Secret Disk

Система защиты конфиденциальной информации и персональных данных, хранящихся и обрабатываемых на персональных компьютерах, ноутбуках или серверах

Версия: 1.2

Редакция от: 11 января 2016 г.

Листов: 27

Автор: Илья Щавинский

Аннотация

Развитие информационных технологий приводит к тому, что проблемы информационной безопасности с каждым годом становятся всё более актуальными и одновременно более сложными. Технологии обработки информации непрерывно совершенствуются, а вместе с ними меняются и практические методы обеспечения информационной безопасности.

Большинство корпоративных решений ИБ, в которые инвестируются крупные средства, фактически направлены на защиту периметра. Однако непосредственно саму корпоративную информацию, данные, которые хранятся в файлах и базах данных также необходимо защищать на всех уровнях и на протяжении всего жизненного цикла.

Как предотвратить несанкционированный доступ к конфиденциальным данным? Как обеспечить защиту информации на корпоративных серверах и разграничить права доступа к данным? Как защитить информацию на съёмных носителях? Как защитить личные данные от системного администратора? Как одновременно совместить удобство и безопасность?

Компания "Аладдин Р.Д." предлагает ряд решений, которые помогают обеспечить необходимый уровень защиты информационных систем. Среди них специализированные продукты линейки Secret Disk – современные и удобные решения для защиты данных на персональных компьютерах, ноутбуках, серверах и системах хранения данных при помощи криптографии.

Настоящий документ посвящён продуктам линейки Secret Disk и ориентирован на широкий круг пользователей: ИТ-менеджеров, администраторов информационной безопасности и руководителей всех уровней. В нём рассмотрены основные риски, связанные с компрометацией конфиденциальной информации, и методы защиты персональных компьютеров и серверов от несанкционированного доступа к данным.

Оглавление

Оценка рисков и последствия нарушения безопасности

До определения требований к системе защиты данных и оценки стоимости решения необходимо определить и понять потенциальные риски при работе с конфиденциальной информацией.

Угрозы информации на персональных компьютерах и ноутбуках

Ежедневно в различных организациях обрабатывается огромное количество информации. Удалённые офисы, "мобильная работа" сотрудников в командировках, надомная работа – всё это предполагает обмен данными между персональными компьютерами и центральными информационными системами. Службы ИБ обычно внимательно соблюдают основные требования безопасности передачи данных, но как только информация достигает персонального устройства, она зачастую оказывается вне периметра корпоративной защиты. Её дальнейшая защита нередко ограничивается только пользовательским паролем на доступ к персональному компьютеру.

Пример зарубежной практики: только в аэропортах США каждую неделю теряется 12 тысяч ноутбуков. Суммарная стоимость потерянных за год устройств оценивается около миллиарда долларов, при этом стоимость утечки корпоративных данных оценивается уже в 25 миллиардов долларов убытков в год.

Прежде всего, персональные вычислительные системы подвержены следующим угрозам.

- По данным статистики, в большинстве случаев проблемы с утечкой информации происходят по вине обслуживающего персонала, администраторов, сотрудников служб поддержки и т.д. Как правило, это люди, которые имеют доступ к конфиденциальным данным.
- Ноутбук с корпоративной информацией может быть утерян или украден, при этом стоимость утраченного оборудования не слишком высока, а данные быстро восстанавливаются при помощи систем резервного копирования. Однако стоимость конфиденциальной информации или последствия её утечки могут быть весьма существенны, а в некоторых случаях - разрушительны для бизнеса. Удивительно, но количество потерь ноутбуков увеличивается с каждым годом. По статистике, более 76% компаний теряют хотя бы один ноутбук в год, из них только 22% потерь связано с кражами.
- Вне офиса любой сотрудник подвержен мошенничеству и обману, а конфиденциальные данные - копированию.
- Четверо из десяти руководителей предприятий сталкиваются с недобросовестными сотрудниками или партнёрами, которые при помощи различных технических или организационных приёмов хотя бы раз осуществляли несанкционированный доступ к компьютерам с конфиденциальной информацией внутри офиса.
- Конфиденциальные данные могут быть скопированы со съёмных носителей во время хранения и транспортировки. Съёмный носитель может быть просто украден.

Угрозы информации в корпоративных информационных системах

Информационные системы, несмотря на то, что их сервера расположены внутри корпоративного периметра безопасности, также подвержены различным угрозам.

- Системные администраторы, обслуживающий персонал, сотрудники сервисного центра - все они могут иметь доступ к серверному оборудованию. Злоумышленник может скопировать данные или похитить жёсткие диски для последующего анализа.

- Системный администратор или ИТ-специалист с расширенными правами администратора может иметь несанкционированный сетевой доступ к конфиденциальным данным на сервере. Например, на сервере может находиться конфиденциальная база данных, с которой работают приложения. Доступ к приложениям строго регламентирован, но у злоумышленника остаётся возможность, используя расширенные права администратора, осуществить сетевой доступ напрямую к базе данных.
- В случае проникновения в офис или центр обработки данных злоумышленник может получить физический доступ к оборудованию.
- Конфиденциальные данные могут остаться на жёстких дисках, которые вывели из эксплуатации в процессе профилактики оборудования. Учёт и контроль таких дисков, как правило, ослаблен.
- Конфиденциальная информация может остаться на серверном оборудовании, которое было утилизировано. "Любопытный" сотрудник сервисной компании может проявить повышенный интерес и попытаться восстановить данные.

БЕЗОПАСНОСТЬ УЧЁТНЫХ СИСТЕМ

Учётные системы являются объектом особой важности и привлекают повышенное внимание злоумышленников, так как содержат максимум информации о деятельности предприятия. Нерешённые задачи безопасности и конфиденциальности финансовой информации могут привести к самым серьёзным последствиям, вплоть до потери бизнеса.

Пример угрозы для учётных систем "1С": стандартные способы разграничения прав доступа в "1С" не работают для многих распространённых угроз, например, кражи баз данных. Злоумышленник может осуществить доступ к хранилищам информации через сетевой доступ, в обход приложений "1С".

Требования законодательства по защите персональных данных (152-ФЗ)

С 1 января 2011 года полностью вступил в силу (начали действовать санкции за неисполнение требований) Федеральный закон от 27.07.2006 года № 152-ФЗ "О персональных данных". Основная цель закона — защитить права и свободы человека при обработке его личной информации, в том числе право на неприкосновенность частной жизни, личную и семейную тайну.

Согласно этому закону, любая организация, обрабатывающая персональные данные, должна обеспечить их конфиденциальность.

