SECRET DISK®

New Generation

Защита персональных и корпоративных данных

Линейка продуктов

Secret Disk NG

Aladdin®

SECURITY SOLUTIONS

Защита конфиденциальной информации на жёстких дисках и сменных носителях

Продукты линейки Secret Disk NG предназначены для защиты конфиденциальной информации на жёстких дисках и съёмных 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 жёстком диске данные всегда зашифрованы, что делает доступ к ним невозможным для злоумышленника, даже в случае кражи или изъятия как отдельного диска, так и всего компьютера.

Для получения доступа к защищённой информации используется двухфакторная аутентификация с помощью аппаратного средства аутентификации – USB-ключа или смарт-карты eToken. Для лиц, не прошедших процедуру аутентификации, скрывается сам факт наличия защищаемой информации на компьютере.

Защита может быть обеспечена для логических дисков, отдельных жестких дисков, дисковых массивов (внешних и внутренних, программных и аппаратных RAID-массивов), а также для съёмных дисков (дискеты, flash-диски).

В каких случаях может быть необходим продукт из линейки Secret Disk NG?

- ✓ Конфиденциальная информация обрабатывается и хранится на ноутбуке, и есть риск его кражи или несанкционированного использования посторонними.
- ✓ За компьютером работает несколько пользователей, и есть риск доступа, случайной или преднамеренной порчи, искажения информации.
- ✓ Конфиденциальная информация переносится на съемных носителях, и есть риск их утери или кражи.
- ✓ Работник IT-отдела, обладая административными привилегиями, необходимыми для обслуживания компьютеров организации, может получить доступ к конфиденциальной информации на жёстком диске компьютера.
- ✓ Конфиденциальная информация находится на жёстком диске компьютера или сервера, который передаётся для технического обслуживания в IT-отдел или внешнюю организацию.
- ✓ Необходимо обеспечить доступ к конфиденциальной информации лишь одному или нескольким сотрудникам и не допустить её попадания в чужие руки, а также скрыть сам факт наличия определённых программ и данных.
- ✓ Необходимо обеспечить экстренное прекращение доступа к данным или уничтожение данных на сервере в случае возникновения нештатных ситуаций (проникновение в офис злоумышленников).

Линейка Secret Disk NG:

- Персональная редакция - Secret Disk NG Personal Edition
- Редакция для рабочих групп - Secret Disk NG Workgroup Edition
- Серверная версия - Secret Disk Server NG
- Сертифицированная версия - Secret Disk NG

Особенности линейки Secret Disk NG

Шифрование данных

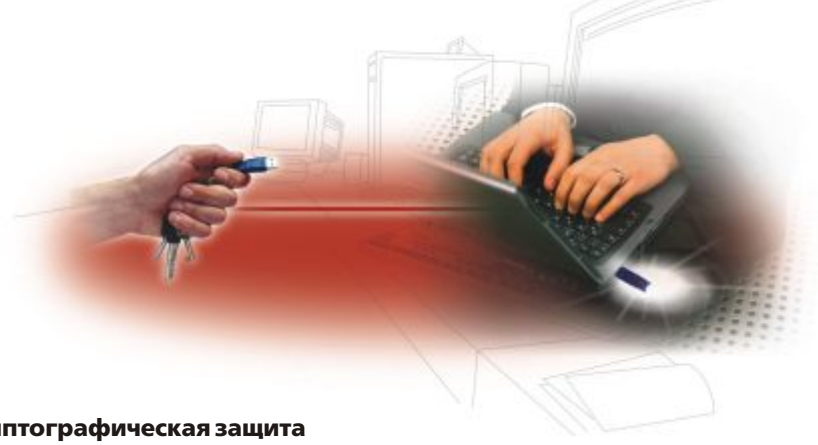
Продукты позволяют шифровать данные, расположенные на основных разделах и логических дисках, на дополнительных разделах базовых жестких дисков, на томах динамических дисков, на съёмных дисках (Flash-диски, ZIP, магнитооптика и др.).

Технология многопоточного шифрования

Применение новаторской технологии многопоточного шифрования позволяет максимально задействовать вычислительные ресурсы современных многопроцессорных систем, систем с многоядерными процессорами и технологией Hyper-Treading, а также повышает эффективность работы системы на однопроцессорных машинах. Благодаря этому в работе прикладных систем не наблюдается заметного снижения производительности при переходе к использованию шифрования данных.

