



Secret Disk для Linux

Release Notes. Комментарии к версии 2.1



Аннотация

Secret Disk для Linux – система защиты информации на рабочих станциях и серверах для ОС семейства Linux. Продукт обеспечивает предотвращение утечек конфиденциальной информации с помощью шифрования. В документе описываются основные отличия версии 2.1 от предыдущих выпусков, а также особенности её использования.

Что нового в версии 2.1

1. Защита системного раздела

- Полнодисковое прозрачное шифрование системного раздела с применением алгоритма ГОСТ Р 34.12-2015 (Кузнечик)
- Поддержка разметки диска стандарта GPT и логических разделов диска типа LVM
- Доступ к загрузке защищенной операционной системы по паролю
- Автоматическая проверка параметров операционной системы
- Автоматическое конфигурирование параметров защиты перед стартом зашифрования
- Разграничение прав доступа между администраторами ИТ и ИБ при включении защиты.

2. Интеграция с SecurLogon

SecurLogon¹ – программное обеспечение для аутентификации пользователей Linux с применением усиленной и строгой многофакторной аутентификации.

- Аутентификация пользователей Secret Disk с использованием аппаратных ключей - смарт-карт и USB-токенов JaCarta
- Автоматическое подключение виртуальных дисков после успешной аутентификации в SecurLogon.

Другие возможности продукта

3. Криптографическая защита информации на виртуальных дисках пользователей.
4. Автоматическая регистрация рабочих станций и пользователей в консоли управления администратора.
5. Динамическая группировка пользователей для применения политик шифрования.
6. Централизованное управление агентами на рабочих станциях.
7. Два интерфейса управления – графический и классическая командная строка.

¹ Приобретается отдельно

8. Универсальный агент, работающий как автономно, так и в режиме централизованного управления.
9. Сертифицированный ФСБ России СКЗИ "Secret Disk Crypto Engine", встроенный в состав ПО.
10. При использовании Secret Disk для Linux доступен пробный период без приобретения лицензии. Продукт в этот период не ограничен в функционале. Переход на рабочую лицензию не требует переустановки.

Secret Disk для Linux. Как работает продукт

Secret Disk для Linux имеет клиент-серверную архитектуру. Ключевые компоненты архитектуры – Программный агент, Менеджмент сервер и Консоль управления.

Secret Disk для Linux позволяет защищать данные с помощью шифрования. В зависимости от задач безопасности можно выбрать механизмы – шифрование виртуального диска, шифрование системного раздела. Механизмы могут быть использованы как по отдельности, так и вместе.

Шифрование системного раздела

Системный раздел – это корневой раздел операционной системы, в котором хранятся основные файлы и настройки самой операционной системы, а также информация об учётных записях пользователей, а часто ещё и информация пользователей. Включение защиты системного раздела осуществляется на введенной в эксплуатацию рабочей станции с установленной ОС.

При включении защиты системного раздела производится диагностика рабочей станции или ноутбука. После успешного завершения диагностики производится предварительная подготовка к шифрованию с помощью Secret Disk. Во время предподготовки автоматически изменяются параметры загрузки ОС, что позволяет корректно реализовать функцию полнодискового шифрования системного раздела (FDE). Процесс зашифрования выполняется в фоновом режиме, не влияет на рабочие процессы и не заметен для пользователя.

После включения функции FDE происходит перезагрузка ОС. При перезагрузке пользователь вводит пароль и далее может пользоваться своим компьютером в обычном режиме. ОС загружается с защищенного раздела, работа модуля защиты системного раздела полностью прозрачна для пользователя и не требует от него дополнительных действий.

Шифрование виртуального диска

Всё содержимое виртуального диска хранится в одном файл-контейнере в зашифрованном виде. Подключенный виртуальный диск операционная система воспринимает как обычный диск. Файл подключенного виртуального диска защищён от удаления.

Данные, хранящиеся на зашифрованных виртуальных дисках доступны только администратору Secret Disk для Linux и пользователям, владеющим ключевым контейнером пользователя и зарегистрированным в Secret Disk для Linux. Остальные пользователи, включая системного администратора, не могут получить доступ к зашифрованным данным.

При записи данных на диск происходит их зашифрование, при чтении — расшифрование. Находящиеся на зашифрованном диске данные всегда зашифрованы.

Защищённый виртуальный диск можно подключать и отключать. Отключенный зашифрованный виртуальный диск выглядит как неформатированный. Для того чтобы подключить зашифрованный диск, пользователь должен иметь ключевой контейнер пользователя, знать его пароль и иметь право доступа к данному диску.