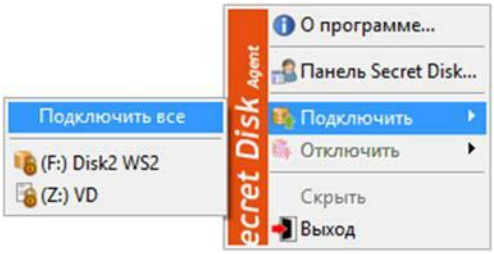
SDA может подключать и отключать защищённые диски. С подключенным диском можно работать как обычно, то есть читать и записывать файлы или отформатировать устройство. С отключенным диском операции невозможны: при попытке обращения к нему ОС сообщит о недоступности устройства.

Защищённые диски можно подключать или отключать несколькими способами.

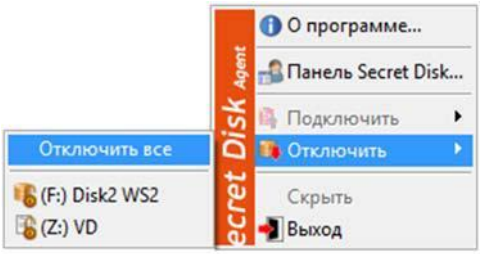
> *Чтобы подключить диск, пользователь должен иметь разрешение на выполнение этого действия.*

5.7.1 С помощью меню значка SDA

1. Подключение дисков.
   - откройте меню значка SDA с помощью правой кнопки мыши, выберите *Подключить*;
   - во втором меню укажите конкретный диск или выберите *Подключить все*.

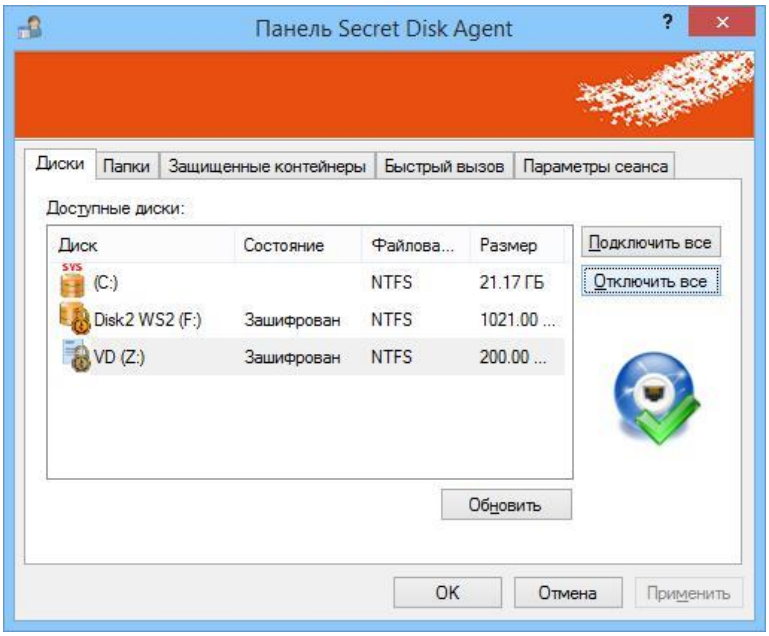


2. Отключение дисков.
   - откройте меню значка SDA с помощью правой кнопки мыши, выберите *Отключить;*
   - во втором меню укажите конкретный диск или выберите *Отключить все.*

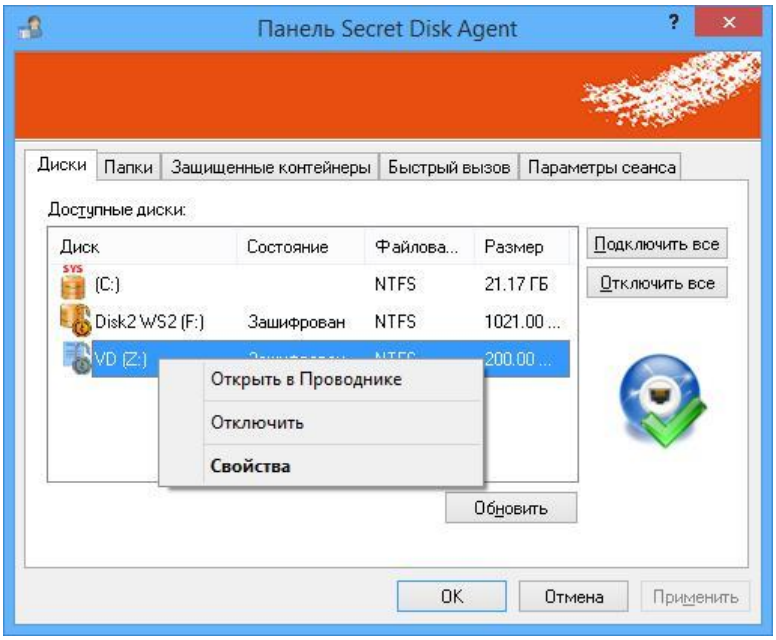


5.7.2 С помощью панели Secret Disk Agent

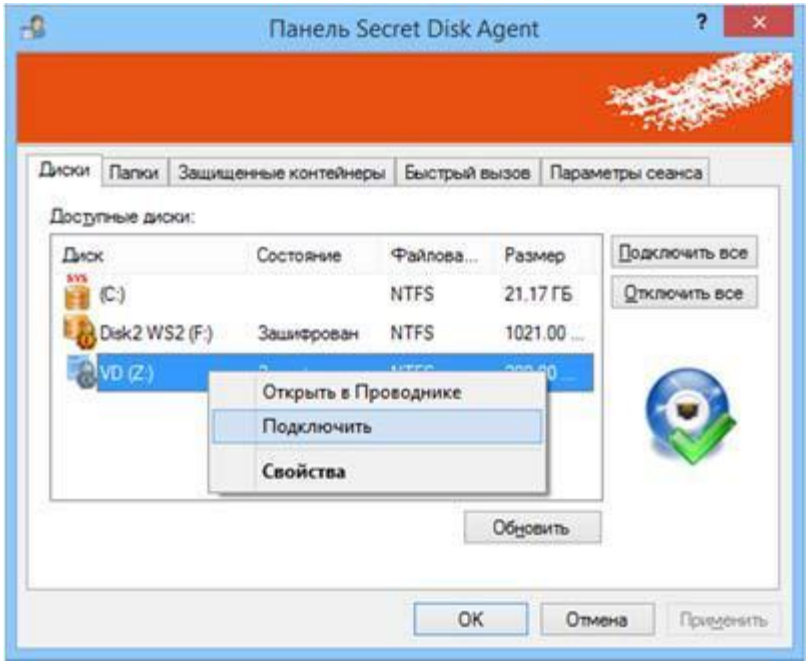
1. Подключение или отключение всех дисков.
   - откройте Панель SDA двойным нажатием мыши по значку SDA в области уведомлений;
   - перейдите на вкладку Диски;
   - нажмите *Подключить все* или *Отключить все* для выполнения нужного действия;
   - закройте панель SDA, нажав *OK* или *Отмена*.



