

Система предотвращения утечек конфиденциальной информации с помощью шифрования



Secret Disk

- ▶ Защита информации на корпоративных ПК и ноутбуках
- ▶ Двухфакторная аутентификация пользователей и администраторов безопасности
- ▶ Разграничение прав доступа к зашифрованной информации
- ▶ Предотвращение утечек информации на USB Mass Storage
- ▶ Защита от действий системных администраторов



ПОЧЕМУ ВАЖНО ЗАЩИЩАТЬ ИНФОРМАЦИЮ НА КОРПОРАТИВНЫХ ПК И НОУТБУКАХ

Традиционно большая часть усилий по обеспечению информационной безопасности направлена на организацию защищённого периметра корпоративной сети. Это гарантированно предотвращает проникновение злоумышленника внутрь ИТ-инфраструктуры организации. Однако, сетевая защита перестаёт быть гарантом безопасности, как только данные покидают периметр. Возрастающая мобильность современных сотрудников, использующих корпоративные ноутбуки во время командировок и встреч, или вынужденных работать из дома, значительно повышает риск утечки конфиденциальной информации.

48%

утечек происходит из-за утери или кражи корпоративного ноутбука¹

69%

доля ноутбуков от общего количества корпоративных ПК выросла до 69% в связи с распространением удалённого режима работы

95%

утраченных данных попадают в распоряжение злоумышленников незашифрованными или с низкой степенью защиты от взлома²

Данные на стационарных ПК также могут быть скомпрометированы - неконтролируемое копирование информации на внешние носители, утеря или кража этих носителей, неограниченные права доступа у системных администраторов и пр.

ЧТО ПОВЫШАЕТ ВЕРОЯТНОСТЬ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ?

- Постоянные выезды сотрудников в командировки или на встречи с корпоративным ноутбуком
- Смешанный режим работы - сотрудник часть времени работает на "удалёнке", а часть в офисе
- Наличие в компании нескольких системных администраторов, обязанности которых пересекаются
- Обмен архивами конфиденциальной информации между сотрудниками и контрагентами
- Неконтролируемое использования USB-флеш накопителей в корпоративной среде
- Большой парк корпоративных ноутбуков, сервисное обслуживание которых производится вне офиса

РЕШЕНИЕ

Решение проблемы – **применение шифрования для работы с конфиденциальной информацией.**

Secret Disk надёжно защищает конфиденциальную информацию, предотвращая кражу данных из корпоративных ноутбуков, ПК и серверов. Для этого используется шифрование на всех логических уровнях:

шифрование дисков (FDE)

Шифрование томов дисков для хранения и переноса данных

шифрование системного диска

Контроль загрузки и защита системного раздела ОС Windows

шифрование файлов и папок

Защита конфиденциальной информации от привилегированных пользователей

защита виртуальных дисков

Криптографическая защита информации в виртуальных дисках (файлы и папки)

защита USB-флеш

Защита информации при использовании флеш-накопителей и USB-HDD

шифрование профилей

Шифрование информации на основе профилей пользователей



Шифрование – бескомпромиссный способ ограничить доступ к конфиденциальной информации. Даже получив доступ к компьютеру или серверу, злоумышленник не сможет воспользоваться данными и расшифровать их. Современные алгоритмы шифрования с большой длиной ключа гарантируют стойкость ко взлому, даже если для этого используется высокопроизводительная вычислительная техника.

¹ По данным компании "Аладдин Р.Д."