Надёжная двухфакторная аутентификация

Для доступа к зашифрованным данным в продуктах линейки применяются смарт-карты и USB-ключи eToken, использующиеся как активные криптографические устройства. Это исключает возможность изготовления дубликатов и несанкционированного доступа к данным.



Надёжная криптографическая защита

Продукты линейки Secret Disk NG для осуществления криптографических преобразований могут применять:

- криптографический драйвер из состава Microsoft Windows (алгоритм Triple DES);
- криптопровайдер КриптоПро CSP или Signal-COM CSP (сертифицированная реализация алгоритма ГОСТ 28147-89);
- пакет дополнительных алгоритмов шифрования Secret Disk NG Crypto Pack (алгоритмы AES с длиной ключа 128 и 256 бит, Twofish с длиной ключа 256 бит).

Интеграция с инфраструктурой открытых ключей

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

Защита от сбоев компьютера в процессе шифрования

Процессы шифрования можно останавливать и возобновлять. Предусмотрена операция перешифрования защищённых дисков со сменой ключа и/или алгоритма шифрования.

Обслуживание защищенных дисков

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

Защита персональных данных - Secret Disk NG Personal Edition

Назначение

Secret Disk NG создает на персональном компьютере скрытые зашифрованные ресурсы – **защищённые диски**, предназначенные для безопасного хранения конфиденциальной информации.

Доступ к защищённой информации может получить только ее владелец либо авторизованные им доверенные лица, имеющие электронный ключ eToken и знающие PIN-код.

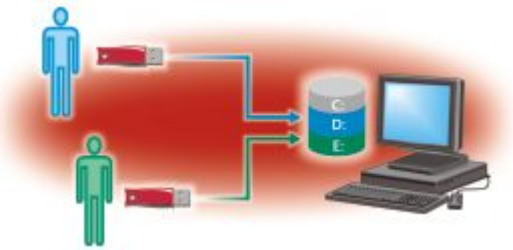
Для других пользователей этот защищённый ресурс не виден и недоступен. Более того, они могут даже и не догадываться о его наличии. В отключенном состоянии защищённый диск выглядит как неразмеченная область жёсткого диска или файл, содержащий "мусор".

Защищённая 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 съёмного зашифрованного диска.

Возможности использования

Защита персональной информации

Защита персональной информации на компьютере с несколькими пользователями

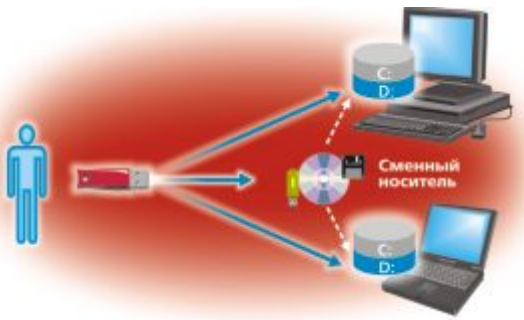


Доступ к защищённым дискам можно получить только при наличии eToken пользователя. На одном компьютере могут работать несколько пользователей, каждый со своим независимым набором защищённых дисков.

Защита данных на компьютерах в пределах организации

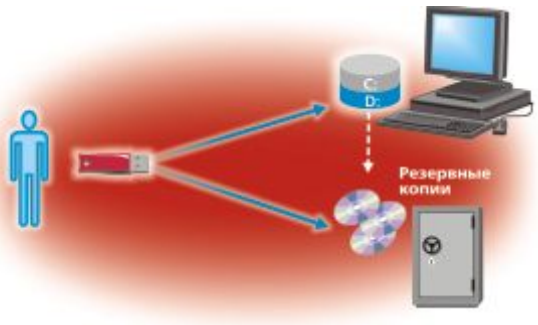
Администратор выполняет централизованное администрирование Secret Disk NG (создание и удаление защищённых дисков, резервное копирование данных) на компьютерах пользователей, а также восстановление доступа к данным в случае потери пользователями ключей.