ЧЕМ ГРОЗИТ НЕИСПОЛНЕНИЕ ЗАКОНА (КРАТКАЯ ВЫДЕРЖКА)

- Нарушение условий, предусмотренных законодательством при осуществлении деятельности в области защиты информации — нарушение установленного законом порядка сбора, хранения, использования или распространения информации влечёт **наложение административного штрафа на должностных лиц** — в размере от одной тысячи до одной тысячи пятисот рублей; на юридических лиц — в размере от десяти тысяч до пятнадцати тысяч рублей, а также **приостановку деятельности организации** (или её подразделения) на срок до 90 суток.
- Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации влечёт **наложение административного штрафа на граждан** в размере от пятисот до одной тысячи рублей **с конфискацией несертифицированных средств защиты информации**, на должностных лиц — в размере от одной тысячи до двух тысяч рублей, а на юридических лиц — в размере от десяти тысяч до двадцати тысяч рублей с конфискацией несертифицированных средств.
- Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечёт уголовную ответственность), лицом, которое имело к ней доступ по служебным или профессиональным обязанностям, влечёт **наложение административного штрафа на должностных лиц** — в размере от четырёх тысяч до пяти тысяч рублей.
- Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование

информации, нарушение работы ЭВМ, системы ЭВМ или их сети, — **наказывается штрафом, либо исправительными работами** сроком от шести месяцев до одного года, **либо лишением свободы** сроком до двух лет.

- 24 февраля 2015 года депутаты Госдумы РФ в первом чтении одобрили инициативу Правительства РФ об **увеличении до 30 раз штрафов** для граждан, должностных и юридических лиц, а также индивидуальных предпринимателей, которые без согласия субъекта занимаются обработкой его персональных данных.

Некоторые примеры и последствия атак на конфиденциальные данные

ПОТЕРИ НОУТБУКОВ

В исследовании Ponemon Institute приняли участие 275 крупных европейских организаций. В результате было установлено, что за 12 месяцев ими было утрачено 72 789 ноутбуков — 265 ноутбуков на каждую компанию. Большая часть из них была утеряна во время поездок (32%) или во время работы за пределами офиса (32%). В 13% случаев утеря ноутбука имела место в рабочей обстановке. Ещё в 13% случаев респонденты не смогли уточнить, где именно они потеряли свои ноутбуки. Отмечается, что лишь 4,5% утраченных ноутбуков возвращались к владельцам.

Убытки вследствие каждой утери ноутбука значительно превышают стоимость нового устройства, и 275 опрошенных организаций ежегодно теряют около 1,29 миллиардов евро из-за утраченных ноутбуков, что составляет около 4,7 миллионов евро на каждую из них.

Ранее проводилось аналогичное исследование и в США. Тогда было опрошено 329 организаций, которыми было утеряно более 86 тысяч ноутбуков, а совокупная величина финансовых потерь составила 2,1 миллиардов долларов.

Сегодня точных данных по России нет, но очевидно, что ситуация будет похожая.

ПРИМЕРЫ И ПОСЛЕДСТВИЯ НЕКОТОРЫХ РЕАЛЬНЫХ АТАК НА КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ

- Горячий спор о краже коммерческой тайны разгорелся между российскими машиностроительными предприятиями, концерном "Тракторные заводы" (КТЗ) и ООО "ЧТЗ-Уралтрак", созданным на базе Челябинского тракторного завода. Гендиректор "ЧТЗ-Уралтрак", ранее работавший в КТЗ, организовал с помощью своих бывших коллег хищение конструкторской документации, касающейся серийно изготавливаемых изделий и перспективных разработок. По предварительным оценкам владельцев коммерческой тайны, им был нанесён крупный ущерб, свыше 50 миллионов рублей (по данным портала Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций: http://pd.rsoc.ru/press-service/subject1/news2289.htm).
- В январе 2011 года база данных клиентов крупнейшего телеком-оператора Vodafone была опубликована в сети. Имена, домашние адреса, номера водительских удостоверений и данные по кредитным картам стали доступны в сети, попав туда "по неосторожности". Эта утечка привела компанию к судебному разбирательству, а также потере доверия клиентов. Более 9000 клиентов подали иск, Vodafone старается максимально оперативно уладить ситуацию (по данным портала Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций: http://pd.rsoc.ru/press-service/news628.htm).
- В результате действий инсайдера Bank of America лишился 10 миллионов долларов. По утверждению представителей банка, инсайдер работал в подразделении, непосредственно отвечающем за безопасность клиентов и противодействие мошенничеству. Он, в частности, контролировал работу сторонних подрядчиков и имел доступ к финансовой информации клиентов. Сообщается, что злоумышленник продал имеющуюся у него информацию мошенникам. Среди скомпрометированных данных номера социального страхования, адреса электронной почты и телефонные номера клиентов банка (из открытых источников: http://www.hardnsoft.ru/news/news_software/15482/).

- Национальная служба здравоохранения США National Health Service признала потерю записей о здоровье более 10 миллионов пациентов. Сообщается, что в сети клиник и госпиталей, относящихся к NHS, зафиксирован целый ряд утечек медицинской информации о пациентах в связи с утерями флеш-накопителей, ноутбуков, дисков с резервными копиями. В отдельных случаях в руках посторонних оказались, помимо прочих данных, номера социального страхования (по данным аналитического центра InfoWatch).
- 4 миллиона 230 тысяч записей пациентов были скомпрометированы в результате кражи одного ноутбука из головного офиса Sutter Health в Сакраменто. По словам представителя Sutter Health, около 3,3 миллионов записей содержали имена, адреса, номера телефонов, e-mail, медицинские регистрационные номера и названия страховых планоы пациентов (по данным аналитического центра InfoWatch).

Построение системы защиты данных

Мероприятия по обеспечению информационной безопасности не приносят доходов. С их помощью можно лишь уменьшить ущерб от возможных инцидентов. Поэтому очень важно, чтобы затраты на создание и поддержание ИБ на должном уровне были соразмерны с ценностью активов организации и связанных с ней информационных систем.

При выборе средств защиты информации целесообразно найти ответы на следующие вопросы:

- Какие существуют источники угроз конфиденциальным данным?
- Каковы будут требования к системам и подсистемам защиты данных?
- Насколько эффективны доступные меры защиты?
- Насколько уязвимы подсистемы средств защиты?

Уровень защиты данных должен соответствовать рискам бизнеса в случае их потерь или потери конфиденциальности, а сами средства защиты должны удовлетворять требованиям регуляторов.

Источники угроз

Злоумышленник — человек, сознательной целью которого является получение доступа к Вашим конфиденциальным данным. Злоумышленник действует целенаправленно и может привлекать значительные технические ресурсы (например, вычислительные мощности) для получения доступа к интересующей его информации. Злоумышленник может постараться применить целый комплекс мер, включая социальную инженерию, физический доступ к компьютеру или серверу с конфиденциальными данными и т.д.

Перечень потенциальных злоумышленников, которые могут получить доступ к конфиденциальным данным, оказывается весьма внушительным.

- Постороннее лицо — например, сотрудник сервисной организации, куда был сдан сервер на ремонт/профилактику.
- "Любопытный" сотрудник — сотрудник организации, который по роду своей деятельности не должен иметь доступа к конфиденциальным данным, но желающий с ними ознакомиться. Скорее всего, такой человек не станет применять целенаправленные действия по получению доступа к конфиденциальным данным, но он может воспользоваться ошибками администрирования, например, возможностью просмотра содержимого диска с конфиденциальной информацией по сети.
- Легальный пользователь системы — сотрудник, обладающий правом доступа к информационной системе, но недостаточными полномочиями для доступа к конфиденциальной информации. Такой человек может попытаться повысить свой уровень полномочий до административного, например, с целью копирования интересующих его файлов (база данных, хранилище электронных писем) для их последующего просмотра.
- Администратор операционной системы – сотрудник, который, по умолчанию, имеет самый высокий уровень прав доступа. Системный администратор имеет возможность обратиться по сети к любому диску сервера с помощью так называемых "административных сетевых ресурсов" вида \\server\D$.

