Aladdin
SECURITY SOLUTIONS
www.aladdin.ru

SECRET DISK® 4

Система защиты конфиденциальности информации и персональных данных для Microsoft® Windows® 2000 / XP / VISTA / 7

Краткая справочная информация

для специалистов
по информационной
безопасности и ИТ,
системных интеграторов,
бизнес-партнеров и заказчиков

В данном документе в краткой табличной форме приведена основная справочная информация по продукту Secret Disk 4, разработанному компанией Aladdin.

Содержание

Краткая информация о продукте

Параметр	Описание
Secret Disk 4	Secret Disk 4 – это программно-аппаратный комплекс для защиты конфиденциальной информации (коммерческой тайны, персональных данных), хранящейся и обрабатывающейся на рабочих станциях под управлением ОС Microsoft Windows 2000 / XP / Vista / Windows 7, обеспечивающий: • криптографическую защиту информации на жестких дисках и съемных носителях от несанкционированного доступа; • защиту файлов операционной системы компьютера от несанкционированного доступа; • двухфакторную аутентификацию пользователей до загрузки операционной системы с помощью электронных ключей и смарт-карт eToken; • многопользовательскую работу с защищенными данными, хранящимися на персональном компьютере; • возможность экстренного отключения зашифрованных дисков; • сокрытие наличия на персональном компьютере конфиденциальной информации.
Модели используемых ключей	**eToken PRO, eToken PRO 72K (Java)** (USB-ключ или смарт-карта), **eToken NG-OTP**, **eToken NG FLASH**. 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. В базовую поставку Secret Disk 4 входит 1 USB-ключ eToken PRO/32K – с лицензией на использование персональной версии Secret Disk 4.
Фото	 Secret Disk 4  Ключи eToken (USB-ключ, комбинированные USB-ключи и смарт-карта)
Используемые технологии	Многопоточное шифрование, фоновое шифрование, цифровые сертификаты стандарта X.509 , USB-ключи / смарт-карты.
Ресурс для получения подробной актуальной информации	www.aladdin.ru

Основное назначение и преимущества продукта	
Назначение	• Защита от несанкционированного доступа к конфиденциальной информации (коммерческая тайна, персональные данные), хранящейся и обрабатывающейся на рабочих станциях под управлением ОС Microsoft Windows 2000 / XP / Vista / Windows 7; • Защита от несанкционированной загрузки ОС и доступа к системному разделу; • Secret Disk 4 не только защищает конфиденциальные данные, но и скрывает сам факт их наличия.
Возможности применения	• **Защита данных на жестких и съемных дисках** методом «прозрачного» шифрования; • **Защита сеанса загрузки операционной системы** с помощью процедуры строгой двухфакторной аутентификации пользователя с использованием электронных ключей eToken.
Основной эффект, достигаемый от использования решения	• **Защита конфиденциальной информации от несанкционированного доступа** со стороны: ▪ **злоумышленников**, получивших физический доступ к носителям данных (жестким дискам), в том числе в случае проникновения в офис компании; ▪ **посторонних лиц,** могущих иметь доступ к компьютерному оборудованию (например, сотрудники сервисного центра, обслуживающего оборудование); ▪ **сотрудников компании,** не обладающих полномочиями для доступа к данной информации (в том числе технических специалистов и системных администраторов). • **Защита сеанса загрузки операционной системы** со стороны: ▪ **неавторизованных лиц,** могущих иметь доступ к компьютерному оборудованию (например, сотрудники компании или сотрудники сервисного центра, обслуживающего оборудование).
Особенности решения	**Защита данных от несанкционированного доступа** • **Данные на защищенных дисках** всегда хранятся в зашифрованном виде. Даже в случае изъятия компьютера или утери диска данные невозможно использовать. • **Образ оперативной памяти,** сохраняемый в спящем режиме («hibernation») или в случае сбоя операционной системы, записывается на защищенный системный раздел. • **Аппаратная двухфакторная аутентификация** с использованием USB-ключей eToken при загрузке операционной системы, и работе с зашифрованными дисками: необходимо не только обладать eToken, но и знать PIN-код к нему. • **Использование "горячих" клавиш для** вызова панели управления Secret Disk, закрытия сеанса и отключения дисков, скрытия/отображения значка на панели задач. • **Запрет доступа по сети к зашифрованным данным**. Доступ по сети к зашифрованным данным запрещен для всех пользователей, включая системного администратора. Для редакции Workgroup Edition допускается разрешить сетевой доступ в пределах возможностей операционной системы. **Удобство работы, обеспечение доступности и целостности данных** • **Фоновые операции шифрования.** Все операции зашифрования, расшифрования и перешифрования проводятся в фоновом режиме. Во время выполнения этих операций пользователь может работать в обычном режиме. • **Смена ключа и алгоритма шифрования выполняется как одна операция**. Для смены ключа и/или алгоритма шифрования не требуется сначала расшифровывать данные (тем самым временно снимать с них защиту), а затем их зашифровывать с новым ключом и/или алгоритмом шифрования. Операция смены ключа выполняется в один проход, благодаря чему в любой момент времени данные надежно защищены. • **Остановка или прерывание процесса зашифрования, перешифрования или расшифрования** не приводят к потере данных. Приостановленный вручную или прерванный из-за отключения питания компьютера процесс может быть возобновлен в любой удобный для вас момент. • **Аварийное восстановление главной загрузочной записи**. В состав Secret Disk 4 входит диск аварийного восстановления, который позволяет восстановить главную загрузочную запись (Master Boot Record – MBR) в случае модификации другими программами.