Безопасные транспортировка и обмен данными



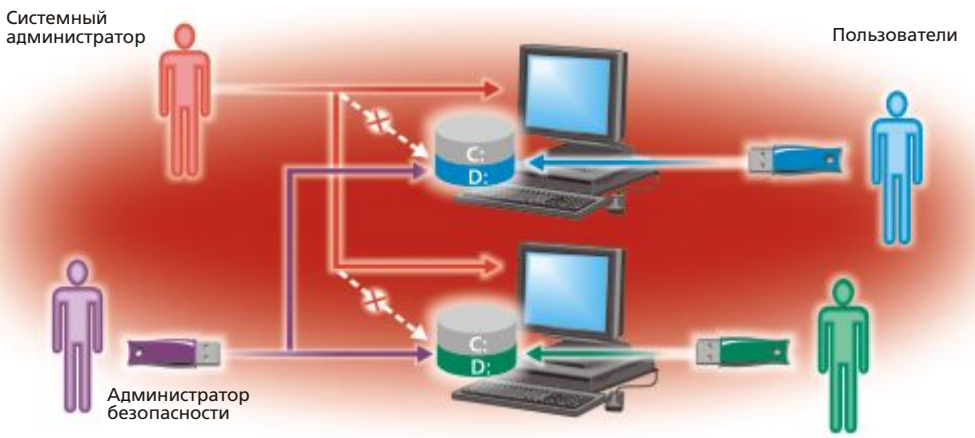
Secret Disk NG можно установить на нескольких компьютерах, организовав безопасный перенос информации между ними в зашифрованном виде на съёмных носителях.

Безопасное резервное копирование



Данные для резервного копирования сохраняются на защищённых дисках, которые затем записываются на съёмные носители (например, на компакт-диски).

Разграничение полномочий и предоставление доступа к данным

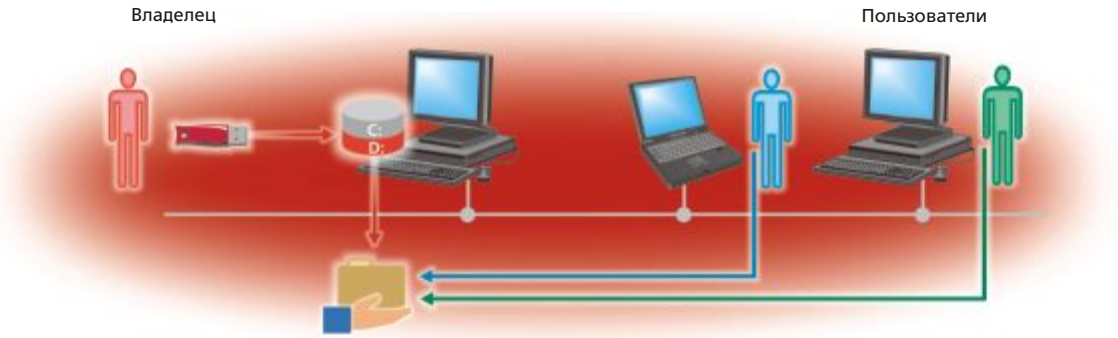


Secret Disk NG поддерживает разграничение функций системного администратора и администратора безопасности.
Системный администратор не обладает привилегиями для доступа к данным на защищённых дисках (даже по сети), выполняя только сервисные операции.
Администратор безопасности комплекса управляет доступом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

Защита данных для рабочих групп - Secret Disk NG Workgroup Edition

Secret Disk NG Workgroup Edition создает на персональном компьютере защищённые диски, предназначенные для организации безопасной коллективной работы с конфиденциальной информацией для небольших групп пользователей (не более 10 одновременных подключений по сети).

Данные для коллективной работы могут быть размещены на защищённых дисках одного из компьютеров в пределах локальной сети. Владелец данных, подключая и отключая защищённый диск, может управлять доступностью общих ресурсов для других компьютеров.



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

Защита данных на серверах - 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 не только надежно защищает данные, но 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 базам данных, почтовым хранилищам и др. Это позволяет исключить риск несанкционированного копирования данных пользователями, имеющими административные полномочия в системе.

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 или охранной сигнализацией), так и с клавиатуры компьютера или мышью. Реакция на сигнал «тревога» определяется для сервера в целом и для каждого защищённого диска в отдельности.

Групповое администрирование: на сервере может быть зарегистрировано неограниченное количество администраторов Secret Disk Server NG.

Удалённое администрирование Secret Disk Server NG выполняется через консоль управления Microsoft или удалённый рабочий стол.

Индивидуальные сценарии для каждого защищенного диска. Эти сценарии могут выполняться перед подключением диска, после подключения, перед отключением, после отключения. Например, после подключения защищенного диска с файлами базы данных Microsoft SQL с помощью сценария может быть запущена сама СУБД.

Надёжная двухфакторная аутентификация администраторов Secret Disk Server NG с использованием цифровых сертификатов X.509: для выполнения административных задач надо иметь персональный цифровой сертификат X.509, установленный в памяти eToken, и знать PIN-код.

