Secret Disk для Linux. Описание продукта

Специалистам по информационной безопасности.

Статус	Для общего использования
Дата	28.08.2024
Номер	0720140000

Авторские права и торговые знаки

Список терминов и определений

ПК	Персональный компьютер.
ККП	Ключевой контейнер пользователя.
ОС	Операционная система.
Токен	Электронное устройство (USB-ключ или смарт-карта), предназначенное для аппаратной реализации процедур ассиметричного шифрования, необходимых для систем шифрования, электронной подписи и двухфакторной аутентификации с использованием сертификатов открытого ключа.
Пользователь ПК	Субъект, который имеет пользовательскую учётную запись в системе Linux на ПК.
Локальный администратор ПК	Привилегированный пользователь ОС семейства Linux (учётная запись с правами администратора ОС).
Алгоритм шифрования	Набор логических правил (математических преобразований), определяющих способ преобразования информации из открытого состояния в зашифрованное (процесс зашифрования) и наоборот, из зашифрованного состояния в открытое (процесс расшифрования).
JaCarta, eToken	Используемые в ПАК SD марки токенов.
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдаёт.
СКЗИ	Средство криптографической защиты информации.
Виртуальный диск	Логическое устройство, представленное в ОС как обычный диск, но отличающееся тем, что информация хранятся в файле на одном из доступных физических дисков.
Защита системного раздела, Full disk encryption, FDE	Функция защиты информации, представляющая собой шифрование всех данных на диске, включая временные файлы, системные файлы и т. д.

1. Описание решаемой проблемы

Для большинства отечественных организаций в 2022 году наступил переломный момент в решении задач импортозамещения, в т.ч. в области информационных технологий. Замена западных ИТ–решений на российские аналоги осложняется требованиями времени.

Многие крупные западные вендоры свернули деятельность в России, отменили техническую поддержку по текущим контрактам и заблокировали аккаунты отечественных организаций в своих системах. Таким образом, переход на российские аналоги является безальтернативным, обязательным решением.

В связи с обострением геополитической обстановки крупные российские компании испытывают трудности с поддержкой непрерывной безопасности своей ИТ–инфраструктуры и информационных активов. Это выражается в атаках, деструктивных технологических акциях и попытках хищения крупных массивов информации.

На этом фоне особенно остро стоит вопрос замещения западных средств криптографической защиты. Угроза "окирпичивания" рабочих станций, зашифрованных зарубежными продуктами, без возможности вернуть доступ к защищаемой информации резко возросла. В таких условиях решение задач импортозамещения является жизненно важным вопросом, требующим максимального внимания и оперативной замены средств шифрования на безопасные отечественные аналоги.

Средство криптографической защиты информации Secret Disk для Linux как нельзя лучше подходит для решения задач экстренного импортозамещения. Secret Disk для Linux является функциональным аналогом распространённых западных средств защиты и обеспечивает значительно большую безопасность защищаемых данных за счёт ряда технологических особенностей:

- Исходный код программного продукта разработан опытной командой "Аладдин Р.Д.". В него не включены сторонние библиотеки. Secret Disk для Linux является полностью отечественным решением.
- Защитные механизмы (шифрование, аутентификация, ключевая схема) наследованы из модуля Secret Disk Crypto Engine (для Windows), являющегося СКЗИ. Модуль сертифицирован ФСБ России по классу КС1, КС2.
- Техническое решение Secret Disk для Linux полностью удовлетворяет рекомендациям ТК 26 и в настоящий момент проходит процедуру сертификации в ФСБ России (СКЗИ КС1, КС2).
- Техническое решение Secret Disk для Linux полностью реализует ряд мер защиты, предъявляемых ФСТЭК России к средствам безопасности и в настоящий момент проходит процедуру сертификации на соответствие этим мерам (СЗИ от НСД УД4).

