



Почему USB- накопители актуальны и сегодня?

#KingstonIsWithYou

Предисловие и содержание

В современную цифровую эпоху, когда 60% всех глобальных корпоративных данных хранится в облаке¹, обсуждение актуальности технологии хранения, которой уже почти тридцать лет, может показаться немного странным. Однако, с момента своего появления эти классические устройства для хранения данных развивались и продолжают развиваться.

Давно прошли те времена, когда USB-накопители были просто стандартным средством соединения файлов, дисков и приложений. Современные решения не только могут похвастаться значительно большей скоростью передачи данных, но также представляют собой надежные и безопасные портативные носители, которые необходимы во многих ситуациях. Но почему USB-накопители по-прежнему актуальны и сегодня, когда облачные решения для хранения данных, казалось бы, могут предложить многие из тех же преимуществ?

В этой электронной книге мы обсудим, какое место занимают USB-накопители в среде, где доминируют облачные технологии. Опираясь на мнение ведущих отраслевых экспертов, мы рассмотрим, как современные организации используют USB-накопители, а также место этих устройств наряду с программным шифрованием, независимыми средами хранения и защитой данных конечных устройств.

Содержание	Страницы
Авторы	3
Рост популярности USB-накопителей	4
Портативное устройство хранения данных, отвечающее растущему спросу	5-6
Шифрование: сравнение аппаратного и программного подхода	7-8
Растущая потребность в защите чувствительных данных	9
Защита финансовых данных	10
Безопасный доступ к данным о здоровье пациентов	11
Место USB-накопителей в будущем облачных хранилищ	12-13
Итоги и информация о компании Kingston	14



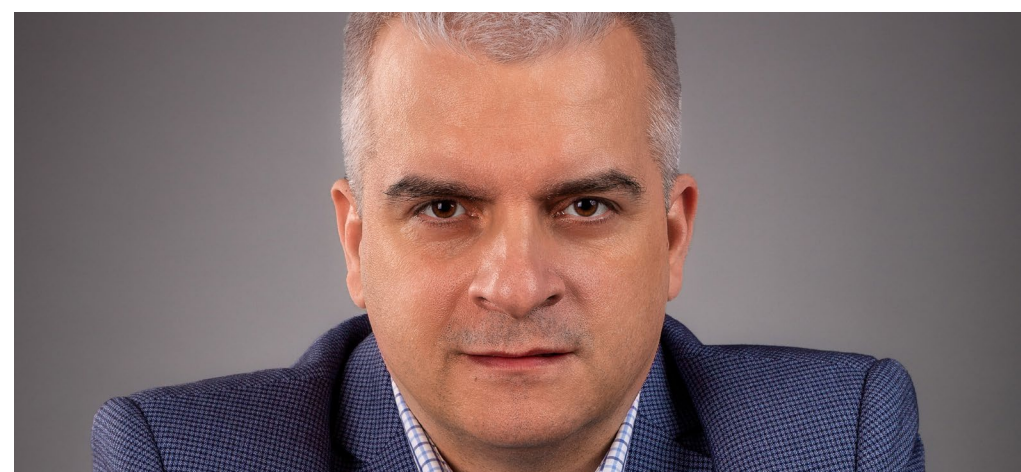
Авторы

В составлении этой электронной книги приняли участие три эксперта в области информационных и развивающихся технологий.



