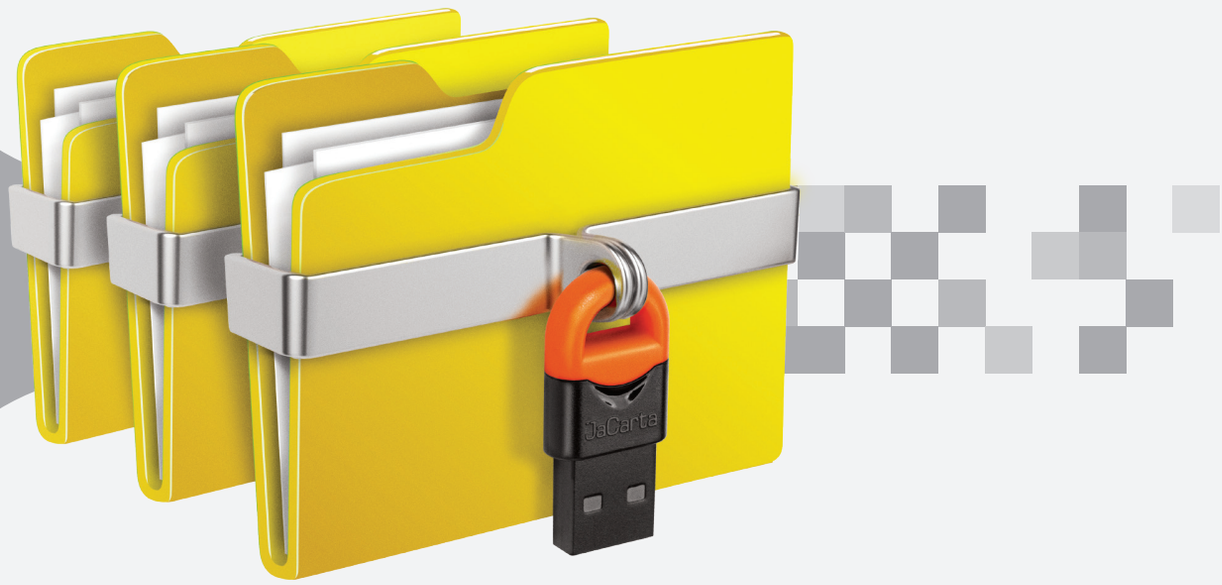
Система защиты информации на дисках и съёмных носителях



Secret Disk

- Прозрачное шифрование файлов, папок, дисков на ПК и серверах
- Защита от утечек информации на USB Mass Storage
- Мониторинг доступа пользователей
- Защита от системных администраторов

Аладдин

Необходимость шифрования информации на запоминающих устройствах и съёмных носителях

Повсеместное использование информационных технологий как в коммерческих, так и в государственных структурах значительно увеличило количество утечек конфиденциальной информации. Согласно исследованию компании "Аладдин Р.Д.", проведённому среди 1800 ИБ-специалистов заказчиков, 38% респондентов столкнулись с утечками конфиденциальной информации и ещё 28% отметили попытки кражи информации.

Чаще всего утекают данные о клиентах и сделках, техническая информация, коммерческая тайна, информация о партнёрах, персональные данные и данные внутренней бухгалтерии.

Несмотря на сложившуюся ситуацию, большая часть усилий по обеспечению информационной безопасности всё ещё традиционно направлена на защиту периметра сети. При этом данные исследования свидетельствуют о том, что 48% утечек происходит в результате кражи или утери ноутбука либо другого носителя информации, а не из-за проникновения в корпоративную сеть.

Российская компания "Аладдин Р.Д." на протяжении многих лет развивает собственное семейство продуктов, предназначенных для защиты информации от несанкционированного доступа и утечек — Secret Disk.