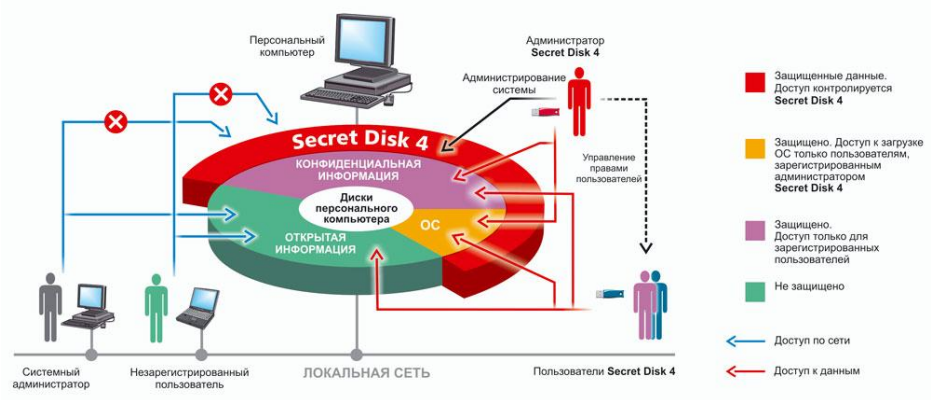
Основное назначение и преимущества продукта	
	• **Защита от сбоев электропитания.** Если во время процесса шифрования произошло внезапно е отключение электричества, шифрование будет приостановлено и позже продолжено с того же момента. **Совместимость и интеграция** ▪ **Использование цифровых сертификатов стандарта X.509** позволяет легко интегрировать Secret Disk 4 в существующую инфраструктуру открытых ключей, построенную на базе как западных (Microsoft CA, RSA Keon, Entrust, Baltimore), так и российских технологий (УЦ КриптоПро, Infotecs, Signal-COM). Если в вашей организации инфраструктура открытых ключей пока не используется, то Secret Disk 4 сам создаст все необходимые для работы сертификаты. ▪ **Поддержка операционных систем**. Система Secret Disk 4 работает в операционных системах семейства Windows - Microsoft Windows 2000 Professional, Microsoft XP, Windows Vista и Windows 7. Поддерживаются как 32-битные, так и 64-битные редакции операционных систем Windows. ▪ **Поддержка многопроцессорных систем и технологии Hyper-Threading.** В Secret Disk 4 поддерживается распараллеливание криптографических вычислений, тем самым обеспечивается рост производительности при применении на мощных многопроцессорных системах или системах с использованием технологии Hyper-Threading.
Основные технологические преимущества	▪ **Шифрование разделов** жестких дисков, логических дисков, съемных носителей. В Secret Disk 4 поддерживаются все типы жестких дисков и дисковых RAID-массивов. ▪ **Создание виртуальных дисков (файлов-контейнеров).** Физически виртуальный диск представляет собой файл, содержимое которого полностью зашифровано. Средствами Secret Disk 4 виртуальный диск монтируется как логический диск и доступен для работы, как и любой другой логический диск, имеющийся в системе. ▪ **Отсутствие встроенных криптографических средств**. Secret Disk 4 не имеет встроенных средств шифрования (в том числе Secret Disk 4 не подлежит обязательному лицензированию как шифросредство). Для осуществления криптографических преобразований могут применяться: • криптографический драйвер режима ядра, входящий в состав Microsoft Windows (алгоритмы AES с длиной ключа 256 бит, TripleDes с длиной ключа 168 бит и RC2 с длиной ключа 128 бит); • криптопровайдеры КриптоПро CSP, Signal-COM CSP, Infotecs CSP (алгоритм шифрования ГОСТ 28147-89 с длиной ключа 256 бит); • подключаемые внешние алгоритмы шифрования Secret Disk Crypto Pack (AES с длиной ключа 128 и 256 бит, Twofish с длиной ключа 256 бит). ▪ **Интеграция с системами PKI**. Secret Disk 4 использует сертификаты X.509 и связанные с ними криптографические ключи для защиты мастер-ключей зашифрованных дисков и аутентификации. ▪ **Поддержка российской криптографии**. Для шифрования дисков и защиты мастер-ключей зашифрованных дисков Secret Disk 4 может использовать сертифицированные криптопровайдеры КриптоПро CSP, Infotecs CSP, Signal-COM CSP (алгоритм ГОСТ 28147-89). ▪ **Технология многопоточного шифрования**. Применение новаторской технологии многопоточного шифрования позволяет эффективно использовать вычислительные ресурсы как мощных многопроцессорных систем, так и повышает эффективность работы системы на однопроцессорных машинах. Благодаря этому в работе прикладных систем не наблюдается заметного снижения производительности при переходе к использованию зашифрованных дисков. ▪ **Перешифрование зашифрованных дисков** со сменой ключа и/или алгоритма шифрования. Возможна остановка/продолжение процесса зашифрования, а также предусмотрена защита от сбоев компьютера в процессе шифрования. ▪ **Переформатирование зашифрованных дисков** со сменой файловой системы. Форматирование и проверка дисков на наличие ошибок может производиться как стандартными средствами операционной системы, так и встроенными инструментами Secret Disk 4. Зашифрованные диски могут иметь формат NTFS, FAT32 или FAT16. ▪ **Многопользовательский режим работы с зашифрованными дисками**. Для организации многопользовательского режима использования компьютера, администратор

Основное назначение и преимущества продукта	
	Secret Disk 4 может давать права на доступ к зашифрованным дискам разным пользователям, а также на загрузку операционной системы с защищенного системного раздела. ▪ **Аппаратная двухфакторная аутентификация** администратора Secret Disk 4 с использованием цифровых сертификатов X.509: для выполнения административных задач надо иметь персональный цифровой сертификат X.509 в памяти eToken, и знать PIN-код.
Основные потребители	▪ **Частные компании**, использующие либо планирующие внедрение информационных систем, обрабатывающих критически важные для их бизнеса данные, кража, модификация или утечка которых может привести к ощутимым потерям, например: • финансовая информация; • информация о клиентах; • Ноу-Хау; • другая информация, **составляющая коммерческую тайну**. ▪ **Органы государственной власти** и местного самоуправления, организации различных форм собственности, **работающие с конфиденциальной информацией и персональными данными**.
Возможность использования решения в государственных структурах	▪ Компания Aladdin имеет все необходимые лицензии: • Гостехкомиссии (ФСТЭК) РФ и ФАПСИ (ФСБ) на деятельность в области разработки, производства, услуг, распространения средств защиты и защищенных систем; • Минэкономразвития на импорт шифровальных средств (eToken) и разрешение ФСБ на ввоз их на территорию России[1]. ▪ Secret Disk 4 сертифицирован ФСТЭК (сертификат №1742 от 24 декабря 2008 года) на соответствие Заданию по безопасности и имеет оценочный уровень доверия ОУД1 (усиленный) в соответствии с требованиями руководящего документа "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий", (Гостехкомиссия России, 2002). Secret Disk 4 может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно, а также ИСПДн до класса 2 включительно. ▪ Электронные ключи и смарт-карты eToken, поддерживаемые в продукте, имеют сертификат № 925/5 ФСТЭК России, подтверждающий возможность использования eToken для создания АС до класса "1Г" включительно, а также для создания информационных систем обработки персональных данных до 2 класса включительно. ▪ Возможность применения совместно с сертифицированными поставщиками средств криптографии (КриптоПро CSP, Infotecs CSP и Signal-COM CSP).
Простота внедрения, адаптация персонала	▪ **Для пользователей** – работа системы абсолютно прозрачна. Установка Secret Disk 4 не требует перенастройки другого ПО и не меняет привычный порядок работы за компьютером. ▪ **Для администратора** – быстрый ввод в эксплуатацию, удобное управление правами пользователей (не нужен доступ к ключам eToken пользователей, используются сертификаты X.509), возможность использования динамических томов и программных массивов RAID, подробные инструкции и документация по настройке системы.
Внедрение и сопровождение решения	▪ Внедрение и сопровождение продукта и решений с его использованием может осуществляться партнерами компании Aladdin. ▪ Гарантийный период на продукт составляет 12 мес. Он может быть продлен до 5 лет.
Системные требования	▪ Операционная система Microsoft: • Windows 2000 Professional (с пакетом обновлений Service Pack 2 и выше); • Windows XP (с установленным Service Pack 2 и выше); • Windows Vista;

