SECRET DISK®

Защита конфиденциальной информации

Линейка продуктов

Secret Disk

Aladdin®
SECURITY SOLUTIONS

Защита конфиденциальной информации на жестких дисках и съемных носителях

Продукты линейки Secret Disk предназначены для защиты конфиденциальной информации и персональных данных на жестких дисках и съемных носителях от несанкционированного доступа, копирования, повреждения, кражи или принудительного изъятия.

Для защиты информации при хранении используется метод «прозрачного» шифрования с помощью стойких алгоритмов. При чтении данных с диска происходит их расшифрование, при записи на диск — зашифрование. Таким образом, записанные на жестком диске данные всегда защищены, что делает доступ к ним невозможным для злоумышленника, даже при краже или изъятии как отдельного диска, так и всего компьютера.

Для получения доступа к зашифрованной информации необходимо провести процедуру двухфакторной аутентификации с помощью USB-ключа или смарт-карты eToken. Для пользователей, не прошедших процедуру аутентификации, скрывается сам факт наличия зашифрованной информации на компьютере.

В Secret Disk 4 реализована защита системного раздела, временных и рабочих файлов, которые хранят информацию о сеансах работы пользователя в различных прикладных программах, историю работы пользователя в сети Интернет (включая пароли доступа к различным сетевым ресурсам), историю переписки пользователя по электронной почте или по сети обмена мгновенными сообщениями (например: ICQ, Microsoft IM) и тому подобную информацию. В сочетании с двухфакторной аутентификацией пользователя до загрузки ОС, защита системного раздела становится надежным барьером, препятствием не только несанкционированному доступу к персональной и корпоративной информации, но и самой загрузке компьютера.

Защита может быть обеспечена для логических дисков, отдельных жестких дисков, дисковых массивов (SAN, программных и аппаратных RAID-массивов), а также для съемных дисков (дискеты, flash-диски, CD, DVD, карты памяти и т.п.).

В каких случаях необходимы продукты линейки Secret Disk?

- Конфиденциальная информация обрабатывается и хранится на ноутбуке, и есть риск его кражи или несанкционированного использования посторонними.
- Необходимо исключить возможность загрузки ОС неавторизованными пользователями.
- За компьютером работает несколько пользователей, и есть риск доступа, случайной или преднамеренной порчи, искажения информации.
- Конфиденциальная информация переносится на съемных носителях.
- Работник IT-отдела, обладая административными привилегиями, необходимыми для обслуживания компьютеров организации, может получить доступ к конфиденциальной информации на жестком диске компьютера.
- Необходимо защитить временные и системные файлы, которые хранят информацию о сеансах работы пользователя в различных прикладных программах, историю работы пользователя в сети Интернет, включая пароли доступа к различным сетевым ресурсам, историю переписки пользователя по электронной почте или в системах обмена мгновенными сообщениями.
- Конфиденциальная информация находится на жестком диске компьютера или сервера, который передается для технического обслуживания .
- Необходимо обеспечить доступ к конфиденциальной информации лишь одному или нескольким сотрудникам и не допустить ее попадания в чужие руки, а также скрыть сам факт наличия на компьютере определенных программ и данных.
- Необходимо обеспечить экстренное прекращение доступа к данным или уничтожение данных на сервере в случае возникновения нештатных ситуаций (проникновение в офис злоумышленников).

SECRET DISK®

Линейка Secret Disk

- **Secret Disk 4** – загрузка компьютера только с ключом eToken, защита системного раздела, шифрование разделов жесткого диска и съемных носителей, работа с файлами-контейнерами.
- **Secret Disk 4 Workgroup Edition** – специальная редакция Secret Disk, позволяющаяя организовать работу в сети с защищенными дисками для небольших групп пользователей.
- **Secret Disk Server NG** – шифрование данных на файловых серверах и серверах приложений.
- **Сертифицированные версии** Secret Disk и Secret Disk Server NG– для коммерческих и государственных организаций для создания АС по классу 1Г и ИСПД 2.

Особенности продуктов линейки Secret Disk

Шифрование данных

Продукты позволяют шифровать данные, расположенные на основных и дополнительных разделах жесткого диска, на томах динамических дисков, на любых съемных носителях (Flash-диски, магнитооптика, карты памяти SD, MS и др.), а также создавать зашифрованные виртуальные диски (файлы-контейнеры), подключаемые в виде логических дисков.