Secret Disk — надёжное средство обеспечения конфиденциальности информации в случае её утечки

Продукты линейки Secret Disk обеспечивают надёжную защиту конфиденциальной информации на десктопах, ноутбуках, серверах и в системах хранения данных. В качестве метода защиты данных используется так называемое "прозрачное" шифрование (быстрое и незаметное для пользователя) накопителей информации (HDD, SSD, USB Mass Storage и т.д.).

Шифрование позволяет надёжно ограничить доступ к конфиденциальной информации: получив доступ к компьютеру или серверу, злоумышленник ничего не добьётся, т.к. для него зашифрованная информация будет представлена набором нечитаемых символов. Расшифровать данные у него не получится — современные алгоритмы шифрования с большой длиной ключа гарантируют стойкость ко взлому, даже если для этого используется высокопроизводительная вычислительная техника (время, необходимое для взлома, измеряется годами).

Secret Disk также дополняет шифрование строгой двухфакторной аутентификацией на основе устройств с аппаратной реализацией стойких криптографических алгоритмов (USB-токены или смарт-карты JaCarta). Их применение создаёт дополнительный барьер для злоумышленника — не имея устройства аутентификации и не зная PIN-код к нему, получить доступ к системе невозможно.

Продукты Secret Disk не имеют встроенных средств шифрования, поэтому не попадают под законодательные ограничения по распространению и не требуют наличия соответствующих лицензий ФСБ России. Для криптографической защиты данных могут применяться отечественный криптоалгоритм ГОСТ Р 34.12-2015, предоставляемый криптопровайдерами КриптоПроCSP или ViPNet CSP, либо криптоалгоритмы AES 256 или TripleDES, предоставляемые криптографическим драйвером режима ядра, входящего в состав Microsoft Windows.

Для кого?

Органы государственной власти и организации различных форм собственности, работающие с конфиденциальной информацией и персональными данными.

Государственные организации, подпадающие под действия требований в области обеспечения конфиденциальности обрабатываемой информации.

Коммерческие организации, обрабатывающие критически важные для их бизнеса данные (персональные данные, финансовая информация, информация о клиентах и партнёрах, ноу-хау и иная информация, составляющая коммерческую тайну).

Преимущества

Применение "прозрачного" шифрования

Применение быстрого шифрования, незаметного для пользователя, позволяет обеспечить надёжную защиту информации без необходимости жертвовать скоростью и удобством работы.

Комплексная защита информации

Одновременное применение шифрования, средств двухфакторной аутентификации и защиты от копирования на съёмные носители позволяет надёжно защитить информацию от несанкционированного доступа.

Поддержка нескольких криптоалгоритмов

Поддержка российских (ГОСТ Р 34.12-2015, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012) и западных (AES, RSA, TripleDES) криптоалгоритмов позволяет выбрать удобный способ шифрования защищаемых данных.

Сертификация ФСТЭК России

Наличие сертификатов соответствия ФСТЭК России позволяет применять Secret Disk 5 и Secret Disk Server NG для защиты информации в ИСПДн до 1 уровня защищённости, в ГИС до 1 класса защищённости, а также при создании АС до класса защищённости 1Г.

Защита от внутренних нарушителей

Пофайловое шифрование позволяет обеспечить защиту от персонала и ИТ-администраторов, имеющих привилегированный доступ к информационным системам.

Реагирование на экстренные случаи

Возможность мгновенного прекращения доступа к данным по сигналу "тревога" и функция необратимого удаления данных позволяют обезопасить защищаемую информацию от злонамеренных действий (например, при попытке рейдерского захвата).

Быстрое реагирование на инциденты безопасности

Централизованный мониторинг действий сотрудников и администраторов позволяет быстро реагировать на инциденты информационной безопасности и проводить ретроспективные расследования.

Высокая производительность и масштабируемость

Оптимизация работы с многоядерными и многопроцессорными системами, в т.ч. в отказоустойчивых кластерных конфигурациях, позволяет использовать Secret Disk Enterprise и Secret Disk Server NG в крупных территориально-распределённых организациях.

