



Secret Disk для Linux

Release Notes. Комментарии к версии 1.2



Аннотация

Secret Disk для Linux – программное средство предотвращения утечек конфиденциальной информации с помощью шифрования, предназначенное для операционных систем семейства Linux. В документе описываются основные отличия версии 1.2 от предыдущих выпусков, а также особенности её использования.

Что нового в версии 1.2

1. Поддержка операционной системы Astra Linux 1.7.0, 1.7.1, 1.7.2, 1.7.3 (ядро 5.4.0-54 generic/hardened) и Astra Linux 1.6 обновление 6 (ядро 4.15.3-2 generic)
2. Поддержка операционной системы РЕД ОС версии 7.3 (ядро 5.10.29) и версии 7.2 (ядро 4.19.204)
3. Усовершенствованный графический интерфейс администратора
4. Управление лицензированием через интерфейс администратора
5. Экспериментальная функция защиты разделов дисков (режим полнодискового шифрования)

Основные возможности

1. Механизм защиты файл-контейнера, который монтируется к папке пользователя как виртуальный диск.
2. Многопользовательский режим – на одной рабочей станции каждый пользователь под своей учетной записью может создать себе защищенный виртуальный диск. Количество пользователей на одной АРМ не ограничено. Защищенный виртуальный диск недоступен для других пользователей.
3. Монопольное управление доступом к ресурсу - действия с виртуальным диском разрешены только пользователю-владельцу.
4. Разграничение ролей на администратора и пользователя Secret Disk для Linux.
5. Два интерфейса управления – графический и классическая командная строка.
6. Настраиваемый язык интерфейса – русский или английский.
7. Обязательная двухфакторная аутентификация пользователей и администраторов с использованием ключевого контейнера (виртуального аутентификатора).
8. Сертифицированный ФСБ России СКЗИ "Secret Disk Crypto Engine", встроенный в состав ПО.
9. Возможность установки подписанных пакетов для Astra Linux из сетевого репозитория.

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 позволяет защищать так называемые виртуальные диски. 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.