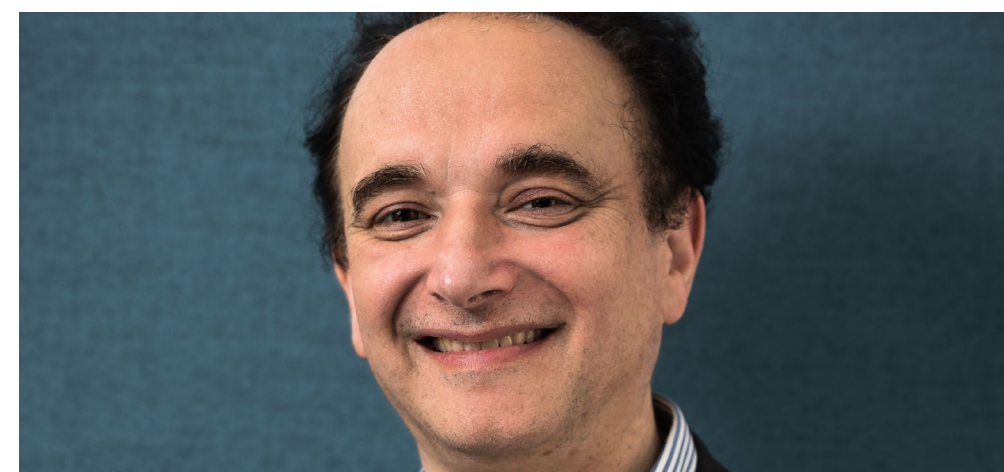
Рафаэль Блум

Рафаэль занимал руководящие должности в сфере технологических продуктов, маркетинговых коммуникаций и развития бизнеса. Его консультативные услуги сосредоточены на новых проблемах в области организационной структуры, продукции и коммуникаций, связанных с технологическими и нормативными изменениями. Эта чрезвычайно разнообразная деятельность основывается на опыте в области управления информацией и методов проектирования с учетом нормативных требований, конфиденциальности данных и новых технологий, таких как AdTech, мобильная связь и 5G, ИИ и машинное обучение.



Томаш Сурдык

Обладая более чем 24-летним опытом работы в сфере ИТ-безопасности в органах государственного управления, Томаш является ведущим специалистом в области информационной безопасности, защиты персональных данных и кибербезопасности. В прошлом он инспектировал системы и сети ИКТ, обрабатывающие секретную информацию и личные данные в правительственной администрации, а также имел доступ к секретной информации в НАТО и ЕС. В течение нескольких лет он являлся владельцем компании, специализирующейся на внедрении решений защиты, которые повышают безопасность бизнес-информации и персональных данных.



Дэвид Кларк

Дэвид признан одним из 10 ведущих инфлюенсеров по версии Thompson Reuter's «30 самых влиятельных экспертов и идеологов в области социальных сетей, управления рисками, соблюдения нормативных требований и регуляторных технологий в Великобритании» и входит в список 50 ведущих мировых экспертов по мнению компании Kingston Technology. Ранее Дэвид занимал ряд должностей в области управления безопасностью, в том числе был руководителем глобального отдела предоставления услуг безопасности и отдела инфраструктуры безопасности в компаниях, входящих в глобальный рейтинг FTSE 100.

Когда более двадцати лет назад на рынке появился первый накопитель с универсальной последовательной шиной (USB), его коллективная совместимость изменила правила игры в области компьютерных технологий. Благодаря предоставлению множеству людей возможности работать с несколькими устройствами, технология USB вскоре эволюционировала, обеспечивая значительно более быструю передачу данных, порт USB 3.0 и еще более широкие возможности, связанные с выпуском первого флеш-накопителя USB в 2000 году.

С тех пор технологии прошли долгий путь с точки зрения требований к мобильному хранению данных и безопасности. Основное внимание уделяется современному поколению USB-накопителей, которые разработаны с учетом очень специфических сценариев использования. С точки зрения предприятия все более широкое распространение удаленной и гибридной работы, использование облачных сервисов и проблемы кибербезопасности формируют потребность в более эффективных решениях. Наряду с этим существуют нормативные требования к хранению данных. Все это часто усугубляется наличием распределенных и сложных систем, которые могут работать как локально, так и в облаке.

Кроме того, возникает увеличение объемов структурированных и неструктурированных данных, таких как документы, электронные письма, фотографии, видео и метаданные. Все это усложняет растущие потребности предприятия в хранении данных.