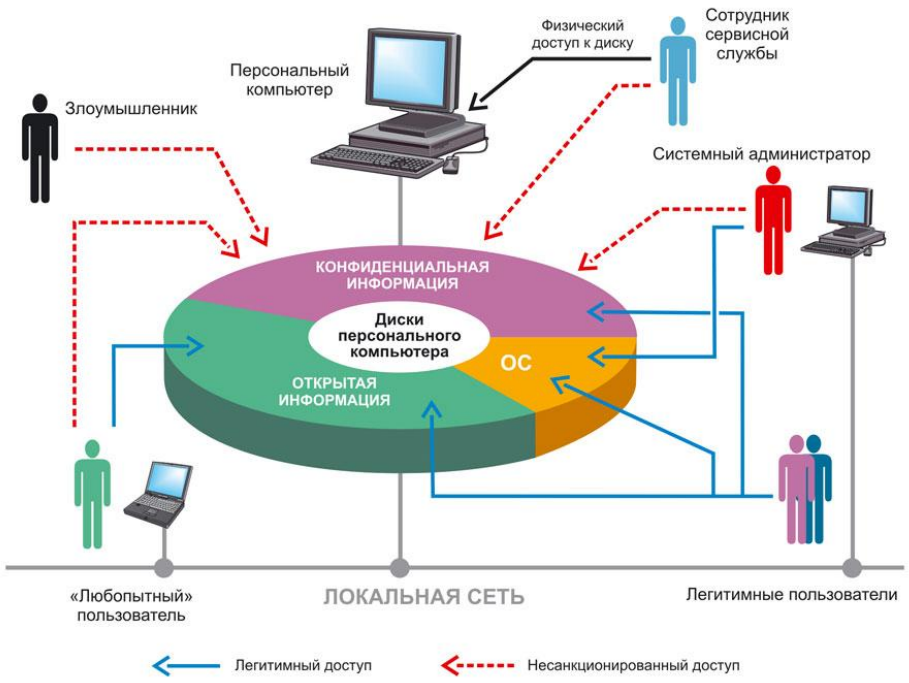
[1] Другие компании, осуществляющие ввоз подобных устройств на территорию России, подобных разрешений и лицензий не имеют.

Основное назначение и преимущества продукта	
	• Windows 7 RC1. ▪ Установленные драйверы eToken (входят в комплект). ▪ 15 мегабайт свободного пространства на диске. ▪ При использовании совместно с сертифицированными российскими поставщиками криптографии – установленный КриптоПро CSP, Infotecs CSP, либо Signal-COM CSP.

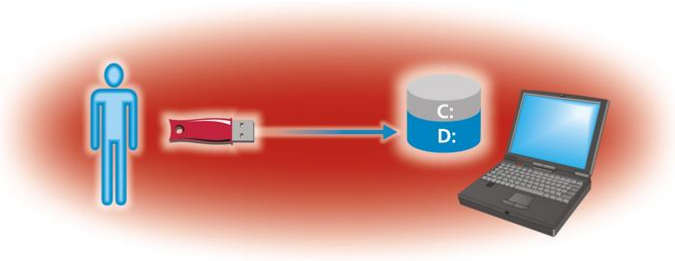
Технические подробности

Параметр	Описание
Архитектура	
Работа пользователей системы	• Администратор Secret Disk 4 устанавливает и управляет Secret Disk 4 на персональном компьютере, устанавливает защиту системного раздела, создаёт зашифрованные диски. Администратор Secret Disk 4 регистрирует пользователей Secret Disk 4 и управляет доступом к данным на зашифрованных дисках и возможностью загрузки операционной системы с защищенного системного раздела. • Незарегистрированные пользователи, включая системного администратора, не имеют доступа к загрузке операционной системы с защищенного системного раздела и доступа, в том числе по сети, к данным на зашифрованных дисках. • Незарегистрированные пользователи обращаются к общим файлам на незашифрованных дисках по сети при наличии прав доступа к таким общим файлам. • Пользователи Secret Disk 4 имеют доступ к загрузке операционной системы с защищенного системного раздела и доступ к данным на зашифрованных дисках. • Пользователи Secret Disk 4 могут нажатием клавиш быстрого вызова закрыть сеанс и отключить подключенные зашифрованные диски; скрыть отображение значка Secret Disk 4 на панели задач.
Компоненты системы	• **Secret Disk 4** — программное обеспечение, осуществляющее защиту информации на дисках и съемных носителях. • **Электронный ключ eToken** — компонент, на котором хранятся лицензия на использование Secret Disk 4, сертификат открытого ключа пользователя и соответствующий ему закрытый ключ. Используется для строгой двухфакторной аутентификации пользователей для загрузки операционной системы и для доступа к зашифрованным данным.
Принцип работы системы	• Защита информации обеспечивается шифрованием данных «на лету». При чтении данных с диска происходит их расшифрование, при записи на диск — зашифрование. Находящиеся на диске данные всегда зашифрованы. Алгоритм шифрования выбирается администратором при создании защищенного диска и может быть изменен в любой момент в процессе работы. • Зашифрованный диск можно подключать и отключать. Отключенный зашифрованный диск выглядит как неформатированный. С подключенным зашифрованным диском вы работаете точно так же, как с обычным диском. Для того чтобы подключить зашифрованный диск, необходимо обладать смарт-картой или электронным ключом eToken, знать PIN-код и иметь соответствующие полномочия по отношению к данному

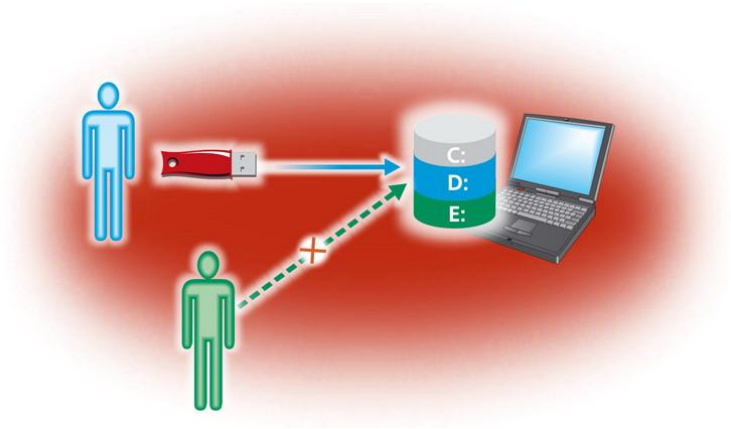
	диску. • При прямом просмотре содержимое отключенного зашифрованного диска выглядит как случайная последовательность битов или, говоря по-другому, «белый шум», поскольку все данные зашифрованы. По содержимому раздела диска невозможно определить, является ли данный раздел просто неформатированным, или же на нем имеется какая-то информация. Так Secret Disk 4 обеспечивает защиту конфиденциальной информации от несанкционированного доступа, а также сокрытие наличия данных на компьютере. • При обращении к интерфейсу Secret Disk 4 администратор должен подключить к компьютеру свой eToken и ввести PIN-код. • Процесс шифрования диска может быть приостановлен администратором или даже прерван (например, из-за перебоев электропитания) - это не повлечет за собой потерю данных. Приостановленный или прерванный процесс шифрования может быть возобновлен в любой удобный момент. По завершении процесса шифрования все содержимое диска становится зашифрованным, что обеспечивает надежную криптографическую защиту хранящихся на нем данных. • Для ноутбуков предусмотрен режим энергосбережения – операции шифрования, перешифрования и расшифрования диска приостанавливаются, если ноутбук переходит на питание от внутренних батарей. При возобновлении питания от сети приостановленный процесс автоматически продолжится. • Администратор Secret Disk 4 устанавливает Secret Disk 4 на персональный компьютер. • Администратор Secret Disk 4 создаёт на персональном компьютере зашифрованные диски, а также устанавливает/снимает защиту системного раздела. • Администратор Secret Disk 4 проводит операции резервного копирования и восстановления мастер-ключей шифрования дисков. • Администратор Secret Disk 4 может зарегистрировать на персональном компьютере произвольное число пользователей и дать им доступ к загрузке операционной системы с защищенного системного раздела, а также доступ к зашифрованным дискам с данными. • Пользователи Secret Disk 4 могут загружать операционную систему с защищенного системного раздела, подключать зашифрованные диски и работать с ними, а также отключать зашифрованные диски. • Пользователи Secret Disk 4 не могут снять защиту с системного раздела и расшифровать диски, проводить операции резервного копирования и восстановления мастер-ключей шифрования, а также не могут перешифровывать зашифрованные диски. • Доступ по сети к содержимому зашифрованных дисков невозможен для любых пользователей локальной сети, включая системного администратора и администратора домена Windows.
Варианты применения	• **Secret Disk 4 для мобильных компьютеров (ноутбуков)** позволяет защищать информацию на жестком диске от несанкционированного доступа. В случае утери или кражи мобильного компьютера, вся информация, хранящаяся на жёстком диске, включая конфиденциальную и персональную информацию (пароли, временные файлы приложений, файл подкачки операционной системы, временные файлы Интернет-браузера, файлы-журналы приложений и т.п.), будет недоступна для чтения. • **Secret Disk 4 для персональных компьютеров в локальной сети,** позволяет защищать информацию на жестком диске от несанкционированного доступа методом прозрачного шифрования. При этом зашифрованная информация будет недоступна по сети, тем самым информация защищена от взлома и проникновения хакеров и недобросовестных сотрудников («инсайдеров»). • **Secret Disk 4 для компьютеров, на которых хранятся персональные данные,** позволяет защитить от несанкционированного доступа персональные данные сотрудников компании и других граждан согласно Федеральному закону о персональных данных № 152-ФЗ от 27 июля 2006 года. • Специальная редакция **Secret Disk 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). • Secret Disk 4 позволяет шифровать информацию на **съёмных устройствах хранения данных (флешках, картах памяти, USB-дисках и т.д.)**, для исключения несанкционированного доступа к этой информации в случае утери или кражи носителя.