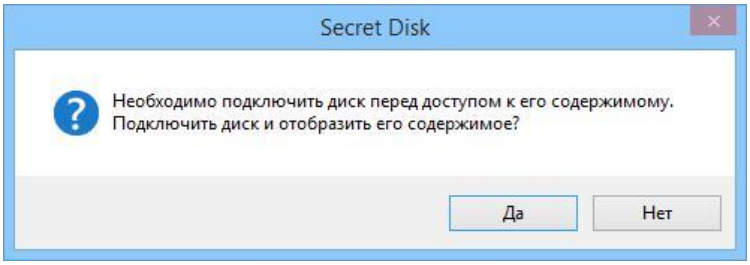
2. Отключение одного диска.
   - откройте Панель SDA двойным щелчком мыши по значку SDA в области уведомлений;
   - перейдите на вкладку Диски;
   - нажмите правой кнопкой мыши по нужном диску в списке доступных;
   - в меню диска нажмите *Отключить.*



3. Подключение одного диска (1-й способ).
   - откройте Панель SDA двойным нажатием мыши по значку SDA в области уведомлений;
   - перейдите на вкладку *Диски;*
   - нажмите правой кнопкой мыши по нужном диску →*Подключить;*



4. Подключение одного диска (2-й способ)
   - откройте панель SDA;
   - на вкладке Диски выберите нужный диск;
   - подтвердите подключение диска перед открытием, которое появится если диск отключен.



5.7.3 Автоматическое подключение и отключение дисков

Подключение и отключение всех дисков одновременно происходит в следующих случаях:

- при входе пользователя в систему обычные и виртуальные диски подключаются автоматически, если это разрешено Администратором;
- при выходе пользователя из системы все диски отключаются;
- при отключении токена диски могут как отключаться, так и оставаться подключенными в зависимости от настройки системы, установленных Администратором;

> *Защищённый системный диск всегда подключается при загрузке компьютера, отключить его нельзя.*

- внешние диски и флэш-накопители подключаются и отключаются при присоединении и отсоединении с компьютером.

5.8 Доступ пользователей к подключённым дискам

При одновременном входе нескольких пользователей в систему, им доступны все подключенные другим пользователем Secret Disk диски и контейнеры. В этом случае доступ пользователей к данным на подключённых дисках определяется настройками безопасности ОС.

> *Использование Secret Disk Agent не отменяет необходимости настраивать разрешения на доступ к файлам и папкам обычными средствами ОС!*

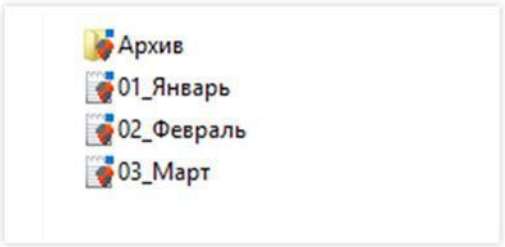
5.9 Защищённые папки

5.9.1 Свойства защищенных папок

Защищённые папки – это папки, файлы в которых зашифрованы. Установку и снятие защиты для папки делает сам пользователь, а не Администратор.

Пользователи, имеющие разрешение на доступ к папке, видят содержимое защищённой папки и могут работать с ним. Остальные пользователи будут видеть содержимое папки как объекты с бессмысленными именами, которые нельзя открыть в каком-либо приложении.

Защищённые папки и объекты в них помечаются дополнительными значками в *Проводнике*.



Файлы в защищённой папке к которым разрешён доступ

Файлы в защищённой папке к которым нет доступа

При создании защищённой папки доступ к ней получает только тот пользователь, который установил защиту. Доступ другим пользователям может разрешить Администратор.

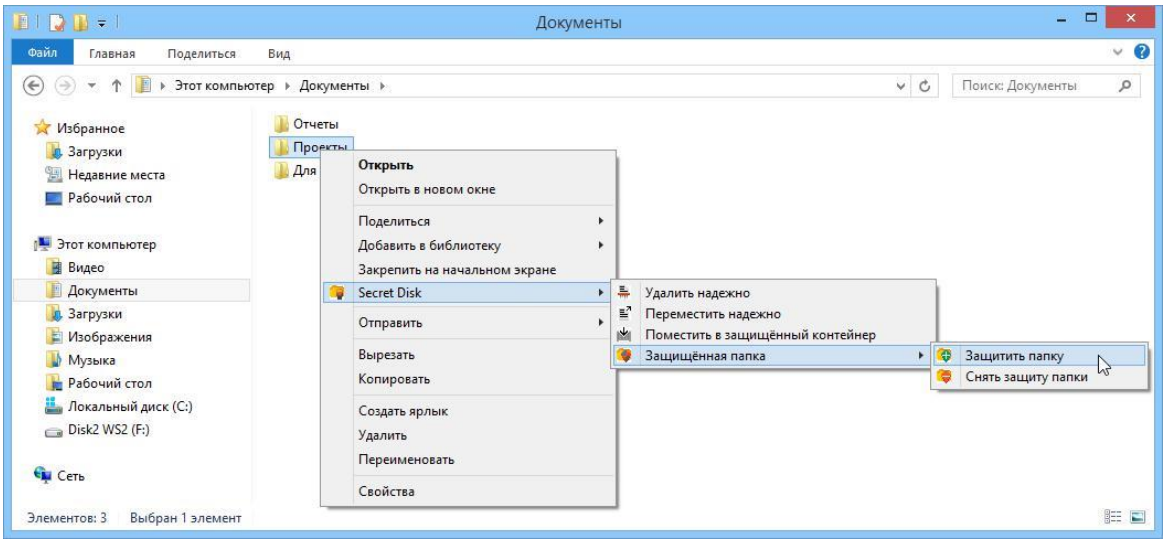
> *Файлы в защищённой папке зашифрованы только тогда, когда они находятся в ней. При копировании или перемещении файлов в обычную папку они будут расшифрованы!*
>
> *Удалённые файлы попадают в Корзину в незащищённом виде.*
>
> *Использование защищенных папок может быть запрещено настройками системы.*

5.9.2 Включение и снятие защиты папки

Включение и снятие защиты папок делается в Проводнике с помощью меню Secret Disk.

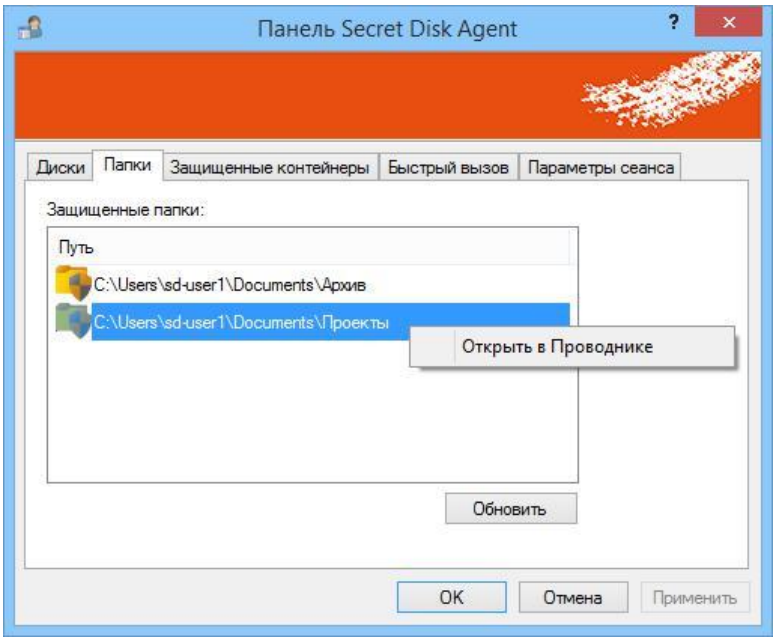
1. Откройте Проводник и выберите нужную папку.
2. Откройте меню *Secret Disk* → *Защищённая папка*.
3. Выберите одну из команд: *Защитить папку* или *Снять Защиту папки*. Подтвердите действие с папкой в появившемся окне.