Надёжность

Защита данных от сбоев во время процесса шифрования, в т.ч. при перезагрузке ОС, а также поддержка отказоустойчивых кластерных конфигураций позволяют быть уверенными в сохранности зашифровываемой и расшифровываемой информации.

Низкая совокупная стоимость владения

Низкая стартовая стоимость приобретения, быстрое внедрение и недорогое сопровождение значительно снижают совокупную стоимость владения любой редакцией Secret Disk.

Редакции Secret Disk

Secret Disk 5

Для защиты персональных компьютеров и ноутбуков

Система Secret Disk 5 разработана специально для индивидуальных предпринимателей и компаний малого и среднего бизнеса, а также руководителей крупных компаний. Возможности системы позволяют защитить конфиденциальную информацию, хранящуюся на персональном компьютере (предполагается, что чаще всего это ноутбук), исключив возможность утечки данных при его утере, краже или сервисном обслуживании.

Современные алгоритмы шифрования и надёжная процедура подтверждения прав пользователя обеспечивают защиту от большинства известных угроз. Secret Disk 5 позволяет защищать не только разделы жёсткого диска, включая системный и логические, но и съёмные носители (USB-диски, Flash-диски, карты памяти). Находящиеся на диске данные всегда зашифрованы. Для доступа к ним необходимо подключить к защищаемому компьютеру устройство JaCarta, содержащее действующую лицензию, и ввести PIN-код. При шифровании системного диска пользователь должен пройти процедуру аутентификации до загрузки операционной системы.

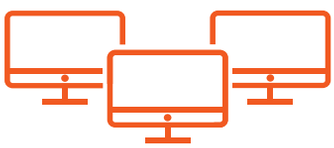
Новейшая функция системы — пофайловое шифрование — защищает данные особым образом: только легитимный пользователь имеет доступ к расшифрованному содержимому и именам файлов, что допускает параллельное создание администратором резервных копий информации в зашифрованном виде даже во время работы. Такой режим защиты является лучшей гарантией сохранения приватности.

Secret Disk 5 поддерживает широкий спектр операционных систем, включая Microsoft Windows 10, с загрузчиками UEFI BIOS и LEGACY BIOS. Могут быть использованы дополнительные драйверные алгоритмы шифрования и/или сопряжение с распространёнными отечественными криптопровайдерами, имеющими сертификат ФСБ России. На одном компьютере допускается комбинирование разных алгоритмов защиты данных.

Сертифицированная ФСТЭК России на соответствие ТУ и отсутствие НДВ по 4-му уровню контроля версия Secret Disk 5 предназначена для защиты от несанкционированного доступа к информации (сертификат соответствия № 3742). Это позволяет использовать систему для защиты информации в информационных системах персональных данных (ИСПДн) до 1 уровня защищённости включительно, в государственных информационных системах (ГИС) до 1 класса защищённости включительно, а также при создании автоматизированных систем (АС) до класса защищённости 1Г включительно.

Secret Disk Enterprise

Для защиты персональных компьютеров и ноутбуков в корпоративной среде с централизованной системой управления



Secret Disk Enterprise — корпоративная система защиты коммерческой информации с централизованным управлением, имеющая клиент-серверную архитектуру. Она призвана помочь администраторам следить за состоянием безопасности на каждом доменном компьютере в организации, одновременно освобождая пользователей от необходимости самим разбираться в вопросах защиты запоминающих устройств.

Применение системы позволяет обеспечить защиту от несанкционированного доступа и раскрытия информации пользователей от злоумышленников, получивших физический доступ к носителям данных, посторонних лиц, имеющих доступ к компьютерному оборудованию (например, сотрудники сервисного центра), а также сотрудников компании, не обладающих соответствующими правами для доступа к данным (например, системные администраторы).