Защита операционной системы

Secret Disk 4 позволяет реализовать двухфакторную аутентификацию пользователя до загрузки операционной системы. Вместе с функцией защиты системного раздела, продукт позволяет исключить несанкционированное использование информационно-вычислительных ресурсов компании.

Надежная криптографическая защита

В продуктах линейки Secret Disk для осуществления криптографических преобразований могут применяться:

- криптопровайдер из состава Microsoft Windows (алгоритмы AES, Triple DES, RC2);
- криптопровайдер КриптоПро CSP, Infotecs CSP или Signal-COM CSP (алгоритм ГОСТ 28147-89) с длиной ключа 256 бит;
- пакет лгоритмов шифрования Secret Disk Crypto Pack (алгоритмы AES с длиной ключа 128 и 256 бит, Twofish с длиной ключа 256 бит).

Надежная двухфакторная аутентификация

Для аутентификации в Secret Disk применяются смарт-карты и USB-ключи eToken, использующиеся как активные криптографические устройства, что исключает возможность неавторизованного копирования ключа.

Интеграция с инфраструктурой открытых ключей

Продукты используют сертификаты X.509 и связанные с ними криптографические ключи для защиты ключей шифрования дисков и аутентификации.

Защита от сбоев компьютера в процессе шифрования

Процессы шифрования можно останавливать и возобновлять. Более того, в случае сбоев операционной системы или перебоев электропитания данные остаются неповрежденными. Предусмотрена операция перешифрования защищенных дисков со сменой ключа и/или алгоритма шифрования, при которой не требуется предварительного расшифрования дисков.

Технология многопоточного шифрования

Применение новаторской технологии многопоточного шифрования позволяет максимально задействовать вычислительные ресурсы современных многопроцессорных систем, систем с многоядерными процессорами и технологией Hyper-Threading, а также повышает эффективность работы системы на однопроцессорных машинах.

Благодаря этой технологии в работе прикладных систем не наблюдается заметного снижения производительности при переходе к использованию шифрования данных.

Обслуживание защищенных дисков

Форматирование, проверка дисков на наличие ошибок и резервное копирование данных может производиться стандартными средствами операционной системы. Защищенные диски могут иметь файловую систему NTFS, FAT32 или FAT16.

Шифрование данных и контроль начальной загрузки - Secret Disk 4

Назначение

Secret Disk 4 позволяет защитить системный раздел жесткого диска и создавать на персональном компьютере скрытые зашифрованные ресурсы – зашифрованные диски, предназначенные для безопасного хранения конфиденциальной информации.

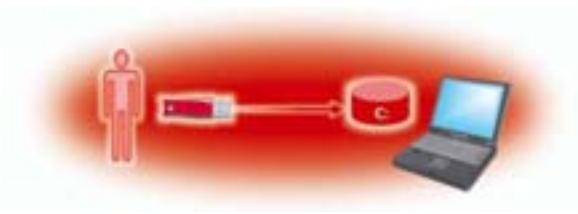
Загрузить ОС и получить доступ к зашифрованной информации может только ее владелец либо авторизованные им пользователи, имеющие электронный ключ eToken и знающие его PIN-код.

В многопользовательском варианте работы Secret Disk 4 каждый пользователь может оперировать только со своим зашифрованным диском. Для других пользователей этот зашифрованный диск не виден и недоступен. Более того, они могут даже и не догадываться о его наличии. В отключенном состоянии зашифрованный диск выглядит как неразмеченная область жесткого диска или файл, содержащий «мусор».

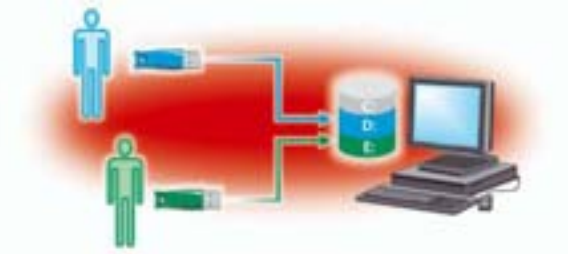
Зашифрованная информация не может быть просмотрена, скопирована, уничтожена или повреждена другими пользователями, любопытными коллегами, администраторами или хакерами, подключившимися к компьютеру по сети. Она также не может быть использована посторонними при ремонте или краже компьютера, либо при утере съемного зашифрованного носителя информации.

