KASPERSKY SECURITY ДЛЯ БИЗНЕСА

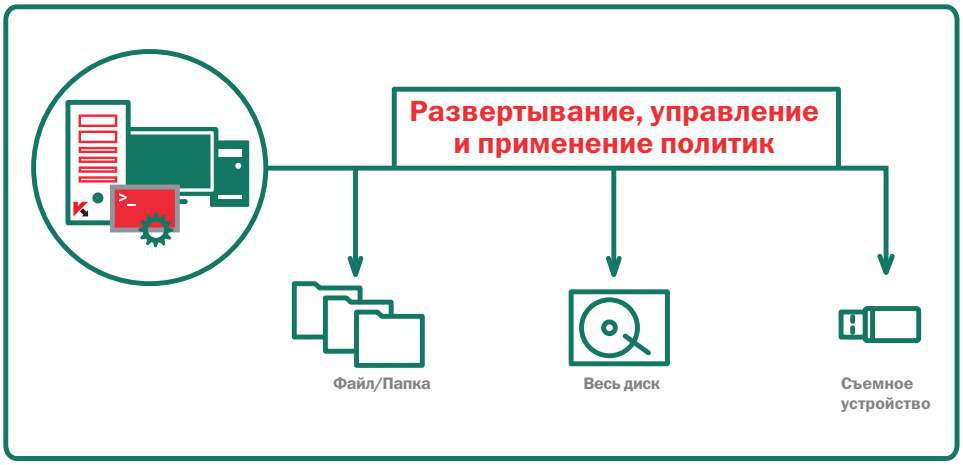
Технология шифрования

Шифрование предотвращает несанкционированный доступ к данным в случае утери носителя информации.

Технология шифрования позволяет избежать утечки ценных данных в случае кражи или утери устройства, на котором они хранятся. В продуктах «Лаборатории Касперского» технология шифрования органично интегрирована с технологиями защиты рабочих мест. Политика шифрования создается и применяется централизованно через единую консоль управления.

Надежная и эффективная защита данных с помощью технологии шифрования «Лаборатории Касперского»:

- ПОЛНОЕ ШИФРОВАНИЕ ДИСКА
- ШИФРОВАНИЕ ФАЙЛОВ И ПАПОК
- ШИФРОВАНИЕ ДАННЫХ НА СЪЕМНЫХ НОСИТЕЛЯХ
- АДМИНИСТРИРОВАНИЕ ИЗ ЕДИНОЙ КОНСОЛИ УПРАВЛЕНИЯ



ПРИЗНАННАЯ В ОТРАСЛИ СИСТЕМА ШИФРОВАНИЯ

«Лаборатория Касперского» использует алгоритм шифрования Advanced Encryption Standard (AES).

ГИБКИЙ ВЫБОР ВИДА ШИФРОВАНИЯ

Для защиты данных на жестких дисках и съемных носителях можно выбрать различные виды шифрования: полное шифрование диска (FDE), шифрование файлов и папок (FLE) или шифрование данных на съемных носителях.

НЕЗАМЕТНОСТЬ ДЛЯ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ

Технология шифрования «Лаборатории Касперского» не оказывает влияния на работу приложений, в том числе во время установки. Обработка защищаемой информации осуществляется «на лету» и не влияет на производительность труда конечного пользователя. Единый вход в зашифрованную систему повышает удобство для пользователя.

Работа системы шифрования «Лаборатории Касперского» не влияет на скорость передачи данных по локальной сети. Данные, предназначенные для внешних пользователей, можно упаковать в специальные контейнеры, защищенные паролем. Для расшифровки контейнера этот пароль необходимо передать получателю по другому каналу связи.

ВОЗМОЖНОСТИ ШИФРОВАНИЯ

ЕДИНАЯ ТЕХНОЛОГИЧЕСКАЯ БАЗА
Поскольку все функции по обеспечению защиты рабочих мест реализованы в рамках единого решения, нет необходимости устанавливать и администрировать отдельные решения для защиты от вредоносных программ, контроля рабочих мест и шифрования.

ВЗАИМОСВЯЗАННЫЕ И ОРГАНИЧНО ИНТЕГРИРОВАННЫЕ ПОЛИТИКИ
Единая технологическая база позволяет администратору создавать комплексные политики. Например, IT-специалист может разрешить подключение только определенных съемных носителей, а также задать применение к этим устройствам политики шифрования (сочетая таким образом политики контроля устройств и технологию шифрования).

ПРЕДУСТАНОВЛЕННЫЕ ПАРАМЕТРЫ ШИФРОВАНИЯ
Параметры шифрования заданы заранее (но могут быть изменены) для часто используемых папок, таких как «Мои документы» и «Рабочий стол», новых папок, расширений файлов и групп расширений файлов (например, для документов Microsoft® Office, архивов сообщений электронной почты и т.д.).

ВОССТАНОВЛЕНИЕ ДАННЫХ В ЭКСТРЕННЫХ СИТУАЦИЯХ
В решении предусмотрен функционал, позволяющий администратору расшифровать данные в случае аппаратного или программного сбоя.

ВОССТАНОВЛЕНИЕ ПОЛЬЗОВАТЕЛЬСКОГО ПАРОЛЯ
Пользователь может восстановить пароль, вводимый перед загрузкой системы, или получить доступ к зашифрованным данным с помощью механизма секретных вопросов.

КАК ПРИОБРЕСТИ

Технология шифрования «Лаборатории Касперского» не продается отдельно, но доступна в следующих продуктах линейки **Kaspersky Security для бизнеса**:

- Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ
- Kaspersky Total Security для бизнеса

НАБОР ДОСТУПНЫХ ФУНКЦИЙ ЗАВИСИТ ОТ ЗАЩИЩАЕМОЙ ПЛАТФОРМЫ
Подробнее: **www.kaspersky.ru**

KESB-DP/Version 0.1/Sept12/Global

KASPERSKY lab