Cryptallit LSM

Защита ноутбуков и рабочих станций вашей организации

Обманчивое удобство или что может пойти не так?

Ноутбуки удобны потому, что с ними ваши сотрудники мобильны: могут свободно перемещаться и работать откуда угодно. Вместе с сотрудниками свободно перемещаются и могут оказаться где угодно ваши конфиденциальные данные. Что может случиться?

- **Потеря или кража.** Люди есть люди – им свойственно ошибаться. Ноутбуки теряют, забывают их в такси, кафе, гостиницах и аэропортах. Счет идет на миллионы в год. По статистике 97% утерянных ноутбуков не возвращаются.
- **Ремонт и обслуживание.** Техника периодически выходит из строя. Когда вы сдаете ноутбук в сервисный центр – физический доступ к нему и носителям данных есть у всех сотрудников центра. В 38% случаев сотрудники сервисов скрытно копируют данные клиентов.
- **Гостиницы, поезда и всё такое.** Во время командировки сотрудники не носят с собой технику круглые сутки. Ноутбук часто остается без присмотра (в номере, купе). В это время доступ к нему и данным на нем есть у обслуживающего персонала и у потенциальных злоумышленников.

В вашей компании есть регламент по защите информации?

Подумайте **не о том, что должно быть** на ноутбуках ваших сотрудников, а о том, **что может там оказаться**. Сотрудники - живые люди и любят чтобы вся нужная информация всегда была под рукой, тем более в дороге. Копируем все на ноутбук – ведь это же удобно! Да и в самолёте без интернета можно поработать...

Что делать?

Логичным ответом на данный вопрос будет – защитить всю имеющуюся информацию на ноутбуках вашей организации. Наиболее надежную защиту данных обеспечит полное шифрование дисков. Это единственный простой способ гарантировать, что утеря ноутбука не приведет к компрометации и разглашению конфиденциальных данных. К тому же, этот способ самый «прозрачный» метод криптографической защиты, гарантирующий вашим сотрудникам полный комфорт при работе с зашифрованной информации.

Что нужно учесть при выборе средства шифрования?

- Bitlocker - точно не подойдет. Средство от Microsoft стало стандартом в мире и не требует дополнительных лицензий, но внедрять его в РФ сегодня опасно из-за санкционных рисков. В любой момент при любом обновлении Windows данные могут оказаться заблокированными. Так же Bitlocker обладает большим количеством уязвимостей. Гораздо надежнее выбрать отечественное решение.
- Прозрачность работы. Работать с зашифрованным компьютером должно быть легко, шифрование не должно вносить дополнительных сложностей.
- Надежность алгоритмов шифрования. Средство должно поддерживать распространенные алгоритмы шифрования, зарекомендовавшие себя за долгие годы применения.
- Безопасность ключей шифрования – мы точно не хотим повторения сценария «сломай за одну минуту», поэтому средство шифрования должно защищать ключи шифрования при хранении и передаче.
- Централизованное управление. Пользователи не станут шифровать ноутбуки самостоятельно, это должна сделать ИТ-служба. Управление шифрованием должно осуществляться с единой консоли администратора.

Какое решение соответствует всем перечисленным требованиям?

Cryptallit LSM — это система полнодискового шифрования персональных компьютеров, которая реализует максимально надежный метод защиты ценной информации с помощью стойких криптографических алгоритмов. Система обеспечивает защиту информации на компьютерах пользователей, а в сочетанием с модулем сетевой безопасности **Cryptallit NSM** и на файловых серверах предприятия под управлением Windows, создавая тем самым замкнутое пространство обработки и хранения конфиденциальной информации.

Как работает система и почему это эффективно?

1. Cryptallit LSM загружается до операционной системы (ОС). Таким образом злоумышленник не сможет получить доступ к данным системы, когда компьютер выключен.
2. После загрузки ОС система работает в качестве низкоуровнего драйвера и оказывает минимальное влияние на скорость работы компьютера.
3. Управление системой осуществляется с централизованной консоли администратора ИБ.
4. Файлы хранятся на диске только в зашифрованном виде. Все!
5. Если пользователь забыл пароль и не может загрузить компьютер – это решается путём получения одноразового пин-кода от администратора безопасности и последующей самостоятельной замены пароля на новый.

Cryptallit LSM
Модуль локальной безопасности

Преимущества продукта

Эффект от использования модуля локальной безопасности ***Cryptallit LSM*** дает ряд значимых преимуществ, которые заметно выделяют его на фоне остальных программ защиты данных.

Отечественное решение

Продукт обладает полной санкционной независимостью. Создан командой российских разработчиков и зарегистрирован в реестре отечественного ПО (№20257 от 27.11.2023)

Надежность защиты

Защитит данные на ноутбуках и рабочих станциях вашей организации и предотвратит доступ к защищенной информации используя самые надежные методы защиты.

Простота и экономичность

Внедрение системы защиты не потребует дорогого проекта, а эксплуатация возможна силами существующих ИТ-специалистов, не имеющих специальных знаний криптографии.

Полная прозрачность

Защитные механизмы системы работают на системном уровне ОС Windows, что делает защиты данных прозрачной для легитимных пользователей.

Очевидная эффективность

Продукт решает конкретную и понятную для руководства организации проблему – защита важной и конфиденциальной информации на рабочих станциях пользователей.

Ощутимый эффект использования

Состояние полной защищенности ценной информации становится стандартом де факто в современном мире. Шифрование это наиболее простой способ достичь такой защищенности.

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