> *Установка или снятие защиты может занять некоторое время, при завершении операции появится окно с сообщением об окончании процесса.*



5.9.3 Список защищённых папок

Все защищённые папки всех пользователей, которые есть на дисках компьютера, отображаются на вкладке *Папки* в Панели SDA. Папки в списке можно открыть двойным нажатием мыши или с помощью контекстного меню.



Список папок обновляется при нажатии на кнопку *Обновить*.

> *При перемещении защищённых папок информация обновится только после перезапуска компьютера и открытия перемещённой папки в Проводнике.*
>
> *Если при открытии защищённой папки вы видите там нерасшифрованные данные, это означает, что у вас нет разрешения на доступ к этой папке. Доступ может предоставить Администратор.*

5.9.4 Доступ пользователей к защищённым папкам

После включения защиты папки доступ к ней разрешён только одному пользователю – тому, кто включил защиту. Доступ другим пользователям должен разрешить Администратор.

После того как Администратор разрешит другому пользователю доступ к папке, оно вступит в силу после перезапуска Secret Disk Agent на компьютере этого пользователя (см. раздел "Выход из приложения и перезапуск Secret Disk Agent").

5.9.5 Удаление защищённой информации в папке

Защищённую папку можно удалить не снимая с неё защиты. При удалении она попадёт в Корзину в защищённом виде.

> *При удалении файлов или папок, находящихся внутри защищённой папки, они попадают в корзину расшифрованными. Там к ним могут получить доступ другие пользователи.*

Используйте функцию *Удалить надёжно*, если хотите полностью удалить конфиденциальную информацию в защищённой папке.

5.9.6 Перемещение защищённой папки

При перемещении защищённой папки она остается зашифрованной, если перемещена в пределах одного и того же диска.

Смонтированная защищённая папка станет незащищённой, если будет перемещена на другой диск, даже если будет использована функция *Переместить надёжно*.

> *Будьте внимательны при перемещении защищённых папок! Проверьте состояние перемещённой папки и установите защиту снова, если это необходимо.*

5.10 Защищённые внешние устройства

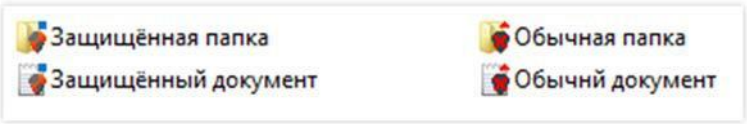
5.10.1 Режим работы внешних устройств

Secret Disk Agent обеспечивает несколько режимов работы с внешними устройствами:

- **обычный режим** – данные на внешних дисках можно читать и записывать как обычно;
- **режим чтения** – данные на внешних дисках можно только читать, запись невозможна;
- **защищённый режим** - новые данные записываются в зашифрованном виде, старые данные остаются доступными только для чтения.

Режим работы с внешним диском устанавливается Администратором для каждого пользователя и действуют на всех рабочих местах, где установлен Secret Disk Agent.

В проводнике файлы и папки на внешнем устройстве помечаются значками, указывающими на их состояние – обычное или защищённое (зашифрованное).



5.10.2 Работа в защищённом режиме

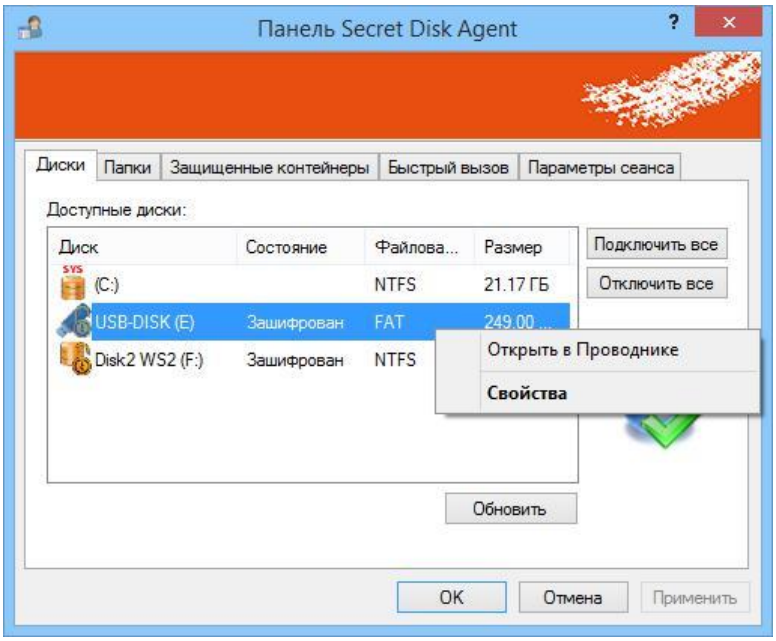
Secret Disk Agent включает защищённый режим работы автоматически при первом подсоединении внешнего диска к рабочей станции.

Пользователь, первым подключивший устройство, "присваивает" его: теперь только он может записывать и читать новые папки и файлы на нём. Другие пользователи смогут прочитать только незащищённые данные, которые были записаны раньше.

Разрешение на доступ к защищённым данным может дать другим пользователям Администратор. Пользователи, которым разрешён доступ, могут использовать внешнее устройство на любой рабочей станции, если войдут в систему под своей учётной записью.

5.10.3 Действия с внешними устройствами

Подключенные внешние устройства отображаются на вкладке *Диски* в Панели Secret Disk Agent. В поле *Состояние* выводится слово "Зашифрован", если устройство находится в защищённом режиме. Для других режимов работы это поле пустое.



Контекстное меню устройства в Secret Disk Agent позволяет открыть диск в Проводнике и увидеть информацию о диске. Переименовать диск или изменить его букву в окне свойств нельзя, для этого следует использовать Проводник.

Внешние диски всегда подключены, действие кнопок *Подключить все* и *Отключить все* на них не распространяется.

5.10.4 Отключение защищённого режима

Для отключения защищённого режима внешнее устройство нужно отформатировать на компьютере, где Secret Disk Agent не установлен или не запущен (выполнена команда Выход).

Если отформатировать внешний диск при работающем Secret Disk Agent, то защищённый режим включиться снова при первом обращении к диску после форматирования.

5.10.5 Особенности защищённого режима

Внешний накопитель фактически становится защищённым в тот момент, когда какой-нибудь пользователь в первый раз подключит его и откроет на компьютере, где работает Secret Disk Agent.

Все файлы и папки, которые находились на устройстве до включения защищённого режима, будут доступны всем пользователям Secret Disk Agent для чтения.

На защищённом внешнем накопителе остаётся общедоступной та информация, которая была записана на нём раньше, но новые данные оказываются защищёнными и доступны тому, кто их записал (и тем, кто получил разрешение на доступ именно к этому устройству).