Для доступа к защищаемым данным до загрузки операционной системы в Secret Disk Enterprise используются USB-токены и смарт-карты, что позволяет предотвратить кражу информации при утере или краже ноутбука. Аутентификаторы доступа централизованно хранятся на защищённом сервере и передаются пользователю по мере необходимости, что позволяет предотвратить их случайную потерю. Это также даёт возможность контролировать доступ сотрудников к защищаемым данным и в любой момент запретить его.

Инструменты мониторинга, реализованные в Secret Disk Enterprise, позволяют диагностировать состояние защищённых дисков на рабочих местах из одного интерфейса. Использование административного Web-портала снижает нагрузку на службу поддержки.

Внедрение корпоративной системы не занимает много времени и может осуществляться собственными силами отдела информационной безопасности. Интерфейс системы максимально упрощён и не требует специальных знаний и подготовки. Гибкие настройки по разграничению доступа к защищённым данным для разных категорий пользователей, включая технические службы, максимально снижают вероятность случайной потери информации и несанкционированного доступа к данным.

В системе Secret Disk Enterprise реализована поддержка нескольких внешних алгоритмов шифрования для усиленной защиты данных, в т.ч. и современных отечественных. Функция использования защищённых контейнеров обеспечивает возможность безопасной передачи документов, их редактирования или подписания, а также их безопасность на компьютерах без установленного агента Secret Disk Enterprise.

Редакция Secret Disk Enterprise, основанная на версии 2.7, в настоящее время проходит сертификационные испытания в лаборатории ФСТЭК России.

Secret Disk Server NG

Для защиты серверов приложений и систем хранения данных

Secret Disk Server NG — система защиты коммерческой информации на серверах компании от несанкционированного доступа, копирования, кражи или принудительного изъятия, способная не только скрывать сам факт наличия на дисках какой-либо информации, но и экстренно блокировать доступ к дискам серверов по сигналу "тревога".

Secret Disk Server NG допускает многопользовательскую работу с защищёнными данными как в формате файлового сервера, так и сервера приложений. В первом случае пользователи получают прозрачный доступ к зашифрованной информации на файловом сервере или в хранилище данных, а во втором — доступ к данным приложений может быть открыт только через сами приложения.

Поддерживается подавляющее большинство современных файловых систем и отказоустойчивых конфигураций.

Система всегда аутентифицирует администратора Secret Disk Server NG при помощи USB-токена или смарт-карты, содержащих специальную лицензию администратора, и PIN-кода для управления любым количеством серверов из единого центра управления Secret Disk Server NG. Допускается использование сторонних сертифицированных ФСБ России криптопровайдеров, в которых реализованы российские криптоалгоритмы.

Экстренное блокирование доступа к данным по сигналу "тревога" может быть активировано широким набором предлагаемых устройств, служб и сценариев, которые включают в себя компьютерные программы, физические кнопки, работающие на размыкание или замыкание, радиопередающие устройства с широким диапазоном действия, а также приёмники сотовой связи, настроенные на определённые команды.

В комплект поставки входит сигнал подачи тревоги с USB-интерфейсом. Гибкость решения позволяет добиться уникальности организации защиты у каждого заказчика.

Лицензионная политика Secret Disk Server NG требует непосредственного подключения USB-токена с лицензией во время работы сервера, но специальные программные сервисы допускают его сетевое подключение.

Secret Disk Server NG зарегистрирована в Едином реестре отечественного ПО (№ 519). Сертифицированная версия Secret Disk Server NG может быть использована при создании автоматизированных систем до класса защищённости 1Г, ГИС до 1 класса защищённости, а также для защиты информации в ИСПДн до 1 уровня защищённости включительно (сертификат ФСТЭК России № 3358).

Возможности

Пофайловое шифрование для предотвращения доступа к защищаемой информации вне текущей сессии легитимного пользователя.

Шифрование системного раздела диска (в т.ч. временных файлов, файлов-журналов, файла подкачки ОС и файла "спящего" режима).