Но если облачное хранилище может решить многие из этих проблем, насколько актуально использование USB-накопителей в современной бизнес-среде?



Многие считают USB-накопители старомодными или тривиальными из-за того, что в прошлом они использовались как более или менее одноразовые устройства с низкой производительностью и низким уровнем безопасности.

- Рафаэль Блум



Портативное устройство хранения данных, отвечающее растущему спросу

Старые модели использования USB-накопителей в качестве портативного хранилища исчезли. Но появились сценарии использования высокопроизводительных USB-накопителей для личного, безопасного локального резервного копирования с дополнительным уровнем защиты данных и конфиденциальности. Это может быть очень важно для конфиденциальных данных, таких как записи отделов кадров, финансовые данные, медицинские записи, защита интеллектуальной собственности (IP) и вся информация, позволяющая установить личность (PII). Кроме того, устройства этого поколения оснащены функциями быстрой передачи данных, хранения, резервного копирования и безопасности, которые можно использовать в следующих случаях:

- ❑ Нормативная информация, которая должна быть передана из рук в руки
- ❑ Юридические и финансовые документы, которые необходимо доставить и распечатать на объекте или за его пределами
- ❑ Любая потенциально враждебная среда, в которой могут представлять угрозу программы-вымогатели
- ❑ Перенос в системы печати, где доступ к сети запрещен

Ведущий поставщик USB-накопителей с шифрованием Kingston Technology идет в ногу с растущим спросом, выпуская такие решения, как [Kingston IronKey™ S1000](#). Этот лучший в своем классе USB-накопитель с шифрованием соответствует самым строгим стандартам и способен обеспечить безопасность конфиденциальных данных с помощью 256-битного шифрования XTS-AES и отдельного крипточипа с надежной защитой от несанкционированного доступа. Кроме того, он сертифицирован по стандарту FIPS 140-2 уровня 3. Это означает, что правительство США официально подтвердило его эффективность в качестве криптографического оборудования, благодаря чему он отлично подходит для организаций, которым требуется дополнительное спокойствие, когда речь идет о защите данных.

Такие USB-накопители с аппаратным шифрованием предлагают решения для централизованного безопасного управления устройствами, независимо от того, находятся ли данные в облаке или локально. Соответствующее нормативным требованиям, простое в использовании и не требующее программного обеспечения хранилище данных с шифрованием также высвобождает ценное время ИТ-специалистов, предлагая решения, предназначенные для быстрого и эффективного развертывания.





Портативное устройство хранения данных, отвечающее растущему спросу



Резервное копирование и архивирование — еще один пример использования USB-накопителей для защиты цифровых активов в долгосрочной перспективе независимо от сторонних облачных сервисов. Несмотря на то, что обращаться с большими объемами данных в облаке действительно легко, проприетарные объекты интеллектуальной собственности по-прежнему могут быть достаточно конфиденциальными, чтобы их стоило хранить на защищенном USB-накопителе с шифрованием, который можно не подключать к Интернету и безопасность которого можно легко обеспечить.

Всегда будут существовать обстоятельства, в которых данные организаций должны находиться под их логическим и физическим контролем, особенно при использовании накопителей с шифрованием. И бывают случаи, когда хранилище данных на жестких или твердотельных накопителях невозможно зашифровать. Эту проблему решают внешние USB-накопители с шифрованием, такие как [Kingston IronKey D300S](#). Этот USB-накопитель оснащен аппаратным 256-битным шифрованием XTS по стандарту Advanced Encryption Standard (AES), который представляет собой тип блочного шифра, позволяющего шифровать 128-битные блоки данных. А когда возникнет необходимость в дополнительном шифровании данных, AES будет использовать режим блочного шифрования XTS, способный обеспечить лучшую и более надежную защиту данных, чем предыдущие режимы.