Для сравнения: **типовая схема использования персонального компьютера в локальной сети предприятия**	
Недостатки типовой схемы	• Возможен доступ к данным со стороны следующих лиц: ▪ **Злоумышленник** (человек, сознательной целью которого является получение доступа к вашим конфиденциальным данным), получивший физический доступ к персональному компьютеру и/или дискам с конфиденциальными данными, и обладающий возможностью привлечения значительных вычислительных ресурсов для получения доступа к данным. ▪ **Постороннее лицо**, получившее легальный доступ к персональному компьютеру (например, при сервисном обслуживании во внешней компании или во внутренней IT-службе). ▪ **Любопытный сотрудник** – сотрудник организации (по роду своей деятельности не должен иметь доступа к конфиденциальным данным, но желающий с ними ознакомиться), который может воспользоваться отсутствием сотрудника на своём рабочем месте или ошибками администрирования, (например, неожиданно представившейся возможностью просмотра содержимого диска с конфиденциальной информацией по сети) или повысить свой уровень полномочий в операционной системе до административного с целью скопировать интересующие файлы в конфиденциальной информацией для последующего просмотра. ▪ **Системный администратор (администратор домена Windows)** (по умолчанию имеет самый высокий уровень прав доступа), имеющий возможность обратиться по сети к любому диску персонального компьютера с помощью так называемых административных сетевых ресурсов).

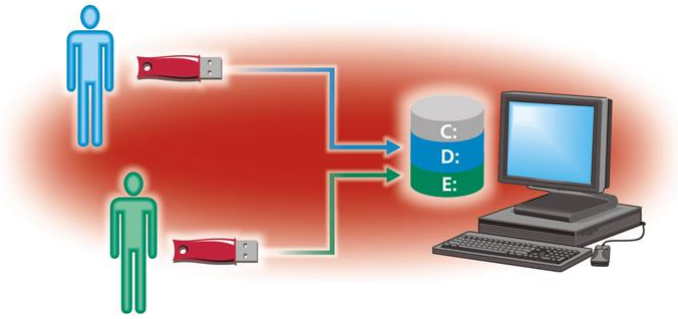
Типовые сценарии установки

1. Мобильный компьютер	
Описание	Secret Disk 4 установлен на мобильном компьютере, защищен системный раздел, зашифрованы остальные разделы жёсткого диска .
Архитектура	
Особенности	Данный сценарий рекомендуется для защиты персональных мобильных компьютеров (ноутбуков), для которых риск утери или кражи очень высок. Шифрование всех разделов жёсткого диска, а также защита системного раздела, позволит избежать попадания конфиденциальной и личной информации в посторонние руки.
Преимущества	• вся информация, включая временные файлы, файл подкачки операционной системы, пароли, файлы-журналы и т.п., хранятся на жёстком диске в защищенном системном разделе и не доступны для несанкционированного просмотра; • неавторизованный пользователь не сможет использовать мобильный компьютер, так как для загрузки операционной системы с защищенного системного диска необходимо пройти процедуру двухфакторной аутентификации с использованием электронного USB-ключа eToken PRO.
Недостатки	• нет возможности скрыть факт использования Secret Disk 4 для защиты системного раздела.

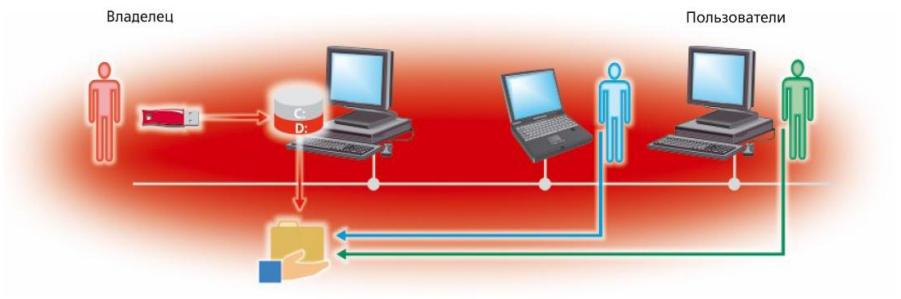
2. Персональный компьютер в локальной сети

Описание	Secret Disk 4 установлен на персональный компьютер, подключённый к локальной сети. За компьютером работает один пользователь.
Архитектура	
Особенности	• пользователь Secret Disk 4 является администратором Secret Disk 4, он устанавливает Secret Disk 4 на персональный компьютер и выполняет операции шифрования несистемных разделов жёсткого диска, а также устанавливает защиту системного раздела; • доступ других пользователей к загрузке операционной системы и к данным, хранящимся на защищенных дисках, полностью запрещён; • доступ к зашифрованным дискам по сети запрещён для всех пользователей, включая системного администратора.
Преимущества	• защита от несанкционированного доступа к конфиденциальной информации, хранящейся на персональном компьютере; • обеспечение работы с персональным компьютером одного пользователя, являющегося администратором Secret Disk 4; незарегистрированный пользователь не сможет даже загрузить операционную систему; • защита конфиденциальной информации, хранящейся на защищенных дисках, от утечки по локальной сети (проникновение в корпоративную сеть хакеров, работа вредоносных шпионских и троянских программ, «инсайдеры» и т.п.).