5.11 Защищённые контейнеры

5.11.1 Использование защищённых контейнеров

Защищённые контейнеры – это зашифрованные файлы виртуальных дисков, предназначенные для двухстороннего обмена информацией между пользователями Secret Disk и внешними пользователями, компьютеры которых не подключены к этой системе и не имеют электронного ключа.

Работу с контейнером поддерживают два приложения - Secret Disk Agent и Secret Disk Reader. Приложение Secret Disk Reader позволяет открывать контейнер с помощью пароля. Его должен установить у себя внешний пользователь-получатель контейнера.

Контейнер и пароль для него создаются пользователем Secret Disk Agent. Он отправляет их получателю, который открывает их в Secret Disk Reader. После этого оба пользователя могут поочерёдно изменять содержимое контейнера и обмениваться информацией, отправляя друг другу экземпляры контейнера.

Файлы контейнеров зашифрованы, поэтому их можно передавать открыто, например, посылать по электронной почте или выкладывать для скачивания.

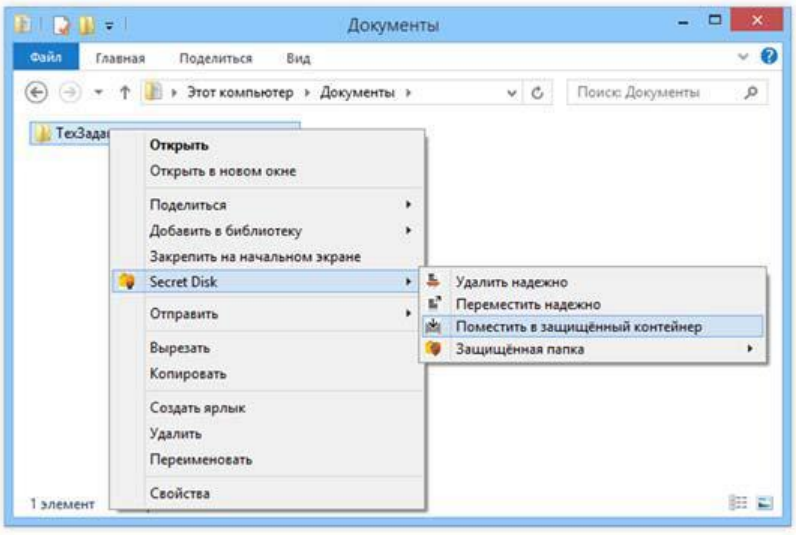
Если пароль к контейнеру передаётся получателю так, чтобы он не мог попасть к посторонним лицам вместе с контейнером, то обмен информацией с помощью контейнеров будет защищён от несанкционированного доступа.

> *Использование контейнеров может быть запрещено настройками системы. Узнайте у Администратора SD, можете ли вы создавать контейнеры.*

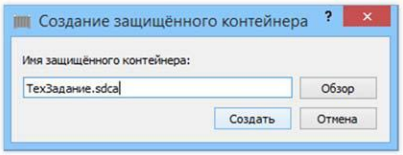
5.11.2 Создание контейнера

Контейнер создаётся в Проводнике с помощью меню Secret Disk. При создании в контейнер можно поместить несколько файлов и папок сразу.

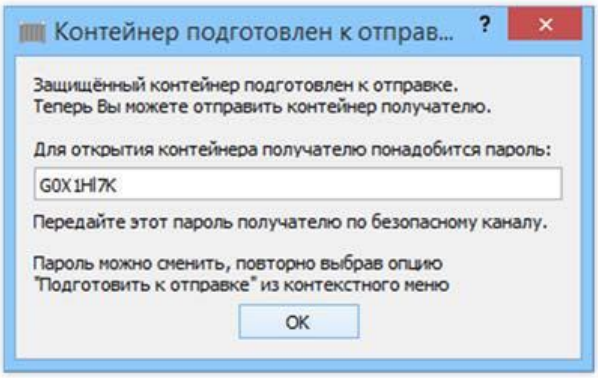
1. Выделите в *Проводнике* нужные файлы и папки, в контекстном меню выберете пункт Secret Disk > Поместить в защищённый контейнер.



2. Выберите место размещения контейнера и его имя и нажмите *Создать*.



3. Запишите пароль или скопируйте его в файл. Этот пароль нужно будет сообщить получателю контейнера. Нажмите *OK*.



Исходные файлы и папки при создании контейнера не удаляются и не изменяются, в контейнер помещается их копия. Файл контейнера имеет расширение ".sdca".

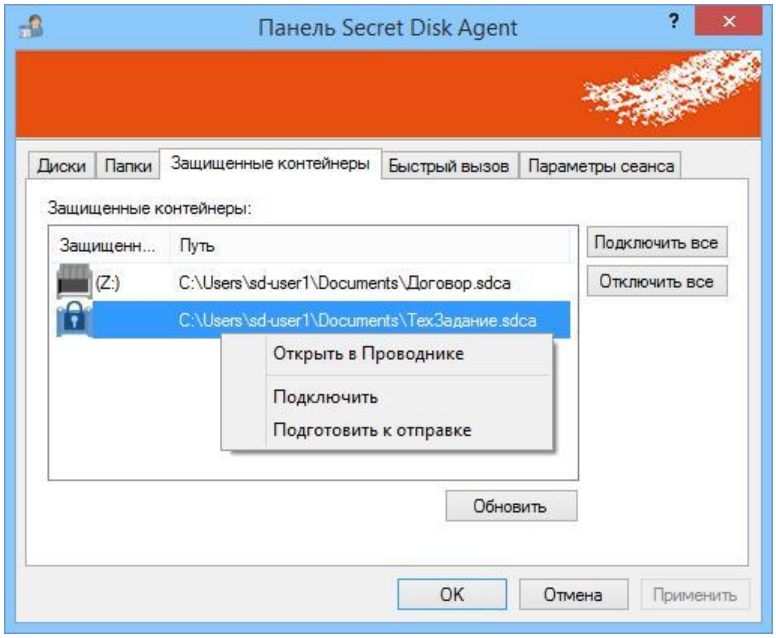
4. Отправьте любым удобным способом файл контейнера получателю и сообщите ему пароль для открытия контейнера.

Не отправляйте пароль вместе с контейнером в одном письме! Используйте другой способ связи или канал передачи данных.

5.11.3 Список контейнеров

Список контейнеров находится в приложении Панель Secret Disk Agent на вкладке *Защищённые контейнеры*. В списке перечислены контейнеры, созданные или открытые текущим пользователем Secret Disk Agent.

Для каждого контейнера указывается месторасположение и имя его файла, а также буква диска, если контейнер подключён как виртуальный диск.



При перемещении файла контейнера вручную, информация о нём в списке не будет соответствовать действительному местоположению файла до тех пор, пока он не будет открыт в Проводнике. При удалении контейнера запись о нём также может оставаться в списке до перезапуска приложения.

> *После перемещения файла контейнера или получения нового экземпляра контейнера, откройте его в Проводнике. Это обновит информацию в списке.*

5.11.4 Действия на вкладке Защищённые контейнеры

Для действий с контейнерами можно использовать кнопки *Подключить все* и *Отключить все*, либо открыть контекстное меню одного контейнера.

