

SECRET DISK® SERVER NG

Комплекс защиты конфиденциальной информации и персональных данных на сервере от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия

Краткая справочная информация

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

Аннотация

В данном документе в краткой табличной форме приведена основная справочная информация по продукту Secret Disk Server NG, разработанному компанией Аладдин Р.Д.

Полное или частичное копирование, использование, а также публичные ссылки на данный документ недопустимы без письменного разрешения на это компании Аладдин Р.Д.

Вопросы или пожелания по содержанию настоящего документа направляйте по адресу techwriters@aladdin-rd.ru.

Содержание

1.	Краткая информация о продукте	3
2.	Технические данные	7
3.	Типовые сценарии установки	10
4.	Типовые сценарии использования	17
5.	Угрозы и контрмеры	21

1. Краткая информация о продукте

Параметр	Описание
Краткое описание	Secret Disk Server NG – комплекс защиты конфиденциальной информации и персональных данных на сервере от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия
Краткое функциональное описание	Secret Disk Server NG – комплекс защиты конфиденциальной информации и персональных данных на сервере, обеспечивающий: <ul style="list-style-type: none">• защита от несанкционированного доступа баз данных, корпоративной почты и другой информации на дисках сервера;• двухфакторную аутентификацию администраторов с помощью электронных ключей и смарт-карт JaCarta / eToken;• предоставление доступа к конфиденциальным данным только доверенным сотрудникам;• многопользовательскую и коллективную работу с защищёнными данными;• возможность экстренного предотвращения несанкционированного доступа к данным;• сокрытие наличия на сервере конфиденциальной информации.
Решаемые задачи	Защита конфиденциальной информации от несанкционированного доступа со стороны: <ul style="list-style-type: none">○ злоумышленников, получивших физический доступ к носителям данных (жёстким дискам), в том числе в случае проникновения в офис компании;○ посторонних лиц, которые могут 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).
Основные потребители	Коммерческие организации, использующие либо планирующие внедрение информационных систем, обрабатывающих критически важные для их бизнеса данные, кража, модификация или утечка которых может привести к ощутимым потерям, например: <ul style="list-style-type: none">• персональные данные;• 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.

Параметр	Описание
<p>Ключевые функции \ возможности</p>	<p>Безопасность</p> <ul style="list-style-type: none"> ○ Шифрование данных. Защищённые данные всегда хранятся в зашифрованном виде. Даже в случае изъятия компьютера или утери диска данные невозможно использовать. Для защиты данных могут применяться стойкие алгоритмы шифрования, предоставляемые: <ul style="list-style-type: none"> ○ подключаемым внешним пакетом дополнительных алгоритмов шифрования Secret Disk Crypto Pack (алгоритмы AES и Twofish); ○ поставщиком службы криптографии КриптоПро CSP, Signal-COM CSP или Vipnet CSP (алгоритм ГОСТ 28147-89); ○ криптографическим драйвером режима ядра, входящего в состав Microsoft Windows (алгоритмы AES и TripleDES). ○ Аппаратная двухфакторная аутентификация администратора при загрузке операционной системы, и работе с зашифрованными дисками: необходимо не только обладать электронным ключом, но и знать пароль к нему. ○ Возможность использования сертифицированных криптопровайдеров. При установке дополнительных поставщиков криптографии (криптопровайдеров) Secret Disk Server NG позволяет защищать данные в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая". Поддерживаются криптопровайдеры КриптоПро CSP, Signal-COM CSP, Infotecs CSP. ○ Экстренное блокирование доступа к данным по сигналу «тревога». Сигнал может быть подан как внешним устройством (например, «красной кнопкой», радиобрелком, охранной сигнализацией или по GSM-каналу), так и с клавиатуры компьютера или мышь. Реакцию на сигнал «тревога» можно настроить как для сервера в целом, так и для каждого зашифрованного диска в отдельности. Перед отключением диска по сигналу «тревога» может быть выполнена остановка сервисов и служб (например, MS SQL Server, MS Exchange Server и т.п.). Возможна интеграция с охранной сигнализацией и системой контроля доступа в помещения. ○ Запрет доступа по сети к зашифрованным данным. Имеется возможность запрета сетевого доступа к защищаемым данным, что предотвращает копирование важных данных злоумышленником с расширенными правами администратора сети. <p>Надёжность</p> <ul style="list-style-type: none"> ○ Восстановление доступа к защищённым данным. В случае утери или поломки электронного ключа в Secret Disk Server NG предусмотрена возможность резервного восстановления доступа к данным. ○ Защита от сбоев во время установки защиты. Процесс шифрования диска может быть приостановлен или даже прерван, например, из-за перебоев электропитания, однако это не повлечёт за собой потерю данных. Приостановленный или прерванный процесс шифрования может быть возобновлён в любой удобный момент. По завершении процесса шифрования всё содержимое диска становится зашифрованным, что обеспечивает надёжную криптографическую защиту хранящихся на нём данных. ○ Поддержка кластеров. Поддерживаются отказоустойчивые кластерные конфигурации защищаемого сервера на базе Windows Server Failover Clustering. <p>Удобство</p> <ul style="list-style-type: none"> ○ Фоновые операции шифрования. Все операции зашифрования, расшифрования и перешифрования проводятся в фоновом режиме. Во время выполнения этих операций пользователи могут работать в обычном режиме. ○ Централизованное/удалённое администрирование позволяет выполнять все задачи по обслуживанию Secret Disk Server NG через интерфейс консоли управления Microsoft или через удалённый рабочий стол. Это устраняет необходимость физического доступа к серверу. При удалённом управлении электронный ключ администратора подключается не к серверу, а к рабочей станции администратора. Сетевой трафик сеанса администрирования защищён при помощи шифрования, что исключает его несанкционированное прослушивание или модификацию. ○ Расширение защищённых дисков при их заполнении. Защищённые диски могут быть созданы на основе томов динамических жёстких дисков. При этом поддерживается их расширение штатными средствами Microsoft Windows. <p>Совместимость</p> <ul style="list-style-type: none"> ○ Поддержка современных серверных операционных систем. Система Secret Disk Server NG работает в операционных системах семейства Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2. Поддерживаются как 32-битные, так и 64-битные редакции операционных систем. ○ Поддержка многопроцессорных систем и технологии Hyper-Threading. В Secret Disk