² По данным High-Tech Bridge SA

РЕШАЕМЫЕ ЗАДАЧИ

ЗАЩИТА ИНФОРМАЦИИ В СЛУЧАЕ УТЕРИ ИЛИ КРАЖИ НОУТБУКА

- Загрузка операционной системы на ноутбуке доступна только авторизованному пользователю
- Доступ в систему возможен только после предъявления USB-токена
- Зашифрованные системные файлы недоступны для неавторизованного пользователя
- Стойкий алгоритм шифрования препятствует автоматизированному криптоанализу информации

ЗАЩИТА ИНФОРМАЦИИ ПРИ ОБМЕНЕ ЕЮ МЕЖДУ СОТРУДНИКАМИ И КОНТРАГЕНТАМИ

- Чувствительная информация хранится в защищённом криптоконтейнере
- Зашифрованные данные, скопированные на внешний носитель информации, недоступны для прочтения злоумышленником на стороннем компьютере
- Расшифровка информации второй доверенной стороной обеспечивается с помощью специальной утилиты

ЗАЩИТА ИНФОРМАЦИИ ОТ ДЕЙСТВИЙ СИСТЕМНОГО АДМИНИСТРАТОРА

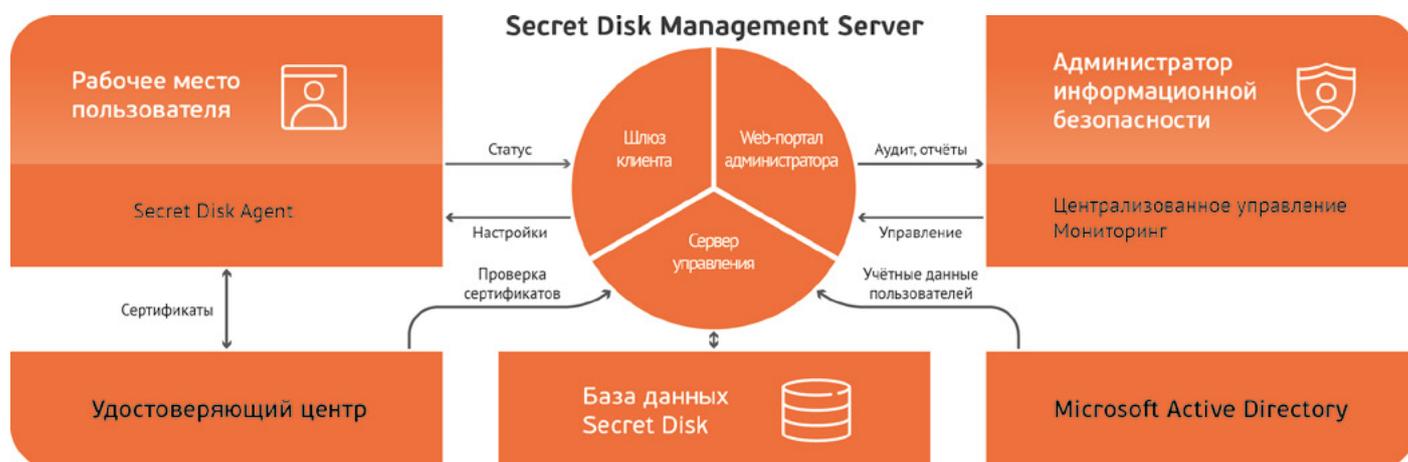
- Несанкционированный доступ к данным по локальной сети невозможен
- Пользователю, независимо от имеющихся у него привилегий, доступны лишь те файлы и папки, которые расположены в его профиле
- Доступ к файлам и папкам прекращается с завершением рабочей сессии

ЗАЩИТА ИНФОРМАЦИИ ПРИ ХРАНЕНИИ И ОБРАБОТКЕ В НЕДОВЕРЕННОЙ СРЕДЕ

Конфиденциальная информация на корпоративном компьютере или ноутбуке защищена при любом сценарии:

- удалённая работа сотрудников
- использование ноутбука в командировках
- ремонт и сервисное обслуживание техники вне офиса

КАК ЭТО РАБОТАЕТ



ПРЕИМУЩЕСТВА



ПРОЗРАЧНОЕ ШИФРОВАНИЕ

Работа Secret Disk не влияет на производительность и незаметна для пользователей



ШИФРОВАНИЕ НА ВСЕХ ЛОГИЧЕСКИХ УРОВНЯХ

Одновременное использование нескольких механизмов шифрования



ИНТЕГРАЦИЯ В ИТ-ИНФРАСТРУКТУРУ

Простота управления и совместимость с ключевыми элементами ИТ-инфраструктуры компании (сеть, ОС, БД)