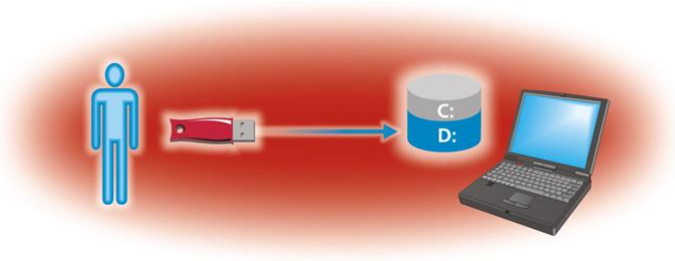
3. Многопользовательский персональный компьютер в локальной сети

Описание	Secret Disk 4 установлен на персональный компьютер, подключённый к локальной сети. За компьютером могут работать несколько пользователей.
Архитектура	
Особенности	• для работы нескольких пользователей необходимо наличие лицензий на Secret Disk 4, записанных в защищённой памяти электронного ключа eToken PRO каждого пользователя; • для обеспечения возможности загрузки операционной системы с защищенного системного раздела, администратор Secret Disk 4 должен зарегистрировать пользователей. Для этого необходим доступ к сертификату X.509 регистрируемого пользователя; • доступ к зашифрованным дискам по сети запрещён для всех пользователей, включая системного администратора; • пользователи Secret Disk 4 могут создавать свои зашифрованные диски на жёстком диске персонального компьютера и съёмных внешних носителях и давать доступ к этим дискам другим пользователям Secret Disk 4.
Преимущества	• защита конфиденциальных данных и разграничение доступа к ним на персональных компьютерах, на которых работает несколько пользователей; • обеспечение работы с персональным компьютером только для пользователей Secret Disk 4, незарегистрированный пользователь не сможет даже загрузить операционную систему; • защита конфиденциальной информации, хранящейся на защищенных дисках, от утечки по локальной сети (проникновение в корпоративную сеть хакеров, работа вредоносных шпионских и троянских программ, «инсайдеры» и т.п.).

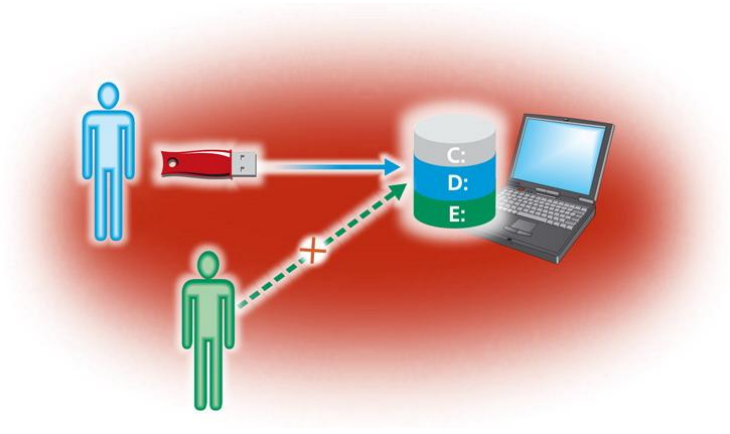
4. Secret Disk 4 для рабочих групп

Описание	Secret Disk 4 установлен на персональный компьютер, подключённый к локальной сети. С защищенными ресурсами могут работать по сети несколько пользователей.
Архитектура	
Особенности	• для разрешения работы по сети необходимо наличие лицензии Secret Disk 4 Workgroup Edition, записанной в защищённой памяти электронного ключа eToken PRO владельца; • уровень доступа к зашифрованным дискам по сети регулируется средствами операционной системы; • количество сеансов ограничено 10 подключениями. • для серверных операционных систем необходим Secret Disk Server
Преимущества	• защита конфиденциальных данных и разграничение доступа к ним на персональных компьютерах, на которых работает несколько пользователей; • обеспечение работы с защищаемыми ресурсами по сети только для разрешенных пользователей с гибкими настройками уровня доступа; • оптимальное решение для небольшой локальной сети.

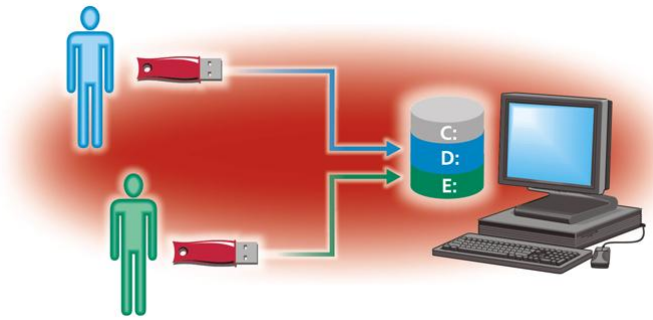
Типовые сценарии использования

1. Защита данных на однопользовательском (мобильном) компьютере	
Существующие риски	1. Утеря или кража мобильного компьютера. 2. Несанкционированное использование посторонними лицами (во время деловых поездок или в домашних условиях).
Назначение	• защита конфиденциальной информации, персональных данных и личной информации, хранящихся на мобильном компьютере, от несанкционированного доступа посторонних лиц; • сокрытие факта наличия защищенной информации на мобильном компьютере.
Архитектура решения	
Сценарий использования	1. Защита содержимого системного раздела средствами Secret Disk 4. 2. Создание средствами Secret Disk 4 зашифрованного диска достаточного объема. 3. Создание резервной копии ключа шифрования защищенного диска и/или резервной копии защищенного хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных пользователях). 3. Настройка клавиш быстрого вызова для быстрого отключения защищенных дисков и сокрытия значка Secret Disk на панели задач. 4. Размещение на защищенном диске файлов с конфиденциальной информацией и/или персональными данными.
Уязвимости существующих решений	• злоумышленник может получить доступ к информации, хранящейся на загрузочном диске мобильного компьютера, в случае получения несанкционированного физического доступа к компьютеру; • нет возможности оперативного и корректного прекращения доступа к данным, хранящимся на жёстком диске, при возникновении нештатных ситуаций; • нет возможности сокрытия факта наличия конфиденциальной информации на мобильном компьютере.