Не следует забывать и о роли "человеческого фактора". В случае ошибки администратора при настройке прав доступ к конфиденциальным данным может получить любой пользователь.

Также источником угроз являются компьютерные вирусы, сетевые черви и троянские программы. Если список программного обеспечения, устанавливаемого на сервере, всегда известен, и само программное обеспечение, как правило, свободно от вирусов, то компьютеры пользователей могут быть заражены вирусами и/или содержать троянские программы.

Используя параметры учётной записи пользователя, работающего в данный момент за заражённым компьютером, вирус может выполнять сканирование сетевых ресурсов и пытаться прочитать

хранящиеся на них файлы. Если таким пользователем является администратор, то вирусу становится доступно содержимое дисков сервера через административные сетевые ресурсы.

Общие требования к системе защиты данных

Каждая организация имеет свой подход к формированию требований к системе защиты данных, при этом учитываются отраслевая специфика, необходимость соблюдения требований регуляторов и множество других факторов.

ОБЩИЕ ТРЕБОВАНИЯ К РЕШЕНИЯМ ПО ЗАЩИТЕ ДАННЫХ

- Обеспечение защиты конфиденциальных данных от:
  - несанкционированного доступа по сети предприятия;
  - несанкционированного доступа через сеть Интернет;
  - несанкционированного физического доступа к оборудованию.
- Сокрытие факта наличия и расположения на персональном компьютере или сервере конфиденциальных данных.
- Обеспечение защиты данных на съёмных носителях.
- Разграничение прав пользователей на доступ к защищённой информации.
- Обеспечение надёжной процедуры подтверждения прав пользователей.
- Обеспечение непрерывного доступа к защищаемым данным для легальных пользователей.
- Обеспечение простоты и удобства использования системы защиты для пользователя.
- Обеспечение централизованного управления системой защиты данных.
- Обеспечение соответствия требованиям регуляторов.

Способы защиты конфиденциальных данных

ШИФРОВАНИЕ

Применение средств шифрования решает задачу ограничения доступа к конфиденциальной информации – никто посторонний, получив доступ к Вашему компьютеру или серверу, не сможет прочитать закрытые данные.

Для злоумышленника зашифрованный диск не отличается от любого другого неформатированного диска. Он не может ни прочесть данные, хранящиеся на нём, ни использовать их против Вас. Используемые современные алгоритмы шифрования с большой длиной ключа гарантируют надёжную защиту и стойкость к взлому даже при помощи высокопроизводительной вычислительной техники.

ОСНОВНЫЕ ТРЕБОВАНИЯ К ШИФРОВАНИЮ ДАННЫХ

- Стойкость защиты должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод шифрования.
- Используемый алгоритм шифрования не должен иметь слабых мест, которыми могли бы воспользоваться криптоаналитики.
- Ключ шифрования должен быть недоступен для злоумышленника. Несоблюдение принципов безопасного использования ключей шифрования может поставить под угрозу защищённость информации, даже при том, что в системе будут реализованы самые криптостойкие алгоритмы.
- Шифрование должно происходить максимально "прозрачно" для пользователя – пользователь не замечает процесса зашифрования и расшифрования данных во время работы.
- Система должна быть максимально устойчива к случайным ошибкам и неправильным действиям пользователей.

АУТЕНТИФИКАЦИЯ

Выполнение проверки прав пользователей на доступ к защищаемым данным является важнейшей функцией системы защиты конфиденциальной информации. Именно поэтому процесс

аутентификации часто становится целью злоумышленников при совершении атаки. Это оправдано, так как подсмотреть, украсть или подобрать пароль доступа гораздо проще, чем расшифровать защищённые данные. Вследствие этого процесс аутентификации пользователей, который полагается исключительно на пароли, не может обеспечить адекватную защиту конфиденциальных данных.

Более надёжным способом является двухфакторная аутентификация – аутентификация, в процессе которой используются аутентификационные факторы нескольких типов. Например, пользователь должен предоставить USB-ключ или смарт-карту и ввести пароль. В этом случае злоумышленник не сможет получить доступ к данным, так как ему придётся не только подсмотреть пароль, но и предъявить физическое устройство, кража которого, в отличие от кражи пароля, практически всегда быстро обнаруживается.

ЭКСТРЕННОЕ ПРЕКРАЩЕНИЕ ДОСТУПА

В чрезвычайных ситуациях, когда становится известно о попытке физического доступа или попытке изъятия серверного оборудования, крайне полезным инструментом защиты становится возможность экстренного прекращения доступа к данным. Система должна по сигналу обеспечить корректное прекращение работы с данными, зашифровать обрабатываемые в текущий момент данные и ограничить возможность доступа к ним неуполномоченным лицам.

Основные угрозы и меры противодействия

Ниже приведена таблица, демонстрирующая краткий перечень упомянутых ранее угроз и меры противодействия им.

Источники угроз	Меры противодействия
Внешние угрозы	
Злоумышленник, получивший физический доступ к вычислительному оборудованию/системам хранения конфиденциальных данных, в том числе, постороннее лицо, получившее легальный доступ к серверу (например, при сервисном обслуживании)	• Криптографическая защита данных на жёстких и съёмных дисках. Данные на зашифрованных дисках всегда хранятся в зашифрованном виде. Зашифрованный диск выглядит как неформатированный. • Сетевой трафик сеанса администрирования зашифрован, что исключает его прослушивание или подмену злоумышленником. • Подача сигнала "тревога" для экстренной блокировки доступа к данным.
"Человеческий фактор" и внутренние угрозы	
Социальная инженерия	Применение двухфакторной аутентификации, ограничивающей возможность утери/разглашения пароля доступа
Возможность получения доступа к данным через сеть предприятия, в том числе административные сетевые ресурсы ("любопытный сотрудник"/ администратор)	• Для каждого зашифрованного диска необходимо определить, будет ли он доступен пользователям по сети или только приложениям, выполняющимся непосредственно на сервере. Например, для защиты от копирования файлов корпоративной базы данных целесообразно разместить их на зашифрованном диске и запретить к нему прямой сетевой доступ пользователей • Криптографическая защита данных на жёстких и съёмных дисках
Повышение пользователем или администратором уровня своих полномочий для доступа к конфиденциальным данным	Протоколирование действий администраторов и аудит использования защищённых ресурсов и действий пользователей/ администраторов

Семейство продуктов Secret Disk

Продукты линейки Secret Disk полностью удовлетворяют всем вышеперечисленным требованиям к защите данных и обеспечивают надёжную защиту конфиденциальной информации на персональных компьютерах, ноутбуках, серверах и в системах хранения данных.