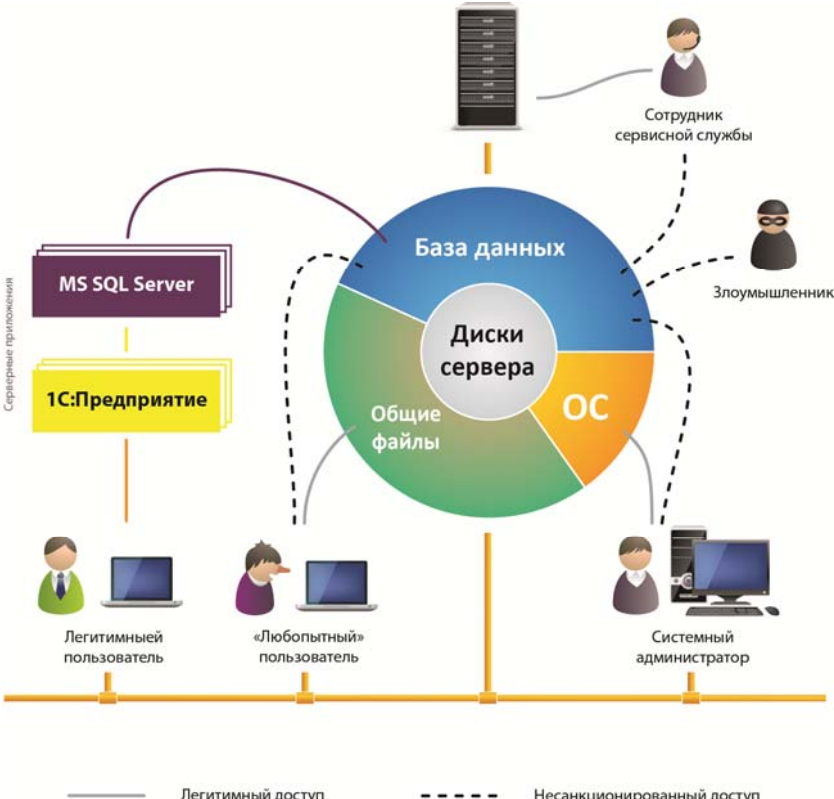
Параметр	Описание
	<p>Server NG поддерживается распараллеливание криптографических вычислений, тем самым обеспечивается рост производительности при применении на многоядерных системах или системах с использованием технологии Hyper-Threading.</p> <ul style="list-style-type: none"> ○ Поддержка работы в виртуальных средах. Secret Disk Server NG поддерживает работу в виртуальных средах, таких как VMware, Hyper-V и другие. ○ Поддержка широкого спектра накопителей позволяет защищать отдельные жёсткие диски сервера, любые дисковые массивы (SAN, программные и аппаратные RAID-массивы), а также съёмные диски. ○ Поддержка цифровых сертификатов стандарта X.509 позволяет легко интегрировать Secret Disk Server NG 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 Server NG сам создаст все необходимые для работы сертификаты.
<p>Сертификаты ФСТЭК, ФСБ</p>	<ul style="list-style-type: none"> ○ Secret Disk Server NG версии 3.2 сертифицирован ФСТЭК (сертификат №1487 от 02 ноября 2007 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 Server NG может использоваться при создании автоматизированных систем до класса защищённости 1Г включительно. ○ Электронные ключи (токены и смарт-карты) eToken и JaCarta, поддерживаемые в продукте, имеют сертификаты соответствия № 925/5 и №1883 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. ○ Имеется возможность применения Secret Disk Server NG совместно с сертифицированными поставщиками средств криптографии (КриптоПро CSP, Vipnet CSP и Signal-COM CSP).
<p>Внедрение и техническая поддержка</p>	<p>Внедрение и сопровождение продукта и решений с его использованием может осуществляться партнёрами компании "Аладдин Р.Д."</p> <p>Гарантийный период на продукт составляет 12 мес.</p>
<p>Лицензирование</p>	<ul style="list-style-type: none"> ○ Secret Disk Server NG для файловых серверов позволяет защищать информацию на дисках сервера, предоставленных в общий доступ по сети. Предлагаются лицензии файл-сервера с ограничением на количество одновременных подключений по сети ко всем защищённым дискам сервера (лицензии файл-сервера на 5, 10, 25, 50, 100, 150, 250 пользователей), либо без такого ограничения (лицензия файл-сервера на неограниченное количество пользователей). ○ Secret Disk Server NG для серверов приложений позволяет защищать от несанкционированного копирования и неавторизованного доступа расположенные на сервере файлы корпоративных баз данных, почтовые хранилища, данные приложений. При наличии лицензии сервера приложений на сервере можно создавать защищённые диски, доступ к которым будут иметь только приложения, исполняемые на самом сервере (например, Microsoft SQL Server) и пользователи, имеющие право локального входа на сервер. Доступ к этим дискам по сети невозможен (даже для администратора домена Windows через административные сетевые ресурсы). Файлы баз данных, почтовые хранилища, данные бизнес-приложений, расположенные на таком защищённом диске, недоступны по сети и могут обрабатываться только приложениями, исполняющимися на сервере. Лицензия сервера приложений не ограничивает число серверных приложений, которые могут работать с данными на защищённом диске, а также число пользователей этих приложений, работающих через приложение с данными на защищённом диске. ○ Комбинированная лицензия Secret Disk Server NG позволяет защищать серверы, выполняющие одновременно функции и сервера приложений, и файлового сервера на 10 или 25 пользователей.
<p>Системные требования</p>	<p>Сервер:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2012 R2 (64-бит) • Microsoft Windows Server 2012 (64-бит). • Microsoft Windows Server 2008 R2 (64-бит); • Microsoft Windows Server 2008 Service Pack 2 (32-бит или 64-бит); • Microsoft Windows Server 2003 R2 Service Pack 2 (32-бит или 64-бит); • Microsoft Windows Server 2003 Service Pack 2 (32-бит или 64-бит).

Параметр	Описание
	<p>Интерфейс администратора:</p> <ul style="list-style-type: none">• Microsoft Windows 8.1 (32-бит или 64-бит)• Microsoft Windows 8 (32-бит или 64-бит)• Microsoft Windows 7 Service Pack 1 (32-бит или 64-бит)• Microsoft Windows Vista Service Pack 2 (32-бит или 64-бит)• Microsoft Windows XP Service Pack 3 (32-бит или 64-бит)• Microsoft Windows Server 2012 R2 (64-бит)• Microsoft Windows Server 2012 (64-бит)• Microsoft Windows Server 2008 R2 (64-бит)• Microsoft Windows Server 2008 Service Pack 2 (32-бит или 64-бит)• Microsoft Windows Server 2003 R2 Service Pack 2 (32-бит или 64-бит)• Microsoft Windows Server 2003 Service Pack 2 (32-бит или 64-бит) <ul style="list-style-type: none">○ Установленные драйверы для JaCarta или eToken○ 1 Гигабайт свободной оперативной памяти○ 20 мегабайт свободного пространства на диске.○ При использовании совместно с сертифицированными российскими поставщиками криптографии – установленный КриптоПро CSP, Vipnet CSP, либо Signal-COM CSP.
Модели поддерживаемых электронных ключей	<ul style="list-style-type: none">○ USB-токены и смарт-карты JaCarta PKI;○ USB-токены и смарт-карты eToken PRO (Java);○ Комбинированный USB-токен eToken NG-FLASH (Java);○ Комбинированный USB-токен eToken NG-OTP (Java);○ eToken PRO Anywhere.


