USB-накопитель Kingston IronKey D500S с аппаратным шифрованием

Сертификат FIPS 140-3 уровня 3 (ожидается), 256-битное аппаратное шифрование XTS-AES, прочный цинковый корпус

Лучший в своем классе USB-накопитель Kingston IronKey™ D500S/SM оснащен флагманскими средствами безопасности военного уровня. Благодаря им IronKey является самым надежным для защиты конфиденциальной информации. Он сертифицирован на соответствие стандарту FIPS 140-3 уровня 3 (ожидается) с новыми расширениями от NIST, предъявляющими требования к безопасному обновлению микропроцессора для повышенной безопасности и более надежной защиты от атак для правительственных и военных пользователей. Шифрование и дешифрование данных осуществляется на самом накопителе D500S, не оставляя никаких следов в хост-системе. Наряду с аппаратным 256-битным шифрованием XTS-AES, накопитель имеет прочный цинковый корпус, который является водонепроницаемым[1], пыленепроницаемым[1], устойчивым к ударам и вибрации в соответствии с системой военных стандартов[2], устойчивым к давлению и заполнен специальной эпоксидной смолой для защиты внутренних компонентов от проникновения.

Накопитель IronKey D500S является важной моделью, изготовленной в соответствии с передовыми практиками защиты от потери данных (DLP) по самым строгим стандартам безопасности военного уровня для соблюдения законов и правил шифрования данных, таких как CMMC, SOC2, NIS2, FISMA, GDPR, PIPEDA, HIPAA, HITECH, GLBA, SOX и CCPA, наряду с TAA. D500S предоставляет больше возможностей, чем любой другой накопитель в данном классе, и является ведущим в отрасли решением для защиты ценных данных конфиденциального характера.

D500S выполняет самопроверку при загрузке. Перегрев или перенапряжение приведет к отключению накопителя. Для большей уверенности в безопасности в D500S используется прошивка с цифровой подписью, что делает его защищенным от атак BadUSB. Защита от атак методом перебора паролей всегда включена и в конечном итоге выполняет криптографическое стирание данных с накопителя, если превышено количество неверных попыток ввода пароля.

Опция с несколькими паролями для доступа к данным поддерживает до трех паролей: администратора, пользователя и одноразовый для восстановления. Администратор может сбросить пароль пользователя, а также включить одноразовый пароль для восстановления доступа, если пароль пользователя забыт.

D500S поддерживает традиционный режим «Сложного» пароля и режим «Парольная фраза»[3]. Парольные фразы могут содержать от 10 до 128 символов. ФБР рекомендует использовать парольные фразы длиной 15 и более символов, состоящие из нескольких слов, так как они более надежные, но при этом более легкие для запоминания, чем сложные пароли.[4]

D500S включает первую в отрасли опцию двух скрытых разделов (Dual Hidden Partition), позволяющую администратору создать два защищенных раздела с самостоятельно определенным размером для администратора и пользователя. Таким образом можно создать скрытое хранилище файлов, которое можно использовать для предоставления файлов в раздел пользователя по мере необходимости. При использовании ненадежных систем или совместном использовании накопителя скрытые хранилища файлов (Hidden File Store) сохраняют данные в безопасности и невидимыми, если к ним нет надлежащего доступа.

С помощью специальной последовательности клавиш администратор может ввести пароль для криптографического стирания накопителя, которое навсегда уничтожит данные и сбросит настройки накопителя для предотвращения несанкционированного доступа в опасных ситуациях.

Чтобы помочь пользователям избежать проблем с клавиатурой, все экраны ввода пароля содержат символ глаза. Нажатие на него позволяет отобразить введенный пароль, чтобы уменьшить количество опечаток. На английском языке[5] также доступна виртуальная клавиатура для защиты вводимого пароля от клавиатурных шпионов и регистраторов экрана.