Общие принципы

Защита информации обеспечивается шифрованием данных "на лету". При записи данных на диск происходит их зашифрование, а при чтении с диска - их расшифрование. Находящиеся на диске данные всегда зашифрованы. При прямом просмотре защищённый диск выглядит как неформатированный, и нельзя определить, имеется ли на нём и где именно расположена какая-либо информация.

Все продукты линейки Secret Disk обладают надёжными механизмами подтверждения прав пользователей на доступ к защищаемой информации. Secret Disk предоставляет наиболее безопасную и надёжную процедуру подтверждения прав пользователя – двухфакторную аутентификацию. Для доступа к данным необходим защищённый электронный ключ и знание пароля к нему.

Продукты Secret Disk не имеют встроенных средств шифрования, а используют внешние, поэтому решения на основе Secret Disk не подпадают под законодательные ограничения по распространению и не требуют наличия соответствующих лицензий ФСБ России.

Для криптографической защиты данных могут применяться стойкие алгоритмы шифрования, предоставляемые:

- подключаемым внешним пакетом дополнительных алгоритмов шифрования Secret Disk Crypto Extension Pack (алгоритмы AES с длиной ключа 128 и 256 бит, Twofish с длиной ключа 256 бит);
- поставщиком службы криптографии КриптоПро CSP или Vipnet CSP (алгоритм ГОСТ 28147-89 с длиной ключа 256 бит);
- криптографическим драйвером режима ядра, входящего в состав Microsoft Windows (алгоритмы AES с длиной ключа 256 бит, TripleDES с длиной ключа 168 бит).

В продуктовой линейке Secret Disk представлены три решения:

- **Secret Disk 4** – для защиты персональных компьютеров и ноутбуков;
- **Secret Disk Server NG** – для защиты серверов приложений и систем хранения данных;
- **Secret Disk Enterprise** – для защиты персональных компьютеров и ноутбуков в корпоративной среде с централизованной системой управления.

Secret Disk 4

Secret Disk 4 – система защиты конфиденциальной информации и персональных данных на персональном компьютере или ноутбуке.

РЕШАЕМЫЕ ЗАДАЧИ

- Защита конфиденциальной информации от несанкционированного доступа со стороны:
  - злоумышленников, получивших физический доступ к носителям данных (жёстким дискам, съёмным носителям), 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, которые не обладают полномочиями для доступа к данной информации (в том числе технических специалистов и системных администраторов).

- Защита сеанса загрузки операционной системы со стороны неавторизованных лиц, которые могут иметь доступ к компьютерному оборудованию (например, сотрудники компании или сотрудники сервисного центра, обслуживающего оборудование);
- Надёжное удаление данных.

Расширенная версия Workgroup Edition включает все преимущества персональной редакции Secret Disk 4 и дополнительно даёт возможность организовать коллективную работу с конфиденциальной информацией небольшой группе пользователей (не более 10 одновременных подключений).

Сертифицированная версия Secret Disk 4 может использоваться при создании автоматизированных систем до класса защищённости 1Г включительно и комплектуется сертифицированными электронными ключами.

Secret Disk Server NG

Secret Disk Server NG – комплекс защиты конфиденциальной информации и персональных данных, хранящихся на сервере, от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия.

РЕШАЕМЫЕ ЗАДАЧИ

- Защита конфиденциальной информации от несанкционированного доступа со стороны:
  - злоумышленников, получивших физический доступ к носителям данных (жёстким дискам), в том числе в случае проникновения в офис компании.
    - В базовый комплект поставки Secret Disk Server NG входит программно-аппаратный комплекс Secret Disk Alarm, состоящий из специализированного ПО и подключаемой к порту USB кнопки тревожной сигнализации. Сигнал "тревога" позволяет отключать защищённые диски, а при определённых настройках на стороне сервера – также удалять с сервера ключевую информацию (защищённое хранилище ключей) и выполнять дополнительные наборы команд. В результате, даже если злоумышленники завладеют нужным электронным ключом или смарт-картой, узнают пароль и будут обладать полным доступом к серверу, они не смогут прочесть информацию, не располагая резервной копией защищённого хранилища.
  - сотрудников компании, не обладающих полномочиями для доступа к данной информации (в том числе технических специалистов и системных администраторов).
    - При обращении к любым инструментам управления администратор Secret Disk Server NG должен подключить к компьютеру свой электронный ключ, указать свой сертификат и ввести пароль. Таким образом, реализуется двухфакторная аутентификация администратора при обращении к элементам управления шифрованием сервера.
  - посторонних лиц, которые могут иметь доступ к компьютерному оборудованию (например, сотрудники сервисного центра, обслуживающего оборудование).
- Реализация защиты высоконагруженных, отказоустойчивых решений.
  - Secret Disk Server NG максимально эффективно использует ресурсы современных многопроцессорных систем, а также поддерживает отказоустойчивые кластерные конфигурации.

Secret Disk Enterprise

Secret Disk Enterprise – корпоративная система защиты конфиденциальной информации с централизованным управлением.

Безотказная работа системы защиты невозможна без эффективной поддержки конечных пользователей, особенно это актуально для средних и крупных организаций. Задача поддержки пользователя, у которого зашифрован жёсткий диск и который находится вне офиса, может быть трудноразрешимой без системы дистанционного централизованного управления.

Система централизованного управления должна помочь администраторам следить за состоянием безопасности на каждом компьютере. В этом случае пользователю уже не нужно самому разбираться в шифровании жёсткого диска, этим должен заниматься администратор информационной безопасности.

Кроме того, при централизованном хранении ключей шифрования предприятие защищено от потери этих ключей, ведь они хранятся на защищённом сервере и передаются пользователю по мере необходимости. Также компания контролирует доступ сотрудников к своим защищаемым данным и в любой момент может запретить такой доступ.

РЕШАЕМЫЕ ЗАДАЧИ

- Защита конфиденциальной информации от несанкционированного доступа со стороны:
  - злоумышленников, получивших физический доступ к носителям данных (жёстким дискам, съёмным носителям), 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, которые не обладают полномочиями для доступа к данной информации (в том числе технических специалистов и системных администраторов).
- Централизованное управление и интеграция в корпоративную инфраструктуру ИБ:
  - централизованное хранение и управление ключами шифрования дисков, информацией о пользователях, их связях с дисками, и т.д.;
  - удобство работы администратора ИБ благодаря администрированию через Web-портал;
  - мастер первоначальной настройки для централизованной системы управления;
  - единый центр мониторинга аккумулирует информацию об активности пользователей, ошибках, предупреждениях в журналах продукта.
- Защита сеанса загрузки операционной системы со стороны:
  - неавторизованных лиц, которые могут иметь доступ к компьютерному оборудованию (например, сотрудники компании или сотрудники сервисного центра, обслуживающего оборудование).
- Мониторинг и протоколирование действий пользователей и состояния зашифрованных ресурсов.
- Надёжное удаление данных.