2. Технические данные

Параметр	Описание
<p>Схема работы</p>	<p>The diagram illustrates the architecture of Secret Disk Server NG. At the center is a server disk labeled 'Диски сервера', divided into five segments: 'Зашифрованные данные' (red), 'Данные приложений' (green), 'Файлы общего доступа' (blue), 'ОС' (yellow), and 'Данные пользователей' (orange). Above the disk are 'Серверные приложения' including 'Почтовый сервер', 'Сервер терминалов', and 'СУБД'. Below the disk is a 'Локальная сеть' (local network) with icons for 'Доверенный пользователь', 'Пользователь', 'Системный администратор', and 'Администратор безопасности'. A legend below the diagram explains the color coding: red for encrypted data with controlled access; green for encrypted data with trusted user access; orange for encrypted data with server application access only; yellow for non-encrypted data; and blue for non-encrypted data with full network access. It also defines line types: grey for data access and red for user management.</p>
<p>Компоненты системы</p>	<ul style="list-style-type: none"> ○ Сервер — компонент Secret Disk Server NG, осуществляющий операции с дисками и защищённым хранилищем ключевой информации. ○ Интерфейс администратора — оснастка консоли управления Microsoft (MMC), позволяющая администратору управлять серверной частью Secret Disk Server NG, в том числе с удалённого компьютера. ○ Электронный ключ администратора — электронный ключ, в памяти которого содержится лицензия администратора Secret Disk Server NG, позволяющая выполнять администрирование Secret Disk Server NG. ○ Электронный ключ сервера — электронный ключ, который содержит лицензию на Secret Disk Server NG. ○ Secret Disk Alarm Service («красная» кнопка) — инструменты для подачи сигнала «тревога», приводящего к запуску на сервере команд, предназначенных для предотвращения несанкционированного доступа к информации в чрезвычайных ситуациях.
<p>Пользователи системы и доступные им функции</p>	<p>Администраторы Secret Disk Server NG:</p> <ul style="list-style-type: none"> • устанавливают Secret Disk Server на серверах • осуществляют удалённое управление сервером Secret Disk Server NG через интерфейс администратора (создают зашифрованные диски, выполняют операции резервного копирования ключей, управляют доступом пользователей к защищаемым данным) <p>Офицер безопасности</p> <ul style="list-style-type: none"> • имеет возможность одним нажатием «красной кнопки», подключённой к его рабочей станции, отключить защищённые диски и удалить хранилище с ключами, тем самым полностью заблокировав доступ к данным.


	<p>Зарегистрированные пользователи:</p> <ul style="list-style-type: none">• имеют доступ к данным пользователей по сети• могут обращаться к общим файлам на незашифрованных дисках по сети, при наличии прав доступа к таким общим файлам• не имеют прямого доступа к защищённым данным приложений (к примеру, хранящимся в базе «1С Предприятие»), доступ возможен только через интерфейс этих приложений. <p>Незарегистрированные пользователи, включая системного администратора:</p> <ul style="list-style-type: none">• не имеют доступа ни к данным пользователей, ни к защищённым данным приложений, ни к средствам администрирования• могут обращаться к общим файлам на незашифрованных дисках по сети, при наличии прав доступа к таким общим файлам
<p>Принципы работы системы</p>	<ul style="list-style-type: none">○ Защита информации обеспечивается шифрованием данных «на лету». При чтении данных с диска происходит их расшифрование, при записи на диск — шифрование. Находящиеся на диске данные всегда зашифрованы. Алгоритм шифрования выбирается администратором при создании защищённого диска и может быть изменён в любой момент в процессе работы.○ Защищённый диск можно подключать и отключать. Отключённый защищённый диск выглядит как неформатированный. С подключённым защищённым диском вы работаете точно так же, как с обычным диском. Для того чтобы подключить защищённый диск, необходимо обладать смарт-картой или электронным ключом администратора, знать его пароль и иметь соответствующие полномочия как на уровне сервера в целом, так и по отношению к данному диску.○ При прямом просмотре содержимое отключённого защищённого 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 Server NG обеспечивает защиту конфиденциальной информации от несанкционированного доступа, а также сокрытие наличия данных на компьютере.○ При обращении к инструментам управления Secret Disk Server NG администратор должен подключить к компьютеру свой электронный ключ, указать свой сертификат и ввести пароль.○ Процесс шифрования диска может быть приостановлен администратором или даже прерван (например, из-за перебоев электропитания) - это не повлечёт за собой потерю данных. Приостановленный или прерванный процесс шифрования может быть возобновлён в любой удобный момент. По завершении процесса шифрования все содержимое диска становится зашифрованным, что обеспечивает надёжную криптографическую защиту хранящихся на нем данных.○ На сервере может быть зарегистрировано произвольное число администраторов Secret Disk Server NG. Любой администратор может добавить нового администратора, однако добавляемый администратор будет иметь доступ только к тем дискам, к которым имеет доступ добавляющий.○ По умолчанию все администраторы равноправны по отношению ко всем защищённым дискам сервера. Вместе с тем в Secret Disk Server NG предусмотрена возможность, коллективной работы администраторов с разграничением доступа: каждому защищённому диску можно сопоставить свой уникальный список администраторов, имеющих полномочия управлять данным защищённым диском.○ Пользователи обращаются к защищённым дискам по сети в зависимости от полномочий, определяемых операционной и файловыми системами. В качестве альтернативы многопользовательского доступа к данным на защищённом диске можно использовать запрет сетевого доступа, например, для дисков, на которых хранятся корпоративные базы данных. Непосредственно обращаться к данным на таком диске будут только соответствующие приложения, установленные на сервере. А пользователи смогут работать с данными не напрямую, а только через интерфейс этих приложений. Доступ по сети к содержимому такого подключённого защищённого диска невозможно будет получить никому, даже администратору домена Windows (через административные сетевые ресурсы).○ В состав Secret Disk Server NG входит программно-аппаратный комплекс Secret Disk Alarm Service, состоящий из программного обеспечения и «красной кнопки». Если в результате возникновения нештатной ситуации возникает угроза несанкционированного доступа к данным, хранящимся на защищённых дисках, нажатие «красной кнопки» приводит к выполнению на сервере команд, экстренно предотвращающих несанкционированный доступ. В частности, предусмотрены