Задачи безопасности, которые решаются за счёт использования Secret Disk для Linux на рабочих станциях организации:

- **Хранение ценной информации на стационарных компьютерах и перенос большого количества файлов на ноутбуках организации**. Дистанционный или гибридный режим работы, частые командировки и просто работа сотрудника на ноутбуке, зачастую сопровождается копированием файлов из информационных систем или файловых хранилищ себе на рабочую станцию. При этом скопированные на диск компьютера данные хранятся в незащищённом, незашифрованном виде. Эти действия часто обосновываются скоростью доступа/обработки, удобством, необходимостью работы вне офиса, и т.п. Однако, такой способ хранения ценной информации обостряет угрозы её утечки и последующей компрометации.
- **Обработка ценной или критичной информации на компьютере в условиях недоверенной среды, сопровождающаяся подключением к недоверенным или публичным сетям**. В такой ситуации угрозы утечки конфиденциальной информации относятся как к стационарным, так и мобильным компьютерам организации.
- **Защита от "админа".** Потенциальная угроза доступа к ценной или критичной информации со стороны привилегированных пользователей (ИТ-администраторов организации).

2. Общие сведения

Secret Disk для Linux —система защиты конфиденциальной информации на дисках компьютеров организации.

2.1 Назначение

Основным назначением Secret Disk для Linux является криптографическая защита (далее – шифрование) данных, обеспечивающая высокую степень конфиденциальности обрабатываемой информации на рабочих станциях пользователей организации.

Система позволяет обеспечить:

- предотвращение доступа к файлам и папкам, содержащим ценную информацию на рабочих станциях организации;
- предотвращение утечки конфиденциальной информации при утере ноутбука;
- надёжное предотвращение доступа к информации при передаче рабочей станции/ноутбука в сервисный центр или при выходе этой техники из строя;
- разграничение прав доступа между администраторами ИТ и ИБ;
- защита информации от злонамеренных действий системного администратора;
- выполнение требований регуляторов по обязательной защите конфиденциальной информации, обрабатываемой на рабочих станциях.

2.2 Противодействие угрозам организации

С точки зрения руководства организации основным эффектом от внедрения Secret Disk для Linux является существенное снижения рисков компрометации критичной информации и всех вытекающих из этого последствий. Использование Secret Disk для Linux позволяет оперативно заменить зарубежные средства шифрования без снижения уровня защиты. Перечень угроз и контрмер, реализуемых Secret Disk для Linux, сопоставим с перечнем всей линейки продуктов Secret Disk:

Таблица 1 – Противодействие угрозам организации

Пример угрозы	Контрмеры, реализуемые с помощью Secret Disk для Linux
• Несанкционированный доступ злоумышленника к незащищённой конфиденциальной информации на дисках рабочих станций. • Хищение или потеря мобильных компьютеров с незащищёнными данными. • Доступ нежелательных лиц к данным, хранящимся на дисках компьютеров или ноутбуков, отправленных для ремонта в стороннюю организацию или в технический отдел. • Отправка конфиденциальной информация по ошибочному адресу и, как следствие, – компрометация отправленной информации. • Получение доступа к защищённой конфиденциальной информации с помощью учётных данных, полученных методами социальной инженерии.	• Криптографическая защита данных методом "прозрачного" шифрования. Данные на защищённых дисках всегда хранятся в зашифрованном виде. Даже в случае изъятия или утери компьютера данные невозможно использовать. • Аутентификация зарегистрированных пользователей Secret Disk для Linux с использованием ключевых контейнеров пользователей (виртуальный аутентификатор). • Применение стойких алгоритмов шифрования ГОСТ и специальных режимов шифрования, рекомендованных для применения в устройствах хранения данных. • Отказ от использования несертифицированных модулей криптографии, входящих в состав операционной системы.

2.3 Меры защиты ФСТЭК

Secret Disk для Linux закрывает следующие мер защиты информации по требованиям ФСТЭК:

Таблица 2 – Соответствие мерам защиты ФСТЭК России

Меры защиты ФСТЭК	Функция безопасности	Возможности Secret Disk для Linux
ИАФ.1 ИАФ.5	Идентификация и аутентификация пользователей	Идентификация и аутентификация пользователя до открытия сеанса работы с защищаемой информации или доступа к управлению средством
ЗНИ.4	Защита данных пользователя	Разграничение доступа к защищаемой информации, предотвращение раскрытия защищаемой информации при нарушении целостности информационной системы
УПД.1 УПД.2 УПД.4 УПД.11	Управление доступом	Разграничение доступа к функциям управления работой средства. Управление параметрами носителей защищаемой информации
РСБ.3	Регистрация событий безопасности	Запись событий работы средства и предоставления доступа в журнал событий операционной системы

2.4 Общие принципы работы Secret Disk для Linux

Secret Disk для Linux имеет клиент-серверную архитектуру.