Сравнение продуктов линейки Secret Disk

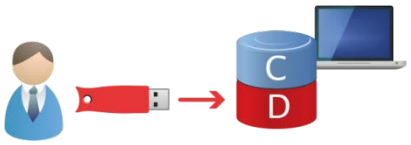
Возможности продукта	Secret Disk Enterprise	Secret Disk Server NG	Secret Disk 4
Защита данных на ноутбуках	●		●
Защита данных на рабочих станциях	●		●
Защита данных на серверах приложений		●	
Защита данных на съёмных носителях	●	●	●
Защита от копирования на внешние носители	●		
Защита разделов жёсткого диска и динамических томов	●	●	●
Защита системного раздела жёсткого диска (защита временных файлов, файлов-журналов, файла подкачки ОС и файла "спящего" режима)	●		●
Защита папок на незащищённом диске	●		
Создание виртуальных дисков (файлов-контейнеров)	●	●	●
Прозрачное ("на лету") шифрование	●	●	●
Двухфакторная аутентификация пользователей (по электронному ключу и паролю) для доступа к защищённым данным	●		●
Двухфакторная аутентификация пользователей до загрузки ОС	●		●
Двухфакторная аутентификация администратора безопасности SD	●	●	●
Централизованное управление	●	●	
Аудит использования защищённых ресурсов	●	●	●
Решение "красная кнопка" (сигнал "тревога")		●	
Наличие версии, сертифицированной ФСТЭК России	●	●	●
Поддержка криптоалгоритмов AES, TripleDES встроенными средствами и криптоалгоритмов ГОСТ 28147-89 с помощью сертифицированных криптопровайдеров	●	●	●
Защита от сбоев питания и операционной системы во время выполнения операций шифрования	●	●	●
Поддержка "спящего" (Hibernation) и "ждущего" (Stand-by) режимов	●		●
Доступ к защищённым данным по сети	●	●	●
Поддержка MS Windows 10	●		

Сценарии построения защиты корпоративной информации

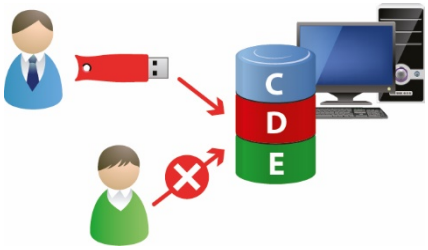
В данном разделе мы рассмотрим типовые сценарии построения корпоративной защиты при использовании решений линейки Secret Disk.

Secret Disk 4

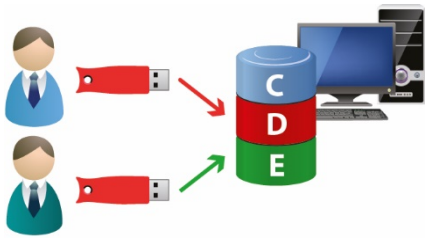
ЗАЩИТА ДАННЫХ НА НОУТБУКЕ

Ситуация	У пользователя есть ноутбук, на котором хранится конфиденциальная информация. Пользователь часто работает вне офиса (ездит в командировки, работает из дома).
Существующие риски	o Утеря или кража ноутбука. o Несанкционированное использование посторонними лицами (во время деловых поездок или в домашних условиях).
Архитектура решения	
Сценарий использования Secret Disk 4 для устранения вышеуказанных рисков	o Защита содержимого системного раздела средствами Secret Disk 4. o Создание средствами Secret Disk 4 зашифрованного диска (логического тома) достаточного объёма. o Создание и сохранение резервной копии ключа шифрования защищённого диска и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных пользователях). o Размещение на защищённом диске файлов с конфиденциальной информацией и/или персональными данными.
Дополнительные преимущества Secret Disk 4 относительно существующих решений	o Защита системного раздела. Злоумышленник не сможет получить доступ к информации, хранящейся на загрузочном диске ноутбука, в случае получения несанкционированного физического доступа к компьютеру. o Сокрытие факта наличия конфиденциальной информации на ноутбуке.

ЗАЩИТА ДАННЫХ НА ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ В ЛОКАЛЬНОЙ СЕТИ

Ситуация	Пользователь имеет персональный компьютер, подключенный к локальной сети. На компьютере хранится конфиденциальная информация.
Существующие риски	o Несанкционированный доступ к данным, хранящимся на персональном компьютере, по локальной сети. o Несанкционированное использование посторонними лицами (во время отсутствия пользователя на рабочем месте). o Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ.
Архитектура решения	
Сценарий использования Secret Disk 4 для устранения вышеуказанных рисков	o Создание средствами Secret Disk 4 защищённого диска (логического тома) достаточного объёма. o Создание диска общего пользования для хранения данных других пользователей. o Создание и сохранение резервной копии ключа шифрования защищённого диска и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных пользователях). o Размещение на защищённом диске файлов с конфиденциальной информацией и/или персональными данными.
Дополнительные преимущества Secret Disk 4 относительно существующих решений	o Возможность оперативного прекращения доступа к защищённым данным при возникновении нештатных ситуаций. o Сокрытие факта наличия конфиденциальной информации на компьютере.

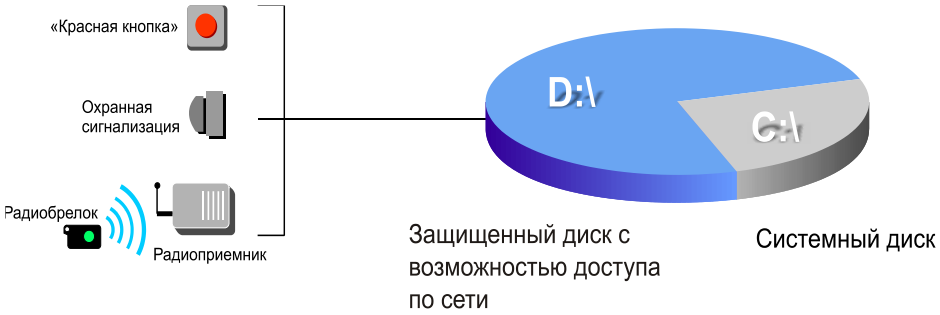
ЗАЩИТА ДАННЫХ НА МНОГОПОЛЬЗОВАТЕЛЬСКОМ КОМПЬЮТЕРЕ

Ситуация	К персональному компьютеру имеют доступ несколько пользователей (например, работа по сменам). На компьютере хранится конфиденциальная информация, к которой должны иметь доступ только определённые пользователи (не все имеющиеся пользователи, работающие с компьютером, должны иметь доступ к конфиденциальной информации, либо каждый пользователь должен работать со своими данными).
Существующие риски	o Несанкционированный доступ к данным со стороны других пользователей, допущенных к работе на персональном компьютере. o Несанкционированный доступ к данным, хранящимся на персональном компьютере, по локальной сети. o Несанкционированное использование посторонними лицами (во время отсутствия пользователя на рабочем месте). o Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ.
Архитектура решения	
Сценарий использования Secret Disk 4 для устранения вышеуказанных рисков	o Создание средствами Secret Disk 4 "персональных" зашифрованных дисков достаточного объёма для каждого пользователя, работающего за персональным компьютером. o Создание и сохранение резервных копий ключей шифрования защищённых дисков и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных пользователях). o Размещение пользователями Secret Disk 4 на доступных лично им защищённых дисках файлов с конфиденциальной информацией и/или персональными данными.
Дополнительные преимущества Secret Disk 4 относительно существующих решений	o Возможность оперативного прекращения доступа к защищённым данным при возникновении нештатных ситуаций. o Сокрытие факта наличия конфиденциальной информации на компьютере.