Централизованное хранение и управление ключами шифрования ресурсов пользователей, информацией о пользователях и их правах.

Создание и использование зашифрованных виртуальных дисков (файлов-контейнеров) с возможностью сетевого хранения.

Двухфакторная аутентификация с использованием USB-токена или смарт-карты JaCarta до загрузки операционной системы.

Поддержка защищённого резервного копирования и восстановления ключей шифрования в случае утери USB-токена или смарт-карты JaCarta.

Централизованное управление операциями и настройками через единую консоль администратора.

Мгновенное прекращение доступа пользователей к информации на сервере (сигнал "тревога").

Интеграция с каталогом пользователей Microsoft Active Directory и инфраструктурой открытых ключей (PKI).

Мониторинг и протоколирование действий пользователей и состояния зашифрованных ресурсов с возможностью ретроспективного расследования инцидентов.

Контроль копирования информации на съёмные носители информации USB Mass Storage.

Шифрование логических разделов жёсткого диска полностью отечественными и международными криптоалгоритмами.

Поддержка международных и российских криптоалгоритмов (AES256, RSA1024/2048, TripleDES, ГОСТ Р 34.12-2015, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012).

Возможность необратимого удаления данных с помощью многократной перезаписи.

Различия редакций Secret Disk

Возможности	Secret Disk 5	Secret Disk Enterprise	Secret Disk Server NG
Шифрование данных на ноутбуках и рабочих станциях	●	●	
Шифрование данных на файловых серверах и серверах приложений			●
Шифрование данных на съёмных носителях	●	●	●
"Прозрачное" шифрование	●	●	●
Поддержка отечественного криптоалгоритма ГОСТ Р 34.12-2015 с помощью внешних криптопровайдеров	●	●	●
Поддержка международных криптоалгоритмов AES и TripleDES с помощью встроенных средств операционной системы	●	●	●
Шифрование системного раздела жёсткого диска (для защиты временных файлов, файлов-журналов, файла подкачки ОС и файла "спящего" режима)	●	●	
Шифрование логических разделов запоминающего устройства и динамических томов	●	●	●
Шифрование отдельных папок	●	●	
Пофайловое шифрование с защитой имён файлов	●	●	
Защита от копирования на внешние носители		●	
Возможность перезагрузки системы во время выполнения операции шифрования	●	●	●
Защита от сбоев во время выполнения операций шифрования	●	●	●
Создание виртуальных дисков (файлов-контейнеров)	●	●	●
Двухфакторная аутентификация пользователей (по USB-токену/смарт-карте и PIN-коду) для доступа к защищённым данным	●	●	
Двухфакторная аутентификация пользователей до загрузки ОС	●	●	
Двухфакторная аутентификация оператора/администратора безопасности Secret Disk	●	●	●
Централизованное управление		●	●
Аудит использования защищённых файлов	●	●	●
Доступ к защищённым данным по сети	●	●	●
Сигнал "тревога" для экстренного прекращения доступа к данным			●
Поддержка "спящего" (Hibernation) и "ждущего" (Stand-by) режимов	●	●	
Поддержка Microsoft Windows 10	●	●	
Наличие действующего сертификата соответствия ФСТЭК России	●		●

Аладдин

+7 (495) 223 00 01
aladdin@aladdin.ru
www.aladdin.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17
Лицензии ФСБ России № 12632Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации услуг ГОСТ Р (РОСС RU.0001.03ГУ00) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015)
Сертификат соответствия - № РОСС RU.ФК14.К00011 от 20.07.18
Система менеджмента качества компании сертифицирована в Системе добровольной сертификации "Военный Регистр" (РОСС RU.И1975.04ГШ02) и соответствует требованиям стандарта ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и дополнительным требованиям ГОСТ РВ 0015-002-2012
Сертификат соответствия - № ВР 21.1.13537-2019 от 25.04.19