Ключевые компоненты архитектуры:

Программный агент

- Реализует функции криптографической защиты информации и двухфакторную аутентификацию пользователя.
- Контролирует доступ пользователя к зашифрованной информации.

Менеджмент сервер

- Обеспечивает контроль и управление служебными функциями системы.
- Использует проприетарную СУБД, в которой безопасно хранится и обрабатывается информация о пользовательских учетных записях, параметрах системы и конфигурации остальных компонентов.

Консоль управления

- Представляет собой графический интерфейс управления и настройки конфигурационных параметров Системы.
- Обеспечивает централизованное управление политиками шифрования на большом количестве рабочих станций.

Рисунок 1 – Архитектура Secret Disk для Linux

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

Шифрование системного раздела

Системный раздел – это корневой раздел операционный 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.

Активации защиты системного раздела предшествует 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. 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 разделов с пользовательскими данными

Этот режим шифрование применяется в случаях, когда пользовательские данные на диске размещены отдельно от операционной системы, например, в разделе "home". Разделы, которые нужно защищать, можно выбрать при установке защиты.

Шифрование дополнительных разделов реализовано по такому же принципу, как и системного раздела. Используется тот же драйвер и процедура активации защиты. При загрузке системы необходимо ввести пароль, чтобы все защищенные разделы были подключены.

Шифрование виртуального диска

Secret Disk для Linux позволяет создавать защищенные виртуальные диски. В операционной системе виртуальный диск выглядит как обычный, физический диск, внутри которого хранятся данные. Он эмулирует реальное дисковое устройство. Буквенный идентификатор присваивается виртуальному диску динамически, при его подключении. Виртуальные диски, созданные средствами Secret Disk для Linux, всегда защищены и их данные зашифрованы. После аутентификации пользователя виртуальный диск монтируется системой и отображается в виде обычной файловой папки на диске.

Всё содержимое виртуального диска хранится в одном файл-контейнере в зашифрованном виде. Подключённый виртуальный диск ОС воспринимает, как обычный диск. Файл подключённого виртуального диска защищён от удаления.

Данные, хранящиеся на зашифрованных виртуальных дисках доступны только администратору Secret Disk для Linux и пользователям, владеющим ключевым контейнером пользователя (далее – ККП) 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. Отключённый 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.

2.5 Шифрование данных

Защищённое хранение данных с применением стойких алгоритмов шифрования, предоставляемые:

- ГОСТ 34.12-2018, ГОСТ 34.13-2018 (шифрование данных);
- ГОСТ 34.10-2018, ГОСТ 34.11-2018 (аутентификация и проверка целостности);
- ГОСТ Р 34.12-2015 (шифрование системного раздела).

2.6 Функции и возможности

1. Полнодисковое прозрачное шифрование системного раздела с применением алгоритма ГОСТ Р 34.12-2015 Кузнечик.
2. Поддержка разметки диска стандарта GPT и логических разделов диска типа LVM.
3. Доступ к загрузке защищенной операционной системы по паролю.
4. Автоматическая проверка параметров операционной системы.
5. Автоматическое конфигурирование параметров защиты перед стартом зашифрования.
6. Разграничение прав доступа между администраторами ИТ и ИБ при включении защиты.
7. Механизм защиты файл-контейнера, который монтируется к папке пользователя как виртуальный диск. После прохождения аутентификации, пользователю предоставляется доступ к папке с защищёнными файлами.
8. Монопольное предоставление доступа к виртуальным дискам – подключение диска и доступ к информации разрешен только пользователю-владельцу.
9. Разграничение ролей на администратора и пользователя Secret Disk для Linux. Это обеспечивает возможность изоляции пользователя от задач безопасности. При этом администратор ИБ не имеет доступа к защищаемым данным, но может управлять параметрами безопасности.
10. Два способа управления средством защиты – графический интерфейс и классическая командная строка. Это позволяют администратору выбрать наиболее удобный способ настройки. При этом командная строка позволяет автоматизировать некоторые функции, удобно интегрируя Secret Disk для Linux с настройкой других параметров ОС Linux.
11. Настраиваемый язык интерфейса – русский или английский.
12. Обязательная двухфакторная аутентификация пользователей и администраторов с использованием ККП.
13. Возможность применения усиленной и строгой многофакторной аутентификации с использованием аппаратных ключей (смарт-карт и USB-токенов JaCarta) благодаря интеграции с SecurLogon.
14. Сертифицированное ФСБ России средство криптографической защиты информации "Secret Disk Crypto Engine", на базе которого реализованы все защитные и контрольные механизмы.
15. Возможность установки подписанных пакетов для ОС Astra Linux из сетевого репозитория.

