Cryptallit LSM

Замена популярного средства шифрования MS Bitlocker без наследия проблем безопасности

Почему компании ищут альтернативу Bitlocker?

Применение программы шифрования информации MS Bitlocker широко распространено в крупных российских компаниях. Такая популярность программы в первую очередь объясняется экономическими причинами: на территории РФ программа бесплатна, даже для корпоративных клиентов. В дополнение к этому, данное средство шифрования отличается своей простотой и низкими затратами на администрирование.
Однако в складывающихся условиях Bitlocker является проблемным и сомнительным средством защиты, использование которого сопряжено с высокой вероятность возникновения критических угроз:

Специалисты команды Cryptallit проводят технический анализ и изучение сценариев атак и уязвимостей программы Bitlocker. Это позволяет нам повышать стойкость ключевых защитных механизмов Cryptallit LSM. Каталог содержащий описание сценариев уязвимостей Bitlocker, может быть предоставлен по запросу.

- *Враждебные действия*: Программа разработана компанией Microsoft, которая с недавнего времени ведет враждебную санкционную политику против российских компаний
- *Эксплуатация уязвимостей*: В программе найдено большое количество уязвимостей, а также проблем, связанных с хранением и использованием ключей шифрования.
- *Возможность атаки*: возможная политически ориентированная атака Microsoft путем безусловного обновления параметров безопасности ОС Windows приведет к блокировке рабочих станций, зашифрованных Bitlocker.
- *Нецелевое использование*: Программа не предназначена для корпоративных сценариев защиты информации, а ориентирована на частное, домашнее применение.
- *Экономическая ловушка*: Для организации, использующей бесплатное средство защиты, переход на профессиональное программное обеспечение сложная организационная задача.

Что такое надежность средства защиты?

К современному средству защиты информации предъявляется множество самых разнообразных требований, связанных с функциональной оснащенностью, простотой эксплуатации и разумной лицензионной политикой. Однако наиболее значимым и востребованным свойством продукта безопасности является надежность его защитных механизмов.
Надежность средства защиты строится на реализации важнейших качеств продукта и команды, которая этот продукт создает:

- **Страна приписки**: продукт должен создаваться, поддерживаться и развиваться отечественным производителем.
- **Легальность**: производитель средства защиты должен иметь все необходимые лицензии и высокую квалификацию в своей предметной области.
- **Эффективная поддержка:** команда продукта обеспечивает прямую, оперативную поддержку своих клиентов.
- **Санкционная безопасность**: использование средства защиты не должно быть сопряжено с санкционными рисками западных производителей.
- **Стойкость**: для защиты информации должны быть реализованы методы, обеспечивающие максимальную степень конфиденциальности информации.
- **Прогрессивное развитие:** дорожные карты развития продукта должны быть ориентированы на решение проблем клиентов.

Cryptallit LSM
модуль локальной безопасности

Как решить проблему перехода с Bitlocker?

Для успешного решения проблемы заказчику нужен функциональный аналог, обеспечивающий реализацию схожих механизмов защиты. При этом сценарии эксплуатации и администрирования нового продукта не должны сильно отличаться от сценариев Bitlocker. Альтернативное решение должно обладать независимостью от инфраструктурных сервисов Microsoft, иначе целесообразность замены можно поставить под большое сомнение. Новый продукт должен уметь функционировать автономно (независимо). **Главное** - альтернативное средство защиты должно решать все уязвимости и проблемы безопасности Bitlocker.

Cryptallit LSM модуль локальной безопасности

Модуль локальной безопасности системы защиты Cryptallit обеспечивает защиту ценной и конфиденциальной информации на ноутбуках и рабочих станциях. Модуль специально создавался с учетом актуальных проблем российских компаний и поэтому является функциональным аналогом MS Bitlocker не имеющим наследия его проблем безопасности.

- защита информации на дисках рабочих станций с помощью стойких криптографических алгоритмов
- контроль загрузки ОС Windows с применением функций аппаратного модуля TPM
- централизованное управление функциями шифрования на рабочих станциях

Технологические преимущества продукта

Использование модуля локальной защиты обладает рядом значимых преимуществ, которые заметно выделяют его на фоне остальных программ защиты данных.

Централизованное управление множеством агентов шифрования позволяет установить защиту сразу на всех компьютерах организации, даже если ИТ-инфраструктура территориально распределена.

Высокая производительность механизмов шифрования позволяет защищать даже маломощные рабочие станции, не переживая за скорость работы ОС и совместимость со старыми версиями аппаратного модуля TPM.

Защищенное хранение, передача и использование ключей шифрования обеспечивает максимальную стойкость системы защиты при попытках атак, основанных на поиске и выявления ключей шифрования.

Использование аппаратного модуля TPM для обеспечения защищенного режима загрузки ОС Windows существенно повышает уровень безопасности рабочей станции и усиливает функции шифрования

Сочетание нескольких режимов доверенной загрузки ОС Windows (TPM, Пароль, TPM+Пароль) позволяет выбрать способ, который максимально точно подходит под рабочие задачи и сценарии организации

Собственная реализация алгоритмов шифрования позволяет достичь максимального уровня прозрачности защитных механизмов, что делает работу системы безопасности незаметной для пользователя

Сравнение продуктов MS Bitlocker и Cryptallit LSM

Ключевым вопросом любого сравнения является набор критериев, по которому оно производится. Набор критериев зависит от факторов эксплуатации и рабочих сценариев защиты информации. В нашем сравнении набор критериев отвечает специфике использования систем защиты конфиденциальности.

// Свойства продукта	Пояснение //	MS Bitlocker	Cryptallit LSA
Санкционная независимость продукта			
Страна приписки производителя прогрммы	Россия, дружественные страны	☒	☑
Регистрация в Реестре отечественных программ	Действующая запись в Реестре отечественных программ	☒	☑
Поддержка режимов загрузки ОС			
Режим загрузки ОС: Прозрачный (TPM)	Режим "автологин" на основе проверки TPM	☑	☑
Режим загрузки ОС: Пароль	Проверка только пароля на этапе загрузки	☑	☑
Режим загрузки ОС: Гибридный (TPM+пароль)	Режим двух проверок Пароль+TPM на этапе загрузки	☑	☑
Криптографические функции			
Шифрование системного раздела ОС Windows	Шифрование диска (C:) в ОС Windows	☑	☑
Шифрование съемных носителей	Шифрование USB-флэш	☑	☑ RM2024
Использование криптографических алгоритмов:			
▪ ГОСТ Р 34.12-2018 - защита данных	Использование актуальных отечественных алгоритмов	☒	☑ RM2024
▪ AES-256 - защита данных	Использование актуальных зарубежных алгоритмов	☑	☑
▪ RSA - защита ключевой информации	Ассиметричное шифрование при защите КШД	☑	☑
Шифрование диска с занулением своб. секторов	Актуальны режим полного шифрования тома диска	☑	☑
Управление и администрирование			
Собственный сервер управления	Собственная реализация консоли управления системой	☒	☑
Собственное хранилище ключей шифрования	Защищенная база хранения КШД - крипто хранилище	☒	☑
Управление ключами шифрования			
Восстановление доступа при утере пароля	Восстановления доступа при утере пароля пользователя	☑	☑
Одноразовый Recovery Key	Использование одноразовых ключей восстановления	☒	☑

***Расширенная версия сравнения может быть предоставлена по запросу**
***RM2024 – функция включена в дорожную карту развития Cryptallit LSM 2024 года.**

https://cryptallit.ru
sales@cryptallit.ru
+7(495)215-27-23