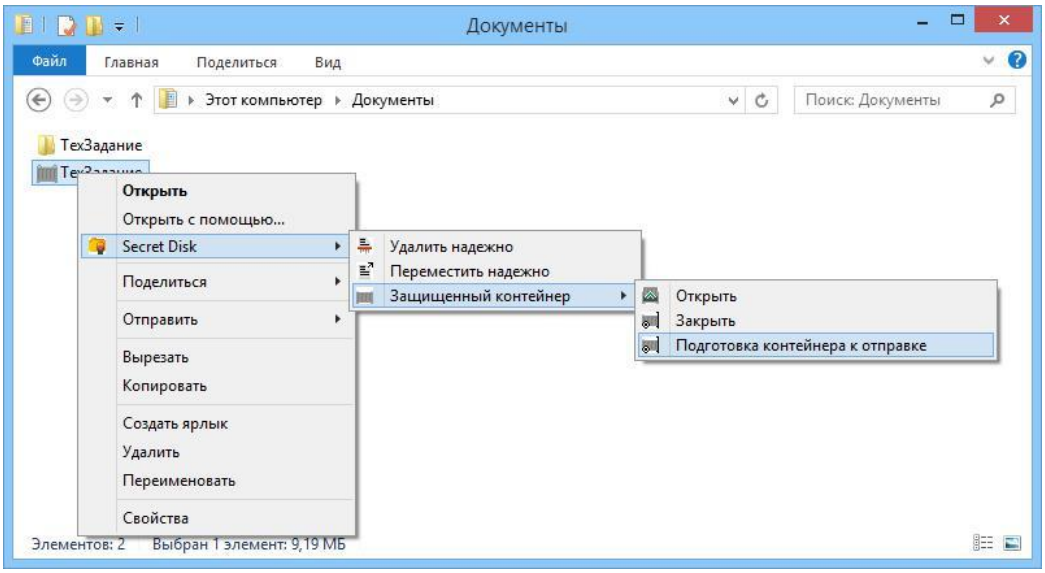
С помощью контекстного меню можно выполнить следующие действия:

1. Открыть контейнер в *Проводнике*.
2. Подключить неподключенный контейнер.
3. Отключить подключённый контейнер.
4. Подготовить контейнер к отправке, поменяв пароль для доступа к нему.

Кроме этих действий, можно открыть контейнер в проводнике с помощью двойного щелчка мыши по имени контейнера в списке.

5.11.5 Действия с контейнерами в Проводнике

1. Двойной щелчок мыши подключает контейнер как диск и открывает его в новом окне.
2. Нажатие правой кнопки открывает контекстное меню со следующими действиями:
   - открыть;
   - закрыть;
   - подготовка контейнера к отправке.



> *При открытии контейнер подключается как диск компьютера. При закрытии контейнера диск отключается, после чего файл контейнера можно отправить получателю.*

5.11.6 Изменение пароля контейнера

Пароль контейнера можно поменять. Обычно это делается перед отправкой контейнера получателю.

1. Откройте контекстное меню для файла контейнера и выберете пункт *Secret Disk* → *Защищённый контейнер* → *Подготовка контейнера к отправке*.
2. Secret Disk Agent выведет окно с новым паролем, который надо сохранить и передать получателю. Новый пароль действителен только для конкретного экземпляра контейнера, пароли у других контейнеров не меняются.

5.11.7 Ёмкость контейнера и размер файла контейнера

Размер виртуального диска контейнера фиксированный, он задаётся автоматически при создании контейнера по следующему правилу: минимальный размер виртуального диска – 100 мбайт, максимальный размер равен утроенному объёму данных, помещаемых в контейнер при его создании.

Размер файла контейнера растёт в зависимости от объёма данных, сохраненных в контейнере. Пока контейнер не заполнен, файл контейнера меньше максимального размера виртуального диска.

Размер виртуального диска контейнера, свободный и занятый объем можно узнать в окне свойств диска, когда контейнер открыт.

5.11.8 Открытие "чужого" контейнера

Пользователь открывает без ввода пароля те контейнеры, которые он создал на этом компьютере. Контейнеры, созданные другими пользователями, также можно открыть в Secret Disk Agent, но при этом будет запрошен пароль. Таким образом, контейнеры можно использовать и для обмена данными между рабочими станциями, являющимися членами одной инфраструктуры Secret Disk.

6. Дополнительные функции Secret Disk Agent

6.1 Надёжное удаление и перемещение файлов и папок

При обычном удалении файлов средствами ОС их данные ещё некоторое время могут присутствовать на диске, пока соответствующие блоки данных не будет записаны вновь. Secret Disk Agent позволяет удалять файлы и папки надёжно, так, чтобы хранившуюся в них информацию нельзя было восстановить ни стандартными средствами Windows, ни сторонними приложениями.

При перемещении файлов и папок с одного дискового устройство или раздела на другое также возможно сохранение данных на устройстве-источнике, так как сначала происходит копирование данных на новое место, а потом – удаление исходных файлов. С помощью Secret Disk Agent удаление исходного файла (папки) при перемещении также можно осуществлять надёжно.

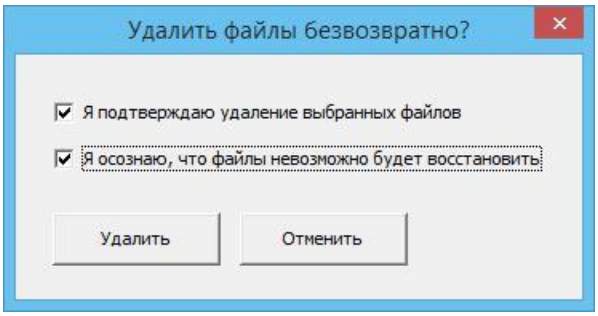
Функции применимы к файлам и папкам как на зашифрованных, так и на незашифрованных дисках.

Надёжное удаление записанной информации осуществляется методом трехкратной перезаписи ранее занятых блоков байтами со значением 255, то есть содержащими единицы во всех разрядах.

6.2 Надёжное удаление

Чтобы удалить файлы и/или папки без возможности восстановления, выполните следующие действия:

1. Откройте *Проводник*, выберите файлы и папки для удаления. Можно выделить несколько объектов.
2. В контекстном меню выберите *Secret Disk* → *Удалить надёжно*.
3. Подтвердите удаление, поставив в отобразившемся окне подтверждения два флажка.
4. Нажмите *Удалить* для удаления объектов. Чтобы отказаться от удаления, нажмите *Отменить*.



> *Файл-ярлык (файл с расширением ".lnk") рекомендуется удалять обычным способом. Удалить ярлык с помощью Secret Disk Agent можно лишь в составе выделенной группы или внутри папки.*

6.3 Перемещение с надёжным удалением

Функция перемещения позволяет перенести файлы и/или папки, удалив их по исходному пути без возможности восстановления. Чтобы воспользоваться этой функцией, выполните следующие действия:

1. Правой кнопкой мыши нажмите на файле, папке или выделенной группе файлов и/или папок, которую необходимо перенести.
2. В контекстном меню выберите пункт *Secret Disk* → *Переместить надёжно*.
3. В отобразившемся окне укажите путь до папки, в которую необходимо перенести выбранные объекты.
4. Нажмите *ОК*.

Файл-ярлык (файл с расширением ".lnk") рекомендуется перемещать обычным способом. Переместить ярлык с надёжным удалением с помощью SDA можно в составе выделенной группы или внутри папки.