<p>Типовая схема хранения данных на сервере предприятия (без применения Secret Disk Server NG)</p>	<p>несколько режимов отключения защищённых дисков и полное удаление защищённого хранилища.</p> 
<p>Недостатки данной схемы</p>	<ul style="list-style-type: none"> ○ Возможен доступ к данным со стороны следующих лиц: ○ Злоумышленник (человек, сознательной целью которого является получение доступа к вашим конфиденциальным данным), получивший физический доступ к серверу 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). ○ Любопытный сотрудник – сотрудник организации (по роду своей деятельности не имеющий доступа к конфиденциальным данным), который может воспользоваться ошибками администрирования или повысить свой уровень полномочий в операционной системе до административного с целью скопировать интересующие файлы (базу данных, хранилище электронных писем). ○ Системный администратор (администратор домена Windows) по умолчанию имеет самый высокий уровень прав доступа и имеющий возможность обратиться по сети к любому диску сервера . ○ Нет возможности оперативного отключения, сокрытия или уничтожения конфиденциальной информации, хранящейся на жёстком диске, в случае возникновения нестандартных ситуаций.


3. Типовые сценарии установки

ОДИН КОМПЬЮТЕР	
Описание	Все компоненты Secret Disk Server NG установлены на одном компьютере.
Архитектура	 <p>«Красная кнопка»</p> <p>Охранная сигнализация</p> <p>Радиоприемник</p> <p>Радио-брелок</p> <p>Secret Disk Server NG</p> <ul style="list-style-type: none"> • Сервер • Рабочая станция администратора • Рабочая станция для подачи сигнала «тревога» <p>Домен Windows</p> <p>— Сигнал «тревога» — Работа с данными</p>
Особенности	Данный сценарий может рекомендоваться только в исключительных случаях, например, при острой нехватке квалифицированного ИТ-персонала.
Преимущества	<ul style="list-style-type: none"> ○ нет внешних признаков наличия установленных компонент Secret Disk Server NG на компьютерах сотрудников (подключённые «красные кнопки», ПО для подачи сигнала тревога, консоль управления и т.д.); ○ никто из сотрудников организации (за исключением системного администратора и администратора Secret Disk Server NG) не знает об установке и использовании Secret Disk Server NG.
Недостатки	<ul style="list-style-type: none"> ○ отсутствие возможности удалённого управления сервером; ○ отсутствие возможности подачи сигнала «тревога» с удалённой рабочей станции; ○ ограниченная дальность подачи сигнала «тревога» с помощью радио-брелока (не более 50 метров от самого сервера).


СЕРВЕР И РАБОЧАЯ СТАНЦИЯ АДМИНИСТРАТОРА

<p>Описание</p>	<p>Серверный компонент установлен на сервер, интерфейс администратора установлен на рабочую станцию администратора.</p>
<p>Архитектура</p>	
<p>Особенности</p>	<ul style="list-style-type: none"> ○ для управления сервером Secret Disk Server NG через удалённый рабочий стол, необходимо установить на сервере как компонент «сервер», так и интерфейс администратора; ○ для управления сервером с помощью консоли управления Microsoft интерфейс администратора должен быть установлен на рабочей станции администратора; ○ для того чтобы были доступны оба способа удалённого управления, необходимо установить интерфейс администратора на оба компьютера; ○ на рабочей станции администратора должен быть установлен драйвер электронного ключа, а для подачи сигнала «тревога» — и Secret Disk Alarm Service. Последний также можно установить как на сервер, так и на рабочую станцию администратора; ○ поскольку для регистрации первого администратора Secret Disk Server NG необходимы административные полномочия на сервере, то при использовании консоли управления Microsoft рабочая станция администратора и сервер должны входить в один и тот же домен или в домены, между которыми установлены доверительные отношения.
<p>Преимущества</p>	<ul style="list-style-type: none"> ○ возможность удалённого управления сервером; ○ возможность подачи сигнала «тревога» с удалённой рабочей станции; ○ значительно увеличивается дальность подачи сигнала «тревога» с помощью радиобрелока (50 метров от рабочей станции для подачи сигнала «тревога», которая, в свою очередь, может быть удалена от сервера в пределах топологии сети); ○ ограничен круг лиц, знающих об установке в организации Secret Disk Server NG (системный администратор и администратор Secret Disk Server NG).

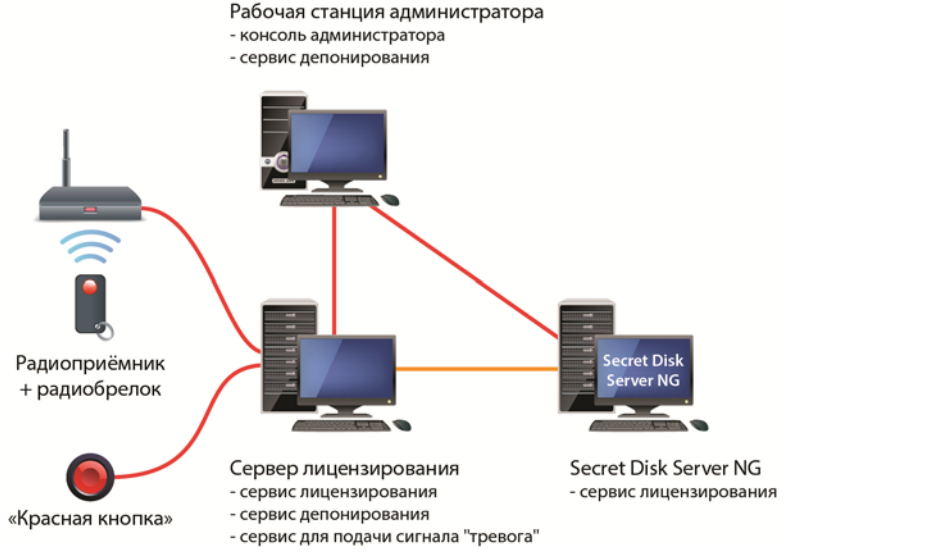
ВЫДЕЛЕННАЯ РАБОЧАЯ СТАНЦИЯ ДЛЯ ПОДАЧИ СИГНАЛА «ТРЕВОГА»