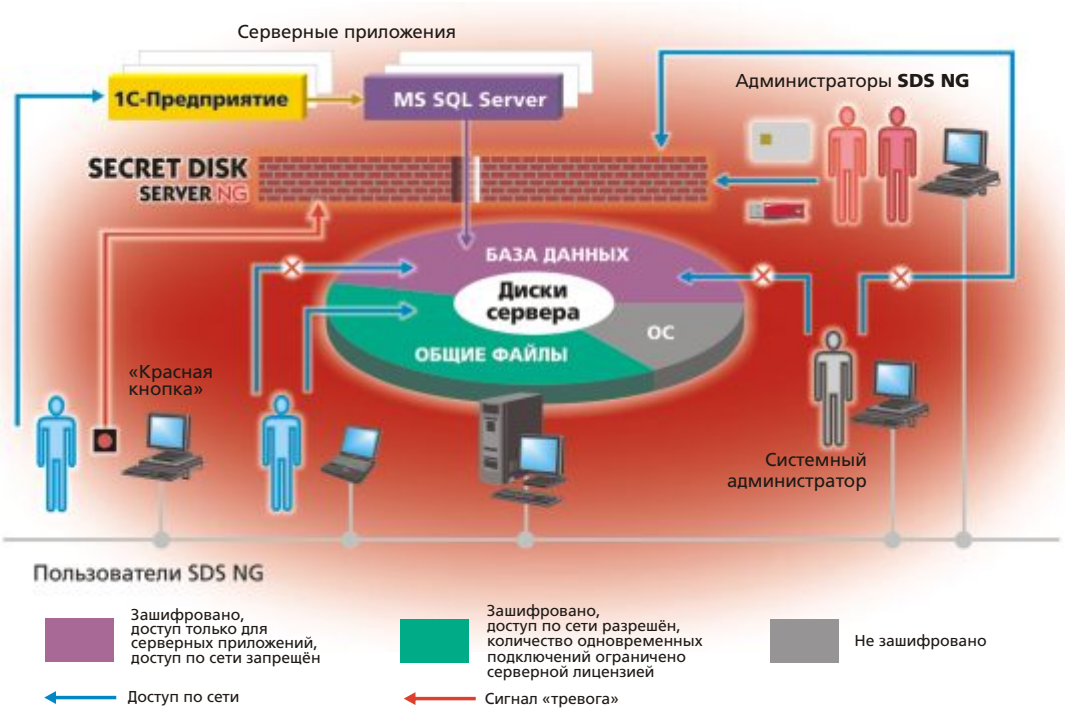
Эксклюзивная особенность

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, например, Acronis True Image (начиная с версии 8).

Возможности использования

Пример защиты корпоративных данных на сервере

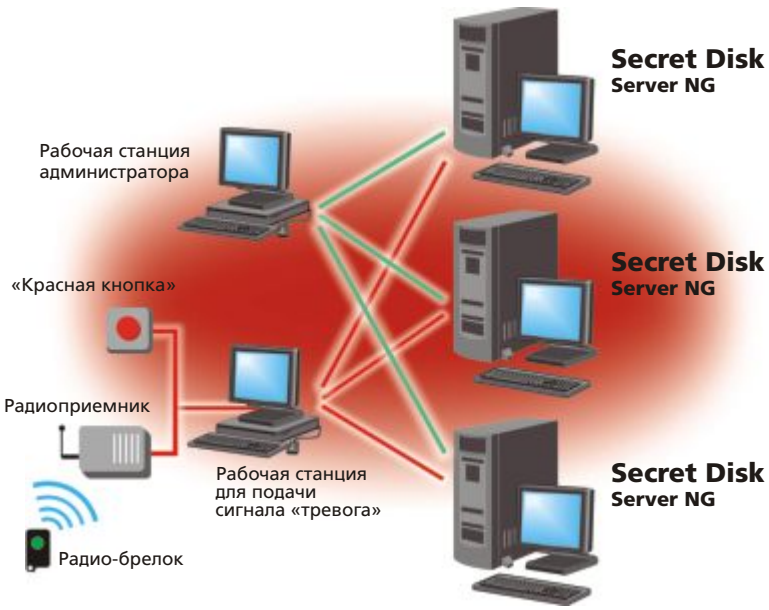


Secret Disk Server NG поддерживает две модели защиты ресурсов – модель файл-сервера с возможностью создания разделяемых сетевых ресурсов и модель сервера приложений с запретом прямого доступа по сети. Обе модели можно использовать на одном сервере (при наличии лицензий).