Возможности использования

Защита персональной информации



Защита информации на компьютере с несколькими пользователями

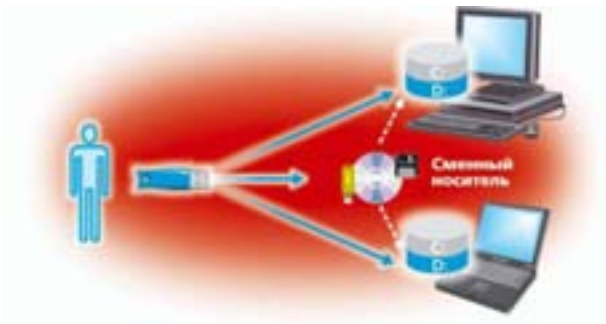


Доступ к зашифрованным дискам можно получить только имея eToken пользователя и зная его PIN-код. На одном компьютере могут работать несколько пользователей, каждый со своим независимым набором зашифрованных дисков.

Защита данных на компьютерах в пределах организации

Администратор управляет Secret Disk (создание зашифрованных дисков, смена ключей шифрования, резервное копирование данных) на компьютерах пользователей, а также выполняет восстановление доступа к данным в случае потери или порчи пользователями ключей eToken.

Безопасные транспортировка и обмен данными

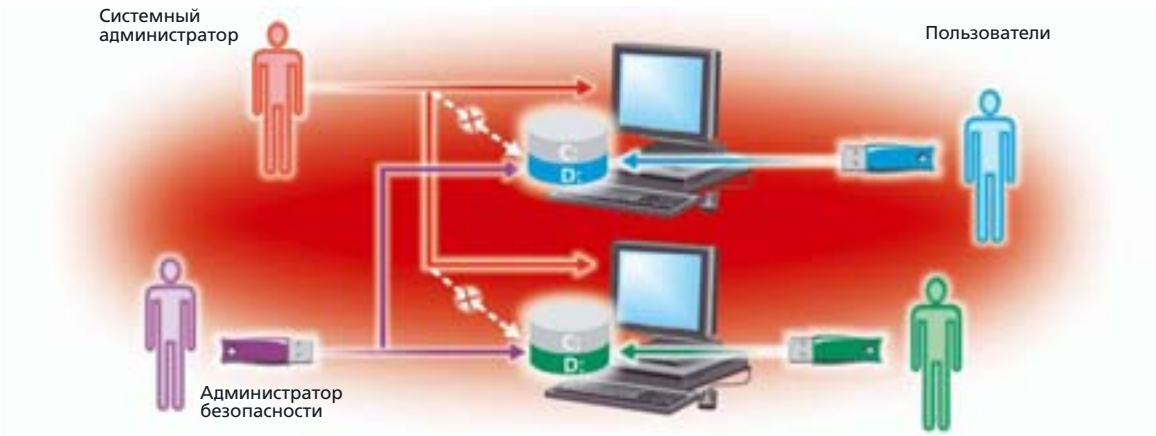


Secret Disk можно установить на нескольких компьютерах, организовав безопасный перенос информации между ними в зашифрованном виде на съемных носителях.

Безопасное резервное копирование

Данные для резервного копирования сохраняются на зашифрованных виртульных дисках, которые затем записываются на съемные носители (например, на компакт-диски).