На мой взгляд, USB-накопители по-прежнему используются и являются неотъемлемой частью обеспечения безопасности данных. Помимо прочего, их используют для быстрой передачи информации между устройствами, а также для соответствующего хранения и защиты данных.

- Томаш Сурдык

Шифрование: сравнение аппаратного и программного подхода



Рассматривая шифрование данных, можно утверждать, что аппаратное шифрование проще в управлении и безопаснее, чем программное. Это связано с тем, что процесс шифрования проходит отдельно от остальной части хост-системы, что значительно затрудняет перехват или взлом данных. Централизованное управление уровня устройств позволяет контролировать накопители через соединения внутренней сети LAN и Интернета, являясь отличным инструментом для выполнения следующих задач:

- ❑ Создание и применение индивидуальных и/или групповых политик использования USB-накопителей с шифрованием
- ❑ Проверка действий с файлами для лучшего контроля перемещения данных в рамках организации и за ее пределами
- ❑ Обеспечение удаленного резервного копирования содержимого для передачи критически важных данных
- ❑ Удаленное выключение устройств в случае потери или взлома USB-накопителя
- ❑ Выполнение удаленного сброса забытых паролей

При правильном управлении авторизованными дисками риск копирования и передачи конфиденциальных данных сводится к минимуму. Кроме того, современные USB-накопители с аппаратным шифрованием предлагают множество дополнительных функций безопасности, которые помогают предотвратить доступ или чтение файлов и сообщений кем-либо, кроме предполагаемого получателя.



Я считаю, что аппаратное шифрование лучше программного. Между методами аппаратного и программного шифрования существуют серьезные различия с точки зрения уязвимости к атакам путем подбора. Устройства с аппаратным шифрованием легко выдерживают такие атаки.

- Томаш Сурдык



Шифрование: сравнение аппаратного и программного подхода



Хотя предприятия и могут рассматривать программное шифрование из соображений стоимости, это может быть немного недальновидным. Программные решения используют ресурсы шифрования хост-устройства совместно с другими программами, поэтому они безопасны лишь настолько, насколько безопасен компьютер, и часто требуют обновлений программного обеспечения, которое без поддержки может сделать вас уязвимым. USB-накопители с программным шифрованием могут подвергаться неограниченному числу атак методом «грубой силы» для подбора пароля, и у них нет способов противостоять программным атакам на основе словаря, в которых очень быстро могут проверяться миллионы сочетаний символов.

Кроме того, программное шифрование также может быть отключено. Любой сотрудник, использующий накопитель с программным шифрованием, может скопировать данные, отформатировать USB-накопитель, и шифрование будет удалено. Затем можно скопировать файлы данных обратно и без проблем использовать накопитель без аутентификации на разных платформах и ОС.

Как упоминалось ранее, при аппаратном шифровании физическое «шифрование» и последующее сохранение данных происходит независимо от хост-системы. Это обеспечивает дополнительный уровень защиты, если системы когда-либо будут взломаны.

Это нельзя упускать из виду, особенно работникам таких отраслей, как финансы, здравоохранение и государственное управление. Это связано со строгими правилами таких нормативов, как Закон о преимуществах и подотчетности медицинского страхования (HIPAA) и Стандарт безопасности данных индустрии платежных карт (PCI DSS), в отношении шифрования конфиденциальной информации.

Соблюдение этих правил за счет использования надежных устройств с аппаратным шифрованием в конечном итоге поможет организациям избежать дорогостоящих штрафов, судебных исков и потенциального ущерба репутации. Хотя накопители с аппаратным шифрованием могут обходиться дороже более дешевых USB-накопителей, судебные издержки, связанные с утечкой данных, могут легко покрыть стоимость сотен накопителей всего за несколько часов юридических консультаций.