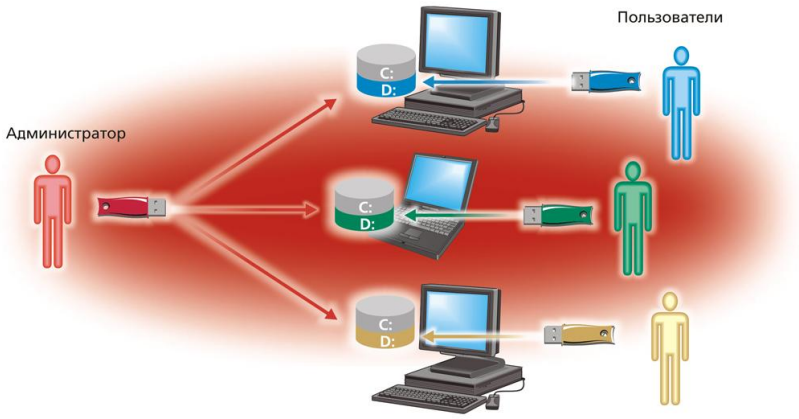
2. Защита данных на многопользовательском компьютере (сценарий 1)

Существующие риски	1. Несанкционированный доступ к данным, хранящимся на персональном компьютере, по локальной сети. 2. Несанкционированное использование посторонними лицами (во время отсутствия пользователя на рабочем месте). 3. Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ.
Назначение	• защита конфиденциальной информации, персональных данных и личной информации, хранящихся на персональном компьютере, к которому имеют доступ несколько пользователей Windows; • сокрытие факта наличия конфиденциальной информации на персональном компьютере.
Архитектура решения	
Сценарий использования	1. Создание средствами Secret Disk 4 защищенного диска достаточного объема. 2. Создание диска общего пользования для хранения данных других пользователей. 4. Создание резервной копии ключа шифрования защищенного диска и/или резервной копии защищенного хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных пользователях). 3. Настройка клавиш быстрого вызова для быстрого отключения защищенных дисков и сокрытия значка Secret Disk на панели задач. 4. Размещение на защищенном диске файлов с конфиденциальной информацией и/или персональными данными.
Уязвимости существующих решений	• злоумышленник может получить доступ к информации, хранящейся на дисках персонального компьютера, в случае получения несанкционированного физического доступа к компьютеру; • при многопользовательской работе возможно случайное или преднамеренное искажение или порча конфиденциальной информации; • нет возможности оперативного и корректного прекращения доступа к данным, хранящимся на жёстком диске, при возникновении нештатных ситуаций; • нет возможности сокрытия факта наличия конфиденциальной информации на персональном компьютере.

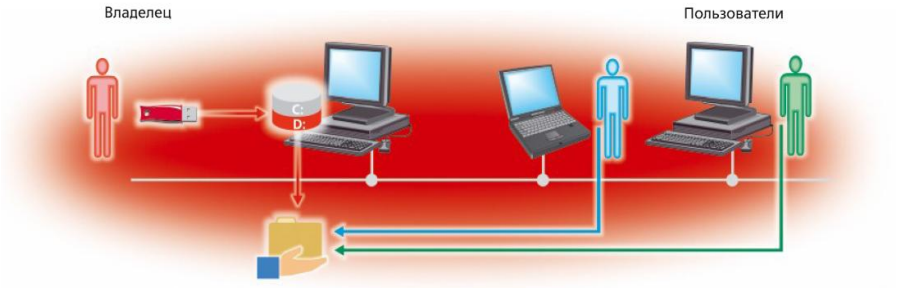
3. Защита данных на многопользовательском компьютере (сценарий 2)

Существующие риски	1. Несанкционированный доступ к данным со стороны других пользователей, допущенных к работе на персональном компьютере. 2. Несанкционированный доступ к данным, хранящимся на персональном компьютере, по локальной сети. 3. Несанкционированное использование посторонними лицами (во время отсутствия пользователя на рабочем месте). 4. Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ.
Назначение	• защита конфиденциальной информации, персональных данных и личной информации нескольких пользователей, работающих в режиме разделения времени с разной конфиденциальной информацией на одном персональном компьютере; • сокрытие факта наличия конфиденциальной информации на персональном компьютере.
Архитектура решения	
Сценарий использования	1. Создание средствами Secret Disk 4 зашифрованного дисков достаточного объема для каждого пользователя, работающего за персональным компьютером. 2. Создание резервной копии ключа шифрования защищенного диска и/или резервной копии защищенного хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных пользователях). 3. Настройка клавиш быстрого вызова для быстрого отключения защищенных дисков и сокрытия значка Secret Disk на панели задач. 4. Размещение пользователями Secret Disk 4 на защищенных дисках файлов с конфиденциальной информацией и/или персональными данными.
Уязвимости существующих решений	• злоумышленник может получить доступ к информации, хранящейся на дисках персонального компьютера, в случае получения несанкционированного физического доступа к компьютеру; • при многопользовательской работе возможен несанкционированный доступ к конфиденциальной информации, а также возможно случайное или преднамеренное искажение или порча конфиденциальной информации; • нет возможности оперативного и корректного прекращения доступа к данным, хранящимся на жёстком диске при возникновении нештатных ситуаций; • нет возможности сокрытия факта наличия конфиденциальной информации на персональном компьютере.

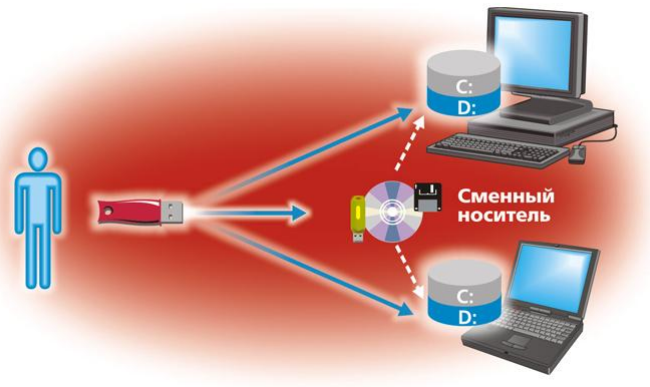
4. Защита данных на компьютерах в корпоративной сети (сценарий 1)

Существующие риски	1. Несанкционированное использование посторонними лицами (во время отсутствия пользователя на рабочем месте). 2. Несанкционированный доступ к данным, хранящимся на персональном компьютере, по локальной сети. 3. Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ.
Назначение	• защита конфиденциальной информации, персональных данных и личной информации пользователей, работающих на персональных компьютерах в корпоративной сети; • сокрытие факта наличия конфиденциальной информации на персональных компьютерах.
Архитектура решения	
Сценарий использования	1. Защита системного раздела жёсткого диска на персональных компьютерах средствами Secret Disk 4. 2. Создание средствами Secret Disk 4 зашифрованного диска достаточного объема на каждом защищаемом персональном компьютере. 3. Создание резервной копии ключа шифрования защищенного диска и/или резервной копии защищенного хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных пользователях). 4. Настройка клавиш быстрого вызова для быстрого отключения защищенных дисков и сокрытия значка Secret Disk на панели задач. 5. Размещение пользователями Secret Disk 4 на защищенных дисках файлов с конфиденциальной информацией и/или персональными данными.
Уязвимости существующих решений	• злоумышленник может получить доступ к информации, хранящейся на дисках персонального компьютера, в случае получения несанкционированного физического доступа к компьютеру; • при многопользовательской работе возможен несанкционированный доступ к конфиденциальной информации, а также возможно случайное или преднамеренное искажение или порча конфиденциальной информации; • нет возможности оперативного и корректного прекращения доступа к данным, хранящимся на жёстком диске при возникновении нештатных ситуаций; • нет возможности сокрытия факта наличия конфиденциальной информации на персональном компьютере.