6.4 Запрет сетевого доступа к защищённым дискам

Администратор может запретить доступ к защищённым дискам по сети. В этом случае пользователь не сможет предоставить доступ другим пользователям для всего защищённого диска или любой папки на нём, даже если у пользователя есть права администратора домена.

6.5 Установка защиты системного диска

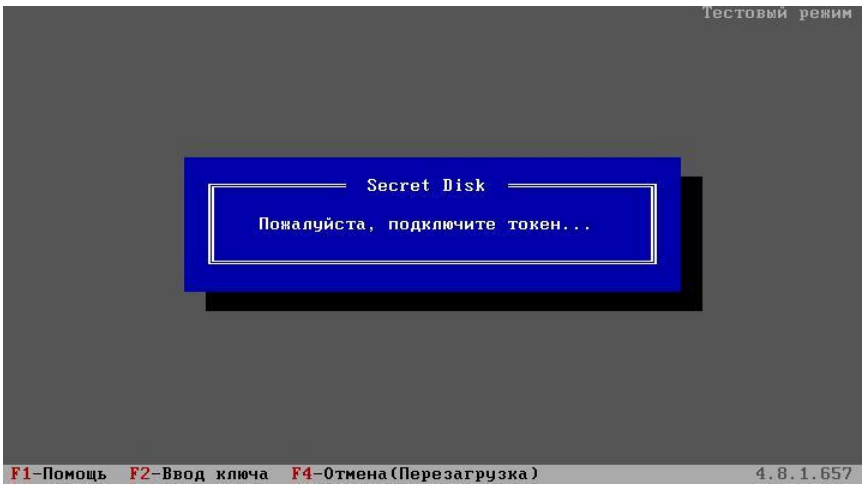
Установку защиты системного диска запускает Администратор Secret Disk. После инициирования установки защиты от пользователя требуется сделать одну тестовую перезагрузку компьютера, в ходе которой проверяется работа Загрузчика Secret Disk.

Если тестовая загрузка пройдёт успешно, то, когда пользователь снова войдёт в систему и запустит Secret Disk Agent, начнётся фоновое шифрование данных на системном диске. В случае неудачной перезагрузки или её отмены, защита системного диска не будет установлена.

О необходимости перезагрузки Secret Disk Agent уведомляет пользователя сообщением в области уведомлений.

При появлении сообщения:

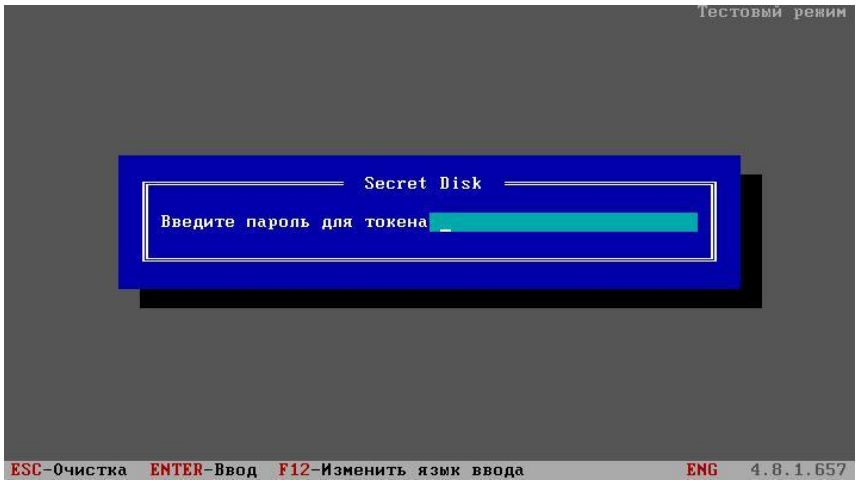
1. Перезагрузите компьютер. Перед загрузкой ОС на экране появится окно запроса электронного ключа.



2. Подсоедините электронный ключ (токен) к компьютеру и введите пароль (PIN-код) электронного ключа.
3. Нажмите *Enter*.

Нажатие клавиши F4 будет означать отказ от установки защиты. Компьютер перезагрузиться и ОС будет загружена в обычном режиме, без запроса токена.

4. После загрузки ОС установка защиты продолжится. Состояние процесса шифрования будет отображаться на вкладке *Диски* панели *Secret Disk Agent*.
5. По завершении установки защиты в поле *Состояние* появится надпись *Защищён*.



Если после перезагрузки окно загрузчика не появляется или защита системного диска не запускается, следует перезагрузить компьютер нажатием сочетания клавиш Ctrl-Alt-Del или кнопки с помощью Reset.

Во время установки защиты системного диска с файлами и папками на компьютере можно работать как обычно и использовать любые приложения, кроме Диспетчера диска. Компьютер можно перезагрузить до окончания установки защиты, в этом случае установка защиты продолжится после входа пользователя в систему.

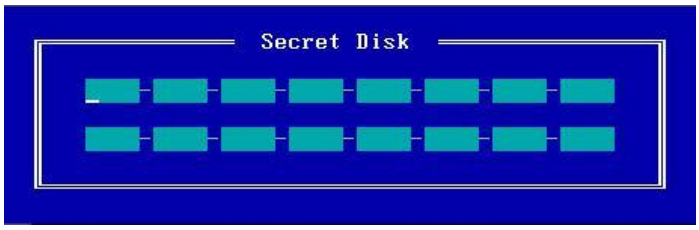
Если во время тестовой перезагрузки произошла ошибка и/или защита системного диска не была установлена, то рекомендуется обратиться в Службу технической поддержки компании "Аладдин Р.Д." чтобы установить причину и устранить её.

6.6 Загрузка компьютера без электронного ключа

В случае недоступности токена ОС компьютера можно загрузить с помощью 64-символьного кода восстановления, который можно получить у Администратора.

Чтобы восстановить доступ к защищённому системному диску без токена, выполните следующее.

1. Обратитесь к Администратору и получите у него код ключа.
2. Во время загрузки компьютера при появлении окна запроса токена с сообщением *Пожалуйста, подключите токен* нажмите клавишу F2.
3. Введите полученный код и нажмите Enter.



После ввода кода загрузка ОС продолжится в обычном режиме.

Код восстановления обеспечивает доступ только к загрузке и доступ к файлам на системном диске компьютера. Все другие защищённые ресурсы будут недоступны. Необходимо получить новый токен для восстановления нормальной работы пользователя.

7. Приложение Modern Secret Disk Agent

7.1 Назначение

Приложение Modern Secret Disk Agent (mSDA) предназначено для работы с защищёнными ресурсами на компьютере пользователя. Возможности этого приложения совпадают с возможностями приложения Панель Secret Disk Agent, но оно имеет современный пользовательский интерфейс, предназначенный для работы на сенсорных экранах и планшетных компьютерах.

7.2 Особенности приложения

Приложение mSDA использует среду исполнения Microsoft WinRT и некоторые его свойства отличаются от традиционных приложений Windows. Описание этих отличий приведено ниже.

> *Предназначено для ОС Windows 8/8.1/10*

Приложение mSDA можно установить только в тех ОС, где имеется среда исполнения WinRT, а именно в Windows 8/8.1 и Windows 10. В ОС Windows 7 это приложение использовать нельзя.

7.2.1 Установка и удаление пользователем

Приложение mSDA не устанавливается сразу для всех пользователей компьютера, как это происходит с обычными приложениями Windows. Установка (и удаление) приложения происходит в учётной записи каждого пользователя отдельно.