D500S также поддерживает два уровня режима «только для чтения» (защиты от записи). И администратор, и пользователь может настроить сессионный режим «только для чтения», чтобы обеспечить защиту накопителя от вредоносного ПО в ненадежных системах. Администратор также может установить глобальный режим «только для чтения», который переводит накопитель в режим «только для чтения» до сброса.

Это также ускоряет двухканальную производительность без снижения безопасности. Накопитель имеет уникальный 8-значный серийный номер, который в электронном виде совпадает с номером, выгравированным на корпусе, вместе со сканируемым штрихкодом для развертывания или проверки накопителя.

D500S предлагает множество вариантов настройки, соответствует требованиям TAA/CMMC и собирается в США.

Модель Managed

Накопители Kingston IronKey D500SM (M = Managed[6]) позволяют централизованно управлять доступом к накопителям и их использованием на крупных предприятиях или в государственных учреждениях.

- Сертификат FIPS 140-3 уровня 3 (ожидается) для обеспечения передовой защиты военного класса
- Опция с несколькими паролями с режимами «Сложный» и «Парольная фраза»
- Первая в отрасли опция двух скрытых разделов (Dual Hidden Partition)
- Пароль для криптографического стирания в опасных ситуациях
- Прочный цинковый корпус для защиты от проникновения, ударов и вибрации в соответствии с военными стандартами, степень защиты IP67: водонепроницаемый/пыленепроницаемый[7]
- Удобный интерфейс
- Полностью настраиваемые функции
- Доступна модель Managed

Ключевые Характеристики

- ## USB-накопитель с аппаратным шифрованием военного класса

  256-битное шифрование XTS-AES с сертификатом FIPS 140-3 уровня 3 (ожидается) с защищенными обновлениями микропроцессора повышает безопасность. Встроенные средства защиты от атак BadUSB и методом перебора паролей. Новая самопроверка накопителя при загрузке, защита от

- ## Пароль для криптографического стирания в опасных ситуациях

  Пароль для криптографического стирани сотрет ключи шифрования, навсегда удалит все данные и сбросит настройки накопителя.

- ## Глобальный и сессионный режимы «только для чтения».

перегрева и перенапряжения для автоматического отключения накопителя при достижении определенных пороговых значений.

- ## Опция с несколькими паролями для восстановления данных

  Используйте пароли администратора, пользователя и одноразовый пароль для восстановления. Администратор может сбросить пароль пользователя и включить одноразовый пароль для восстановления доступа пользователя к данным, если пароль пользователя забыт.

- ## Режимы сложного пароля и парольной фразы

  Выберите режим: «Сложный пароль» или «Парольная фраза». Парольными фразами могут быть полные предложения или несколько слов, которые помните только вы - от 10 до 128 символов. Символ в виде глаза для всех введенных паролей помогает уменьшить вероятность опечаток.

- ## Первая в отрасли опция двух скрытых разделов

  Администратор может создать два скрытых раздела самостоятельно определяемого размера для администратора и пользователя. Таким образом можно создать скрытое хранилище файлов, чтобы обеспечить безопасность и невидимость данных, если к ним нет надлежащего доступа. Два скрытых раздела могут обеспечить дополнительную защиту в ненадежных системах или при необходимости совместного использования накопителя.

  И администратор, и пользователь может настроить сессионный режим «только для чтения», чтобы обеспечить защиту накопителя от вредоносного ПО в ненадежных системах. Администратор также может установить глобальный режим «только для чтения», который переводит накопитель в режим «только для чтения» до сброса.

- ## Прочный корпус, соответствующий строгим стандартам IronKey

  Цинковый корпус устойчив к ударам и заполнен эпоксидной смолой для физической защиты от несанкционированного доступа. Сертификация MIL-STD-810F: защита от механических ударов, вибрации и падения. Водонепроницаемость[1] и пыленепроницаемость[1] по стандарту IP67.