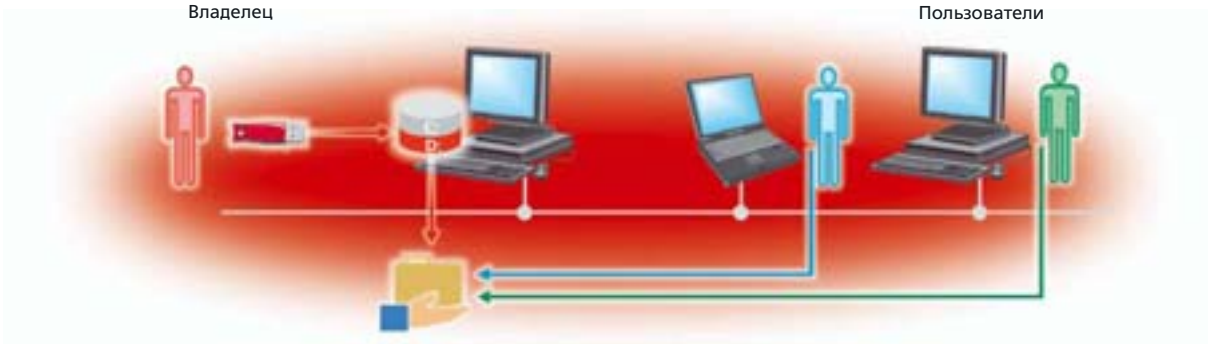
Разграничение полномочий и предоставление доступа к данным



Secret Disk поддерживает разграничение функций системного администратора и администратора безопасности.
Системный администратор не обладает привилегиями для доступа к данным на зашифрованных дисках (даже по сети), выполняя только сервисные операции.
Администратор безопасности управляет доступом к данным на зашифрованных дисках для зарегистрированных пользователей.

Для рабочих групп - Secret Disk 4 Workgroup Edition

Специальная редакция Secret Disk 4 Workgroup Edition создает на персональном компьютере защищенные диски, предназначенные для организации безопасной коллективной работы с конфиденциальной информацией в сети для небольших групп пользователей (не более 10 одновременных подключений по сети). Владелец данных, подключая и отключая защищенный диск, может управлять доступностью общих ресурсов для других компьютеров.



Общие ресурсы создаются на защищенных дисках средствами операционной системы. При подключении защищенного диска он не только появляется в системе, но и происходит автоматическое восстановление всех общих ресурсов.

Для серверов - Secret Disk Server NG

Назначение

Secret Disk Server NG - система защиты корпоративных баз и конфиденциальных данных на серверах от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия. Система надежно защищает данные и скрывает сам факт их наличия на сервере.

Secret Disk Server NG может быть использован как самостоятельное решение, а также как элемент комплексной системы защиты корпоративной информации.

Secret Disk Server NG позволяет полностью запретить сетевой доступ к данным, хранящимся и обрабатывающимся на серверах приложений, например файлам баз данных, почтовым хранилищам и др. Это позволяет исключить риск несанкционированного копирования данных пользователями, имеющими административные полномочия в системе.

Защита информации осуществляется методом «прозрачного» шифрования с помощью стойких алгоритмов шифрования. Защитить можно отдельные жесткие диски сервера, любые дисковые массивы (SAN, программные и аппаратные RAID-массивы), а также съемные диски (например, подключаемые к серверу для резервного копирования). При чтении данных с диска происходит их расшифрование, при записи на диск — зашифрование. Находящиеся на диске данные всегда зашифрованы, что делает доступ к ним невозможным для злоумышленника даже если он получит доступ как к отдельному диску, так и к самому серверу.

Возможности

Экстренное прекращение доступа к данным по сигналу «тревога». Сигнал «тревога» подается для экстренного предотвращения доступа к защищаемым данным, например, в случае появления злоумышленника. Сигнал может быть подан как внешним устройством (например, «красной кнопкой», радио-брелком, охранной сигнализацией или по GSM-каналу), так и с клавиатуры компьютера или мышью. Реакцию на сигнал «тревога» можно настроить как для сервера, так и для каждого зашифрованного диска в отдельности.

Групповое администрирование: Secret Disk Server NG допускает неограниченное количество администраторов.

Удаленное администрирование Secret Disk Server NG выполняется через консоль управления Microsoft (MMC) или удаленный рабочий стол (RDP).

Индивидуальные сценарии для каждого зашифрованного диска. Эти сценарии могут выполняться перед подключением диска, после подключения, перед отключением, после отключения. Например, после подключения зашифрованного диска с файлами базы данных Microsoft SQL с помощью сценария может быть запущена сама СУБД. В качестве сценария может применяться как скрипт (js, vbs, cmd и т. д.), так и любая утилита.