2.7 Централизованное управление

Выполнение большинства сервисных операций и действий с дисками пользователей через административный портал с возможностью локального или удалённого управления. От конечных пользователей при работе не требуется специальных знаний и квалификации, что значительно упрощает внедрение и эксплуатацию средства защиты.

2.8 Гибкая ключевая схема

- Аутентификация пользователей производится на основе индивидуальных ККП, которые могут размещаться на съёмных носителях или рабочей станции пользователя. Данные шифруются симметричными ключами.
- Ключи шифрования данных обрабатываются автоматизированно. Администратор ИБ может управлять функциями шифрования, но не имеет возможности ознакомления с защищаемой информацией.
- В отдельных случаях (например, утрата пользователем аппаратного носителя) регламент предусматривает визуализацию ключа шифрования и передачу его пользователю для экстренного доступа к данным. Система защиты, при этом, считает ключ шифрования скомпрометированным. Такие действия Администратор ИБ выполняет только в исключительных ситуациях.
- Ключи шифрования передаются, между компонентами системы, только в защищённом виде. При этом выполняются все требования и рекомендации ТК 26. Спулов или временных файлов с ключевой информацией не применяется – т.е. ключевая информация никогда не записывается на диск компьютера в открытом виде.
- Процесс аутентификации с помощью ККП можно гибко и разнообразно интегрировать с имеющейся в ОС на базе Linux системой плагинов аутентификации – PAM.

3. Технические требования и характеристики

3.1 Системные требования

Secret Disk для Linux поддерживает ряд отечественных сертифицированных операционных систем и предъявляет следующие требования к среде функционирования

Таблица 3 – Системные требования

Поддерживаемые операционные системы	Astra Linux Special Edition 1.7
Объём оперативной памяти	не менее 2 ГБ
Свободное место на диске	не менее 1 ГБ

3.2 Технические характеристики

Таблица 4 – Параметры

Объекты с защиты	Подключаемый пользователем виртуальный диск Системный раздел с разметкой GPT или LVM
Размеры защищаемых ресурсов	Виртуальный диск объемом от 100 МБ до 1 ТБ Системный раздел от 1 ГБ
Поддерживаемые файловой системы	EXT4
Тип аутентификации	Двухфакторная аутентификация с ключевым контейнером пользователя в виде файла
Основные криптографические алгоритмы	ГОСТ 34.12-2018, ГОСТ 34.13-2018 (шифрование данных); ГОСТ 34.10-2018, ГОСТ 34.11-2018 (аутентификация и проверка целостности) ГОСТ Р 34.12-2015 (шифрование системного раздела)
Интерфейс управления	Графический интерфейс пользователя Утилиты командной строки
Поддерживаемые языки	Русский, Английский

4. Роли пользователей и их функции

В Secret Disk для Linux используется ролевая модель управления полномочиями пользователей: права доступа в системе назначаются присвоением каждой учётной записи одной или нескольких ролей, обладающих определённым набором прав.

1. Администратор информационной безопасности

Администратор информационной безопасности (далее – Администратор ИБ) выполняет все действия, связанные с созданием защищённых ресурсов и предоставлении прав доступа к ним. Также он управляет настройками самой системы Secret Disk для Linux, её политиками и ролями пользователей.

Действия Администратора ИБ, осуществляемые через портал управления или утилиты командной строки:

- управление пользователями Secret Disk для Linux: добавление, удаление, блокирование, назначение ролей;
- создание и удаление виртуальных дисков;
- создание и удаление ККП.

Действия с защищаемыми ресурсами: (зашифрование, расшифрование, присоединение, отсоединение и т.д.)

2. Пользователь

Пользователь имеет доступ к данным, защищённым средствами Secret Disk для Linux. Для этого используется приложение, установленное на рабочей станции.
Для доступа к защищённым ресурсам Пользователь активирует программу Secret Disk для Linux в системном трее и вводит пароль. При успешной авторизации, осуществляется монтирование защищённого виртуального диска к целевой папке и предоставление доступа пользователю к этой папке.