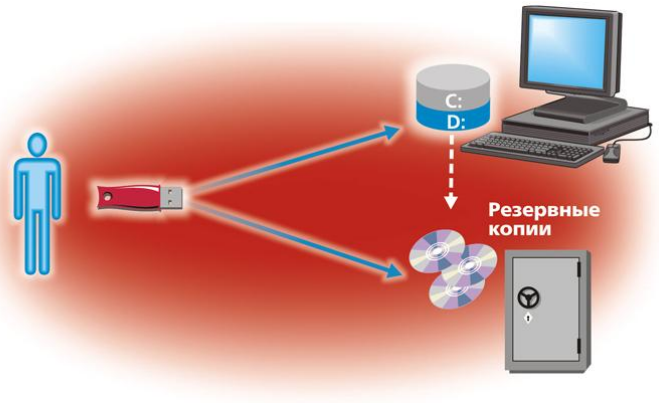
5. Защита данных на компьютерах в корпоративной сети (сценарий 2)

Существующие риски	1. Несанкционированное использование посторонними лицами (во время отсутствия пользователя на рабочем месте). 2. Несанкционированный доступ к данным, хранящимся на персональном компьютере, по локальной сети.
Назначение	• Защита конфиденциальной информации, хранящейся на защищаемом ресурсе (в том числе находящейся в общем доступе), от несанкционированного доступа в обход встроенных в операционную систему средств аутентификации, авторизации и контроля доступа • сокрытие факта наличия конфиденциальной информации на персональных компьютерах.
Архитектура решения	
Сценарий использования	1. Защита системного раздела жёсткого диска на персональных компьютерах средствами Secret Disk 4. 2. Создание средствами Secret Disk 4 зашифрованного диска достаточного объема на каждом защищаемом персональном компьютере. 3. Создание резервной копии ключа шифрования защищенного диска и/или резервной копии защищенного хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных пользователях). 4. Настройка клавиш быстрого вызова для быстрого отключения защищенных дисков и сокрытия значка Secret Disk на панели задач. 5. Размещение на защищенном диске файлов для общего доступа, установка прав доступа к ним на уровне файловой системы. 6. Размещение пользователями Secret Disk 4 на защищенных дисках файлов с конфиденциальной информацией и/или персональными данными.
Уязвимости существующих решений	• Злоумышленник может получить доступ к информации, хранящейся на диске, в обход разрешений, установленных на уровнях операционной и файловой систем (например, при извлечении дисков и подключении их к другому компьютеру) • нет возможности оперативного и корректного отключения доступа к данным, находящимся в общем сетевом доступе и/или использовании при возникновении нештатных ситуаций; • нет возможности сокрытия факта наличия конфиденциальной информации на персональном компьютере.

6. Защита данных при транспортировке и обмене

Существующие риски	1. Утеря или кража съёмных носителей. 2. Несанкционированный доступ к данным, хранящимся на съёмных носителях.
Назначение	• защита конфиденциальной информации, переносимой с одного персонального компьютера на другой посредством съёмных носителей информации (USB-дисков, ZIP, дискет, CD- и DVD-дисков и т.п.).
Архитектура решения	
Сценарий использования	1. Создание средствами Secret Disk 4 виртуального зашифрованного диска (файла-контейнера). 2. Создание резервной копии ключа шифрования виртуального зашифрованного диска. 3. Копирование зашифрованного файла-контейнера и копии ключа шифрования на съёмный носитель. 4. Размещение пользователями Secret Disk 4 на защищенных дисках файлов с конфиденциальной информацией и/или персональными данными. 5. Перенос съёмного носителя на другой персональный компьютер с установленным Secret Disk 4 и подключение виртуального зашифрованного диска с использованием резервной копии ключа шифрования.
Уязвимости существующих решений	• злоумышленник может получить доступ к информации, хранящейся на съёмных носителях, в случае их утраты или кражи; • при работе с конфиденциальной информаций на разных компьютерах возможен несанкционированный доступ к конфиденциальной информации со стороны других пользователей, а также возможно случайное или преднамеренное искажение или порча конфиденциальной информации.

7. Защита данных при резервном копировании

Существующие риски	1. Утеря или кража съёмных носителей с резервными копиями конфиденциальной информации. 2. Несанкционированный доступ к резервным копиям конфиденциальной информации, хранящейся на съёмных носителях.
Назначение	• защита конфиденциальной информации и персональных данных, сохраняемых системой резервного копирования.
Архитектура решения	
Сценарий использования	1. Создание средствами Secret Disk 4 виртуального зашифрованного диска (файла-контейнера). 2. Размещение пользователями на зашифрованном диске файлов с конфиденциальной информацией и/или персональными данными. 3. Создание резервной копии ключа шифрования виртуального зашифрованного диска. 4. Сохранение резервных копий зашифрованного диска системой резервного копирования на съёмные носители. 5. Хранение съёмных дисков с резервными копиями зашифрованного диска в безопасном хранилище. 6. Восстановление файла-контейнера зашифрованного диска средствами системы резервного копирования и подключение зашифрованного диска в случае необходимости.
Уязвимости существующих решений	• злоумышленник может получить доступ к информации, хранящейся на съёмных носителях системы резервного копирования, в случае их утраты или кражи.

Угрозы и контрмеры

Внешние угрозы		
Источник угроз	Пример воздействия угрозы	Контрмеры, реализуемые с помощью Secret Disk 4
Злоумышленник, получивший физический доступ к персональному компьютеру и/или дискам с конфиденциальными данными и обладающий возможностью привлечения значительных вычислительных ресурсов для получения доступа к данным. **Постороннее лицо, получившее легальный доступ к серверу (например, при сервисном обслуживании**) **Стихийное бедствие (пожар, наводнение), проникновение в ИС, физическое проникновение чужих лиц в помещение**	Персональный компьютер целиком или только носители с конфиденциальной информацией были похищены с целью извлечения информации. Мобильный компьютер был утерян или украден во время выездной работы сотрудника. Персональный компьютер и/или диск, содержащий конфиденциальную информацию, был отправлен для ремонта в стороннюю организацию или в технический отдел. Экстренная эвакуация оборудования (например, в случае пожара) требует его выключения. Экстренное выключение, особенно во время выполнения операций шифрования данных, может привести к нарушению целостности информации на дисках.	• Криптографическая защита данных на жестких и съемных дисках методом их «прозрачного» шифрования. Данные на защищенных дисках всегда хранятся в зашифрованном виде. Даже в случае изъятия компьютера или утери съемного диска данные невозможно использовать. • Для криптографической защиты данных могут применяться проверенные временем стойкие алгоритмы шифрования, предоставляемые: ▪ криптографическим драйвером режима ядра, входящего в состав Microsoft Windows (алгоритмы AES с длиной ключа 256 бит, TripleDES с длиной ключа 168 бит); ▪ поставщиком службы криптографии КриптоПро CSP, Signal-COM CSP или Infotecs CSP (алгоритм ГОСТ 28147-89 с длиной ключа 256 бит); ▪ подключаемым внешним пакетом дополнительных алгоритмов шифрования Secret Disk Crypto Pack (алгоритмы AES с длиной ключа 128 и 256 бит, Twofish с длиной ключа 256 бит). • Регулярная смена ключа защищенного диска и/или алгоритма шифрования. Смена ключа выполняется как одна операция. Для смены ключа и/или алгоритма шифрования не требуется сначала расшифровывать данные (тем самым временно снимать с них защиту), а затем их зашифровывать с новым ключом и/или алгоритмом шифрования. Операция смены ключа выполняется в один проход, благодаря чему в любой момент времени данные надежно защищены. • Сетевой доступ к зашифрованным данным запрещён. • Система защиты от сбоев гарантирует целостность данных при сбоях электропитания и в других нештатных ситуациях. • Режим энергосбережения для ноутбуков – операции шифрования, перешифрования и расшифрования диска приостанавливаются, если ноутбук переходит на питание от внутренних батарей. При возобновлении питания от сети приостановленный процесс автоматически продолжится. • Клавиши быстрого реагирования позволяют мгновенно отключить зашифрованные диски в случае проникновения злоумышленников в офис.