Интеграция в инфраструктуру обеспечения безопасности

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

Централизованное управление



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

Сертифицированная версия Secret Disk NG

Назначение

Сертифицированная версия Secret Disk NG предназначена для защиты конфиденциальной информации пользователей в системах под управлением сертифицированной версии Microsoft Windows XP. Данная версия предназначена для государственных предприятий и других организаций, предъявляющих требования к обязательной аттестации средств и систем на соответствие требованиям по защите информации.

Особенности

Функциональный аналог Secret Disk NG Personal Edition, прошедший сертификацию во ФСТЭК России по схеме сертификации производства и получивший сертификат №1111 от 12 декабря 2005 года. Данный сертификат подтверждает установленное в ходе испытаний и анализа исходного кода продукта:

- выполнение продуктом своей функциональности;
- отсутствие в нём недекларированных возможностей (таких как программные закладки, «back door» и т.п.).

Включает сертифицированный электронный ключ eToken PRO 32K (Сертификат Гостехкомиссии России №925 от 28 июня 2004 года) в качестве аппаратной составляющей комплекса.

Демо-версии продуктов

С веб-сайта Аладдин (www.aladdin.ru) можно бесплатно загрузить демо-версии основных продуктов линейки для защиты персональных и корпоративных данных – Secret Disk NG Personal Edition и Secret Disk Server NG.
Для работы с демо-версией достаточно иметь USB-ключ или смарт-карту eToken.

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

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

Модель eToken NG-OTP имеет встроенный генератор одноразовых паролей.

Продукты линейки Secret Disk NG могут использоваться с любой моделью eToken.

Выбор нужного продукта

Продукты линейки Secret Disk NG / Задача	Персональная редакция	Редакция для рабочих групп	Серверная версия	Сертифицированная версия
Защитить личные данные	✓			✓
Защитить данные для коллективной работы		✓	✓	
Защитить файл-сервер			✓	
Защитить почтовый сервер, сервер приложений, сервер СУБД			✓	
Получить сертифицированное решение				✓

Сервис и обучение

По требованию заказчика возможен выезд технического специалиста для установки Secret Disk Server NG и обучения администратора.
Компания Aladdin предлагает серию мастер-классов для обучения персонала заказчика работе с продуктами линейки Secret Disk NG.

Технические характеристики

Secret Disk NG Personal Edition \ Secret Disk NG Workgroup Edition	
Поддерживаемые платформы	Microsoft Windows 2000 Professional, Windows XP Professional\Home Edition
Типы поддерживаемых дисков	Разделы базовых дисков (Basic Disk Partiton) Тома динамических дисков (Dynamic Disk Volume) Съёмные диски (USB-drive, ZIP, магнитооптика и др.) Виртуальные диски (файлы-контейнеры)
Типы файловых систем	NTFS, FAT 12 / 16 / 32 С возможностью преобразования из одного типа в другой
Размер виртуальных дисков	От 1 МБ до 2 ТБ
Типы USB-ключей и смарт-карт	eToken PRO (16 КБ, 32 КБ, 64 КБ), eToken R2 (16 КБ, 32 КБ) eToken NG-OTP (32 КБ, 64 КБ)
Подключаемые внешние алгоритмы шифрования	RC2 (128 бит), TripleDES (168 бит), ГОСТ 28147-89 (256 бит), AES (128 и 256 бит), Twofish (256 бит)
Аутентификация пользователя	Двухфакторная (eToken + PIN-код)
Гарантийное обслуживание	12 месяцев
Secret Disk Server NG	
Поддерживаемые платформы	Microsoft Windows 2000, Windows XP, Windows 2003 Server
Типы поддерживаемых дисков	Разделы базовых дисков (Basic Disk Partiton) Тома динамических дисков (Dynamic Disk Volume) Съёмные диски (USB-drive, ZIP, магнитооптика и др.)
Типы файловых систем	NTFS, FAT 16 / 32
Размер защищаемых дисков	До 64 ТБ (для NTFS), до 8 ТБ (для FAT32), до 4 ГБ (для FAT 16)
Типы USB-ключей и смарт-карт	eToken PRO (16 КБ, 32 КБ, 64 КБ), eToken NG-OTP (32 КБ, 64 КБ) В базовую поставку входят два ключа eToken PRO
Подключаемые внешние алгоритмы шифрования	TripleDES (168 бит), ГОСТ 28147-89 (256 бит), AES (128 и 256 бит), Twofish (256 бит)
Возможность подключения других алгоритмов шифрования	Да, через библиотеки ядра
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	
Поддерживаемые платформы	Windows XP Professional (сертифицированная версия)
Типы поддерживаемых дисков	Разделы базовых дисков (Basic Disk Partiton) Тома динамических дисков (Dynamic Disk Volume) Съёмные диски (USB-drive, ZIP, магнитооптика и др.) Виртуальные диски (файлы-контейнеры)
Типы файловых систем	NTFS, FAT 12/16/32 С возможностью преобразования из одного типа в другой
Размер виртуальных дисков	От 1 МБ до 2 ТБ
Типы USB-ключей и смарт-карт	eToken PRO (16 КБ, 32 КБ, 64 КБ), eToken R2 (16 КБ, 32 КБ) USB-ключ eToken PRO 32K (сертифицированная версия) в комплекте
Подключаемые внешние алгоритмы	ГОСТ 28147-89 (256 бит)
Аутентификация пользователя	Двухфакторная (eToken + PIN-код)
Гарантийное обслуживание	12 месяцев