Растущая потребность в защите чувствительных данных



«
Шифруйте все данные как можно быстрее, выполняйте резервное копирование с использованием методологии 321 (USB может подойти благодаря своей доступности) и реализуйте возможность быстрой микросегментации. - Дэвид Кларк
»

Когда дело доходит до защиты конфиденциальных данных от потери и кражи, каждая организация обязана обеспечить наличие на своих устройствах адекватных функций безопасности. Также важно учитывать, что, хотя существует множество постоянно развивающихся киберугроз, уровень цифровой зрелости и собственные навыки пользователей по управлению данными конечных устройств остаются важным фактором риска, если его не устранить. Внутренние угрозы, в число которых входят потеря контроля над данными или USB-накопителей, передача данных за пределы безопасной среды, использование незашифрованных USB-накопителей и обмен паролями, могут быть результатом недостаточной осмотрительности конечных пользователей. Всего этого можно избежать, проводя соответствующее обучение и используя подходящие USB-накопители.

Предварительное планирование и хорошо отработанная структура коммуникаций также играют важную роль в борьбе с реальными угрозами для самого существования компании. Современные киберугрозы нацелены на слабые места организаций.

Наилучшее время для создания плана использования USB с шифрованием наступает еще до того, как он реально потребуется. Внедрите USB-накопители с шифрованием и политики в общую стратегию безопасности организации. Без рекомендаций и плана использования USB-накопителей с шифрованием вам не на чем строить стратегию защиты, и ваша организация оказывается открытой для рисков на всех уровнях, включая несоблюдение нормативных требований, таких как Общий регламент по защите данных (GDPR), статья 32 которого, в частности, указывает, что конфиденциальные данные должны быть зашифрованы.

«
Организация должна иметь четкое представление о всех своих данных, включая их уровень важности и/или чувствительности, а также план защиты, в первую очередь касающийся наиболее важных данных и включающий либо физическое удаление связи с данными, либо отключение конкретного источника данных. Крайне важна возможность быстро изолировать затронутые системы, а также наличие задокументированного и отработанного на практике плана. - Рафаэль Блум
»

«
Пользователи работают с чувствительными данными. Потеря этих данных повышает степень ответственности и существенно влияет на имидж и безопасность компании. Для защиты конфиденциальных данных следует использовать различные решения безопасности, в том числе шифрование данных. - Томаш Сурдык
»

Наряду с соображениями безопасности существуют также стандарты соответствия, которым должны следовать решения для хранения и резервного копирования данных. Некоторые из этих практик, такие как необходимость управления графиками хранения данных и обеспечения их соблюдения, являются общими для разных вертикалей, в то время как к другим, например, к переносу корпоративных данных в облако, относятся совершенно по-разному.

Во многих вертикалях, таких как сектор финансовых услуг, вступили в силу нормативные правила, которые сделали обязательным надлежащее управление данными. Банки изначально очень сдержанно относились к использованию сторонних ресурсов для хранения и резервного копирования, и многие до сих пор настаивают на том, чтобы владеть всей своей инфраструктурой хранения и обработки данных.

Финансовые учреждения также обязаны соблюдать растущий список правил и стандартов безопасности данных, таких как Закон Сарбейнса-Оксли (SOX) и Общий регламент по защите данных (GDPR). Однако по мере роста числа мобильных сотрудников и подрядчиков возрастает риск утечки данных и несоблюдения требований, налагаемых такими законами и стандартами.

Правда заключается в том, что усилия по обеспечению соответствия могут быть сведены на нет с поразительной легкостью, если мобильные сотрудники не смогут защитить свои цифровые удостоверения, портативные рабочие места, записи клиентов и хранящиеся у них финансовые данные. Вот почему все больше организаций переходят на решения для мобильной безопасности, такие как [USB-накопители с шифрованием Kingston IronKey](#), для защиты цифровых удостоверений и приложений независимо от того, куда их берут сотрудники.



Если принять во внимание общее смещение тенденций в сторону более распределенного ИТ-пространства и масштабируемости облачной инфраструктуры, легко заметить, что большинство отраслей и большая часть малых и средних предприятий больше не заботятся об управлении охлаждаемыми серверными. - **Рафаэль Блум**



Здравоохранение — еще одна отрасль, где безопасность данных важна как никогда. Информация о пациентах подвергается еще большему риску кражи: в 2021 году в результате утечек было раскрыто 45,67 миллиона медицинских записей, что является самым большим годовым показателем с 2015 года². Когда дело доходит до хранения и резервного копирования данных, медицинские записи представляют собой важную и всеобъемлющую медицинскую информацию, которая позволяет учреждениям здравоохранения безопасно лечить своих пациентов.

Они могут включать в себя все, от файлов электронной медицинской карты пациента (EHR), содержащих истории болезни, анализы, фотографии и рентгенографические изображения, до административных файлов, включая платежные ведомости, страхование пациентов и кредиторскую задолженность. Столкнувшись с растущим количеством мобильных сотрудников и глобальным рынком здравоохранения, который претерпевает серьезные потрясения и преобразования, неудивительно,



Программы-вымогатели, например, тоже представляют собой своего рода растущую отрасль, поэтому каждая организация, которая обрабатывает конфиденциальные данные, должна подумать о том, как действовать в условиях экстремального давления. - **Рафаэль Блум**



что современные учреждения здравоохранения обеспокоены безопасностью данных.

Кроме того, неспособность предвидеть риски и соблюдать строгие требования, такие как Закон о преемственности и подотчетности медицинского страхования (HIPAA) или Закон о применении медицинских информационных технологий в экономической деятельности и клинической практике (HITECH), может привести к дорогостоящей утечке медицинских данных, что может еще больше подорвать доверие пациентов, партнеров и регулирующих органов.

С помощью таких решений, как линейка USB-накопителей с шифрованием Kingston IronKey, учреждения здравоохранения могут с помощью одной консоли устанавливать политики для паролей, использования приложений, восстановления и т. д., как всего для нескольких, так и для тысяч накопителей. Мобильные и непосредственно взаимодействующие с пациентами сотрудники могут получить возможность поддерживать больше пациентов с помощью удобных решений, которые избавят их от необходимости устанавливать драйверы или другое программное обеспечение для безопасного доступа к сохраненным данным. В то же время пользователи и администраторы могут легко и быстро заблокировать данные, где бы они ни находились.



Место USB-накопителей в будущем облачных хранилищ



Облачные хранилища данных — это и наше настоящее, и будущее. Но я по-прежнему утверждаю, что физическая защита данных, например с использованием USB-накопителей с шифрованием, является самым безопасным способом. Пользователи не могут полностью контролировать то, что происходит в облаке. Однако мы можем контролировать данные на USB-накопителях с шифрованием, которые мы защищаем и храним сами. Кроме нас, никто не может получить доступ к этим носителям.

- Томаш Сурдык



Тем не менее, в отношении облачных хранилищ данных есть еще много ограничений. Для них требуется сетевое подключение, которое не только определяет, как и когда можно создавать резервные копии или передавать файлы, но и создает дополнительные проблемы с безопасностью. Когда компания обязывает сотрудников использовать облако, она не обязательно может контролировать, откуда осуществляется доступ к данным. Таким образом, простой доступ к VPN с использованием личного или общедоступного соединения Wi-Fi повышает риск взлома. Кроме того, облачные сервисы очень привлекательны для злоумышленников, поскольку большая часть всех вредоносных программ (61%) теперь доставляется через облачные приложения³.



Возможно, разумно рассмотреть, что происходит в случае недоступности облака, сценарии, в которых данные должны быть доступны на 100%, и когда длительное хранение данных может создать уязвимость. - Дэвид Кларк



Теперь, когда преимущества USB-накопителей очевидны, какова их роль в будущем облачных хранилищ данных?

Десять лет назад USB-накопители пользовались огромным спросом как основной инструмент для удобного хранения и передачи данных. Однако благодаря новым гибридным моделям работы и все более распределенным командам облако теперь обеспечивает быстрый и простой доступ к хранимой информации со многих устройств. Когда-то флеш-накопители были чрезвычайно популярны из-за того уникального удобства, которое они предлагали для перемещения файлов. Сегодня облачные сервисы хранения данных предлагают еще более простой перенос файлов.





С другой стороны, шифрование USB может быть выполнено либо с помощью аппаратного обеспечения устройства, либо программным образом. Аппаратно-ориентированное шифрование без использования ПО является наиболее эффективным средством защиты от кибератак. Это отличное, несложное решение для защиты от утечек данных, которое может обеспечить соответствие жестким стандартам с максимальной безопасностью данных, чтобы помочь организациям уверенно управлять угрозами и снижать риски.

Благодаря своей автономности, для USB-накопителей с аппаратным шифрованием не требуется программный компонент на хост-компьютере. Отсутствие программной уязвимости также исключает возможность атак методом грубой силы, прослушивания и хеширования памяти. USB-накопители с программным шифрованием также подвержены риску того, что любой пользователь может отключить шифрование, отформатировав накопитель на любом компьютере и используя накопитель для хранения конфиденциальных данных без защиты.

USB-накопители с аппаратным шифрованием также предлагают исключительные физические средства для обеспечения безопасности данных. Пользователь или администратор может задать критерии доступа к информации. Кроме того, эти накопители могут интегрироваться с существующими локальными решениями для конечных устройств. Это удобное

и экономичное решение для многих сценариев, когда облачное хранилище данных не работает или не является столь эффективным решением. Например, когда необходимо сохранить данные с устройств, не подключенных к сети, данные, которые должны остаться личными, или данные, требующие доступа в автономном режиме.



Если мы разделим данные на «горячие» и «холодные» в зависимости от уровня их ежедневной полезности для организации, то может быть более эффективно размещать «холодные» данные в облаке и больше полагаться на локальные USB-накопители для «горячих» данных, когда непрерывность работы и высокая производительность являются более важными для организации или для конкретной важной для бизнеса функции или процесса. - **Рафаэль Блум**



Хотя мы не в силах предсказать появление будущих инноваций, мы можем предложить отмеченный наградами портфель USB-накопителей, включающий динамичный диапазон решений с шифрованием для всех уровней требований к защите мобильных данных. От USB-накопителей с буквенно-цифровой клавиатурой для удобной защиты PIN-кодом и сертификации FIPS 140-2 уровня 3 для высочайшего уровня шифрования и защиты от несанкционированного доступа до технологии SuperSpeed USB 3.1, которая не ставит под угрозу безопасность, продукты Kingston IronKey помогут вам решить задачи, связанные с данными. Наши USB-накопители — это мощные и эффективные решения для переноса и хранения мобильных данных.

Наша специализированная команда экспертов готова поддержать вас на каждом этапе вашего пути хранения данных, предложив надежную помощь в поиске правильного решения для хранения данных, отвечающего вашим потребностям.

Мы обладаем навыками и техническими возможностями, которые помогут вам сохранить конфиденциальную информацию в безопасности и обеспечить соблюдение новых правил, независимо от того, хотите ли вы создать план с USB-накопителями с шифрованием, выбрать лучшие варианты для вашего бизнеса или создать и внедрить политики безопасности. Предлагая высоко персонализированное обслуживание, мы стремимся предоставлять продукты, которые поддерживают ваши приоритеты в хранении данных и позволяют справиться с беспрецедентной скоростью, с которой меняется мир бизнеса.

1. Statista - <https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data>
2. SC Magazine - <https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015>
3. Infosecurity Magazine - <https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers>



О компании Kingston

За 35 лет работы компания Kingston накопила знания, позволяющие выявлять и решать проблемы заказчиков, связанные с мобильными данными. Благодаря этому ваши сотрудники смогут работать легко и безопасно, не ставя под угрозу свою организацию.