

# Cryptallit LSM

Защита информации на дисках ноутбуков и рабочих станций организации



Модуль локальной безопасности системы **Cryptallit LSM**, обеспечивает защиту информации на дисках ноутбуков и рабочих станций под управлением ОС Windows. Высокий уровень безопасности достигается за счет сочетания криптографических методов защиты и контроля доступа к защищаемой информации. Cryptallit LSM позволяет зашифровать всю информацию на компьютере, противодействуя ее утечкам.

**Cryptallit LSM** будет наиболее востребованным для защиты организаций с большим количеством мобильных сотрудников, использующих ноутбуки или работающих на «удаленке», а так же организаций с региональными отделениями или филиалами, между которыми активно передвигаются командировочные сотрудники. Вынос ноутбука за пределы периметра организации сопряжен с возникновением большого количества угроз утечки ценной и важной информации, поэтому выбор средства защиты информации в таких условиях должен гарантировать превентивную защиту информации, рассчитанную на сценарии физического доступа злоумышленников к диску потерянного или похищенного компьютера.

## Возможности Cryptallit LSM

### Шифрует и контролирует доступ

Функции продукта реализуют полнодисковое шифрование, что дает максимальный уровень прозрачности системы защиты для авторизованных пользователей.

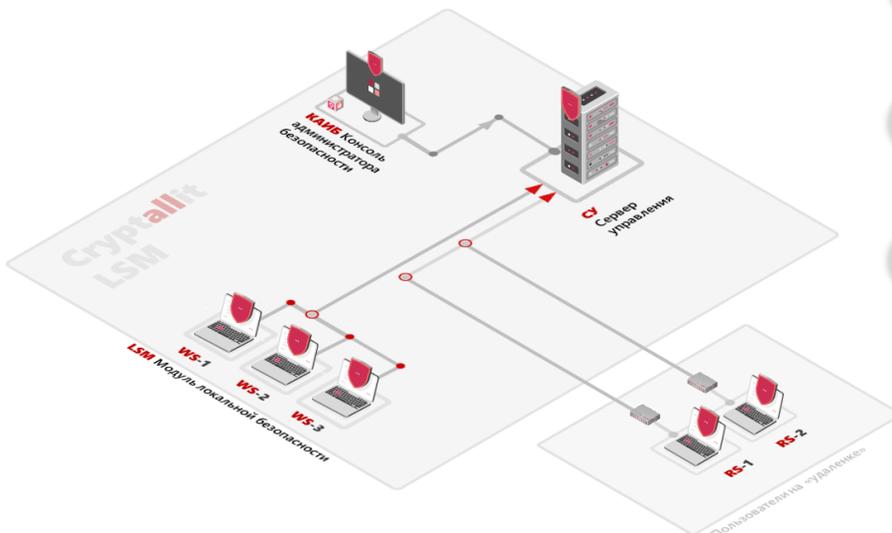
### Противодействует краже информации

При физическом доступе посторонних лиц к компьютеру в случае его кражи, передачи в ремонт или просто на время оставленном, например, в гостиничном номере, доступ к информации будет невозможен, так как она защищена шифрованием, что предотвратит ее утечку.

### Контролирует загрузку ОС Windows

Обеспечение контроля загрузки ОС существенно усиливает защиту компьютера, а выбор различных режимов загрузки позволяет настроить систему соответствии с различными рабочими сценариями организации. Реализованы режимы: – «прозрачная» загрузка, на основе проверки аппаратного модуля TPM, ввод пользовательского пароля и гибридный (TPM+пароль)

## Схема Cryptallit LSM



**Централизованное управление агентами на рабочих станциях**



**Простая интеграция с существующей инфраструктурой**



**Простой и быстрый ввод системы защиты в рабочую эксплуатацию**

## Технологические преимущества продукта

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



### Централизованное управление

Сервер управления множеством агентов шифрования позволяет установить защиту сразу на всех компьютерах организации, даже если сегменты ИТ-инфраструктуры территориально распределены.



### Высокая производительность

Применение производительных алгоритмов шифрования позволяет защищать любые рабочие станции, не переживая за скорость работы ОС Windows и прикладных программ



### Защита ключей шифрования

Защищенная генерация, хранение и использование ключей шифрования дает максимальную стойкость защиты при попытках атак, основанных на поиске и выявлении ключей шифрования.



### Безопасная загрузка ОС Windows

Использование аппаратного модуля TPM реализует защищенный режим загрузки ОС Windows существенно повышая уровень безопасности рабочей станции.



### Режимы загрузки ОС Windows

Реализация нескольких режимов доверенной загрузки ОС Windows (TPM, Пароль, TPM + Пароль) позволяет выбрать способ, максимально подходящий под рабочие задачи организации.



### Полный комфорт пользователя

Оптимизированная реализация алгоритмов шифрования данных позволяет достичь максимальной прозрачности системы защиты, что делает ее работу незаметной для пользователя.



<https://cryptallit.ru>



[sales@cryptallit.ru](mailto:sales@cryptallit.ru)



+7(495)215-27-23