О компании Aladdin

Aladdin Software Security R.D. (основана в 1995 г.) - ведущий российский разработчик и поставщик средств аутентификации, продуктов и решений для обеспечения безопасного доступа к корпоративным ресурсам и защиты информации, лидер в области защиты программного обеспечения от несанкционированного использования.
Aladdin - компания-эксперт в области решения проблем «AAA» (Аутентификация, Авторизация и безопасное Администрирование), имеет хорошие деловые и партнерские отношения с большинством ведущих российских компаний - системных интеграторов и мировых IT-вендоров: Cisco Systems, IBM, Microsoft, Novell, RSA Security ,Oracle, SAP и др., неоднократно называлась Аппаратом Совета Безопасности РФ и Комитетом Государственной Думы по безопасности «Компанией года», входит в ТОП-100 российского IT-рынка (рейтинги CNews) и в число крупнейших IT-компаний РФ (рейтинги РА «Эксперт»).

SECRET DISK®
New Generation

Отзывы о Secret Disk NG

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

«Я попробовал Secret Disk NG 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».

Денис Нивников
Обозреватель PC Week

«Нередко аппаратные средства защиты данных создают проблемы не только злоумышленникам, охотящимся за конфиденциальной информацией, но и самим пользователям: для подсоединения электронных ключей приходится пробираться к задней стенке ПК, а интерфейс программ, обслуживающих эти ключи, понятен лишь программистам, их написавшим...

Но испытанный нами программно-аппаратный комплекс Secret Disk NG избавлен от таких недостатков. Благодаря продуманному и удобному интерфейсу, а также автоматическому подключению дисков работа с Secret Disk NG не вызовет затруднений даже у неопытного пользователя

Программно-аппаратный комплекс Secret Disk NG обеспечивает довольно высокий уровень защиты при сравнительно небольшой стоимости и замечательной простоте применения: по сравнению с более ранней испытанной нами версией в Secret Disk NG стали намного удобнее и интерфейс, и инструменты совместного доступа…

Secret Disk NG заслужил самую высокую оценку наших экспертов».

«Новое поколение Secret Disk», PC Week № 39, 21 октября 2003

Юрий Курочкин
Обозреватель журнала
«Connect! Мир связи»

«Для владельца ключа eToken засекреченный диск ничем не отличается от других на его компьютере: его видно в «проводнике», на него можно записывать и с него можно считывать любые файлы из программ, с которыми работает данный пользователь. Однако стоит извлечь eToken из компьютера, как вся эта информация становится невидимой. Посторонний человек, оказавшись перед компьютером, не найдет в нём сведений о засекреченных дисках и даже не догадается об их наличии.

Разработчики продуктов Secret Disk уже в течение нескольких лет усовершенствуют свои программы. Третья версия системы, с которой ознакомилась наша редакция, отличается предельной простотой и удобством в работе с нею».

«Информация под замком», Connect! Мир связи, №8, 2003

Тел: (495) 231-3113
E-mail: aladdin@aladdin.ru
Web: www.aladdin.ru
Лицензии Гостехкомиссии России №№ 0037, 0054 от 18.02.03
Лицензии ФАПСИ №№ ЛФ/07-2635-38 от 24.04.02