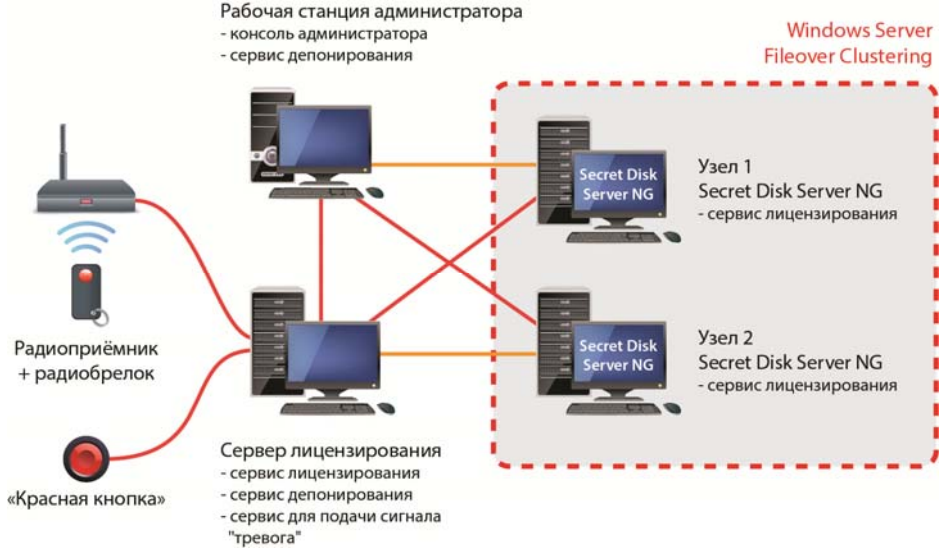
<p>Описание</p>	<p>Аналогичен сценарию с сервером и рабочей станцией администратора, но присутствует отдельная рабочая станция для подачи сигнала «тревога».</p>
<p>Архитектура</p>	
<p>Особенности</p>	<ul style="list-style-type: none"> ○ Для осуществления управления сервером Secret Disk Server NG через удалённый рабочий стол Вам необходимо установить на сервере как компонент «сервер», так интерфейс администратора. ○ Если для управления сервером Вы хотите подключаться к нему через консоль управления Microsoft, то интерфейс администратора должен быть установлен на Вашей рабочей станции. Для того чтобы Вам были доступны оба способа удалённого управления, установите интерфейс администратора на оба компьютера. ○ В любом случае, на рабочей станции администратора должен быть установлен драйвер электронного ключа. ○ Secret Disk Alarm устанавливается на отдельной рабочей станции (на одной или нескольких). Кроме того, при желании его можно установить также и на сервере, и на рабочей станции администратора. ○ Поскольку для регистрации первого администратора Secret Disk Server NG необходимы административные полномочия на сервере, при использовании консоли управления Microsoft рабочая станция администратора и сервер должны входить в один и тот же домен или в домены, между которыми установлены доверительные отношения. ○ Данный сценарий может быть рекомендован в большинстве случаев. Однако при наличии в организации службы охраны рекомендуется использовать следующий сценарий.
<p>Преимущества</p>	<ul style="list-style-type: none"> ○ возможность удалённого управления сервером; ○ возможность подачи сигнала «тревога» с удалённой рабочей станции; ○ нет ограничения дальности подачи сигнала «тревога» с помощью радио-брелока (50 метров от рабочей станции для подачи сигнала «тревога», которая, в свою очередь, может быть удалена от сервера в пределах топологии сети).
<p>Недостатки</p>	<p>Наличие внешних признаков установленных компонент Secret Disk Server NG на компьютерах сотрудников (подключённые «красные кнопки», ПО для подачи сигнала «тревога», консоль управления).</p>

ПОДАЧА СИГНАЛА «ТРЕВОГА» СЛУЖБОЙ ОХРАНЫ	
Описание	Сценарий аналогичен предыдущему случаю, но в качестве рабочей станции для подачи сигнала «тревога» может выступать компьютер сотрудника службы охраны.
Архитектура	
Особенности	<ul style="list-style-type: none"> ○ В качестве рабочей станции для подачи сигнала «тревога» может выступать, например, компьютер офицера безопасности. Этот компьютер может не быть членом доверенного домена, на нем обычно устанавливается ПО для систем контроля и управления доступом (СКУД). ○ Данный сценарий может быть рекомендован при наличии в организации службы охраны.
Преимущества	<ul style="list-style-type: none"> ○ возможность удалённого управления сервером; ○ возможность подачи сигнала «тревога» с удалённой рабочей станции; ○ нет ограничения дальности подачи сигнала «тревога» с помощью радио-брелока (50 метров от рабочей станции для подачи сигнала «тревога», которая, в свою очередь, может быть удалена от сервера в пределах топологии сети).


НЕСКОЛЬКО СЕРВЕРОВ	
Описание	Ситуация, аналогичная описанным выше сценариям, но в пределах одного домена Windows присутствуют несколько серверов Secret Disk Server NG.
Архитектура	 <p>Рабочая станция администратора</p> <p>«Красная кнопка»</p> <p>Радиоприемник</p> <p>Рабочая станция для подачи сигнала «тревога»</p> <p>Радио-брелок</p> <p>Secret Disk Server NG</p> <p>Secret Disk Server NG</p> <p>Secret Disk Server NG</p> <p>— Сигнал «тревога» — Управление SDS NG</p>
Особенности	<ul style="list-style-type: none"> ○ при необходимости защиты данных на нескольких серверах Вы можете приобрести дополнительные электронные ключи сервера или лицензии сервера для имеющихся у Вас ключей и установить компонент «сервер» на каждом из этих серверов; ○ управление несколькими серверами Secret Disk Server NG можно осуществлять централизованно. Для этого нужно использовать подключение к удалённым рабочим столам или на рабочей станции администратора подготовить консоль управления Microsoft с несколькими оснастками Управление Secret Disk Server, подключёнными к разным серверам; ○ в Secret Disk Alarm Service предусмотрена возможность подачи сигнала «тревога» одновременно нескольким серверам.
Преимущества	<ul style="list-style-type: none"> ○ Централизованное администрирование и сопровождение серверов с одной рабочей станции (запуск/останов, подключение/отключение дисков, подача сигнала «тревога»); ○ нет ограничения дальности подачи сигнала «тревога» с помощью радио-брелока (50 метров от рабочей станции для подачи сигнала «тревога», которая, в свою очередь, может быть удалена от сервера в пределах топологии сети).