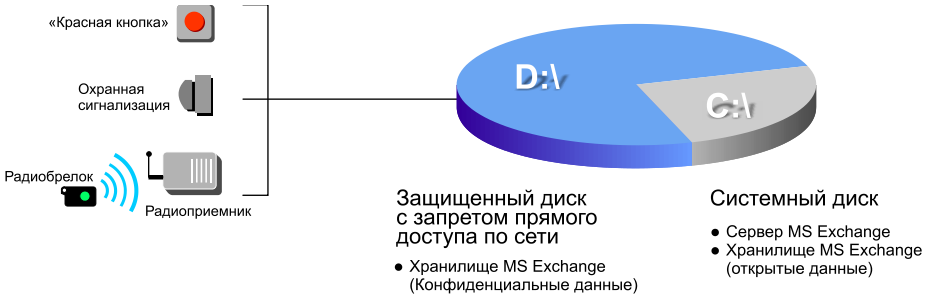
Secret Disk Server NG

Secret Disk Server NG поддерживает две модели защиты – модель файл-сервера с возможностью создания разделяемых сетевых ресурсов и модель сервера приложений с запретом прямого доступа к данным по сети. Обе модели можно использовать на одном сервере. В зависимости от типа лицензии прямой доступ к защищённым базам данных по сети может быть запрещён для всех сотрудников, включая системного администратора, а разрешён только через работающие приложения, что предотвращает несанкционированный доступ к данным через сетевые ресурсы и оптимально подходит для защиты баз данных и корпоративной почты.

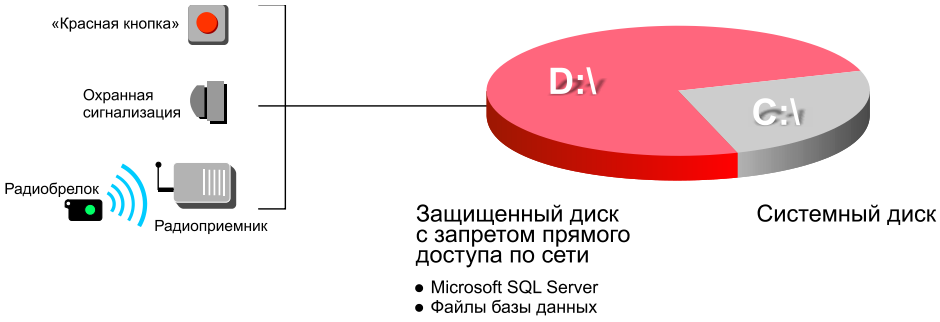
ЗАЩИТА ДАННЫХ НА ФАЙЛ-СЕРВЕРЕ

Задача	o Защита конфиденциальной информации, хранящейся на файловом сервере (в том числе находящейся в общем доступе), от несанкционированного доступа в обход встроенных в операционную систему средств аутентификации, авторизации и контроля доступа. o Блокирование доступа к информации по сигналу "тревога". o Сокрытие факта наличия конфиденциальной информации на файл-сервере.
Архитектура решения	
Сценарий использования	o Размещение файл-сервера в охраняемом помещении. Охранная сигнализация, установленная в серверной комнате, может быть использована для подачи серверу сигнала "тревога". o Создание средствами Secret Disk Server NG защищённого диска достаточного объёма (с разрешением прямого доступа к нему по сети). o Создание резервной копии ключа шифрования защищённого диска и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных администраторах). o Настройка реакции на сигнал "тревога". o Размещение на защищённом диске файлов для общего доступа, установка прав доступа к ним на уровне файловой системы. o Задание прав сетевого доступа к защищённому диску (средствами операционной системы).
Дополнительные преимущества SecretDisk Server NG относительно существующих решений	o Возможность оперативного прекращения доступа к защищённым данным, при возникновении нештатных ситуаций. o Сокрытие факта наличия конфиденциальной информации на сервере.

ЗАЩИТА ДАННЫХ НА ПОЧТОВОМ СЕРВЕРЕ

Задача	o Защита данных почтового сервера (почтовые ящики, общие папки и др.) от попыток прочтения файлов на уровне ОС (как обычные файлы) в обход встроенных средств аутентификации, авторизации и контроля доступа. o Блокирование доступа к информации по сигналу "тревога". o Сокрытие факта наличия конфиденциальной информации на файл-сервере.
Архитектура решения	
Сценарий использования	o Размещение почтового сервера в охраняемом помещении. Охранная сигнализация, установленная в серверной комнате, может быть использована для подачи сигнала "тревога" серверу. o Создание средствами Secret Disk Server NG защищённого диска достаточного объёма и запрет прямого доступа по сети к нему. o Создание резервной копии ключа шифрования защищённого диска и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных администраторах). o Настройка реакции на сигнал "тревога". o Установка ПО почтового сервера и файлов почтового хранилища на защищённом диске. o 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	o Злоумышленник не может скопировать файлы хранилища почтового сервера (локально или по сети), посмотреть их содержимое или восстановить данные на новый сервер. o Возможность оперативного прекращения доступа к защищённым данным при возникновении нештатных ситуаций (обнаружение вторжения в ИС, физическое проникновение посторонних лиц в помещение, пожар и пр.). o Сокрытие факта наличия конфиденциальной информации на сервере.
ЭТО ВАЖНО ЗНАТЬ!	o 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). o 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. o Для обеспечения полноценное защиты почтовых систем рекомендуется использовать защищённые контейнеры, предлагаемые программным комплексом Secret Disk Enterprise.

ЗАЩИТА ДАННЫХ НА СЕРВЕРЕ ПРИЛОЖЕНИЙ (1С, SAP И ДР.)

Задача	o Защита данных бизнес-приложений (в том числе баз данных) от попыток прочтения файлов на уровне ОС (как обычные файлы) в обход встроенных в бизнес-приложения средств аутентификации, авторизации и контроля доступа. o Блокирование доступа к информации по сигналу "тревога". o Сокрытие факта наличия конфиденциальной информации на сервере приложений.
Архитектура решения	
Сценарий использования	o Размещение сервера в охраняемом помещении. Охранная сигнализация, установленная в серверной комнате, может быть использована для подачи серверу сигнала "тревога". o Создание средствами Secret Disk Server NG защищённого диска достаточного объёма и запрет прямого доступ по сети к нему. o Создание резервной копии ключа шифрования защищённого диска и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных администраторах). o Настройка реакции на сигнал "тревога". o Размещение данных бизнес-приложения на созданном защищённом диске. o Определение сценариев, которые будут выполняться после подключения защищённого диска и перед отключением защищённого диска (остановка бизнес-приложения).
Дополнительные преимущества Secret Disk Server NG относительно существующих решений	o Злоумышленник не может скопировать файлы бизнес-приложения (локально или по сети), произвести прямой просмотр их содержимого или восстановление данных на новом сервере. o Возможность оперативного прекращения доступа к защищённым данным при возникновении нештатных ситуаций (обнаружение вторжения в ИС, физическое проникновение посторонних лиц в помещение, пожар и пр.). o Сокрытие факта наличия конфиденциальной информации на сервере.