Надежная двухфакторная аутентификация администраторов Secret Disk Server NG с использованием цифровых сертификатов X.509: для выполнения административных задач надо иметь персональный цифровой сертификат X.509, записанный в защищенную память ключа eToken, и знать его PIN-код.

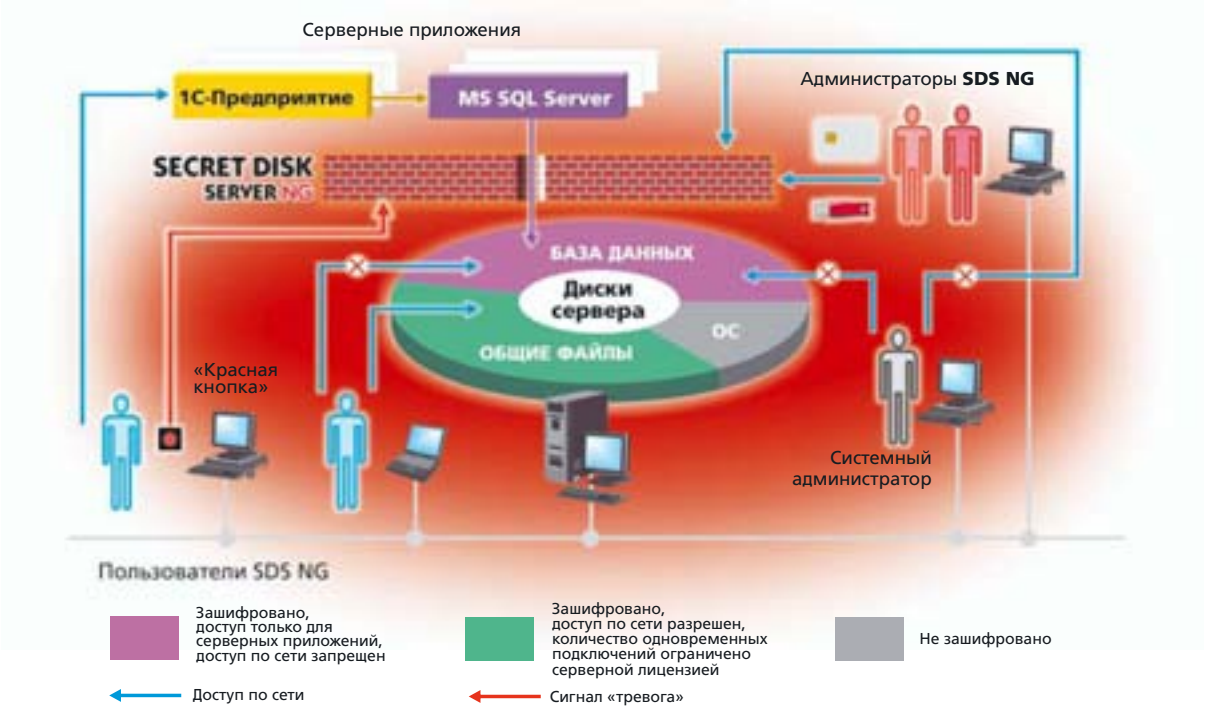
Эксклюзивная особенность

Возможность резервного копирования зашифрованных разделов и открытых в эксклюзивном режиме файлов **без остановки работающих сервисов** и приложений (например, MS Exchange, SQL Server).

Резервное копирование может производиться в фоновом режиме с помощью встроенной в ОС утилиты NTBackup или продуктами третьих фирм.