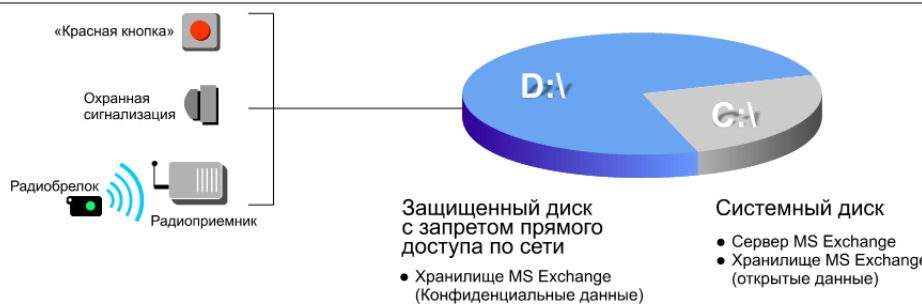
ИСПОЛЬЗОВАНИЕ СЕРВИСА ДЕПОНИРОВАНИЯ ДАННЫХ

<p>Описание</p>	<p>Серверный компонент установлен на сервере, интерфейс администратора установлен на рабочую станцию администратора, а программное обеспечение для подачи сигнала тревога – на сервер лицензирования.</p>
<p>Архитектура</p>	 <p>Рабочая станция администратора - консоль администратора - сервис депонирования</p> <p>Радиоприёмник + радиобрелок</p> <p>«Красная кнопка»</p> <p>Сервер лицензирования - сервис лицензирования - сервис депонирования - сервис для подачи сигнала "тревога"</p> <p>Secret Disk Server NG - сервис лицензирования</p>
<p>Особенности</p>	<ul style="list-style-type: none"> ○ Сервер лицензирования - выделенная рабочая станция, которая должна работать в режиме 24/7. ○ Управление удаленными серверами, на которых установлен Secret Disk Server NG можно осуществлять централизованно, с одной рабочей станции администратора. Для этого нужно использовать подключение к удаленным рабочим столам или на рабочей станции администратора подготовить консоль управления Microsoft с несколькими оснастками Управление Secret Disk Server, подключенными к разным серверам. ○ В Secret Disk Alarm Service предусмотрена возможность централизованной подачи сигнала "тревога" с одной рабочей станции на все удаленные серверы.
<p>Преимущества</p>	<ul style="list-style-type: none"> ○ Выделенный сервер лицензирования позволяет избавиться от необходимости подключения электронных ключей с лицензиями к серверу с установленным Secret Disk Server, тем самым скрывая на нем наличие средств защиты. ○ Возможность удаленного централизованного управления серверами. ○ Возможность подачи сигнала "тревога" с удаленной рабочей станции. ○ Снижение совокупной стоимости владения информационной системой за счет централизованных процедур администрирования и уменьшения числа приобретаемых лицензий администратора Secret Disk Server NG. ○ Нет ограничения дальности подачи сигнала "тревога" с помощью радиобрелока (50 метров от рабочей станции для подачи сигнала "тревога", а рабочая станция может быть удалена от сервера в пределах топологии сети).

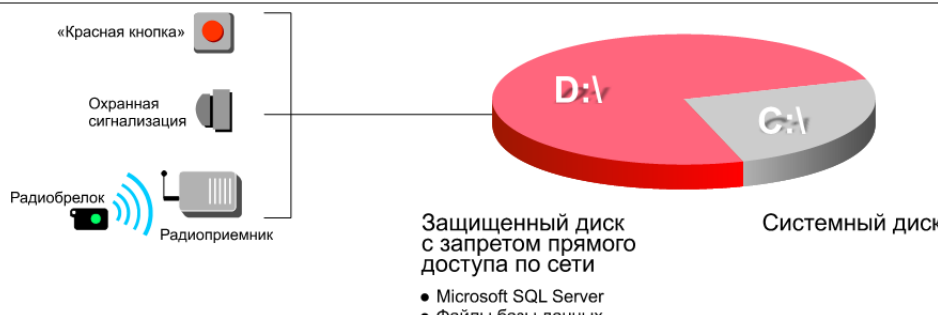
КЛАСТЕР	
Описание	Серверный компонент установлен на узлах кластера, интерфейс администратора на рабочую станцию администратора, а программное обеспечение для подачи сигнала тревога – на сервер лицензирования.
Архитектура	
Особенности	<ul style="list-style-type: none"> ○ Сервер лицензирования - выделенная рабочая станция, которая должна работать в режиме 24/7. ○ Управление узлами кластера, на которых установлен Secret Disk Server NG можно осуществлять централизованно, с одной рабочей станции администратора. Для этого нужно использовать подключение к удаленным рабочим столам или на рабочей станции администратора подготовить консоль управления Microsoft с оснасткой Управление Secret Disk Server, подключенной к узлам кластера. ○ В Secret Disk Alarm Service предусмотрена возможность централизованной подачи сигнала "тревога" с одной рабочей станции на все узлы кластера.
Преимущества	<ul style="list-style-type: none"> ○ Использование отказоустойчивых кластеров для создания файлового хранилища. ○ Сервер лицензирования позволяет хранить все электронные ключи с лицензиями сервера на одном компьютере. ○ Возможность удаленного централизованного управления узлами кластера. ○ Возможность подачи сигнала "тревога" с удаленной рабочей станции. ○ Снижение совокупной стоимости владения информационной системой за счет централизованных процедур администрирования и уменьшения числа приобретаемых лицензий администратора Secret Disk Sever NG. ○ Нет ограничения дальности подачи сигнала "тревога" с помощью радиобрелока (50 метров от рабочей станции для подачи сигнала "тревога", а рабочая станция может быть удалена от сервера в пределах топологии сети).

4. Типовые сценарии использования

ЗАЩИТА ДАННЫХ НА ФАЙЛ-СЕРВЕРЕ	
Задача	<ul style="list-style-type: none"> ○ Защита конфиденциальной информации, хранящейся на файл-сервере (в том числе находящейся в общем доступе), от несанкционированного доступа в обход встроенных в операционную систему средств аутентификации, авторизации и контроля доступа. ○ Блокирование доступа к информации по сигналу «тревога». ○ Соккрытие факта наличия конфиденциальной информации на файл-сервере.
Архитектура решения	
Сценарий использования	<ul style="list-style-type: none"> ○ Размещение файл-сервера в охраняемом помещении. Охранная сигнализация, установленная в серверной комнате, может быть использована для подачи серверу сигнала «тревога». ○ Создание средствами Secret Disk Server NG защищённого диска достаточного объёма (с разрешением прямого доступа к нему по сети) ○ Создание резервной копии ключа шифрования защищённого диска и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных администраторах). ○ Настройка реакции на сигнал «тревога». ○ Размещение на защищённом диске файлов для общего доступа, установка прав доступа к ним на уровне файловой системы. ○ Задание прав сетевого доступа к защищенному диску (средствами операционной системы).
Дополнительные преимущества Secret Disk Server NG относительно существующих решений	<ul style="list-style-type: none"> ○ Возможность оперативного прекращения доступа к защищённым данным, при возникновении нештатных ситуаций; ○ Соккрытие факта наличия конфиденциальной информации на сервере.