ЗАЩИТА ДАННЫХ НА ТЕРМИНАЛЬНЫХ СЕРВЕРАХ

Задача	o 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. o Блокирование доступа к информации по сигналу "тревога". o Сокрытие факта наличия конфиденциальной информации на сервере приложений.
Сценарий использования	o Размещение терминального сервера в охраняемом помещении. Охранная сигнализация, установленная в серверной комнате, может быть использована для подачи серверу сигнала "тревога". o Создание средствами Secret Disk Server NG защищённого диска достаточного объёма и запрет прямого доступ по сети к нему. o Создание резервной копии ключа шифрования защищённого диска и/или резервной копии защищённого хранилища (с ключами шифрования, информацией об имеющихся дисках, а также зарегистрированных администраторах). o Настройка реакции на сигнал "тревога". o Размещение данных и приложений, с которыми осуществляется работа на терминальном сервере, на защищённом диске. o Настройка работы терминального сервера для запрещения подсоединения запоминающих устройств локального компьютера пользователя с помощью средств удалённого рабочего стола. o В целях защиты конфиденциальной информации от копирования на терминальном сервере не следует устанавливать приложения, способные передавать данные по сети.
Дополнительные преимущества Secret Disk Server NG относительно существующих решений	o Возможность оперативного прекращения доступа к защищённым данным при возникновении нештатных ситуаций (обнаружение вторжения в ИС, физическое проникновение посторонних лиц в помещение, пожар и пр.). o Сокрытие факта наличия конфиденциальной информации на сервере.

Сигнал "тревога" и экстренное блокирование доступа

Интерфейс подключения внешних устройств (кнопок, датчиков и пр.) открыт и документирован в эксплуатационной документации, что позволяет подключать к системе практически любые устройства. Система контролирует не только нажатие "красной кнопки", но и постоянно диагностирует её состояние так, чтобы кнопка не могла быть случайно или умышленно отключена и не сработать в нужный момент. Реакция на сигнал "тревога" настраивается как для каждого из защищённых дисков в отдельности, так и для всего сервера.

Механизм реакции на сигнал "тревога" позволяет отключать защищённые диски, а при определённых настройках – удалять защищённое хранилище. В результате, даже если злоумышленники завладеют необходимым электронным ключом, узнают пароль и будут обладать полным доступом к серверу, они не смогут получить доступ к информации.

Отработка сервером сигнала "тревога" происходит в два этапа. Вначале для каждого из защищённых дисков выполняются:

- сценарий, предусмотренный для выполнения перед отключением диска (может быть пропущен для сокращения времени реакции данного диска на сигнал "тревога");
- удаление ключей шифрования диска из памяти сервера;
- сценарий, предусмотренный для выполнения после отключения диска (может быть пропущен для сокращения времени реакции данного диска на сигнал "тревога").

После отработки "тревоги" каждым из защищённых дисков происходит отработка сигнала "тревога" для сервера целиком – например, удаление с диска сервера защищённого хранилища.

Для восстановления доступа к защищённой информации достаточно подключить заново зашифрованные диски с консоли администратора. Для этого нужно подключить электронный ключ администратора и ввести пароль. Если же реакцией сервера на сигнал "тревога" было предусмотрено удаление защищённого хранилища, то вначале потребуется восстановить защищённое хранилище из резервной копии.

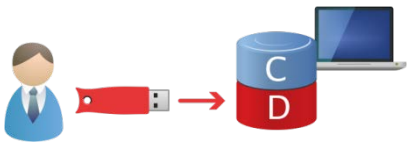
Сигнал "тревога" может быть подан:

- с помощью программного обеспечения посредством клавиатуры компьютера или мыши на одном или нескольких компьютерах локальной сети;
- при нажатии физической "красной кнопки", подключенной к одному из компьютеров локальной сети;
- от радио-брелока (приобретается дополнительно: в комплект входят радиоприёмник, подключаемый к USB- или COM-порту сервера, и до 12 радио-брелоков);
- от различных датчиков, обнаруживающих несанкционированное проникновение в серверную комнату или вскрытие серверной стойки: датчики открывания дверей, движения, изменения объёма;
- от кодового замка, используемого для защиты при входе в помещение и имеющего код входа под принуждением;
- с сотового телефона путём звонка на заданный номер и ввода требуемой комбинации цифр;
- при помощи любой комбинации корректно установленных вышеперечисленных средств.

Интерфейс подключения внешних устройств открыт и документирован, что позволяет подключать к системе практически любые устройства. При наличии нескольких серверов Secret Disk Server NG в одной сети каждый элемент тревожной сигнализации может быть настроен как на конкретный сервер, так и на все сервера.

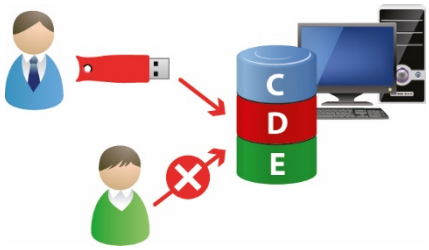
Secret Disk Enterprise

ЗАЩИТА ДАННЫХ НА НОУТБУКЕ В КОРПОРАТИВНОЙ СЕТИ (СЦЕНАРИЙ 1)

Существующие риски	o Несанкционированный доступ к данным, хранящимся на персональном компьютере, по локальной сети при работе в офисе. o Утеря или кража в деловой поездке. o Несанкционированное копирование конфиденциальной информации на съёмный носитель при открытом сеансе Secret Disk. o Использование общественных незащищённых Интернет-соединений для пересылки конфиденциальной информации по электронной почте. o Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ.
Задача	o Защита конфиденциальной информации, персональных данных и иной информации, хранящихся на персональном компьютере. o Сокрытие факта наличия конфиденциальной информации на персональном компьютере.
Архитектура решения	
Сценарий использования	o Регистрация пользователя и рабочей станции (ноутбука) в Secret Disk Enterprise. o Создание защищённого диска. o Защита системного раздела средствами Secret Disk Enterprise. o Настройка профиля пользователя на сервере Secret Disk Enterprise для: - разрешения кэширования ключей от защищаемых ресурсов; - запрета либо разрешения копирования информации на съёмные носители. o Размещение на защищённом диске файлов с конфиденциальной информацией и/или персональными данными. o Создание и использование пользователем защищённых контейнеров для передачи конфиденциальной информации через почтовые программы по открытым каналам связи. o Создание и использование пользователем при необходимости защищённых папок с конфиденциальными данными для усиления криптографической защиты.