Приложение нельзя удалить с помощью настройки "Программы и компоненты", это делается через контекстное меню плитки (значка) приложения на экране "Пуск".

Первая установка mSDA начинается автоматически после входа пользователя в свою учётную запись.

> *Удаление и переустановку mSDA пользователю нужно делать самому.*

7.2.2 Полноэкранный режим

Приложение mSDA в ОС Windows 8/8.1 по умолчанию запускается в полноэкранном (планшетном) режиме независимо от типа компьютера. Запустить его в обычном окне нельзя, так как такой режим не поддерживается ОС.

В ОС Windows 10 запуск в полноэкранном режиме происходит только на планшетных компьютерах и приложение mSDA может работать как в полноэкранном, так и в обычном режиме (пользователь сам выбирает режим экрана).

7.2.3 Администратор не может работать с Modern Secret Disk Agent

Только обычные пользователи могут использовать приложения для среды исполнения WinRT. Поэтому, пользователи с правами локального или сетевого администратора, не могут запустить mSDA: оно либо не запустится, либо будет выведено сообщение об ошибке. Таким пользователям следует использовать Панель Secret Disk Agent для управления защищёнными ресурсами.

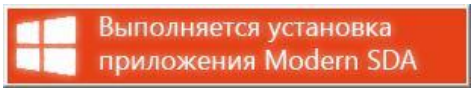
7.2.4 Установка из Магазина приложений

В настоящее время приложение mSDA **нельзя** установить из Магазина Приложений Microsoft, но эта возможность может появиться в будущем.

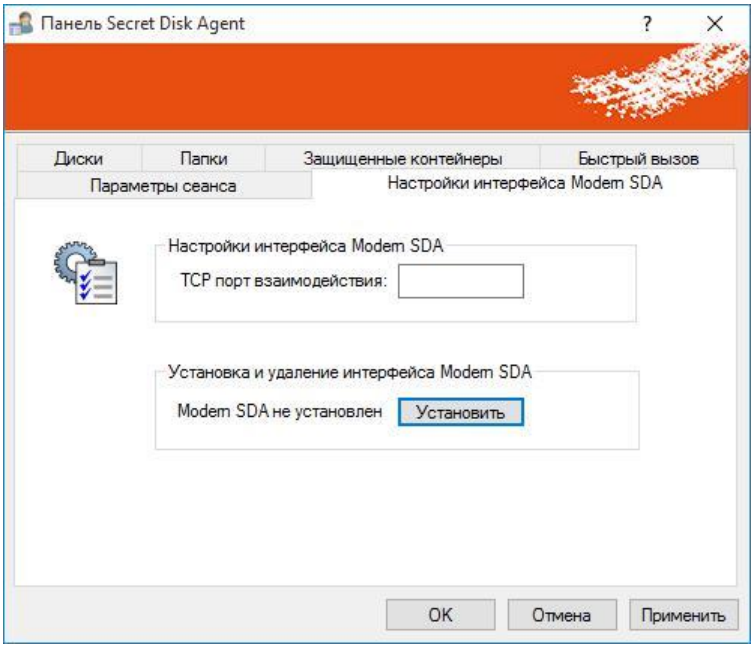
7.3 Использование приложения

7.3.1 Установка mSDA

После установки пакета Secret Disk Agent на компьютере, приложение mSDA будет устанавливаться автоматически у каждого пользователя сразу после его входа (логина) в систему. Установка будет сопровождаться уведомлением. После установки плитка приложения появится на экране Пуск.



Чтобы установить приложение вручную после удаления или при переустановки пакета SDA необходимо открыть Панель Secret Disk Agent и нажать кнопку *Установить* на вкладке "Настройки интерфейса Modern SDA".



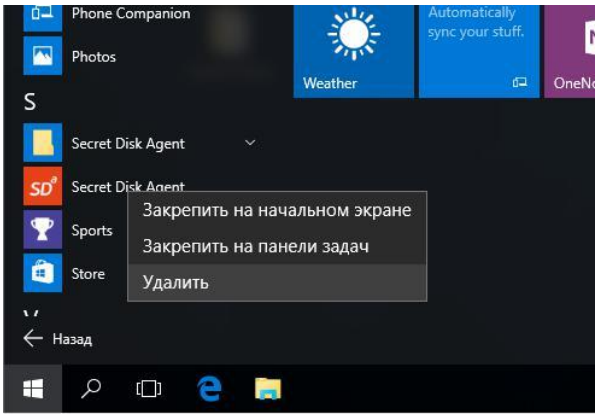
7.3.2 Удаление и переустановка mSDA

Приложение mSDA не удаляется с помощью настройки "Программы и компоненты" при удалении пакета SDA. Удалить mSDA должен сам пользователь и сделать это можно двумя способами:

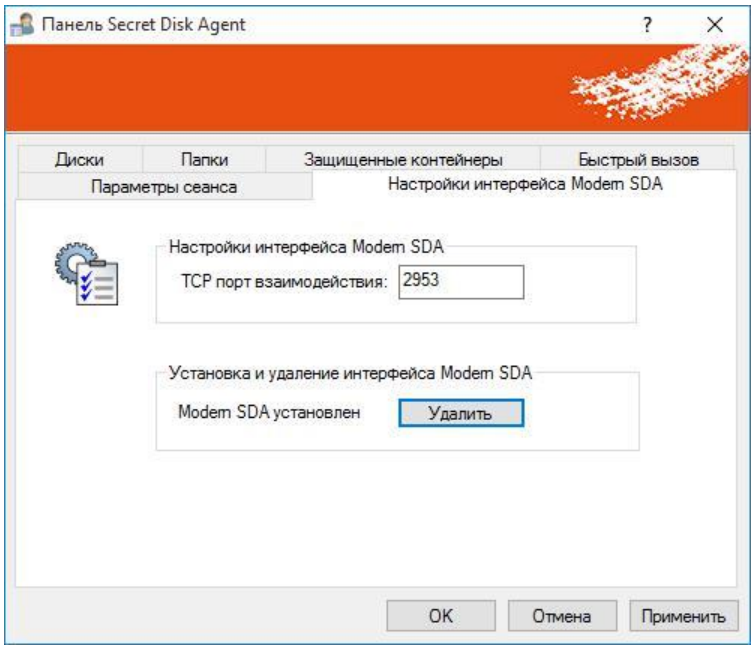
1. С помощью системного меню приложения на экране Пуск.
2. Из Панели Secret Disk Agent.

При переустановке (обновлении) пакета SDA, каждому пользователю нужно установить новую версию mSDA самостоятельно, предварительно удалив старую.

Для удаления mSDA с помощью с системного меню нужно открыть экран Пуск, вызвать меню приложения, нажав правой кнопки мыши на плитке SDA, и выбрать "Удалить".