ЗАЩИТА ДАННЫХ НА ПОЧТОВОМ СЕРВЕРЕ	
Задача	<ul style="list-style-type: none"> ○ Защита данных почтового сервера (почтовые ящики, общие папки и др.) от попыток прочитать файлы на уровне ОС (как обычные файлы), в обход встроенных средств аутентификации, авторизации и контроля доступа; ○ блокирование доступа к информации по сигналу «тревога»; ○ сокрытие факта наличия конфиденциальной информации на файл-сервере.
Архитектура решения¹	 <p>«Красная кнопка»</p> <p>Охранная сигнализация</p> <p>Радиобрелок</p> <p>Радиоприемник</p> <p>Защищенный диск с запретом прямого доступа по сети</p> <ul style="list-style-type: none"> ● Хранилище MS Exchange (Конфиденциальные данные) <p>Системный диск</p> <ul style="list-style-type: none"> ● Сервер MS Exchange ● Хранилище MS Exchange (открытые данные)
Сценарий использования	<ul style="list-style-type: none"> ○ Размещение почтового сервера в охраняемом помещении. Охранная сигнализация, установленная в серверной комнате, может быть использована для подачи сигнала «тревога» серверу. ○ Создание средствами Secret Disk Server NG защищённого диска достаточного объёма и запрет прямого доступа по сети к нему. ○ Создание резервной копии ключа шифрования защищённого диска и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных администраторов). ○ Настройка реакции на сигнал «тревога». ○ Установка ПО почтового сервера и файлов почтового хранилища на защищённом диске. ○ Определение сценариев, которые будут выполняться после подключения защищённого диска (запуск почтового сервера) и перед отключением защищённого диска (завершение работы почтового сервера).
Дополнительные преимущества Secret Disk Server NG относительно существующих решений	<ul style="list-style-type: none"> ○ Злоумышленник не может скопировать файлы хранилища почтового сервера (локально или по сети), посмотреть их содержимое или восстановить данные на новый сервер. ○ Возможность оперативного прекращения доступа к защищённым данным, при возникновении нештатных ситуаций (обнаружение вторжения в ИС, физическое проникновение чужих лиц в помещение, пожар и пр.). ○ Сокрытие факта наличия конфиденциальной информации на сервере.
ЭТО ВАЖНО ЗНАТЬ!	<ul style="list-style-type: none"> ○ Использование почтовых клиентов, обеспечивающих шифрование локального почтового ящика пользователя, решает задачу защиты уже полученных писем. Однако если письмо было отослано в незашифрованном виде, то в процессе доставки оно будет храниться в открытом виде на всех промежуточных почтовых серверах, а на почтовом сервере получателя оно будет храниться в открытом виде вплоть до момента его загрузки почтовым клиентом (если письма не хранятся на сервере). ○ В течение всего времени хранения (а это может быть от нескольких минут до нескольких дней или даже недель) злоумышленник, получивший доступ к файлам почтового хранилища на сервере, может прочесть письмо.

¹ На примере Microsoft Exchange Server

ЗАЩИТА ДАННЫХ НА СЕРВЕРЕ ПРИЛОЖЕНИЙ (1С, SAP И ДР.)	
Задача	<ul style="list-style-type: none"> ○ Защита данных бизнес-приложений (в том числе баз данных) от попыток прочесть файлы на уровне ОС (как обычные файлы) в обход встроенных в бизнес-приложения средств аутентификации, авторизации и контроля доступа; ○ блокирование доступа к информации по сигналу «тревога»; ○ сокрытие факта наличия конфиденциальной информации на сервере приложений.
Архитектура решения¹	 <p>«Красная кнопка»</p> <p>Охранная сигнализация</p> <p>Радиобрелок</p> <p>Радиоприемник</p> <p>Защищенный диск с запретом прямого доступа по сети</p> <ul style="list-style-type: none"> • Microsoft SQL Server • Файлы базы данных <p>Системный диск</p>
Сценарий использования	<ul style="list-style-type: none"> ○ Размещение сервера в охраняемом помещении. Охранная сигнализация, установленная в серверной комнате, может быть использована для подачи серверу сигнала «тревога». ○ Создание средствами Secret Disk Server NG защищенного диска достаточного объема и запрет прямого доступ по сети к нему. ○ Создание резервной копии ключа шифрования защищенного диска и/или резервной копии защищенного хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных администраторов). ○ Настройка реакции на сигнал «тревога». ○ Размещение данных бизнес-приложения на созданном защищенном диске. ○ Определение сценариев, которые будут выполняться после подключения защищенного диска и перед отключением защищенного диска (остановка бизнес-приложения).
Дополнительные преимущества Secret Disk Server NG относительно существующих решений	<ul style="list-style-type: none"> ○ Злоумышленник не может скопировать файлы бизнес-приложения (локально или по сети), произвести прямой просмотр их содержимого или восстановление данных на новом сервере; ○ Возможность оперативного прекращения доступа к защищенным данным, при возникновении нештатных ситуаций (обнаружение вторжения в ИС, физическое проникновение чужих лиц в помещение, пожар и пр.). ○ Сокрытие факта наличия конфиденциальной информации на сервере.

¹ На примере защиты СУБД Microsoft SQL Server

ЗАЩИТА ДАННЫХ НА ТЕРМИНАЛЬНЫХ СЕРВЕРАХ

Задача	<ul style="list-style-type: none">○ Защита данных, находящихся на локальных дисках терминального сервера, от несанкционированного доступа, в том числе – от их копирования пользователями терминального сервера на свои локальные рабочие станции;○ блокирование доступа к информации по сигналу «тревога»;○ сокрытие факта наличия конфиденциальной информации на сервере приложений.
Сценарий использования	<ul style="list-style-type: none">○ Размещение терминального сервера в охраняемом помещении. Охранная сигнализация, установленная в серверной комнате, может быть использована для подачи серверу сигнала «тревога».○ Создание средствами Secret Disk Server NG защищённого диска достаточного объёма и запрет прямого доступ по сети к нему.○ Создание резервной копии ключа шифрования защищённого диска и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных администраторах).○ Настройка реакции на сигнал «тревога».○ Размещение данных и приложений, с которыми осуществляется работа на терминальном сервере, на защищённом диске.○ Настройка работы терминального сервера для запрещения подсоединения запоминающих устройств локального компьютера пользователя с помощью средств удалённого рабочего стола.○ В целях защиты конфиденциальной информации от копирования на терминальном сервере не следует устанавливать приложения, способные передавать данные по сети.
Уязвимости существующих решений	<ul style="list-style-type: none">○ Возможность оперативного прекращения доступа к защищённым данным, при возникновении нештатных ситуаций (обнаружение вторжения в ИС, физическое проникновение чужих лиц в помещение, пожар и пр.).○ Сокрытие факта наличия конфиденциальной информации на сервере.

