Аладдин рд

Secret Disk

Криптографическая защита информации с обязательной двухфакторной аутентификацией пользователей

- Прозрачное шифрование системного раздела и логических томов для защиты от утери диска или ноутбука
- Пофайловое шифрование важной информации для блокировки доступа системных администраторов
- Шифрование имён файлов как повышение уровня защищённости
- Поддержка специальных защищённых контейнеров для безопасного хранения информациия
- Реализация сигнала тревоги для мгновенного прекращения

Внесено в Единый реестр отечественного ПО для госзакупок

Secret Disk Server NG

Компаниям с развитой инфраструктурой необходима надёжная защита важной информации на серверах от несанкционированного доступа, копирования, кражи или неправомерного изъятия, способная не только скрывать сам факт наличия на дисках какой-либо информации, но и экстренно блокировать доступ к ней по сигналу "тревога".

Система 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.

Система всегда аутентифицирует администратора Secret Disk Server NG при помощи USB-токена или смарт-карты JaCarta/eToken и пароля для управления любым количеством серверов из единого центра управления Secret Disk Server NG. Допускается использование сторонних криптопровайдеров (КриптоПро CSP, Infotecs ViPNet CSP и др.) которые реализуют российские стандарты алгоритмов шифрования и сертифицированы ФСБ России.

Экстренное блокирование доступа к данным по сигналу "тревога" может быть активировано широким набором предлагаемых устройств, служб и сценариев.

Сертифицированная версия Secret Disk Server NG основана на версии Secret Disk Server NG 3.8, не содержит встроенной криптографии и может быть использована при создании автоматизированных систем до класса защищённости 1Г, а также для защиты информации в ИСПДн до 1 класса включительно (сертификат ФСТЭК России № 3358 от 6 марта 2015 г.).

Secret Disk 5

Программный комплекс Secret Disk 5 разработан специально для индивидуальных предпринимателей и компаний малого и среднего бизнеса. Однако не меньшей популярностью он пользуется и в корпоративном секторе среди высшего менеджмента.

Он защищает важную информацию и персональные данные на персональном компьютере или ноутбуке, чтобы не допустить утечки данных при утере, краже ноутбука, при сервисном обслуживании и даже при отсутствии на рабочем месте владельца данных.

Современные алгоритмы шифрования и надёжная процедура подтверждения прав пользователя обеспечивают защиту от большинства известных угроз. Решение 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 компьютеру персональный USB-токен JaCarta/eToken, содержащий действующую лицензию, и ввести пароль. При шифровании системного диска пользователь аутентифицируется до загрузки операционной системы.

Пофайловое шифрование защищает данные пользователя особым образом: только сам 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 двойной защиты шифрованием является лучшей гарантией сохранения приватности.

Поддерживается широкий спектр пользовательских операционных систем до Microsoft Windows 10 включительно, UEFI и Legacy BIOS, дополнительные драйверные алгоритмы шифрования, сопряжение с распространёнными отечественными криптопровайдерами, имеющими сертификат ФСБ России, что даёт возможность применять криптографический алгоритм ГОСТ 28147-89 с длиной ключа 256 бит.

Гибкая лицензионная политика новой версии популярного продукта предоставляет возможность бесплатной поддержки и обновления на весь период действия лицензии.

Сертифицированная версия Secret Disk 5 не содержит криптографии, предназначена для защиты от несанкционированного доступа к информации и классифицирована по 4-му уровню контроля отсутствия недекларированных возможностей (сертификат ФСТЭК России № 3742 от 12 мая 2017 года).

Secret Disk Enterprise

Корпоративная система защиты важной информации с централизованным управлением ориентирована на крупные компании, использующие службы каталогов Microsoft Active Directory.

Система позволяет защитить данные на клиентских устройствах (персональных компьютерах и ноутбуках), не требуя от пользователей специальной подготовки, снижая затраты на обучение и повышая уровень безопасности данных в компании.

Комплекс Secret Disk Enterprise управляет политиками шифрования, ведёт мониторинг действий пользователей и аудит состояния криптографической защиты ресурсов на рабочих станциях пользователей. Для доступа к защищаемым данным до загрузки операционной системы используются USB-токены и смарт-карты JaCarta/eToken, что предотвращает кражу информации при утере ноутбука или сервисном обслуживании.

Новейшие функции контроля копирования информации на внешние на внешние USB-носители (флешки, съёмные диски) исключают риск прямой утечки данных, а криптографическая защита папок значительно расширяет список сценариев применения Secret Disk Enterprise.

Функция защищённых контейнеров обеспечивает возможность безопасного сохранения документов, их редактирования или подписания и последующего зашифрования на компьютерах без установленного агента Secret Disk Enterprise.

Версия Secret Disk Enterprise, основанная на версии 2.6, не содержащая встроенной криптографии, в настоящее время проходит сертификационные испытания в лаборатории ФСТЭК России.

Выбор нужного продукта

Возможности продукта	Secret Disk Server NG	Secret Disk 5	Secret Disk Enterprise
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)		●	●
Пофайловое шифрование с защитой имён файлов		●	●
Создание виртуальных дисков (файлов-контейнеров)	●	●	●
Прозрачное ("на лету") шифрование	●	●	●
Двухфакторная аутентификация пользователей (по токену/смарт-карте и паролю) для доступа к защищённым данным		●	●
Двухфакторная аутентификация пользователей до загрузки ОС		●	●
Двухфакторная аутентификация администратора безопасности Secret Disk	●	●	●
Централизованное управление	●		●
Аудит использования защищённых ресурсов	●	●	●
Решение "красная кнопка" (сигнал "тревога") для прекращения доступа к данным	●		
Наличие сертификата ФСТЭК России	●	●	●
Поддержка криптоалгоритмов AES, TripleDES встроенными средствами и криптоалгоритмов ГОСТ 28147-89 с помощью сертифицированных криптопровайдеров	●	●	●
Возможность перезагрузки системы во время выполнения операции шифрования	●	●	●
Поддержка "спящего" (Hibernation) и "ждущего" (Stand-by) режимов		●	●
Доступ к защищённым данным по сети	●	●	●
Поддержка MS Windows 10		●	●

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17.
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17.
Лицензия Министерства обороны РФ № 1384 от 22.08.16.
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.
Apple Developer.

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

ID: 3941-060717