Возможности использования

Пример защиты корпоративных данных на сервере

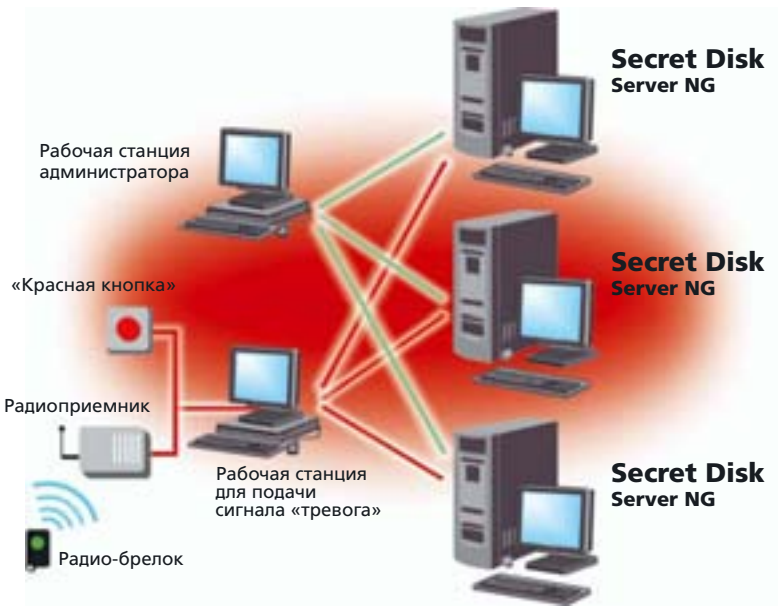


Secret Disk Server NG поддерживает две модели защиты ресурсов – модель файл-сервера с возможностью создания разделяемых сетевых ресурсов и модель сервера приложений с запретом прямого доступа по сети. Обе модели можно использовать на одном сервере (при наличии соответствующих лицензий в памяти eToken сервера).

Интеграция в инфраструктуру обеспечения безопасности

Различные компоненты комплекса Secret Disk Server NG можно размещать в различных комбинациях в пределах локальной сети, организуя защищенную и удобно управляемую инфраструктуру.

Удаленное управление



Административные интерфейсы и обеспечение подачи сигнала «тревога» могут быть настроены как для работы с отдельным сервером, так и с группой серверов.

Сертифицированные версии Secret Disk

Назначение

Сертифицированные версии Secret Disk предназначены для защиты конфиденциальной информации и персональных данных в системах под управлением Microsoft Windows. Данные версии предназначены для государственных предприятий и организаций, предъявляющих требования к обязательному использованию сертифицированных средств защиты информации и аттестации автоматизированных систем на соответствие требованиям по защите информации (до класса защищенности **1Г** включительно).

Особенности

Secret Disk NG Personal Edition, Secret Disk 4 и Secret Disk Server NG имеют сертификаты ФСТЭК России. Данные сертификаты подтверждают, что продукты Secret Disk могут использоваться при создании автоматизированных систем до класса защищенности 1Г включительно, а также при создании информационных систем обработки персональных данных (ИСПДн) до 2 класса включительно.

Демонстрационные версии продуктов

С Web-сайта Aladdin (www.aladdin.ru) можно бесплатно загрузить полнофункциональные демонстрационные версии продуктов Secret Disk.
Для работы с демонстрационной версией достаточно иметь любой USB-ключ или смарт-карту eToken.
Основные отличия демонстрационных версий от коммерческих – ограниченный период работы 30 дней и использование нестойких ключей шифрования дисков.

eToken – персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП.

eToken выпускается в форм-факторе USB-ключа или смарт-карты.

Модель eToken NG-OTP имеет встроенный генератор одноразовых паролей.

Модель eToken NG-FLASH имеет встроенную Flash-память объемом до 4ГБ.

Продукты линейки Secret Disk могут использоваться с любой моделью eToken.

Выбор нужного продукта

Продукты линейки Secret Disk / Задача	Secret Disk 4 Lite	Secret Disk 4	Сертифицированная версия Secret Disk NG Personal Edition	Secret Disk Server NG
Защитить данные на персональном компьютере	✓	✓	✓	
Ограничить возможность загрузки ОС, защитить системный раздел, файл подкачки, временные файлы, файлы спящего режима		✓		
Защитить данные для коллективной работы на одном компьютере		✓	✓	
Защитить файловый сервер				✓
Защитить сервер приложений (почтовый сервер, сервер СУБД, терминальный сервер)				✓
Защитить данные для коллективной работы по сети				✓
Получить сертифицированное решение		✓	✓	✓
Обеспечить интеграцию с российскими СКЗИ (КриптоПро CSP, Signal-COM CSP, Infotecs CSP)		✓	✓	✓

Сервис и обучение

По желанию заказчика возможен выезд технического специалиста для установки продуктов Secret Disk и обучения администратора. Работы на территории заказчика выполняются силами рекомендованных партнеров компании Aladdin.

Компания Aladdin разработала авторизованный учебный курс по защите конфиденциальной информации с помощью продуктов Secret Disk, предназначенный для сертификации технических специалистов.