Внутренние угрозы		
Источник угроз	Пример воздействия угрозы	Контрмеры, реализуемые с помощью Secret Disk 4
«Любопытный» сотрудник	Социальная инженерия. Попытка под различными предлогами получить аутентификационные данные / полномочия для администрирования Secret Disk, установленным на персональном компьютере. Пользователь имеет возможность получить физический доступ к персональному компьютеру во время отсутствия его владельца. Пользователь может получить доступ по сети к дискам другого персонального компьютера. Пользователь, работающий на компьютере общего пользования, имеет возможность получить доступ к файлам других пользователей данного компьютера.	• Двухфакторная аутентификация администраторов безопасности и зарегистрированных пользователей Secret Disk 4 с использованием цифровых сертификатов X.509: для выполнения административных задач и получения доступа к зашифрованным данным надо иметь персональный цифровой сертификат X.509, установленный в памяти eToken, и знать PIN-код. Таким образом, недостаточно узнать только PIN-код или только завладеть eToken – необходимы оба фактора. Пропажу eToken пользователю легко обнаружить и сообщить о ней для принятия необходимых дополнительных мер по защите информации. • При отключении электронного ключа eToken, доступ к защищенным данным автоматически блокируется. Без электронного ключа и знания PIN-кода невозможно получить доступ к защищенной информации во время отсутствия владельца персонального компьютера. • Данные, обрабатываемые пользователями и хранящиеся на защищенных дисках, не доступны по сети. • Доступ к защищенным дискам возможен только при наличии электронного ключа eToken и знания PIN-кода. Администратор безопасности Secret Disk 4 разграничивает доступ к защищенным дискам для разных пользователей.
Администратор домена Windows	Администратор домена Windows имеет неограниченный доступ ко всем компьютерам домена, в том числе к содержимому их дисков по сети через административные сетевые ресурсы и в режиме удаленного рабочего стола.	• Secret Disk 4 запрещает прямой сетевой доступ к защищенным дискам даже для администратора домена через административные сетевые ресурсы.

Дополнительная информация

Aladdin – надежность, безопасность, совместимость	
Сертификаты безопасности	Secret Disk 4 сертифицирован ФСТЭК (сертификат №1742 от 24 декабря 2008 года) на соответствие Заданию по безопасности и имеет оценочный уровень доверия ОУД1 (усиленный) в соответствии с требованиями руководящего документа "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий", (Гостехкомиссия России, 2002). Secret Disk 4 может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно, а также ИСПДн до класса 2 включительно. Secret Disk 4 базируется на использовании электронных ключей eToken PRO. Сертификаты безопасности на ключи eToken: • Сертификат №925/5 ФСТЭК России (для защиты конфиденциальной информации и использования в АС до класса "1Г" вкл, а также для применения в ИСПДн до 2 класса включительно) • FIPS 140-1 Level 2 (на весь ключ) • FIPS 140-1 Level 3 (физическая защищенность) • ITSec LE4 (на чип смарт-карты) • ITSec LE4 (на Операционную систему смарт-карты) • ITSec LE4 (на реализацию цифровой подписи) • Common Criteria, Уровень – EAL 4/5 • Экспертное заключение Службы Безопасности Украины (на соответствие требованиям нормативных документов систем технической защиты информации с уровнем доверия Г2 оценки корректности реализации заявленных функций, на соответствие стандартам реализованных в eToken PRO и RTE 3.0 криптографических алгоритмов)
Награды и дипломы за eToken, обеспечивающий безопасный доступ	• «Лучший продукт в области информационной безопасности» – Национальная отраслевая премия по безопасности «ЗУБР-2005» • Лауреат премии «Лучший продукт в области информационной безопасности» («Национальная отраслевая премия по безопасности», 2004 г.) • «Технология 2003 года» - диплом и Памятный знак (Аппарат Совета Безопасности РФ, Комитет Государственной Думы по безопасности, журнал «Бизнес и безопасность в России») • «Информатизация правоохранительных систем - ИПС-2001» -диплом (Академия управления МВД России, Международная Академия информатизации) • «Продукт года» – диплом (Аппарат Совета Безопасности РФ, Комитет Государственной Думы по безопасности, журнал «Бизнес и безопасность в России») • «За достижения в индустрии безопасности» (ITE Group) • 2003—SC Awards Council «Best Encryption Solution» Winner • 2003—Readers Trust Award «Best Encryption Solution» Finalist • 2003—SC Awards Council «Best Communication Security» Highly Commended • 2003—SC Awards Council «Best Access Control» Highly Commended • 2002—Principle Award «Best Security Hardware» Winner • 2002—SC Awards Council «Best Encryption Solution» Highly Commended • 2001—Principle Award «Best Security Hardware» Winner • 2001—Readers Trust Award «Best Encryption Product» Commended
Сертификаты совместимости от ведущих вендоров (на eToken)	• Microsoft (Designed for Windows XP) • Cisco Systems (Cisco Systems Verified, Cisco AVVID Partner) • Computer Associates (CA Smart Certified Solution) • Novell (Novell NMAS Partner) • IBM Corporation (Ready for Tivoli) • Check Point Software Technologies (OPSEC Certified) • Entrust (Entrust Ready) • RSA Security (RSA Keon Ready, RSA SecurID Ready, RSA ACE/Server 5 Ready)

	• SAP AG (SAP Certified Integration) • Baltimore (PKIWorld partner program, Technology Partner) • VeriSign

Secret Disk 4 – Мобильность и удобство использования	
Необходимо ли ждать завершения операций шифрования?	Не требуется, все операции зашифрования, перешифрования и расшифрования проводятся в фоновом режиме и не мешают обычной работе пользователя персонального компьютера. Все операции шифрования могут быть приостановлены и продолжены по желанию пользователя.
Используются ли дополнительные устройства считывания для подключения идентификаторов к компьютеру?	USB-ключи eToken PRO, eToken NG-OTP и eToken NG-FLASH напрямую подключаются к USB-порту, дополнительных считывателей не требуется. При использовании смарт-карт eToken PRO требуется любой PC/SC-совместимый карт-ридер, например, ASEDrive, поставляемый компанией Aladdin.
Есть ли система централизованного контроля и управления идентификаторами, обработки потерянных или вышедших из употребления идентификаторов, дистанционного восстановления данных в памяти идентификаторов?	TMS (Token Management System), производитель - Aladdin.
Инфраструктура	
Техническая поддержка от производителя / поставщика на русском языке	Есть.
Наличие необходимых лицензий у поставщика, разрешений на экспорт/импорт идентификаторов	Aladdin имеет все необходимые лицензии ФСТЭК России и ФСБ России на деятельность в области разработки, производства, услуг, распространения средств защиты и защищенных систем (не вкл. гостайну), а также необходимые разрешения на ввоз/вывоз eToken.
Наличие интеграторов, имеющих опыт и специалистов по внедрению решения	Десятки партнеров Aladdin по всей территории РФ с опытом внедрения «под ключ» решений на основе Secret Disk.