Дополнительные преимущества Secret Disk Enterprise относительно существующих решений	o Защита системного раздела. Злоумышленник не сможет получить доступ к информации, хранящейся на загрузочном диске ноутбука, в случае получения несанкционированного физического доступа к компьютеру. o Централизованное резервное копирование ключей шифрования. Администратор безопасности может восстановить доступ к данным даже в случае утери/поломки электронного ключа пользователем. o Быстрая установка и настройка клиентского программного обеспечения на рабочих местах пользователей за счёт использования групповых политик Microsoft Active Directory. o Гибко настраиваемая система ролей и полномочий позволяет адаптировать систему под организационные условия любого предприятия. o Поддержка при необходимости работы с защищёнными дисками и данными вне доступа к корпоративной сети. o Централизованное управление и мониторинг - в системе ведётся несколько журналов, по которым администратор может следить за работой пользователей, легко диагностировать нештатные ситуации и оперативно принимать необходимые меры. o Доступность как централизованно созданных защищённых ресурсов, так и создаваемых пользователем. o Защита папок и почтовых вложений в едином клиентском приложении, встроенная в операционную систему.

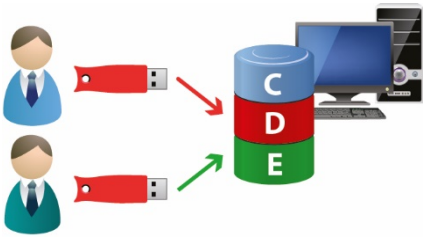
ЗАЩИТА ДАННЫХ НА МНОГОПОЛЬЗОВАТЕЛЬСКОМ КОМПЬЮТЕРЕ В КОРПОРАТИВНОЙ СЕТИ (СЦЕНАРИЙ 2)

Существующие риски	o Несанкционированный доступ к данным, хранящимся на персональном компьютере, по локальной сети. o Несанкционированное использование посторонними лицами (во время отсутствия пользователя на рабочем месте). o Копирование конфиденциальной информации на незащищённые съёмные носители. o Пересылка по электронной почте незащищенной конфиденциальной информации. o Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ.
Задача	o Защита конфиденциальной информации, персональных данных и личной информации, хранящихся на персональном компьютере, к которому имеют доступ несколько пользователей Windows. o Сокрытие факта наличия конфиденциальной информации на персональном компьютере.
Архитектура решения	

Сценарий использования	o Регистрация пользователя и рабочей станции в Secret Disk Enterprise. o Создание диска общего пользования для хранения данных других пользователей. o Создание защищённого диска. o Настройка профиля пользователя на сервере Secret Disk Enterprise для: - запрета кэширования ключей от защищаемых ресурсов; - запрета предоставления доступа к защищённым данным в локальной сети; - запрета копирования информации на съёмные носители. o Размещение на защищённом диске файлов с конфиденциальной информацией и/или персональными данными. o Создание и использование пользователем защищённых контейнеров для передачи конфиденциальной информации через почтовые программы. o Создание и использование пользователем при необходимости защищённых папок с конфиденциальными данными нанезащищённых ресурсах.
Дополнительные преимущества Secret Disk Enterprise относительно существующих решений	o Быстрая установка и настройка клиентского программного обеспечения на рабочих местах пользователей за счёт использования групповых политик Microsoft Active Directory. o Гибко настраиваемая система ролей и полномочий позволяет адаптировать систему под организационные условия любого предприятия. o Поддержка при необходимости работы с защищёнными дисками и данными вне доступа к корпоративной сети. o Централизованное управление и мониторинг - в системе ведётся несколько журналов, по которым администратор может следить за работой пользователей, легко диагностировать нештатные ситуации и оперативно принимать необходимые меры. o Доступность как централизованно созданных защищённых ресурсов, так и создаваемых пользователем. o Защита папок и почтовых вложений в едином клиентском приложении, встроенная в операционную систему.

ЗАЩИТА ДАННЫХ НА МНОГОПОЛЬЗОВАТЕЛЬСКОМ КОМПЬЮТЕРЕ В КОРПОРАТИВНОЙ СЕТИ (СЦЕНАРИЙ 3)

Существующие риски	o Несанкционированный доступ к данным со стороны других пользователей, допущенных к работе на персональном компьютере. o Несанкционированный доступ к данным, хранящимся на персональном компьютере, по локальной сети. o Несанкционированное использование посторонними лицами (во время отсутствия пользователя на рабочем месте). o Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ.
Задачи	o Защита конфиденциальной информации, персональных данных и личной информации нескольких пользователей, работающих в режиме разделения времени с разной конфиденциальной информацией на одном персональном компьютере. o Сокрытие факта наличия конфиденциальной информации на персональном компьютере.

Архитектура решения	
Сценарий использования	o Регистрация пользователей и рабочей станции в Secret Disk Enterprise. o Создание средствами Secret Disk Enterprise защищенных дисков достаточного объёма для каждого пользователя, работающего за персональным компьютером. o Размещение пользователями Secret Disk Enterprise на защищённых дисках файлов с конфиденциальной информацией и/или персональными данными.
Дополнительные преимущества Secret Disk Enterprise относительно существующих решений	o Быстрая установка и настройка клиентского программного обеспечения на рабочих местах пользователей за счёт использования групповых политик Microsoft Active Directory. o Гибко настраиваемая система ролей и полномочий позволяет адаптировать систему под организационные условия любого предприятия. o Поддержка при необходимости работы с защищёнными дисками и данными вне доступа к корпоративной сети. o Централизованное управление и мониторинг - в системе ведётся несколько журналов, по которым администратор может следить за работой пользователей, легко диагностировать нештатные ситуации и оперативно принимать необходимые меры. o Централизованное резервное копирование ключей шифрования. Администратор безопасности может восстановить доступ к данным даже в случае утери/поломки электронного ключа пользователем. o Сокрытие факта наличия конфиденциальной информации на компьютере.

Заключение

Линейка продуктов Secret Disk эффективно решает задачу по обеспечению защиты конфиденциальной информации на малых, средних и больших предприятиях.

Несмотря на высокую функциональность и не менее высокую надёжность, решения данной линейки предельно просты в установке и использовании.

Важными преимуществами линейки Secret Disk являются:

- использование двухфакторной аутентификации пользователя и администратора при помощи электронного ключа и пароля;
- защита системного раздела жёсткого диска;
- возможность загрузки операционной системы по электронному ключу;
- возможность экстренной блокировки доступа к данным по сигналу "тревога";
- широкий выбор типов защиты: папки, тома, виртуальные диски, защищённые контейнеры;
- поддержка необратимого удаления данных;
- возможность криптографической защиты почтовых вложений;
- контроль утечек конфиденциальной информации через съёмные носители;
- возможность запрета сетевого доступа к защищаемым данным;
- оптимизация работы с многоядерными и многопроцессорными системами, в том числе в отказоустойчивых кластерных конфигурациях;
- поддержка резервного копирования и восстановления ключей шифрования в случае утери электронного ключа;
- защита данных от сбоев во время установки защиты;
- наличие сертификатов ФСТЭК России;
- возможность использования российских сертифицированных криптоалгоритмов.

Используя решения линейки Secret Disk, Вы будете уверены, что Ваши информационные активы под надёжной защитой!

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Microsoft Silver OEM Hardware Partner, Microsoft Silver Cloud Platform Partner, Apple Developer

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru