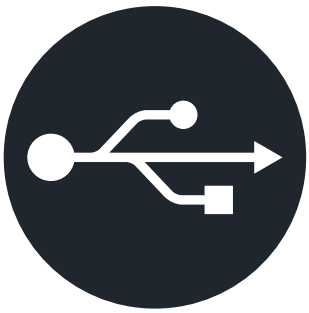
# Как разрешить доступ к USB-накопителю

без ущерба для безопасности вашего устройства

#KingstonIsWithYou #KingstonIronkey

# Введение

В январе 1996 года выход официальной спецификации USB 1.0 знаменовал собой новую эру единообразия, удобства и универсальности как для поставщиков периферийных устройств, так и для конечных пользователей. 27 лет спустя поддерживается обратная совместимость с каждой версией, и USB остается важнейшим элементом интерфейса компьютерного оборудования, начиная от серверов и до смартфонов.



Благодаря простоте подключения и постоянно увеличивающейся скорости портативные USB-накопители заняли одни из ведущих позиций. Да, платой за такое удобство было снижение защиты данных. В современном мире без использования надлежащих инструментов по защите данных, пользователи, которые небрежно относятся к использованию портативных USB-накопителей, подвергают себя и других опасности возможной утечки данных. Это может дорого обходиться для конечных пользователей и даже может поставить под угрозу всю организацию или правительство.

Помимо защиты хост-среды, USB-накопитель также должен быть защищен паролем и аппаратным шифрованием на устройстве. Это обеспечивает наиболее надежную защиту от вторжений. Мы обсудим некоторые передовые методы более безопасного использования USB-накопителей, а также более подробно рассмотрим USB-накопители в целом.

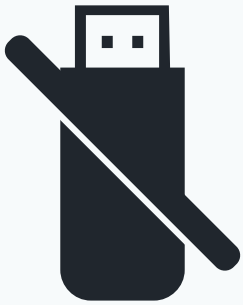
Идеальным является комбинированный подход, однако первостепенное значение имеют надежность шифрования и аппаратные компоненты самого USB-накопителя. Эти накопители приносят выгоду в различных секторах, начиная от финансов и до здравоохранения, производства и вооруженных сил. Они также играют свою роль в дистанционной работе, когда доступ к сети либо недоступен, либо уязвим, либо непрактичен.

Доступны USB-накопители с аппаратным шифрованием, которые имеют различные сертификационные рейтинги и обеспечивают ряд функций безопасности. Учитывая их характеристики и возможности для настройки, пригодность этих накопителей в качестве автономных решений также подтверждается тем, что они находят свое место в любой чувствительной среде.

# Управление порта: USB-накопитель соответствует требованиям программного обеспечения для предотвращения потери данных, предназначенного для управления оконечными устройствами.

На протяжении десятилетий приложения для защиты от вирусов и вредоносных программ обеспечивали защиту на самом фундаментальном уровне, автоматически сканируя загружаемые файлы и подключенные устройства и сообщая о подозрительном содержимом или предпринимая действия в отношении него. Защита, обеспечиваемая антивирусным ПО нового поколения (NGAV), делает в этом отношении шаг вперед. Вместо того, чтобы полагаться исключительно на постоянно обновляемую базу данных сигнатур вирусов, NGAV добавляет функции машинного обучения и обнаружения на основе поведения, которые могут выявлять и устранять неизвестные угрозы.

Однако это не единственное оружие в арсенале, и для тех, кому нужна надежная защита пользовательских периферийных устройств и так далее, программное обеспечение для предотвращения потери данных (DLP) для управления оконечными устройствами предоставляет средства, позволяющие отказать в любом доступе к портам USB и другим точкам доступа.



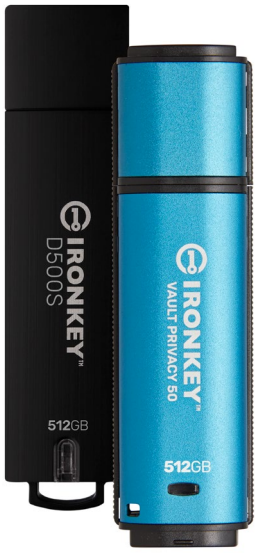
Подход к безопасности «Блокировать все порты», безусловно, может устранить риск и, в некоторых случаях, может быть желательным, но такая политика часто может оказаться очень грубым инструментом с нежелательными последствиями.

Тем не менее, некоторые ИТ-администраторы предпочитают отклонять запросы на открытие USB-портов на пользовательских машинах, так как на подобных оконечных устройствах это позволило бы получить прямой доступ через брандмауэр предприятия. Такая осторожность понятна, но когда дело доходит до разрешения доступа к USB-накопителю, предоставление этих прав не должно представлять серьезную проблему для безопасности при соблюдении определенных предварительных условий.

Важным требованием является набор приложений для управления оконечными устройствами, который включает сканирование для обнаружения угроз в решениях для защиты от вирусов и вредоносных программ, а также централизованный мониторинг и управление всеми оконечными устройствами пользователей.

Как правило, этот простой подход проявляется в различных формах в унифицированных решениях от популярных поставщиков, например, таких как McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection и WinMagic SecureDoc.

## Уточнения белых списков




Когда дело доходит до защиты USB-накопителей, применяемый метод зависит от требуемого уровня защиты. Простой, но эффективный подход — включить USB-накопители в белый список, используя их идентификаторы поставщика (VID) и идентификаторы продукта (PID). Одна из особенностей всех периферийных USB-устройств заключается в том, что у каждого производителя есть уникальный VID, но PID изменяется для каждого выпускаемого нового продукта.

Использование только VID производителя сделало бы белый список слишком обширным, чтобы быть безопасным, поскольку разрешение получило бы любое USB-устройство, которое было когда-либо изготовлено данным производителем. PID обеспечивает более высокую точность и требует, чтобы доступ к хост-системе предоставлялся только определенной модели.

Хотя это решение и является улучшением, оно все же не идеально. USB-накопители пользуются огромной популярностью, поскольку пользователи могут приобретать собственные устройства разрешенных моделей. Учитывая это, Kingston Technology предлагает индивидуальный подход к повышению безопасности USB-накопителей.

В рамках программы изготовления на заказ можно создать пользовательские профили PID для конкретной организации и применить их к ряду USB-накопителей с шифрованием от Kingston. Компании, развертывающие устройства со специальным идентификатором продукта, не только выигрывают от упрощенного ведения белого списка, но и значительно повышают безопасность. Без соответствующего пользовательского PID даже кажущиеся идентичными устройства, приобретенные сотрудниками самостоятельно, будут лишены доступа.

Хотя использование пользовательских идентификаторов PID позволит ИТ-администраторам быстро и легко внедрять новые USB-устройства хранения данных, более детальной альтернативой является использование

индивидуальных серийных номеров устройств, которые присутствуют на большинстве USB-накопителей с шифрованием от компании Kingston. Для этого необходимо, чтобы каждый уникальный серийный номер устройства был зарегистрирован в пакете управления оконечными устройствами. Первоначально для этого потребуется обработки силами ИТ-персонала, и компания Kingston может предоставить список серийных номеров для каждого заказа (они всегда являются буквенно-цифровыми и непоследовательными). Выбор этого способа позволяет применять гораздо более гибкие политики, основанные на владении отдельным накопителем, с дополнительным преимуществом в виде точного отслеживания происхождения устройств, что может быть бесценным в сценариях криминалистической ИТ-экспертизы. Некоторые накопители Kingston содержат серийный номер и штрихкод на корпусе для электронного сканирования, а другие накопители можно настроить, добавив на их корпуса штрихкод и серийный номер; эти элементы можно использовать для отслеживания перемещения накопителей.

По умолчанию системы управления оконечными устройствами предоставляют доступ к идентификатору VID/PID для блокировки портов и внесения в белый список. Kingston предлагает более универсальный способ использования этих функций для создания более гибких политик, облегчающих использование USB-накопителей. При внедрении соответствующего способа идентификации общая позиция «Блокировать все порты» не только чрезмерно упрощена, но и становится ненужной.

## Безопасные, соответствующие нормативным требованиям решения для удаленных пользователей

Когда дело доходит до безопасности, ведение белых списков устройств относится только к половине проблемы, или, другими словами, предоставляют только половину решения.


Удобство и простота USB-накопителей делает их незаменимыми во многих компаниях и учреждениях, где портативность очень важна для беспроблемной передачи данных. В большинстве случаев, для соблюдения нормативных требований и требований ИТ-гигиены, необходимо предоставлять персоналу зашифрованные USB-накопители для таких задач. Благодаря сочетанию защиты паролем и шифрования устройства портативное хранилище предотвращает доступ к конфиденциальным данным в случае утери, кражи или оставления устройства в потенциально уязвимой ситуации.

Универсального решения не существует, поскольку методы шифрования различаются, и наиболее существенные отличия обнаруживаются при сравнении программных и аппаратных решений для шифрования. Итак, какое из них лучше? Это зависит от ваших потребностей, но более важным будет вопрос: «Какое из них безопаснее?»

Программное шифрование — это, по сути, бюджетный выбор, который удовлетворит требованиям ряда секторов с менее интенсивными операциями. Он также подойдет компаниям, передача данных в которых не считается конфиденциальной, и которые более озабочены соблюдением политик.

Тем не менее, методы программного шифрования также являются его уязвимым местом, поскольку для них требуются клиентские приложения, которые полагаются на компьютер для выполнения задач шифрования. Следовательно, по аналогии, устройство хранения с программным шифрованием безопасно настолько, насколько безопасен хост-компьютер.

Подверженность взлому также возрастает, поскольку хакеры, имеющие доступ к памяти компьютера, могут выявить ключи шифрования/дешифрования. Данные на накопителе также могут подвергаться атакам методом грубой силы, поскольку защита доступа паролем не поможет, если к зашифрованным файлам можно получить доступ и скопировать их.

Помните, что для программного шифрования, вероятно, время от времени потребуется обновление программного обеспечения, что может усложнить внедрение, создав дополнительную нагрузку на ИТ-персонал. Хуже всего то, что программное шифрование может быть полностью удалено разочарованными сотрудниками, у которых возникают проблемы с переносимостью накопителя на разные платформы. Пользователи накопителей могут скопировать зашифрованные данные с накопителя на компьютер, переформатировать накопитель, сделав его незашифрованным, а затем скопировать данные обратно на накопитель. На этом этапе данные будут незащищенными и полностью уязвимыми для взлома. В целях соблюдения законов и нормативных требований к конфиденциальности данных это неприемлемо, поскольку безопасность USB-накопителя может быть отключена.

# Шифрование на чипе: надежное и быстрое решение

В противоположность этому, USB-накопитель с аппаратным шифрованием функционирует независимо от компьютера, поскольку он оснащен встроенным в физический накопитель выделенным процессором, который управляет шифрованием. Используется процесс постоянного шифрования с защитой от взломов пароля с использованием грубой силы; зашифрованные данные недоступны и не могут быть скопированы.

В USB-накопителях Kingston корпоративного и военного уровня с аппаратным шифрованием применяется 256-битное шифрование AES в режиме XTS. Технология 256-битного шифрования AES, одобренная во всем мире, обеспечивает строгую защиту данных. Благодаря использованию двух отдельных ключей на разных этапах процесса шифрования/дешифрования режим XTS действует подобно двойному шифрованию данных.

В процессе использовании ключ шифрования создается генератором случайных чисел контроллера накопителя, который разблокируется паролем пользователя. Поскольку аутентификация происходит внутри криптооборудования устройства, ключи шифрования и другие критически важные функции безопасности защищены от распространенных атак, таких как BadUSB, атаки холодной перезагрузки, вредоносный код и атаки методом грубой силы.

Одним из наиболее очевидных преимуществ аппаратного шифрования является существенное повышение производительности по сравнению с накопителями с программным шифрованием, так как не требуется передача задач шифрования на хост-компьютер. Весь процесс происходит внутри накопителя.

USB-накопители с аппаратным шифрованием, такие как Kingston IronKey D500S, представляют собой изначально зашифрованные, защищенные паролем устройства. При использовании сначала виден только защищенный от записи том программы запуска, поскольку он содержит приложение, используемое для аутентификации пароля и разблокировки основного зашифрованного тома хранения. Эта процедура позволяет избежать установки каких-либо драйверов или программного обеспечения на хост-компьютер.

Кроме того, USB-накопители с аппаратным шифрованием Kingston оснащены прошивкой с цифровой подписью, что исключает любые манипуляции с микропрограммой внутри устройства. Наличие этого дополнительного уровня безопасности обеспечивает защиту от таких типов атак, как BadUSB, в которой используется внутренняя уязвимость встроенного ПО USB-устройства. Успешная подобная атака может привести к скрытому выполнению команд или запуску вредоносного кода на хост-компьютере.

Конечно, подход с блокировкой всех портов ограничит риск взломов типа BadUSB, но зачем жертвовать производительностью, используя такие устаревшие методы? Как подчеркивалось выше, можно поддерживать безопасность среды и при использовании портативных запоминающих устройств, если существуют простые процедуры закупки и развертывания для внедрения USB-накопителей с аппаратным шифрованием.

# Безопасная и соответствующая нормативным требованиям удаленная работа

Для удаленных сотрудников, которые работают вне средств защиты, обеспечиваемых безопасной рабочей средой организации, необходим пересмотр стратегии, а также новый взгляд на приоритеты.


Когда дело доходит до планирования безопасности удаленной работы, есть ли какое-то преимущество в блокировке портов USB на ноутбуке вашего сотрудника только для того, чтобы они подключались через Интернет для доступа к серверу для загрузки или получения документов? Когда сотрудник находится в пути, единственным доступным может оказаться открытое интернет-соединение, такое как незащищенная или ненадежная точка доступа Wi-Fi, и с этим связан широкий спектр опасностей, которые значительно увеличивают

вероятность взлома. Такие угрозы, как перехват данных и наблюдение с использованием спуфинга, атаки типа «человек посередине» (MitM) и сетевая прослушка — это лишь некоторые из все более изощренных методов взлома, доступных киберпреступникам. Риску подвергаются даже сети VPN.

Сетевое подключение организации к Интернету — это просто еще одно оконечное устройство, и из-за внутренней уязвимости оно чрезвычайно уязвимо и становится целевой точкой входа. Открытие его для удаленного доступа несет с собой собственные риски безопасности, особенно когда речь идет о конфиденциальных данных.

Предоставление удаленным сотрудникам защищенных паролем USB-накопителей с аппаратным шифрованием эффективно устраняет потенциальные сетевые уязвимости. Однако для таких закупок требуется более тщательное изучение доступных USB-накопителей и их соответствия требованиям каждой удаленной рабочей среды. И вопрос не в выборе емкости накопителя или принятии решения о том, следует ли регистрировать серийный номер устройства. Речь идет о физической конструкции самого устройства.

## Меры защиты от взлома: надежные варианты

Основной вопрос заключается в том, защищен ли USB-накопитель с аппаратным шифрованием от несанкционированного доступа. Насколько защищено устройство от такого вмешательства, отражено в таких стандартах, как FIPS 140-3. Он имеет несколько уровней, в которых изучается устойчивость физической конструкции накопителя без использования криптографических методов.


Соответствующая сертификация FIPS-197 учитывает только атрибуты аппаратного шифрования и относится к таким устройствам, как IronKey Vault Privacy 50 и внешний твердотельный накопитель Vault Privacy 80, которые ориентированы на предприятия и не должны соответствовать требованиям военных стандартов к безопасности данных. Эти накопители дешевле, но не защищены от физического взлома.

Согласно сертификации FIPS 140-3 уровня 3 (ожидается) методы, используемые для выявления несанкционированного доступа к устройствам, оцениваются как соответствующие военным стандартам. Компания Kingston поставляет накопителя, соответствующие FIPS 140-3 уровня 3, предприятиям, правительствам и вооруженным силам во всем мире.

Использование эпоксидной смолы для покрытия всех электронных деталей накопителя, необходимых для обеспечения безопасности, и приклеивание внутренних компонентов к корпусу создает еще один уровень защиты. Любая попытка открыть металлический корпус будет чрезвычайно затруднена и приведет к поломке внутренних микросхем и других компонентов, что в конечном итоге сделает накопитель нефункциональным. При наличии этой твердой и непрозрачной эпоксидной смолы вмешательство в жизненно важные компоненты накопителя становится практически невозможной задачей. Такие устройства, как Kingston IronKey D500S и S1000 имеют эту дополнительную меру безопасности.

Средства защиты устройств не ограничиваются лишь физическими мерами, и Kingston IronKey S1000 выводит защиту от несанкционированного доступа на новый уровень. Встроенный в IronKey S1000 крипточип может обнаружить любое физическое вмешательство и сделает накопитель непригодным для использования сразу после включения устройства. Использование USB-накопителей с аппаратным шифрованием для доступа и передачи конфиденциальных файлов — это практичный шаг, который упрощает удаленную работу и эффективно гарантирует безопасность на местах.

Обязательно изучите аппаратные особенности и функции безопасности USB-накопителей, чтобы узнать, соответствуют ли они вашим потребностям и варианту использования. Каждую модель USB-накопителей необходимо проверять отдельно, с получением надежных сертификаций, помогающих принимать эти решения. Какими бы ни были ваши приоритеты, компания Kingston по доступной цене предлагает ряд USB-накопителей с аппаратным шифрованием и вариантов настройки, подходящих для различных сред: от соответствия общим нормативным требованиям до самых жестких военных спецификаций.

# Безопасность прежде всего: нет сетей, нет проблем

Сегодня у офиса нет границ, и, поскольку работа из дома получает все большее распространение, многие компании обращают внимание на проблемы уязвимости удаленного доступа. Многие впервые сталкиваются с этими сложностями и ищут более безопасные способы приспособиться к этой развивающейся тенденции.

Для удовлетворения этих потребностей в широком спектре отраслей, USB-устройства хранения данных с аппаратным шифрованием уже хорошо зарекомендовали себя и предлагают безопасное решение для тех случаев, когда передача данных по сети может быть непрактичной или нежелательной по ряду причин.

В сфере финансов регулирующие органы часто запрашивают данные для проверки деятельности компании и соблюдения ею нормативных требований. Риск утечки данных слишком велик, чтобы рассматривать возможность использования сети для передачи конфиденциальных документов, содержащих точную информацию об инвестициях, рыночной торговле и другой конфиденциальной банковской деятельности. Простым и эффективным решением является доставка этой информации на USB-накопителе с аппаратным шифрованием.

Использование защищенных USB-накопителей для передачи файлов в медицинских учреждениях — повседневное явление. Это также удобно для врачей или консультантов, которые захотят проанализировать записи, обратиться к ним для исследования или представить примеры из практики студентам-медикам. Существуют также более практические потребности, когда речь идет о проприетарных системах, таких как устройства диагностической визуализации, где доступ к сети отсутствует или небезопасен. Используя совместимые USB-накопители с аппаратным шифрованием, файлы можно легко передавать для использования в другом месте.

## Что следует и чего не следует делать

✓ **Используйте соответствующие нормативным требованиям, защищенные накопители** и просмотрите спецификации, чтобы приобрести накопители, соответствующие потребностям каждого развертывания.

✗ **Не допускайте использования случайных накопителей или политику использования собственных устройств (BYOD)** — для любой компании потеря незашифрованных накопителей сопряжена со слишком высоким риском финансового и репутационного ущерба.

✓ **Разверните пакет управления оконечными устройствами** и используйте USB-накопители с аппаратным шифрованием, которые предлагают специальные функции ведения белого списка.

✗ **Не предоставляйте дело случаю.** Правильно оцените требования к локальной и удаленной рабочим средам.

✓ **Проводите обучение сотрудников** по вопросам безопасности. В их же собственных интересах, чтобы компания оставалась защищенной от нарушений безопасности.

✗ **Не делайте безопасность настолько болезненной,** чтобы пользователи искали обходные пути, которые могут привести к использованию теневых ИТ-решений. Тот факт, что политика тотального контроля применялась всегда, не означает, что она подойдет для всех сценариев. Рабочая среда меняется, и, выбирая правильные решения, можно разрабатывать и внедрять новые политики.