- ## Уникальный 8-значный серийный номер и сканируемый штрихкод

  Экономия времени за счет простоты считывания или сканирования штрихкода при вводе в эксплуатацию и возврате, а также во время любой физической инвентаризации.

- ## Полностью настраиваемый

  Включайте, отключайте, изменяйте функции и профиль накопителя. Программа нанесения логотипа (кастомизация).

Спецификации

Основные сертификаты	FIPS 140-3 уровня 3 (ожидается) MIL-STD-810F Соответствие TAA/CMMC, собрано в США
Интерфейс	USB 3.2 Gen 1
Емкость*	8 ГБ, 16 ГБ, 32 ГБ, 64 ГБ, 128 ГБ, 256 ГБ, 512 ГБ
Разъем	Type-A
Скорость[8]	USB 3.2 Gen 1 8–128 ГБ: 260 МБ/с (чтение), 190 МБ/с (запись) 256 ГБ: 240 МБ/с (чтение), 170 МБ/с (запись) 512 ГБ: 310 МБ/с (чтение), 250 МБ/с (запись) USB 2.0 8GB – 512 ГБ: 30 МБ/с (чтение), 20 МБ/с (запись)
Размеры	77,9 x 21,9 x 12,0 мм
Водонепроницаемость/ пылезащищенность[9]	Сертификация по стандарту IP67
Рабочая температура	от 0 до 50 °C
Температура хранения	от –20 до 85 °C
Совместимость	USB 3.0/USB 3.1/USB 3.2 Gen 1

Варианты кастомизации	D500S: включение, отключение, изменение функций и профиля накопителя. Программа нанесения логотипа. D500SM: Изменение профиля накопителя. Программа нанесения логотипа.
Гарантия и поддержка	D500S: 5-летняя гарантия и бесплатная техническая поддержка D500SM: 2-летняя гарантия и бесплатная техническая поддержка
Совместимость	Windows® 11, 10, macOS® версии 11.x – 14.x, Linux[10] Kernel версии 4.4 и выше

Номера Деталей

Серийные накопители

IKD500S/8GB
IKD500S/16GB
IKD500S/32GB
IKD500S/64GB
IKD500S/128GB
IKD500S/256GB
IKD500S/512GB

Сериализуемые накопители с управлением - Serialized Managed

IKD500SM/8GB
IKD500SM/16GB
IKD500SM/32GB
IKD500SM/64GB
IKD500SM/128GB
IKD500SM/256GB
IKD500SM/512GB

Изображение Продукта

* Часть перечисленной емкости устройств хранения на основе флеш-памяти используется для форматирования и прочих функций, поэтому недоступна для хранения данных. В связи с этим фактически доступная емкость для хранения данных меньше, чем указано на упаковке или поверхности продукции. Для получения дополнительной информации обратитесь к руководству Kingston по флеш-памяти, расположенному по адресу Kingston's Flash Memory Guide

1. См. технические характеристики. Допускается использование только сухих и чистых устройств.
2. Сертификация MIL-STD-810F: защита от механических ударов, вибрации и падения.
3. Режим «Парольная фраза» не поддерживается в Linux.
4. Из fbi.gov: Oregon FBI Tech Tuesday: Создание цифровой защиты с помощью паролей, 18 февраля 2020 г
5. Виртуальная клавиатура: поддерживает только американский английский в среде Microsoft Windows и macOS.
6. Служба управления SafeConsole приобретается отдельно.
7. Допускается использование только сухих и чистых устройств.
8. Скорость может варьироваться в зависимости от аппаратного и программного обеспечения, а также модели использования.
9. Сертификация IPX8 IEC 60529: водонепроницаем при закрытом колпачке. Допускается использование только сухих и чистых устройств.
10. Поддержка функций в Linux ограничена. Подробнее см. в руководстве пользователя. Для некоторых дистрибутивов Linux требуется наличие прав пользователя superuser (root) для корректного выполнения команд IronKey в окне терминального приложения.