Aladdin также предлагает серию мастер-классов для обучения сотрудников компании заказчика работе с продуктами линейки Secret Disk.

Технические характеристики

Secret Disk 4	
Поддерживаемые платформы	Microsoft Windows 2000 Professional, Windows XP (32 и 64 разрядные версии), Windows Vista (32 и 64 разрядные версии), Windows 7 (32 и 64 разрядные версии)
Типы поддерживаемых дисков	Разделы базовых дисков (Basic Disk Partition) Тома динамических дисков (Dynamic Disk Volume) Съемные диски (USB-drive, магнитооптика и др.) Виртуальные диски (файлы-контейнеры)
Типы файловых систем	NTFS, FAT, FAT 32
Размер дисков	От 1МБ до 2ТБ
Типы USB-ключей и смарт-карт	eToken PRO (все модели), eToken NG-OTP (все модели), eToken NG-FLASH (все модели)
Подключаемые внешние алгоритмы шифрования	AES (128 и 256 бит), Twofish (256 бит), TripleDES (168 бит), RC2 (128 бит), ГОСТ 28147-89 (256 бит)
Аутентификация пользователя	Двухфакторная (eToken + PIN-код)
Гарантийное обслуживание*	12 месяцев
Secret Disk Server NG	
Поддерживаемые платформы	Windows 2003 Server (32 и 64 разрядные версии), Windows 2008 Server (32 и 64 разрядные версии), Microsoft Windows 2000, Windows XP (32 и 64 разрядные версии), Windows Vista (32 и 64 разрядные версии)
Типы поддерживаемых дисков	Разделы базовых дисков (Basic Disk Partition) Тома динамических дисков (Dynamic Disk Volume) Съемные диски (USB-drive, магнитооптика и др.) Виртуальные диски (файлы-контейнеры) Внешние хранилища (SAN)
Типы файловых систем	NTFS, FAT, FAT 32
Размер защищаемых дисков	До 64ТБ (для NTFS), до 8ТБ (для FAT32), до 4ГБ (для FAT16)
Типы USB-ключей и смарт-карт	eToken PRO (все модели), eToken NG-OTP (все модели), eToken NG-FLASH (все модели
Подключаемые внешние алгоритмы шифрования	AES (128 и 256 бит), Twofish (256 бит), TripleDES (168 бит), RC2 (128 бит), ГОСТ 28147-89 (256 бит)
Возможность подключения других алгоритмов шифрования	Есть, через внешние крипто-библиотеки
Аутентификация администраторов	Двухфакторная (eToken + PIN-код)
Возможность подачи сигнала «тревога»	С помощью «Красной кнопки», радиокнопки, GSM-реле С помощью утилиты в системном трее или командной строки Возможна интеграция с охранными сигнализациями и системами СКУД
Гарантийное обслуживание*	12 месяцев
Сертифицированная версия Secret Disk NG Personal Edition	
Поддерживаемые платформы	Microsoft Windows 2000, Windows XP
Типы поддерживаемых дисков	Разделы базовых дисков (Basic Disk Partition) Тома динамических дисков (Dynamic Disk Volume) Съемные диски (USB-drive, магнитооптика и др.) Виртуальные диски (файлы-контейнеры)
Типы файловых систем	NTFS, FAT, FAT 32
Размер виртуальных дисков	От 1МБ до 2ТБ
Типы USB-ключей и смарт-карт	Сертифицированные модели eToken PRO, eToken NG-OTP, eToken NG-FLASH
Подключаемые внешние алгоритмы	ГОСТ 28147-89 (256 бит)
Аутентификация пользователя	Двухфакторная (eToken + PIN-код)
Гарантийное обслуживание*	12 месяцев

* Гарантийное обслуживание включает техническую поддержку

О компании Aladdin

Aladdin – ведущий российский разработчик и поставщик средств аутентификации, продуктов и решений для обеспечения безопасного доступа к корпоративным ресурсам и защиты информации.