РОССИЙСКИЕ И ЗАРУБЕЖНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Поддержка российских и зарубежных криптоалгоритмов



ЗАЩИТА ОТ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

Пофайловое шифрование защищает от действий системных администраторов с привилегированным доступом



СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Сертифицированное средство шифрования (ИСПДн до УЗ1, ГИС до 1 класса, АС до класса 1Г)

ДЛЯ КОГО?



SECRET DISK ENTERPRISE

Организациям с большим парком компьютеров и ноутбуков и сложной ИТ-инфраструктурой

Централизованное управление и контроль большого количества рабочих мест, клиент-серверная архитектура.

Срочная лицензия на 1 год. Сервер управления входит в стоимость.



SECRET DISK SERVER

Организациям с большим количеством серверов, хранящих и обрабатывающих конфиденциальную информацию

Защита файловых серверов и серверов приложений.

Бессрочная лицензия. В стоимость включен 1 год технической поддержки.



SECRET DISK 5 (PERSONAL)

Организациям и предприятиям малого и среднего бизнеса

Защита персональных рабочих мест (персональные компьютеры, ноутбуки).

Срочная лицензия на 1 год.

СРАВНЕНИЕ РЕДАКЦИЙ

Возможности	Secret Disk Enterprise	Secret Disk Server	Secret Disk 5 (Personal)
Шифрование			
Модуль шифрования Secret Disk Crypto Engine ^{NEW}			•
Шифрование данных на основе профилей пользователей ^{NEW}			•
Шифрование системного раздела жёсткого диска	•		•
Шифрование логических разделов жёсткого диска	•	•	•
Шифрование виртуальных дисков	•	•	•
Шифрование файлов и папок	•		•
Шифрование данных на USB-флеш накопителях	•		•
Управление и мониторинг			
Централизованное управление	•	•	
Мониторинг, протоколирование и аудит действий пользователей	•	•	
Резервное копирование и восстановление ключей шифрования в случае утери USB-токена	•	•	•
Строгая двухфакторная аутентификация			
Двухфакторная аутентификация администратора безопасности Secret Disk	•	•	•
Двухфакторная аутентификация пользователей до загрузки ОС	•		•
Применение USB-токенов, смарт-карт и PIN-кодов для доступа к защищённым данным	•		•
Совместимость с ИТ-инфраструктурой			
Поддержка обновлений ОС Windows 10 на зашифрованном системном разделе ^{NEW}	•		•
КриптоПро CSP 5.0 ^{NEW}	•	•	•
Microsoft Active Directory	•		
Public Key Infrastructure (PKI)	•	•	•
Российские криптоалгоритмы ГОСТ Р 34.12-2015, ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012	•	•	•
Международные криптоалгоритмы AES256, RSA1024/2048 и TripleDES	•	•	•



**СЕРТИФИКАТ
ФСТЭК РОССИИ**
ТУ, РД НДВ4



**СЕРТИФИКАТ
ФСБ РОССИИ**
КC1, КC2



**РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО**
№ 513, № 514, № 519, № 4322



+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 № 1823 от 26.08.19
Система менеджмента качества АО "Аладдин Р.Д.", соответствующая требованиям ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и дополнительным требованиям ГОСТ РВ 0015-002-2012, сертифицирована в двух системах: Росаккредитация, сертификат соответствия № RU CMS-RU.ФК14.00263 (срок действия до 20.07.2021); система добровольной сертификации "Военный регистр", сертификат соответствия № ВР 21.1.13537-2019 (срок действия до 24.04.2022)

© 1995-2021, АО "Аладдин Р.Д.". Все права защищены.