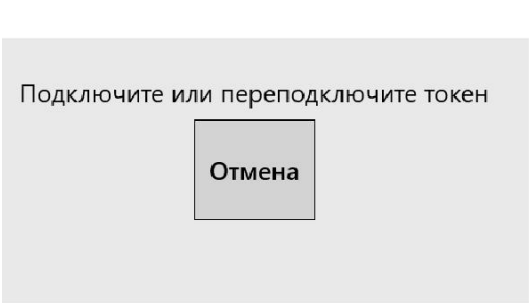


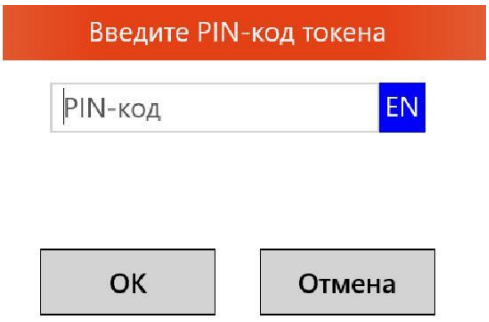
Удалить приложение mSDA из Панели Secret Disk Agent можно кнопкой "Удалить" на вкладке "Настройки интерфейса Modern SDA".



7.3.3 Подключение токена и начало работы

Запустить mSDA можно с помощью плитки на экране Пуск или кнопкой в окне запроса PIN-кода. При запуске приложение отобразит состояние защищённых ресурсов, если они уже подключены, либо выведет запрос на подключение токена. После подключения токена mSDA появится поле для ввода PIN- кода.



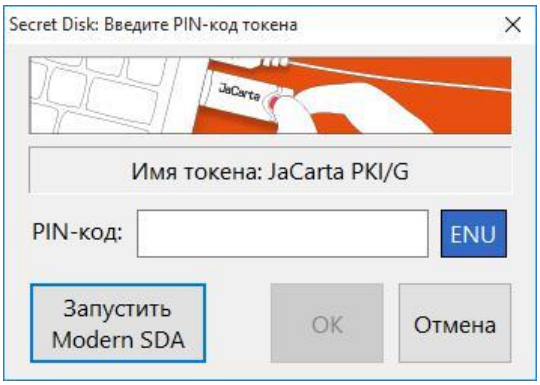


Внимание! Если автоматический старт сеанса SDA при подключении токена не разрешён настройками системы или если используемая модель токена не распознаётся автоматически

при подключении, то запрос PIN-кода не появится в mSDA. В этом случае нужно запустить вручную Secret Disk Agent.

7.3.4 Запуск mSDA из окна запроса PIN-кода

Приложение mSDA также можно запустить из окно запроса PIN-кода токена с помощью кнопки.



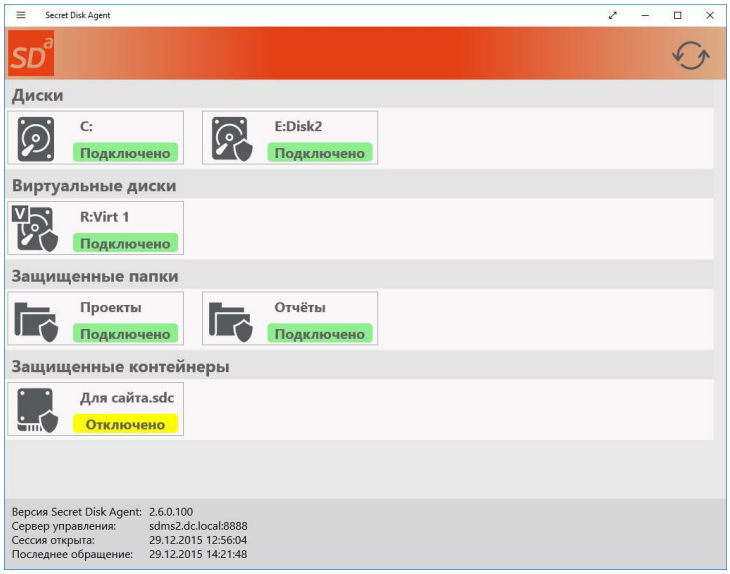
*Если приложение **mSDA** не запущено пользователем, то при подключении токена или при запуске традиционного приложения **Secret Disk Agent** появится окно запроса PIN-кода токена. Приложение **mSDA** в этом случае можно запустить кнопкой в этом окне, нажав её до ввода кода. Приложение mSDA запустится и запросит PIN-код.*

7.3.5 Окно mSDA

Приложение mSDA имеет одно окно, в котором отображается состояние самого приложения, дисков компьютера и всех других защищённых ресурсов.

В нижней панели выводится информация о самом приложении и о текущей сессии (сеансе) работы с управляющим сервером. Информация обновляется периодически с определённым интервалом (по умолчанию 1 минута). Для принудительного обновления можно использовать кнопку *Обновить*, расположенную в правом верхнем углу окна.

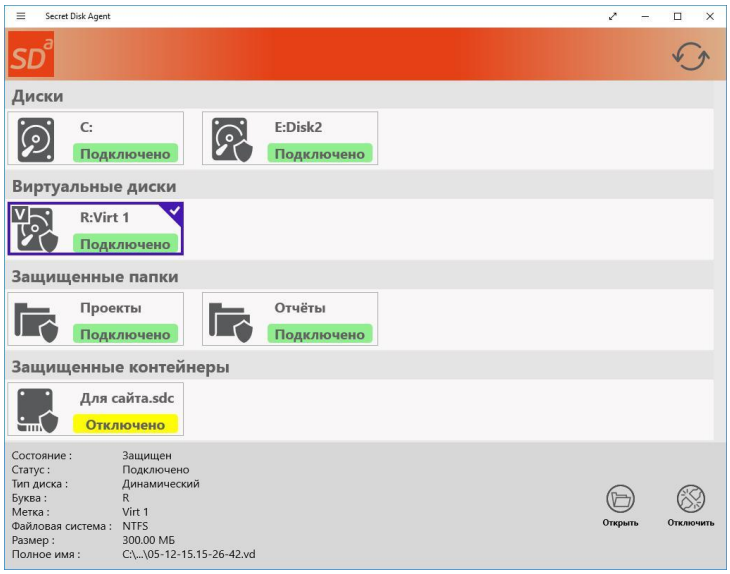
При выделении плитки какого-либо ресурса с помощью щелчка мыши или касанием сенсорного экрана в нижней панели выводится информация о выбранном ресурсе.



7.3.6 Управление защищёнными ресурсами

Каждая плитка защищённого ресурса в окне mSDA постоянно показывает основную информацию о нём: букву и метку диска или имя папки и состояние подключения. Выполнение фоновой операции отображается с помощью специального значка (часов), появляющегося поверх основного значка в плитке.

Для получения подробной информации о каком-либо ресурсе и выполнения действий с ним, его нужно выделить мышью или касанием сенсорного экрана.



С помощью mSDA можно выполнить такие же действия с защищёнными ресурсами, что и в приложении Панель Secret Disk Agent *Отключить*, *Подключить*, *Открыть*, *Изменить букву виртуального диска*. Эти действия подробно описаны в соответствующих разделах этого руководства.

7.3.7 Завершение работы mSDA

С помощью приложения mSDA **нельзя** завершить сеанс работы Secret Disk Agent. Это действие можно выполнить командой "*Выход*" в меню значка SDA.

Также сессия работы может завершатся автоматически при отключении токена или при выходе пользователя из своей учётной записи. Такое поведение настраивается системным Администратором.

При завершении сессии любым способом все защищённые ресурсы, кроме системного диска, отключаются.

8. 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.

8.1 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.

Приложение А

9. Контакты

9.1 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.

9.2 Техподдержка

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

Регистрация изменений

Версия	Изменения
1.0	Полное обновление документа.
2.0	Обновление шаблона

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