В последние годы компания активно развивает свой бизнес в направлении услуг для крупных корпоративных клиентов, что позволило ей войти в ТОП-100 российского IT-рынка (рейтинг CNews) и в число крупнейших IT-компаний РФ (рейтинг РА «Эксперт»). Продукты Aladdin и комплексные решения на их основе востребованы в различных секторах отечественной экономики, в том числе в банковском, государственно-административном, а так же в ТЭК и ряде других.

Позиции лидера в области защиты программного обеспечения от несанкционированного использования и эксперта в области решения проблем «ААА» (Аутентификация, Авторизация и Аудит действий в сети) подкреплены 13-летним опытом работы на российском рынке, а также прочными партнерскими отношениями с ведущими российскими системными интеграторами и мировыми IT-вендорами: Microsoft, Cisco Systems, Oracle, Citrix, Check Point, IBM и др.

Соблюдение ключевых требований российского законодательства в сочетании с инновационным подходом позволили компании получить целый ряд престижных статусов и наград. Так, по решению Аппарата Совета Безопасности РФ и Комитета Государственной Думы по безопасности компании Aladdin неоднократно присваивался титул «Компании года». В 2005 году компания Aladdin стала лауреатом Национальной Премии в области Безопасности ЗУБР в номинации «Лучшее техническое средство для защиты информации» (eToken PRO). В сентябре 2007 года Secret Disk 4 занял первое место в открытом конкурсе «Продукт года» в номинации «Защита информации».

SECRET DISK

Отзывы о Secret Disk

Роберт Фариш,
IDC
Региональный менеджер
по России, Украине,
Центральной Азии

«Я попробовал Secret Disk в качестве средства защиты ноутбука. Поработав с ним несколько недель, я буквально пристрастился к нему.

Он не вызывает никаких проблем при установке на компьютер и обеспечивает настоящее спокойствие духа в случае, если вдруг ноутбук будет потерян или его украдут.

Сейчас я использую Secret Disk для защиты как конфиденциальных данных, так и их резервных копий».

Владимир Митин
Научный редактор
PC Week

«Большое количество пользователей, в первую очередь руководители и топ-менеджеры, в последние несколько лет «пересели« на ноутбуки и сразу же попали в так называемую группу риска. Почему? Да потому, что их компьютеры слишком много знают и риск того, что ноутбук будет потерян, украден и доступ к содержащейся в нем информации получит кто-то посторонний, слишком велик. А утечка критически важной бизнес-информации может обернуться для предприятия большими бедами.

В июне 2007 года российская компания Aladdin Software Security R.D. выпустила четвертую версию оригинальной системы защиты конфиденциальных данных Secret Disk, предназначенной для шифрования информации на разных видах встроенных и съемных носителей.

Разработчики Secret Disk позаботились о надежности системы шифрования. Благодаря журналированию всех операций записи/чтения информации на зашифрованные диски Secret Disk устойчив к сбоям, в том числе к внезапным отключениям электропитания.

Все операции шифрования Secret Disk 4 осуществляет «на лету», поэтому у пользователя не возникает проблем при работе за персональным компьютером с установленной системой защиты.».

«Теперь Secret Disk шифрует все разделы жестких дисков», PC Week, №3 (спецвыпуск), 22 сентября 2007 г.

Александр Рябцев
Обозреватель
PC Magazine

«К нам на тестирование поступил набор Secret Disk 4 с электронным USB-ключом eToken PRO с объемом памяти 32 Кбайт. Ключи имеют самостоятельное программное обеспечение eToken Run Time Environment. Установка этого ПО, как и собственно программы Secret Disk, проходит быстро и не вызывает сложностей; все же мы рекомендуем предварительно ознакомиться с руководством (в печатном или электронном виде), чтобы разобраться с системой понятий и терминологией. Интерфейс Secret Disk 4 не перегружен и снабжен достаточно подробной справочной системой».

«Секретный диск» Аладдина», PC Magazine, Russian Edition, №1 (199), январь 2008 г.

ID: 02776-0609

Тел.: (495) 223-0001
E-mail: aladdin@aladdin.ru
Web: www.aladdin.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (продлены до 18.02.13)
Лицензии ФСБ России № 2683Р от 02.09.05, №№ 4205П, 4206Х, 4207Р от 22.06.07 и № 4898П от 14.12.07
Microsoft Certified Partner, IBM Business Partner, Oracle Business Partner

Microsoft CERTIFIED Partner