5. Угрозы и контрмеры

ВНЕШНИЕ УГРОЗЫ		
Источник угроз	Пример воздействия угрозы	Меры противодействия, реализуемые с помощью Secret Disk Server NG
<p>Злоумышленник, получивший физический доступ к серверу и/или диску с конфиденциальными данными и обладающий возможностью привлечения значительных вычислительных ресурсов для получения доступа к данным.</p> <p>Постороннее лицо, получившее легальный доступ к серверу (например, при сервисном обслуживании)</p> <p>Стихийное бедствие (пожар, наводнение), проникновение в ИС, физическое проникновение чужих лиц в помещение</p>	<p>Сервер целиком или только носители с конфиденциальной информацией были похищены с целью извлечения информации.</p> <p>Сервер, содержащий конфиденциальную информацию, был отправлен для ремонта в стороннюю организацию или в технический отдел.</p> <p>Часть дисков в массиве RAID сервера были заменены на новые в ходе регулярного сервисного обслуживания, и старые диски (с которых можно извлечь информацию) были использованы для других нужд.</p> <p>Экстренная эвакуация оборудования (например, в случае пожара) требует его выключения. Экстренное выключение может привести к нарушению целостности информации на дисках.</p>	<ol style="list-style-type: none"> Криптографическая защита данных на жёстких и съёмных дисках методом их «прозрачного» шифрования. Данные на защищённых дисках всегда хранятся в зашифрованном виде. Даже в случае изъятия сервера или утери съёмного диска данные невозможно использовать. Для криптографической защиты данных могут применяться проверенные временем стойкие алгоритмы шифрования, предоставляемые: <ul style="list-style-type: none"> подключаемым внешним пакетом дополнительных алгоритмов шифрования Secret Disk Crypto Pack (алгоритмы AES и Twofish); поставщиком службы криптографии КриптоПро CSP, Signal-COM CSP или Vipnet CSP (алгоритм ГОСТ 28147-89); криптографическим драйвером режима ядра, входящего в состав Microsoft Windows (алгоритмы AES и TripleDES). Регулярное перешифрование защищённых дисков со сменой ключа и/или алгоритма шифрования. Перешифрование диска выполняется как одна операция. Не надо сначала расшифровывать данные (тем самым временно снимая с них защиту), а затем зашифровывать данные с новым ключом и/или по другому алгоритму. Данные всегда надёжно защищены. Сетевой трафик сеанса администрирования криптографический защищён, что исключает его прослушивание или подмену злоумышленником. Сигнал «тревога» может быть подан как внешним устройством (например, «красной кнопкой», радиобрелком или охранной сигнализацией), так и с помощью обычного пользовательского интерфейса (из командной строки, с использованием мыши). Реакция на сигнал «Тревога» определяется для сервера в целом и для каждого защищённого диска в отдельности. Предусмотрены возможности отключения дисков, полного удаления всех конфигурационных данных и ключевой информации. Для каждого защищённого диска могут быть определены индивидуальные сценарии. Эти сценарии могут выполняться перед подключением диска, после подключения, перед отключением, после отключения. Например, после подключения защищённого диска с файлами базы данных Microsoft SQL с помощью сценария может быть запущена сама СУБД.

ВНУТРЕННИЕ УГРОЗЫ		
Источник угроз	Пример воздействия угрозы	Меры противодействия, реализуемые с помощью Secret Disk Server NG
«Любопытный» сотрудник	<p>Социальная инженерия. Попытка под различными предложениями получить аутентификационные данные / полномочия для администрирования сервера.</p> <p>Пользователь, работающий с файлами на общем диске сервера (но не являющийся сотрудником финансового отдела), имеет доступ к файлам базы данных 1С (расположенным на том же диске) и имеет возможность сделать полную копию файлов БД.</p>	<ol style="list-style-type: none"> 1. 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 электронного ключа, и знать пароль. Таким образом, недостаточно узнать только пароль или только завладеть электронным ключом – необходимы оба фактора. Пропажу электронного ключа пользователю легко обнаружить и сообщить о ней для принятия необходимых дополнительных мер по защите информации. 2. Данные, обрабатываемые приложениями, выполняющимися на сервере, могут быть расположены на защищённых дисках с запретом прямого доступа по сети к их содержимому. Таким образом, файлы БД не могут быть скопированы пользователями на локальный компьютер. 3. При защите файлового сервера серверная лицензия определяет максимальное количество одновременных подключений по сети ко всем защищённым дискам.
Администратор домена Windows	<p>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.</p> <p>Ошибки администрирования.</p>	<ol style="list-style-type: none"> 1. Для каждого защищённого диска нужно определить, будет ли он доступен по сети или только приложениям, выполняющимся непосредственно на сервере. При запрете средствами Secret Disk Server NG прямого сетевого доступа к защищённому диску он также становится недоступен для администратора домена через административные сетевые ресурсы. 2. Основным интерфейсом администратора Secret Disk Server NG является оснастка консоли управления Microsoft. Эта оснастка встроена в консоль управления компьютером и хорошо знакома администраторам, что значительно уменьшает вероятность случайных ошибок при администрировании.



Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО «Аладдин Р. Д.». Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией «Аладдин Р. Д.» без предварительного уведомления. В данном документе компания «Аладдин Р. Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО «Аладдин Р. Д.».

Владельцем товарных знаков Apple, iPad, iPhone, Mac OS, OS X является корпорация Apple Inc. Владелец товарного знака IOS является компания Cisco (Cisco Systems, Inc). Владелец товарного знака Windows Vista и др. — корпорация Microsoft (Microsoft Corporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

Телефон: +7 (495) 223-00-01
Факс: +7 (495) 646-64-40
aladdin@aladdin-rd.ru
www.aladdin-rd.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (бессрочно), № 2874 от 18.05.12 Microsoft Silver OEM Hardware Partner, Oracle Gold Partner, Apple Developer

Лицензия ФСБ России № 12632 Н от 20.12.12

Сертификат соответствия СМК ГОСТ Р ИСО 9001-2011

© 1995–2014, ЗАО «Аладдин Р. Д.»
Все права защищены