В этом случае на первый план выходит IronKey Keypad 200 (KP200) компании Kingston. В этом накопителе, независимом от ОС, отсутствует том программы запуска для ввода пароля, но вместо нее имеется буквенно-цифровая клавиатура, которая разблокирует устройство для использования на любой платформе. Подобно швейцарскому армейскому ножу, использование USB-накопителей с аппаратным шифрованием распространяется и на производственные среды, помогая безопасно переносить приложения, созданные в мире ИТ-исследований и разработок, на оборудование, управляемое платформами эксплуатационных технологий (ОТ). KP200 — одно из самых простых и доступных безопасных решений для работы со смешанными платформами, в которых также используется Linux.

USB-накопители с аппаратным шифрованием также играют жизненно важную роль в правоохранительных органах. Они защищают и надежно передают материалы по делу, изображения и другие доказательства оперативникам на местах, следственным группам и группам судебно-медицинских экспертов. Компания Kingston предлагает дополнительное преимущество, поскольку может поставлять накопители с встроенным серийным номером, напечатанным на внешнем корпусе вместе со штрихкодом. Выпуск и каталогизация накопителей становятся простыми и легко отслеживаемыми операциями. Это так же просто, как вручную зарегистрировать серийный номер, или так же быстро, как отсканировать штрихкод — аудит и управление материально-техническими ресурсами не может быть еще проще. Эта функциональность является стандартной для накопителей Kingston IronKey D500S, D500SM и S1000B/E, но также доступна и для других моделей с аппаратным шифрованием в рамках программы индивидуальной настройки Kingston.

# Безопасность и мобильность устройств хранения данных: современное состояние

Защита паролем, аппаратное шифрование, защита от несанкционированного доступа, детализированный белый список оконечных устройств, соответствующая военным стандартам сертификация FIPS 140-3 уровня 3 (ожидается) и оперативное ведение журнала — это стандартные функции USB-накопителей компании Kingston, которые можно использовать без задержки.

Эти надежные средства защиты гарантируют, что USB-накопитель и его данные останутся в безопасности в хост-среде. Хотя заявленные спецификации могут производить впечатление, случайный выбор модели без каких-либо исследований не обязательно обеспечит идеальное соответствие более строгим требованиям некоторых организаций.

Как независимый производитель, компания Kingston предлагает широкий спектр вариантов для удовлетворения потребностей клиентов. В рамках программы индивидуальной настройки Kingston доступны передовые решения, призванные обеспечить удобство работы пользователей.

Настройка безопасности выходит за рамки предоставления организации собственного идентификатора PID USB-устройства для внесения в белый список. Профиль безопасности программы запуска также можно сконфигурировать, используя пятнадцать различных настроек: от контактных данных и сведений о компании до включения подсказок пароля и определения максимального количества попыток ввода пароля. На внешней стороне корпуса может быть размещен фирменный знак (логотип) компании, а также доступны различные цвета для конкретных накопителей. При заказе от пятидесяти накопителей все эти функции обеспечивают простой путь интеграции для развертывания устройств.

Если приложение для управления оконечными устройствами, подходящее для защищенных USB-накопителей, пока отсутствует, есть решение управления для организаций, которые хотят управлять своим парком накопителей Kingston, включая возможности удаленного сброса паролей.

Благодаря повсеместности использования и удобству технология USB пережила множество других многообещающих технологий, и для многих задач неизменными факторами остаются скорость и удобство USB-накопителей. Легкодоступные и всегда безопасные, защищенные USB-накопители — это простое решение, которое можно оценить уже сейчас.

Зачем беспокоиться об утечках сетевых данных в удаленных средах? С USB-устройствами хранения данных с аппаратным шифрованием Kingston IronKey решение проблемы находится буквально у вас на ладони.

Чтобы узнать подробнее о возможностях, предлагаемых компанией Kingston, посетите веб-сайт kingston.com/ironkey. Для получения ответов на более конкретные вопросы обратитесь к нашим специалистам по USB-накопителям с шифрованием.

**#KingstonIsWithYou #KingstonIronkey**

**ДАННЫЙ ДОКУМЕНТ МОЖЕТ БЫТЬ ИЗМЕНЕН БЕЗ ПРЕДВАРИТЕЛЬНОГО УВЕДОМЛЕНИЯ.**
**©2023 Kingston Technology Corporation**, 17600 Newhope Street, Fountain Valley, CA 92708 USA.
Все права защищены. Все товарные марки и зарегистрированные товарные знаки являются собственностью своих законных владельцев.