KINGSTON IRONKEY™

Аппаратное или программное шифрование?

Понимание ключевых различий и выбор лучшего варианта для ваших нужд.

В продолжающейся борьбе за безопасность данных разница между аппаратным и программным шифрованием заключается в том, где именно находится защита и насколько она уязвима при реальном использовании. В USB-накопителях и SSD-накопителях то, где реализовано шифрование, определяет, насколько надежно защищены данные и насколько сильно они зависят от системы, вокруг которой работают.

АППАРАТНОЕ	ИЛИ	ПРОГРАММНОЕ
Обработка ключей шифрования Ключи шифрования генерируются внутри аппаратного обеспечения и хранятся на диске.		**Обработка ключей шифрования** Пароль пользователя используется непосредственно как ключ шифрования, а ключи могут находиться в памяти системы.
Защита от атак методом перебора паролей Предназначено для защиты от атак методом перебора путем ограничения количества попыток, после чего устройство может автоматически стереть данные, чтобы предотвратить доступ к конфиденциальной информации при потере или краже накопителя.		**Защита от атак методом перебора паролей** Уязвимость при атаках методом подбора пароля, когда компьютер пытается ограничить число попыток расшифровки, но злоумышленники могут получить доступ к памяти компьютера и обнулить счетчик попыток.
Требования к программному обеспечению или драйверу Не требуется установка драйверов или программного обеспечения на хост-систему.		**Требования к программному обеспечению или драйверу** Требуется установка программного обеспечения и драйверов, при этом совместимость с операционной системой может отличаться.
Ресурсы шифрования Используется специализированный криптографический процессор, встроенный непосредственно в накопитель.		**Ресурсы шифрования** Используются центральный процессор (ЦПУ) и системные ресурсы хост-компьютера для шифрования и расшифровки данных.
Зависимость / уязвимость хост-системы Безопасность внедрена внутрь устройства, которое остается защищенным даже при подключении к ненадежным или зараженным компьютерам.		**Зависимость / уязвимость хост-системы** Безопасность зависит от операционной системы хоста и становится более уязвимой при заражении компьютера вредоносным ПО.
Статус шифрования Шифрование всегда включено и не может быть отключено, его нельзя обойти.		**Статус шифрования** Шифрование может быть включено, отключено или настроено неправильно.
Влияние на производительность Минимальное влияние на производительность, так как шифрование выполняется аппаратным процессором.		**Влияние на производительность** Может негативно влиять на производительность, поскольку шифрование использует общие ресурсы процессора.
Гибкость Шифрование привязано к конкретному USB-накопителю или SSD-накопителю.		**Гибкость** Может быть реализовано практически на любом носителе.

Программное шифрование обеспечивает гибкость, в то время как аппаратное шифрование делает безопасность изолированной и менее подверженной системным рискам. Понимание того, как каждый вариант защищает данные и управляет доступом, помогает выбрать подходящий уровень безопасности для ваших рабочих процессов с учетом профиля рисков.

www.kingston.com/ironkey